
GAZİ ÜNİVERSİTESİ
Gazi
1926

SES KULLANILARAK YAPILAN SİBER SALDIRILARIN İNCELENMESİ

Bilge LALE

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

TEMMUZ 2025

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Bilge LALE
08/07/2025

SES KULLANILARAK YAPILAN SİBER SALDIRILARIN İNCELENMESİ

(Yüksek Lisans Tezi)

Bilge LALE

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Temmuz 2025

ÖZET

Son yıllarda dijital dünyada siber saldırılar ve hatta sesle yapılan siber saldırılar bireyler, kuruluşlar ve kritik altyapılar için giderek daha büyük bir güvenlik tehdidi haline gelmiştir. Bu tür saldırılar genellikle sesli komutlarla cihazlara izinsiz erişim sağlama, cihaz kontrolünü ele geçirme ve ses teknolojilerindeki güvenlik açıklarından faydalanma amacı taşımaktadır. Akıllı asistanlar, akıllı hoparlörler ve mobil cihazlar gibi sesle aktive edilen teknolojilerin hızla yaygınlaşması, kötü niyetli saldırganlar için yeni saldırı türleri oluşturmuştur. Sesli komutlara dayalı sistemlerin günlük yaşamda artan şekilde kullanılmasıyla sesle yapılan siber saldırıların türleri çeşitlenmiş ve bu saldırıların potansiyel etkileri çok daha ciddi bir tehdit boyutuna ulaşmıştır. Ancak literatürde bu alanda yapılan araştırmalar, sesle yapılan siber saldırıların farklı türlerini, saldırı yöntemlerini ve bu saldırıların hedef sistemler üzerindeki olası etkilerini kapsamlı bir biçimde ele almamaktadır. Mevcut çalışmalar genellikle belirli saldırı türlerine odaklanmakta ve bu tehditlerin daha geniş kapsamlı analizine yer verilmemektedir. Bu tez, ses tabanlı siber saldırıların çeşitli türlerini, kullanılan saldırı yöntemlerini ve bu saldırıların hedef sistemler üzerindeki etkilerini derinlemesine incelemiş; ayrıca Türkiye'deki güncel siber güvenlik ortamında bu saldırıların hukuki ve etik boyutlarını da ele almıştır. Literatürdeki eksiklikler göz önünde bulundurularak tez, sesle yapılan siber saldırılar konusunda önemli bir bilgi boşluğunu doldurmayı ve dijital güvenlik politikalarına katkıda bulunmayı amaçlamaktadır. Bu çalışma sesle yapılan siber saldırılara dair farkındalık yaratmayı, etkili güvenlik stratejileri geliştirmeyi ve dijital güvenlik politikalarını güçlendirmeyi hedeflemektedir.

Bilim Kodu	:	92401
Anahtar Kelimeler	:	Ses, ses tabanlı saldırılar, ses teknolojileri, siber güvenlik, siber saldırı, veri ihlali.
Sayfa Adedi	:	203
Danışman	:	Doç. Dr. Nursel YALÇIN

EXAMINATION OF CYBER ATTACKS MADE BY USING VOICE

(M. Sc. Thesis)

Bilge LALE

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

July 2025

ABSTRACT

In recent years, cyber-attacks and even voice-based cyber-attacks in the digital world have become an increasingly greater security threat for individuals, organizations and critical infrastructures. Such attacks generally aim to gain unauthorized access to devices through voice commands, take control of devices and exploit security vulnerabilities in voice technologies. The rapid proliferation of voice-activated technologies such as smart assistants, smart speakers and mobile devices has created new types of attacks for malicious attackers. While voice-based systems are increasingly used in daily life, the types of voice-based cyber-attacks have diversified and the potential effects of these attacks have reached a much more serious threat dimension. However, studies in this field in the literature do not comprehensively address the different types of voice-based cyber-attacks, attack methods and the possible effects of these attacks on target systems. Existing studies generally focus on specific types of attacks and do not include a more comprehensive analysis of these threats. This thesis has examined in depth the various types of voice-based cyber-attacks, the attack methods used and the effects of these attacks on target systems; it also addresses the legal and ethical dimensions of these attacks in the current cyber security environment in Türkiye. Considering the gaps in the literature, the thesis aims to fill a significant knowledge gap on voice-based cyberattacks and contribute to digital security policies. This study aims to raise awareness on voice-based cyberattacks, develop effective security strategies, and strengthen digital security policies.

Science Code	:	92401
Key Words	:	Voice, Voice-based attacks, Voice technologies, Cyber security, Cyber-attack, Data breach.
Page Number	:	203
Supervisor	:	Assoc. Prof. Nursel YALÇIN

TEŞEKKÜR

Hem ders döneminde hem tez sürecinde bilgisi ve anlayışıyla bana yol gösteren, farklı alanlarda yeni bakış açıları kazanmamı sağlayarak tez konumun şekillenmesine katkıda bulunan değerli danışmanım Doç. Dr. Nursel YALÇIN'a en içten teşekkürlerimi sunuyorum.

Yüksek lisans eğitimim süresince gerek derslerde kazandırdıkları bilgilerle gerekse de teknik ve hukuki düşünme becerilerimi geliştirmeme sağladıkları katkılarla bana rehberlik eden Gazi Üniversitesi Bilişim Enstitüsündeki kıymetli hocalarıma; bu süreçte bana her zaman motivasyon veren ve yanımda olduklarını hissettiren arkadaşlarıma; son olarak da çağdaş ve aydınlık fikirler ışığında sorumluluk sahibi bir birey olmamda pay sahibi olan, hayatım boyunca maddi ve manevi desteklerini hiç esirgemeyen aileme çok teşekkür ederim.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ ix

ŞEKİLLERİN LİSTESİ x

RESİMLERİN LİSTESİ xi

SİMGELER VE KISALTMALAR xii

1. GİRİŞ 1

2. SES KULLANILARAK YAPILAN SİBER SALDIRILAR VE VERİ İHLALİ KAVRAMLARI 11

2.1. Siber Saldırı ve Ses Kullanarak Yapılan Siber Saldırı Kavramı 11

2.2. Veri İhlali ve Kişisel Veri Kavramları 22

3. SES KULLANILARAK YAPILAN SİBER SALDIRI TÜRLERİ 29

3.1. İlgili Çalışmalar 30

3.2. Vishing Saldırıları 49

3.3. Sesli Kimlik Hırsızlığı 58

3.4. Fiziksel Ses Taklidi ile Gerçekleştirilen Saldırılar 63

3.5. Deepfake Teknolojisi ile Gerçekleştirilen Saldırılar 69

3.6. Sesli Asistanlar Aracılığıyla Gerçekleştirilen Saldırılar 81

3.7. Ultrasonik Ses Dalgalarıyla Yapılan Saldırılar ve DolphinAttack 95

3.8. NUIT Tekniği ile Yapılan Saldırılar 103

3.9. SurfingAttack Saldırıları 111

3.10. HDD Üzerine Yapılan Ultrasonik Ses Tabanlı Saldırılar 117

3.11. Kriptografi ve Steganografi Yöntemi ile Gerçekleştirilen Ses Tabanlı Saldırılar 130

3.12. Akustik Dinleme Saldırıları 141

4. SESLE İLGİLİ VERİ İHLALLERİNİN İNCELENMESİ VE HUKUKİ SÜREÇ 151

4.1. Avrupa Birliği Mevzuatı (GDPR) 151

4.2. Türkiye'de Mevzuat (KVKK ve İlgili Kanunlar) 153

4.3. Hukuki Sorumluluklar ve Uygulamalar 155

5. ARAŞTIRMA YÖNTEMİ 163

5.1. Veri Toplama Süreci ve Seçim Kriterleri 167

5.2. Literatür Bulguları ve Analizler 168

6. SONUÇ VE ÖNERİLER 177

KAYNAKLAR 181

ÖZGEÇMİŞ 203

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 3.1. Genel olarak vishing ve sesli kimlik hırsızlığı arasındaki temel farklar 59

Çizelge 3.2. Sesli kimlik hırsızlığı ve sesli kimlik dolandırıcılığı arasındaki farklılıkları gösteren çizelge 61

Çizelge 3.3. Ultrasonik ses dalgalarıyla gerçekleştirilen siber saldırı türlerinin genel karşılaştırması 129

Çizelge 3.4. Steganografi ve kriptografi karşılaştırması..... 138

Çizelge 3.5. Keylogger kullanım örnekleri..... 145

Çizelge 5.1. Ses kullanılarak yapılan siber saldırıların sistematik derleme ve meta sentez yöntemiyle incelenmesi sürecinde izlenen aşamaları gösteren işlem basamakları 165

Çizelge 5.2. Literatürde yer alan ses tabanlı saldırılar ve savunma yöntemleri 173

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 2.1. Ses dalgası üzerinde genlik, dalga boyu, periyot, zaman ve mesafe özelliklerinin gösterimi 17

Şekil 2.2. Ses teknolojisi kullanılarak gerçekleştirilen siber saldırılarda yer alan aşamalara bir örnek 19

Şekil 3.1. Yaygın vishing yöntemlerine ilişkin bir diyagram 53

Şekil 3.2. Deepfake ile ses üretimine ilişkin bir şema 72

Şekil 3.3. Sesli deepfake oluşturma çemberi 73

Şekil 3.4. Basit bir sesli komutu manipülasyonu saldırısının aşamaları 84

Şekil 3.5. Sesli asistanların ve komutların manipülasyonuna ilişkin genel diyagram 86

Şekil 3.6. HDD'ye yönelik ses tabanlı saldırıların basamaklar 122

RESİMLERİN LİSTESİ

Resim **Sayfa**

Resim 2.1. Man-in-the-Middle saldırısını gösteren diyagram 14

Resim 3.1. Bir saldırganın deepfake içeriği oluşturması sürecine ilişkin temsili bir görsel..... 70

Resim 3.2. Bu örnekte sesli komutlar aracılığıyla manipüle edilen bir akıllı hoparlör dolayısıyla meydana gelen bir saldırı sonucu maddi zarar gerçekleşmiştir.. 87

Resim 3.3. İnsan kulağının duyabildiği ve duyamadığı frekans aralıklarını karşılaştırmalı olarak betimleyen görsel 96

Resim 3.4. Siri'ye ve akıllı ev sistemlerine yönelik bir saldırı örneği..... 98

Resim 3.5. NUIT saldırısının gerçekleştirilmesine ilişkin bir örnek 106

Resim 3.6. Bir hard diskin iç yapısı 117

Resim 3.7. Disk üzerinde iz (track) ve kesim (sector) oluşturulması 118

Resim 3.8. HDD başlık montajı ve disk yüzeyinin yer değiştirmesini gösteren bir görsel..... 124

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile aşağıda sunulmuştur.

Simgeler	Açıklamalar
dB	Desibel
f	Frekans
Hz	Hertz, frekans birimi, saniyedeki titreşim sayısı
kHz	Kilohertz, 1.000 Hertz
ms	Milisaniye, 1/1000 saniye
T	Periyot
v	Sesin yayılma hızı
λ	Dalga boyu

Kısaltmalar	Açıklamalar
AB	Avrupa Birliği
AI	Artificial Intelligence / Yapay Zekâ
AI/ML	Yapay Zekâ / Makine Öğrenimi
CRM	Customer Relationship Management / Müşteri İlişkileri Yönetimi
DoS	Denial of Service / Hizmet Engelleme
DdoS	Distributed Denial of Service / Dağıtık Hizmet Engelleme
GDPR	General Data Protection Regulation / Genel Veri Koruma Tüzüğü
HDD	Hard Disk Drive / Sabit Disk Sürücüsü
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things / Nesnelerin İnterneti
KVKK	Kişisel Verilerin Korunması Kanunu
LSB	Least Significant Bit / En az anlamlı bit

MD5	Message Digest Algorithm 5
MITM	Man-in-the-Middle / Ortadaki Adam Saldırısı
ML	Machine Learning / Makine Öğrenimi
NLP	Natural Language Processing / Doğal Dil İşleme
NUIT	Near-Ultrasound Inaudible Trojan
OECD	Organization for Economic Cooperation and Development / Ekonomik İş birliği ve Kalkınma Örgütü
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RSA	Rivest-Shamir-Adleman / Asimetrik şifreleme algoritması
SHA	Secure Hash Algorithm
SQL	Structured Query Language
TCK	Türk Ceza Kanunu
TLS	Transport Layer Security / Güvenli İletişim Protokolü
TMK	Türk Medeni Kanunu
TRDizin	Türkiye Atıf Dizini
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
VPN	Virtual Private Network / Sanal Özel Ağ
YÖK	Yükseköğretim Kurulu
YZ	Yapay Zekâ

1. GİRİŞ

Son yıllarda dijital dünyada karşılaşılan siber saldırılar yalnızca teknoloji uzmanları için değil, tüm toplumlar için önemli bir güvenlik tehdidi haline gelmiştir. Bu saldırılar, bireylerin kişisel verilerinden büyük şirketlerin önemli altyapılarına kadar geniş bir yelpazede zarara yol açabilmektedir. Artan siber tehditler, dijital güvenlik önlemlerinin yeniden değerlendirilmesini ve geliştirilmesini zorunlu kılmaktadır. Özellikle teknoloji ve iletişim alanındaki hızla gelişen yenilikler, yeni saldırı yöntemlerinin ortaya çıkmasına neden olmuştur. Günümüzde siber saldırılar genellikle veri ihlalleri, izinsiz erişim ve veri manipülasyonu gibi olgularla sonuçlanmakta ve bu tür saldırıların kapsamı, klasik güvenlik önlemlerinin yetersizliğini gözler önüne sermektedir. Bu bağlamda, ses teknolojilerinin yaygınlaşması, sesle yapılan siber saldırıların önemli bir tehdit olarak karşımıza çıkmasına yol açmıştır.

Bilişim ve bilgisayar alanındaki teknolojik gelişmeler sayesinde bilişim sistemleri, bilgisayarlar ve internetin kullanımı hayatın vazgeçilmez bir unsuru haline gelmiştir. Bilişim ve internetin bu denli yaygın hale gelmesi kullanıcılara bir yandan kolaylık sağlarken diğer yandan oluşan güvenlik sorunları ve veri ihlalleri sebebiyle sistemlerin kötüye kullanılmasına sebep olmaktadır (Aslay, 2017). Bu nedenle hem kişi düzeyinde hem de toplum genelinde istenmeyen etkiler meydana gelmektedir.

Siber suç kavramı da bir bilgisayar ve internet ağı içeren herhangi bir suçu ifade eden bilgisayar suçu olarak bilinir, ayrıca internet erişimiyle işlenen geleneksel suçları ifade eder (Hatipoğlu ve diğerleri, 2021).

Ses teknolojilerinin de gelişimiyle siber saldırılarda ses faktörü araç olarak kullanılmaya başlanmıştır. Günlük hayatımızın bir parçası haline gelen sesli asistanlar, akıllı hoparlörler ve diğer sesli cihazlar da saldırganlar için bir hedef haline gelmiştir. Günümüzde telefon görüşmelerinin yüksek sıklığı, telefon kayıtlarının saklanabilmesi ve ses teknolojilerinin giderek artması göz önüne alındığında ses analizlerinin adli alanda önemli bir araç haline gelmesi şaşırtıcı değildir (Deng ve diğerleri, 2023).

Sesle yapılan siber saldırılarda saldırganlar, genellikle sesli komutlar manipüle ederek veya sahte ses kayıtları kullanarak hedef cihazlara zarar vermeye ya da kişisel bilgilere erişmeye çalışırlar (Yan ve diğerleri, 2020).

Sesle yapılan siber saldırılar, bir kişinin sesi kullanılarak gerçekleştirilebileceği gibi bir cihazı doğrudan sese maruz bırakarak da gerçekleştirilebilir. Bu tür saldırılar arasında sesli arama dolandırıcılığı, sesli komutları manipüle etme, sesli kimlik avı ve sesli mesajlaşma saldırıları gibi saldırı türleri yer almaktadır. Son zamanlarda ortaya çıkmış bir saldırı yöntemi olarak ultrasonik ses dalgalarıyla bir cihazı veya sistemleri hedef alma şeklindeki saldırılar da bulunmaktadır.

Sesli kimlik avı dolandırıcılığı saldırıları, vishing "voice phishing" yani ses ve kimlik avı olarak tanımlanmaktadır. Bir kişinin telefon numarasını kullanarak arama yapar ve hedef kişiyi dolandırmaya çalışır (Kim ve diğerleri, 2018).

Hofing ve diğerlerine (2023) göre sesli komutları manipüle etme saldırısı, bir kişinin sesli komutlarının değiştirilerek sesli asistanlar aracılığıyla cihaz veya sistemlerin istenmeyen eylemleri gerçekleştirmesine neden olan bir saldırı türüdür. Sesli asistanlar, kullanıcı ile konuşma yoluyla etkileşim kuran ve gelen komutlara göre çeşitli görevleri yerine getiren yazılımlardır. Bu sistemler, doğal dil işleme, makine öğrenmesi ve derin öğrenme gibi yapay zekâ teknolojileri sayesinde komutları analiz eder ve uygun yanıtları üretir. Günümüzde yaygın olarak kullanılan bazı sesli asistanlar arasında Siri, Google Asistan, Samsung S Voice, Cortana ve Alexa gibi örnekler yer almaktadır. Saldırganlar, bu yazılımlar üzerinden kullanıcı adına komutlar göndererek, cihazların kontrolünü ele geçirebilmekte ve güvenlik açıklarını istismar edebilmektedir. J. Li ve diğerlerine (2023) göre sesli asistanlar, her yıl istikrarlı bir şekilde büyüyen bir pazar payına sahip olsa da hem gizlilik hem de güvenlik sorunlarına ve büyük ekonomik kayıplara neden olmaktadır. Böylelikle de kullanıcıların kişisel hassas bilgileri tehlikeye düşmektedir. Bu nedenle, sesli komut sistemlerini yanıltabilen saldırı tekniklerinin araştırılması ve bu sistemlerin güvenliğinin arttırılması gerekmektedir (Khodabakhsh ve diğerleri, 2016).

Ses taklitçiliği sosyal mühendislik yoluyla gerçek bir insan tarafından konuşulan özgün sesin değiştirilerek, yeniden oluşturularak veya doğrudan fiziksel yollarla taklit edilerek (Boyd ve diğerleri, 2023) karşıdaki kimsenin manipüle edilmesi ve bu şekilde saldırganın bir menfaat

elde etmeye çalıştığı bir sosyal mühendislik yöntemidir. Sosyal mühendislik gizli bilgilere erişim sağlamak için hiçbir şeyden haberi olmayan kişileri hedefleyen, bu bilgilerin daha sonra yasa dışı amaçlarla kullanılması ya da karaborsada veya karanlık ağlarda üçüncü taraflara satılmasını amaçlayan siber güvenlik tehdididir (Wang ve diğerleri, 2020). Burada kural olarak saldırganlar genellikle üç aşamalı bir süreci takip eder: Hedef hakkında istihbarat toplamak, güven oluşturmak, saldırıyı gerçekleştirmek (Kishore ve diğerleri, 2023).

Ses taklidinin sentetik bir medya üzerinden gerçekleştirilmesi ise "deepfake" kavramını ifade eder (Firc ve diğerleri, 2023). Deepfake teknolojisi ile kişilerin sesleri taklit edilebilir, görüntüleri değiştirilebilir ve sahte üretilmiş ses kayıtları ya da videolarla mağdurlar kandırılarak kişisel veriler ele geçirilebilir. Deepfake teknolojisi, hızla gelişen yapay zekâ ve görüntü işleme teknolojileri sayesinde yaygın hale gelen, Deep Learning (Derin Öğrenme) ve Fake (Sahte) kelimelerinin birleşimiyle oluşturulmuş, Türkçe olarak "derin sahtecilik" denilen bir kavramdır (Anıkaydın, 2022). Deepfake teknolojisinin günümüzdeki popülaritesi ve kolay erişilebilirliği, bu teknolojinin siber alanda ne gibi tehditlere ve etkilere sahip olabileceğinin araştırılmasını gerektirmektedir. Firc ve diğerlerine (2023) göre, deepfake teknolojisinin şu anda bilinen kullanımları kullanım amacına göre iki ana kategoriye ayrılabilir: Faydalı ve kötü amaçlı. Seow ve diğerlerine (2022) göre deepfake kötü niyetli olarak kullanıldığında kamuoyunun kurumlara olan güvenini azaltmak, önde gelen kişilerin itibarını zedelemek ve insanları etkilemek dahil olmak üzere siyasi ve sosyal güçlere zarar verici sonuçlar doğurabilmektedir.

Kriptografi ve steganografi yöntemi ile ses dosyalarının içine metinler gizlenebilmektedir (Phipps ve diğerleri, 2022). Kriptografi şifreleme bilimidir (Arda, 2011), steganografi ise bilgiyi gizleme bilimine verilen addır. Vural'a (2019) göre kriptografi mesajın içeriğinin korunması ile ilgilenirken steganografi mesajın varlığının gizlenmesi ile ilgilenmektedir. Steganografi verinin gizli ve güvenli bir şekilde iletilmesini sağlar; amacı, iki kişi arasındaki iletişimin üçüncü bir şahıs tarafından fark edilmesini engellemektir. Bu işlemler metin, ses, resim veya video dosyaları içerisine veriyi gizleyerek yapılır. Gizlenen veriler herhangi bir metin dosyası içerisinde olabileceği gibi herhangi bir görüntü içerisine başka bir görüntüyü gizleme şeklinde de olabilmektedir. Yine aynı şekilde, bir ses veya video dosyasının içine bir metin dosyası da saklanabilir. Ses steganografisi en önemsiz bite kodlama, parçalı kodlama, faz kodlaması, yaygın spektrum ve yankı gizleme gibi yöntemlerle

gerçekleştirilmektedir. Bu yöntemlerden herhangi biriyle yapılan siber saldırı türünde, bir ses dosyasına gizlenen veriler nedeniyle bir yere aktarılmaması gereken kişisel ya da toplumsal düzeydeki özel ve gizli bilgiler, içeriğine hiç ulaşılmadan kolaylıkla başka ortamlara ve kişilere aktarılabilir. Bu nedenle de çeşitli düzeylerde veri ihlalleri gerçekleşebilir ve dolayısıyla da birçok zarar meydana gelebilir.

Ultrasonik ses dalgalarıyla yapılan siber saldırılar (DolphinAttack adı da verilmektedir), insan kulağının duyamayacağı frekans seviyesine sahip ses dalgalarını kullanarak bir cihazı veya sistemi hedef alır. Bu tür saldırılarla ultrasonik sinyalleri kullanarak cihazlara zarar verme ya da ultrasonik sinyalleri kullanarak cihazlardan veri çalmak amaçlanmaktadır (Zhang ve diğerleri, 2017).

NUIT (Near-Ultrasound Inaudible Trojan) adı verilen teknik, sesli asistanlara karşı internet üzerinden uzaktan yürütülebilen ve duyulamayan saldırıyı ifade eder. Duyulmayan saldırı sinyalleri ile sessiz tepkiler genellikle uçtan uca gerçekleşir ve fark edilmez. Ancak bazı hallerde akıllı bir cihazın duyulamayan bir komuta verdiği yanıt duyulabilir ve dolayısıyla mağduru saldırıların varlığı konusunda uyarabilir. Bazı hallerde ise saldırganın herhangi bir özel donanım kullanması gerekmez; bunun yerine saldırgan, kurbanın mikrofonlarına ve bunlarla ilişkili sesli kontrol sistemine saldırmak için kurbanın kendi konuşmalarını kullanabilir. NUIT tekniğinin iki örneği vardır, bunlar kurbanın kendi konuşması ile kurbanın mikrofonunun aynı cihazda olup olmamasına göre farklılık gösterir. Her iki halde de uzaktan yürütülen bu saldırı nedeniyle birçok olumsuz sonuç meydana gelmektedir (Xia ve diğerleri, 2023).

SurfingAttack adı verilen ve yine ultrasonik ses dalgalarıyla gerçekleştirilen saldırı türünde ise ses kontrollü cihaz ile saldırgan arasında katı malzemelerdeki akustik iletimin özelliklerinden yararlanılmaktadır. Katı malzeme üzerindeki yönlendirilmiş dalgalardan yararlanan SurfingAttack kötü amaçlı bir web sitesini ziyaret etmek, casusluk yapmak, sahte bilgiler enjekte etmek gibi etkileşimli olmayan saldırıların yanı sıra SMS tabanlı iki faktörlü kimlik doğrulama şifrelerini kırma ve hileli aramalarla kurbanın sentetik sesini kullanarak telefon dolandırıcılığı yapma gibi çeşitli yeni saldırılara da olanak sağlayabilir. (Yan ve diğerleri, 2020).

Siber saldırıların amacı, belirtildiği gibi, hedef sistemlerin işlevselliğini bozmak, bilgi çalmak, bilgileri manipüle etmek, yasal olmayan yollarla para kazanmak veya diğer kötü amaçlar için kullanılabilecek kişisel verileri ele geçirmektir. Kişisel verilerin siber saldırılar ya da iç ve dış birtakım tehditler üzerinden yasadışı şekilde elde edilmesi ile veri ihlalleri meydana gelmektedir. Bu veri ihlalleri özel hayatın gizliliği, E-Ticaret, devlet belgeleri, E-Devlet kurumu, haberleşmenin gizliliği gibi alanlarda meydana gelmektedir. Veri ihlallerine ilişkin yazılım, güvenlik sistemi, kriptolama vb. teknik tedbirler kadar verilerin depolandığı işyerlerinin ya da kuruluşların yönetim anlayışı gibi konular da güvenlik açısından çok boyutlu olarak ele alınmalıdır (Kutlu ve diğerleri, 2017).

6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre kişisel veri, kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Gündüz ve Yücel'e (2023) göre de siber bağlamda bir kişinin adı, soyadı, adresi, telefon numarası, görüntüsü ve resmi, ses kaydı, genetik bilgileri, hobileri, ziyaret ettiği internet siteleri gibi bilgiler kişisel veri kapsamda değerlendirilir.

Kişisel verilere yönelik suçlara ilişkin düzenlemeler genel olarak 5237 sayılı Türk Ceza Kanunu'nun çeşitli maddelerinde yer almaktadır. Siber saldırılar hatta sesle yapılan siber saldırılar nedeniyle kişisel verilere yönelik olarak bu tür suçlar artmakta; hukuki, maddi, itibari ihtilaflar doğabilmektedir. Bu durumların önüne geçilebilmesi için öncelikle kişilerin siber saldırılar konusunda bilinçli olması, gerekli görüldüğü takdirde eğitim almaları gerekmektedir. Çeşitli önlemler alınarak riskler ve meydana gelebilecek saldırılar büyük ölçüde azaltılabilir.

Siber güvenlik konusu uluslararası güvenlik çalışmaları için önemli bir konumdadır, insan hakları hukuku açısından da oldukça önemli bir yer tutmaktadır. Siber suçların insan haklarına olan müdahalesini azaltmak için siber güvenliğe özel önem verilmesi gerekmektedir. Bu güvenliği sağlama konusunda devletlere, sivil toplum kuruluşlarına, uluslararası kuruluşlara veya şirketlere birçok görev düşmektedir (Kiraz, 2021).

Türkiye'deki literatür taramaları, sesle yapılan siber saldırılara dair kapsamlı bir çalışmanın bulunmadığını ortaya koymuştur. TRDizin ve YÖK Ulusal Tez Merkezi gibi veri tabanlarında yapılan aramalar, bu konuya dair yeterli sayıda kaynağa rastlanmadığını göstermektedir. Uluslararası literatür taramaları ise genellikle belirli saldırı türlerine

odaklanmış, ancak sesle yapılan siber saldırıların tüm yönleriyle ele alındığı bir derlemeye rastlanmamıştır. Bu literatür boşluğu, tez çalışmasının önemini pekiştirmektedir ve sesle yapılan siber saldırıların sistematik bir şekilde incelenmesini gerekli kılmaktadır.

Bu tez, sesle yapılan siber saldırıların çeşitli türlerini, bu saldırıların hedef sistemler üzerindeki etkilerini ve bu tehditlere karşı alınabilecek güvenlik önlemlerini derinlemesine incelemiştir. Literatür taramaları, Scopus, ScienceDirect, IEEE Xplore ve Web of Science gibi uluslararası veri tabanlarında, 2013-2024 yılları arasında yayımlanan akademik çalışmalara odaklanmıştır. Toplam 59 akademik çalışma seçilerek analiz edilmiştir. Meta-sentez yöntemiyle gerçekleştirilen bu değerlendirmeler, sesle yapılan saldırıların etkilerini ve bu saldırılara karşı geliştirilebilecek güvenlik önlemlerini kapsamlı bir şekilde ortaya koymuştur. Ayrıca çalışma PRISMA Kontrol Listesi'ne uygun olarak gerçekleştirilmiş, bilimsel geçerliliği artırılmıştır.

Tez, sadece bireysel güvenliği ele almakla kalmayıp kurumsal veri güvenliği ve devlet düzeyindeki altyapıların korunmasını da ele almıştır. Sesle yapılan saldırıların hukuki boyutları da incelenmiş, bu saldırıların yaratacağı etik ve yasal sorunlar dijital güvenlik politikalarını yeniden şekillendirme gerekliliğini doğurmuştur. Bu bağlamda sesli asistanlar ve benzeri teknolojilere yönelik güvenlik önlemlerinin geliştirilmesi sadece teknik değil, aynı zamanda yasal ve etik sorumlulukları da kapsamaktadır.

Ayrıca tez, sesle yapılan siber saldırılar konusunda farkındalık yaratmayı ve dijital güvenlik alanındaki politikaların güçlendirilmesine katkıda bulunmayı amaçlamıştır. Literatürdeki eksiklikleri gidermek ve sesle yapılan saldırıların çeşitliliği ile bu saldırılara karşı alınabilecek önlemleri araştırmak suretiyle, gelecekte yapılacak çalışmalara önemli bir temel oluşturulmuştur. Ayrıca yeni güvenlik protokollerinin geliştirilmesi ve dijital güvenlik politikalarına dair öneriler sunulmuştur. Bu doğrultuda, sistematik derleme ve meta-sentez yöntemleri kullanılarak ses tabanlı siber saldırılar üzerine mevcut literatür kapsamlı bir şekilde analiz edilmiştir. Çalışma, bu saldırı türlerinin yaygınlığını ve etkilerini ortaya koyarak okuyucuların konuya dair farkındalığını artırmayı hedeflemektedir.

Problem durumu

Siber saldırılar, son yıllarda teknoloji kullanıcıları için giderek artan bir tehdit haline gelmiştir. Bu saldırılar, iş bilgisayarlarında ya da kişisel bilgisayarlarda ve ağlarda yer alan önemli belgelere ve sistemlere zarar vermeyi, bunların kontrolünü ele geçirmeyi veya bunlara erişim sağlamayı amaçlar. Bu saldırılarda genel olarak kötü niyetli kişiler, kullanıcıların seslerini kaydederek bu ses kayıtlarını manipüle edip sahte sesler oluşturabilmekte, bu kayıtları daha sonra söz konusu kişilerin aleyhine kullanabilmektedirler. Benzer şekilde sesli asistanlar ve sesli komutlar manipüle edilmekte, sosyal mühendislik yoluyla kişiler suistimal edilmekte, gelişen ses teknolojileri kötü amaçlı şekilde kullanılabilmektedir. Bunun sonucunda da bireysel ve toplumsal gizlilik sınırlarının aşılması nedeniyle veri ihlalleri meydana gelebilir, çeşitli suç eylemlerinin sayısı artabilir. Bu durum, ses teknolojileri kullanılırken ayrıca dikkatli olunması ve veri ihlallerine karşı etkili önlemler alınması gerektiğini göstermektedir.

Araştırmanın amacı

Bu çalışmanın amacı ses kullanılarak yapılan siber saldırıların yöntemlerini ve meydana getireceği sonuçlarını incelemek, gerçekleşen veri ihlalleri üzerine odaklanıp riskleri ve tehlikeleri analiz etmek, söz konusu tehditlere karşı önlem almasına yardımcı olmaktır. Bu çalışma ile ses kullanılarak gerçekleştirilen saldırıların nasıl gerçekleştiğinin, kullanılan yöntemlerin, hedef sistemler üzerindeki etkisinin incelenmesi ve siber güvenlik mekanizmalarının bu saldırılara karşı nasıl koruma sağlayabileceğinin araştırılması ve elde edilen kaynakların sistematik olarak derlenmesi hedeflenmektedir.

Araştırma soruları

Çalışma, şu sorular üzerinde odaklanılarak ilerleyecektir:

1. Siber saldırı kavramı nedir?
2. Siber saldırılar hangi amaçlarla düzenlenir?
3. Ses kavramı nedir?
4. Ses kullanılarak yapılan siber saldırı türleri nelerdir?
5. Ses kullanılarak yapılan siber saldırıları türlerinin gerçekleştirilme yöntemleri nelerdir?

6. Ses kullanılarak yapılan siber saldırılara ilişkin olarak literatürdeki çalışmalara göre hangi tür önlemler alınmış ve bu saldırılara karşı hangi tür önlemler önerilmiştir?
7. Ses kullanılarak yapılan siber saldırılar sonucunda bireysel ve toplumsal düzeyde hangi zararlar meydana gelebilir?
8. Ses kullanılarak yapılan siber saldırılar gerçekleştirilirken ilgili sistemlerin hangi güvenlik açıklarından yararlanılmış ve sızılmıştır?
9. Ses kullanılarak yapılan siber saldırılar sonucunda meydana gelen zararlar veri ihlali oluşturur mu?
10. Ses kullanılarak yapılan siber saldırılar sonucunda meydana gelen zararların ve veri ihlallerinin hukuki boyutu nedir?
11. Ses kullanılarak yapılan siber saldırılara karşı hangi önlemler alınmalı ve hangi savunma stratejileri geliştirilmelidir?

Araştırmanın önemi

Bu çalışmanın hazırlanması için yapılan literatür taramasında ses kullanılarak yapılan siber saldırıların türlerine, bu saldırıların gerçekleştirilme yöntemlerine ve meydana getireceği sonuçlara ilişkin olarak Türkçe olarak hazırlanmış kapsamlı ve yeterli bir çalışma bulunamamıştır. Günümüzün vazgeçilmez bir parçası olan teknoloji ve dolayısıyla ses teknolojilerine yönelik bu saldırılar ile ilgili yeterli bir çalışmanın varlığı gerekmektedir.

Sınırlılıklar

Çalışma, ses kullanılarak yapılan siber saldırı türlerinin gerçekleştirilme şekilleri, meydana getireceği sonuçlar ve bu sonuçlar dolayısıyla ortaya çıkabilecek veri ihlallerinin incelenmesi ile sınırlı olacaktır.

Bu kapsamda TRDizin ve YÖK Ulusal Tez Merkezi'nde "ses" + "siber saldırı" olarak arama yapılmış ve bir sonuç bulunamamıştır.

Daha sonra Scopus, ScienceDirect, IEEE Xplore ve Web of Science veri tabanlarında 2013-2024 yıllarıyla, sadece açık kaynaklarda yer alma koşuluyla ve "başlık, özet veya yazarın belirttiği anahtar kelimeler" filtrelemesi ile sınırlandırma yapılarak öncelikle "voice" + "cyber attacks", "audio" + "cyber attacks" ve "sound" + "cyber attacks" kelime grupları

aratılmıştır. Burada karşılaşılan literatürün kapsamı oldukça geniş olduğundan yukarıdaki sınırlılıklar korunarak arama sonuçlarını sadece saldırı yöntemleriyle ilgili çalışmalara indirgemek amacıyla "voice" + "cyber attacks" + “method”, "audio" + "cyber attacks" + “method” ve "sound" + "cyber attacks" + “method” kelime grupları kullanılmış ve bu kapsamda toplam 102 akademik çalışmaya ulaşılmıştır. Söz konusu çalışmalar içerik olarak incelenmiş ve ses ile yapılan siber saldırı türlerini betimleyen 59 akademik çalışma, bu çalışmada sistematik derleme yöntemiyle derlenmek ve incelenmek üzere seçilmiştir.

Çalışmanın ikinci bölümünde, kuramsal olarak ses kullanılarak yapılan siber saldırılar ve veri ihlali kavramlar ile bu kavramlarla ilişkili olan diğer terimler ele alınmış ve çalışmanın ana çerçevesi oluşturulmuştur.

Üçüncü bölümde, literatür taramasında karşılaşılan en yaygın ses kullanılarak yapılan siber saldırı türlerinden 11 tanesi detaylı bir şekilde incelenmiştir.

Dördüncü bölümde, üçüncü bölümde incelenen saldırılar neticesinde meydana gelen ve adli bilişimde büyük önem taşıyan sesle ilgili veri ihlallerinin incelenmesi yapılmıştır. Ayrıca konuşmacı tespitinden de bahsedilmiştir. Ayrıca dördüncü bölümde genel ve güncel olarak hukuki süreçten ve bununla ilgili olarak sesle ilgili delillerin elde edilmesi, sesle ilgili delillerin hukuki boyutu ve saldırılar nedeniyle gerçekleşen veri ihlallerinin hukuki boyutu üzerinde durulmuştur.

Beşinci bölümde çalışmanın araştırma yöntemi ayrıntılı olarak ele alınmıştır. Bu kapsamda ses kullanılarak gerçekleştirilen siber saldırıların sistematik bir derleme yöntemiyle incelenmesi süreci açıklanmıştır. Öncelikle sistematik derleme yönteminin dayandığı bilimsel ilkeler, yöntemin seçilme gerekçesi ve araştırma soruları bağlamında sağladığı katkılar ortaya konulmuştur. Daha sonra veri toplama süreci, literatür tarama stratejileri, kullanılan veri tabanları, anahtar kelime kombinasyonları ve uygulanan dahil etme ve hariç tutma kriterleri açıklanmıştır. Ayrıca literatürden elde edilen bulgular doğrultusunda, sesle yapılan saldırıların hedefleri, kullanılan yöntemler ve oluşturdukları güvenlik açıkları sistematik olarak ortaya konulmuştur. Böylece çalışmanın genel amacına hizmet edecek şekilde kapsamlı ve disiplinler arası bir değerlendirme süreci tamamlanmıştır.

Sonuç ve öneriler başlıklı altıncı bölümde ise çalışmanın genel bir özeti yapılmış ve çalışma kapsamında gelecek çalışmalar için önerilere yer verilmiştir. Ayrıca çalışmanın literatüre katkısından bahsedilmiş ve sonuçların çıkarımları yapılmıştır.

2. SES KULLANILARAK YAPILAN SİBER SALDIRILAR VE VERİ İHLALİ KAVRAMLARI

Bu bölümde siber güvenlik alanında büyük bir yer tutan ve giderek daha fazla önem kazanan siber saldırıların genel kavramsal çerçevesi ele alınacaktır. İlk olarak siber saldırıların tanımı yapılacak ve bu saldırıların bazı yaygın türleri üzerinde durulacaktır. Siber saldırıların teknolojinin hızlı gelişimiyle nasıl çeşitlendiği ve bireyler ile kurumlar için oluşturduğu potansiyel tehditler tartışılacaktır. Ayrıca sesin siber saldırılar içerisindeki rolü incelenecek; özellikle sesli komutlar ve ses içerikli veriler aracılığıyla yapılan saldırıların nasıl gerçekleştirildiği, bu tür saldırıların güvenlik açıkları yaratma şekilleri üzerine temel bilgiler verilecektir. Bölümde ayrıca veri ihlali, kişisel veri ve kişisel verilerin güvenliği kavramları üzerinde durulacak; verilerin siber saldırılar karşısındaki savunma stratejileri hakkında temel bir bakış açısı sunulacaktır. Bu bağlamda siber saldırılarla mücadeleye yönelik kullanılan güvenlik önlemleri ve teknolojilerin nasıl evrildiği tartışılacaktır. Ayrıca yapılan literatür taraması kapsamında bu kavramların bireylerin siber güvenlik farkındalıklarını nasıl etkilediği üzerinde durulacaktır. Bu bölüm, konu ile ilgili temel kavramların ve literatürdeki önemli katkıların derinlemesine bir incelemesini sunarak sonraki bölümlerde yapılacak daha kapsamlı analizler için bir kavramsal temel oluşturacaktır.

2.1. Siber Saldırı ve Ses Kullanarak Yapılan Siber Saldırı Kavramı

Siber saldırı kavramı

"Siber" terimi, "sibernetik" kelimesinden türetilmiştir. Bu kavram, 1958 yılında makineler ile canlılar arasındaki iletişimi araştıran Louis Couffignal tarafından geliştirilen sibernetik bilimine dayanmaktadır. Siber saldırılar ise, yalnızca dijital sistemlere yönelik bir tehdit oluşturmamakla kalmayıp, aynı zamanda kişilik haklarına da bir saldırı niteliği taşımaktadır (Taşdöğen, 2019). Siber saldırı, “sistem güvenliğini hedef alan akıllı bir tehdit kaynaklı saldırı” olarak tanımlanır (Shirey, 2000: 13,43). Bu tanıma göre, kasıtlı olmayan tehditler sebebiyle ortaya çıkan durumlar siber saldırı olarak değerlendirilmez.

Siber saldırılar, günümüzde dijital dünyanın en büyük tehditlerinden biridir. Bu saldırılar bilgisayar korsanları, siber suçlular veya diğer kötü niyetli aktörler tarafından gerçekleştirilebilir. Siber tehdit terimi ise, siber saldırıların arkasında duran kişilerin

kullandıkları yöntemleri ve davranışları ifade eder. Siber saldırı gerçekleştiren kişilerin amaçları maddi kazanç sağlama, şöhret kazanma ve bu durumla övünme, karşı tarafa maddi ya da manevi zarar verme, belirli bir amaç doğrultusunda kişi ve kurumlara ait önemli bilgileri ele geçirmektir (Uluyol ve Demirci, 2022: 11, 17). Bu amaçlar doğrultusunda siber saldırıların hedefleri arasında devlet kurumları, finansal kuruluşlar, sağlık kuruluşları, işletmeler hatta bireysel kullanıcılar yer alabilir.

Siber saldırı kaynaklarını ise genel olarak dört ana grupta toplamak mümkündür:

- Hacker ve Siber Suçlular: Türk Dil Kurumu tarafından "bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi, bilgisayar programlama alanında standartların üzerinde beceriye sahip olan ve böylece ileri düzeyde yazılımlar geliştirebilen ve kullanabilen" kişiler olarak tanımlamaktadır. Bunlar kişisel bilgisayarlara, mobil cihazlara veya organizasyonların, şirketlerin ve kamu kuruluşlarının bilgisayar ağlarına izinsiz giriş yapan bireylerdir (Yılmaz ve Sağıroğlu, 2013).
- İç (Dahili) Saldırganlar: Herhangi bir organizasyonun içinde belirli amaçlar doğrultusunda dahili sistemlere saldıran kurumsal kişilerdir. Bu saldırılar genellikle organizasyonun gizliliğini veya güvenliğini tehdit edecek şekilde gerçekleştirilir.
- Siber Aktivistler: Kendi görüşleri doğrultusunda toplumsal veya politik sorunları kötü ya da uygunsuz bulup bu sorunları gündeme getirmek amacıyla kamu veya özel sektörün siber alanlarına saldıran kişi veya gruplardır. Bu tür saldırılar genellikle sosyal adaletin sağlanması veya siyasi değişim talebiyle ilişkilidir.
- İstihbarat Kurumları: Ülkeler, uluslararası siber dünyada birbirlerini tehdit olarak görmeye başlamışlardır. Bu tehdit algısı sebebiyle, ülkeler siber savunma ve saldırı ekipleri oluşturmakta ve diğer ülkelere ait kritik verilere erişim sağlamaya çalışırken aynı zamanda hedef ülkelerin kritik alt yapılarına siber saldırılar gerçekleştirmeye devam etmektedir (Ulusal Siber Olaylara Müdahale Merkezi, 2014: 3, 12).

Siber saldırılar, kaynaklar yani saldırganlar tarafından birçok farklı yöntemle gerçekleştirilebilir. Örneğin: bilgi hırsızlığı, kimlik avı, fidye yazılımı, zararlı yazılım, DdoS saldırıları… Bilgi hırsızlığı, hassas verileri ele geçirmek için kullanılan bir yöntemdir. Kimlik avı, sahte web siteleri veya e-postalar aracılığıyla kullanıcıların kişisel bilgilerini çalmak için kullanılır. Fidye yazılımı, hedef sistemlerin dosyalarını şifreleyerek para talep etmek için kullanılır. Zararlı yazılım, hedef sistemlere zarar vermek veya bilgi çalmak için

kullanılır. DdoS saldırıları, hedef sistemleri aşırı yükleyerek çökertmek için kullanılır. Bu saldırı türleri saldırganları amacına göre ya da saldırıda kullanılan araçlara göre çeşitlilik gösterir. Aşağıda birkaç yaygın siber saldırı türlerine örnek verilmiş ve bunlar ayrı ayrı tanımlanmıştır.

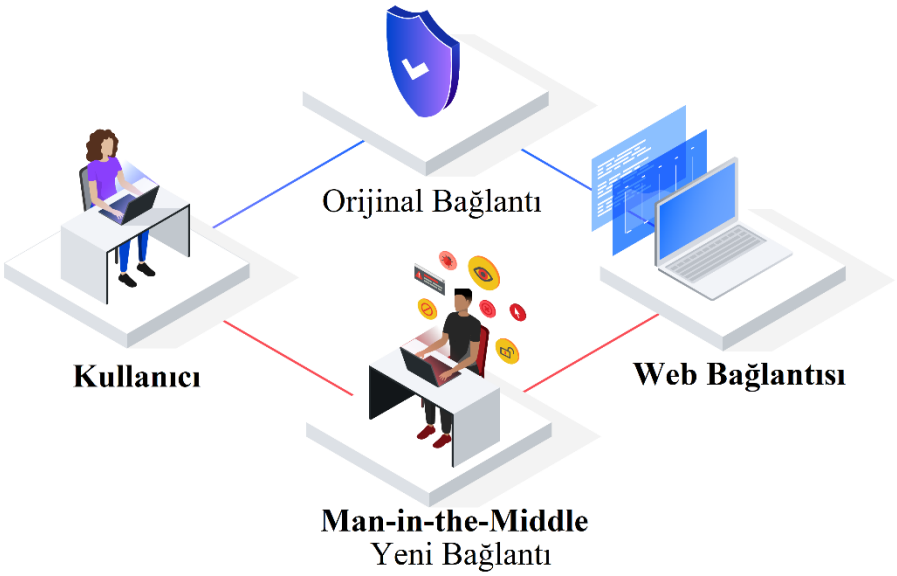
Sniffing temel olarak verinin yolunu kesmektir; amacı şifreleri (e-posta, web, vb.), e-posta mesajlarını, transfer edilen dosyaları ele geçirmektir (Kaya, 2010). Sniffing ile network üzerindeki paketler yakalanabilir, içeriği okunabilir. Bu saldırıdan korunmak için bilgisayarlar arasındaki bağlantıların şifreli olması gerekmektedir.

Malware kötü niyetli yazılımlara verilen addır. Kişilerin izni olmadan bilgisayar sistemlerine sızdırılan kötü amaçlı yazılımlardır. Bilgisayarları veya ağları çalışamaz hale getirir, sistemler üzerinde kolaylıkla gizlenir, çoğalır veya saldırganlara erişim izni verip sistemi uzaktan kontrol edebilme yetkisi verir.

Phishing saldırıları, kimlik avı saldırıları olarak adlandırılır. Bu yöntemde saldırganlar kişilere güvenilir kaynaklardan gelmiş gibi gösterilen e-postalar yollar ve kişilerin site bilgilerini, kredi kartı bilgilerini çalmaya çalışırlar. Genellikle e-posta ile gönderilen linklere tıklayan mağdurlar, klonlanmış sitelere yönlendirilir ve bu siteye girdikleri bilgiler saldırganlar tarafından ele geçilirmiş olur (Amerikan Psikoloji Derneği, 2014).

İngilizce olarak Denial of Services ve Distributed Denial of Services ifade edilen DoS saldırıları, bazı çevrimiçi hizmetlerin düzgün çalışmasını engellemeye çalışmak için yapılır. Saldırganlar bir web sitesine veya bir veri tabanına çok fazla sayıda istek yollar, sistemi meşgul ederler ve bu da sistemlerin çalışmasını durdurmasına yol açar. DdoS saldırıları ise DoS saldırılarının birden fazla bilgisayardan yapılmasıyla meydana gelir (Söğüt ve diğerleri, 2021).

Man-in-the-Middle saldırısında saldırgan, kendini gizleyerek kurbanı kendi ağı üzerinden erişmek istediği servise yönlendirir. Saldırgan, kurbanın erişmek istediği Wi-Fi ağını taklit eder, kurban yanılarak saldırganın Wi-Fi ağına girdiğinde yaptığı her işlem, saldırgan tarafından görülebilir, kurbanın verilerini saldırgan tarafından toplanabilir. Bu saldırı türüne ilişkin bir diyagram aşağıda gösterilmiştir (Resim 2.1):



Resim 2.1. Man-in-the-Middle saldırısını gösteren diyagram (Lindemulder ve Kosinski, 2024)

SQL Injection saldırıları saldırganların, zayıf yapılandırılmış web uygulamalarındaki SQL sorgularına kötü amaçlı kod ekleyerek veri tabanlarına izinsiz erişim sağlamasına dayalı bir saldırı türüdür. Çoğu web uygulaması, kullanıcıdan aldığı verileri SQL veri tabanlarına iletir. Eğer uygulama kullanıcılardan gelen verileri yeterince güvenli bir şekilde işlerse saldırganlar, bu verileri manipüle ederek zararlı SQL komutları ekleyebilir. Bu komutlar veri tabanındaki verilere izinsiz erişim sağlamak, verileri değiştirmek veya silebilmek amacıyla kullanılabilir. SQL Injection, genellikle veri tabanı yönetim sistemlerindeki güvenlik açıklarından yararlanır. Saldırgan, doğru sorguları kullanarak veri tabanını kontrol altına alabilir ve hassas bilgileri elde edebilir. (Atac, 2023).

Cryptojacking, bir saldırganın başkasının bilgisayarını veya cihazını kullanarak kripto para madenciliği yapmasıdır. Saldırganlar, kurbanın bilgisayarına kötü amaçlı yazılım yerleştirerek veya tarayıcıda çalışan JavaScript kodları kullanarak bu işlemi gerçekleştirirler. Bu yazılımlar, kurbanın işlem gücünü çalarak saldırganın kripto para üretmesine olanak tanır. Cryptojacking, genellikle kurbanın bilgisayarında performans düşüşüne yol açar ve enerji tüketimini artırır. Ayrıca kurban fark etmeden uzun süre boyunca kripto para üretimi yapılır, bu da büyük zararlara yol açabilir. (Mutombo ve diğerleri, 2025).

Eavesdropping Attack yani dinleme saldırısı, bir ağ üzerinden iletilen verilerin izinsiz olarak dinlenmesi ve ele geçirilmesi amacıyla yapılan bir siber saldırı türüdür. Bu saldırılar,

genellikle internet ya da yerel ağlar gibi ağ iletişimi sağlayan platformlarda gerçekleştirilir. Saldırgan, ağ üzerinden aktarılan verileri dinleyerek kullanıcıların kredi kartı bilgileri, şifreler, kişisel mesajlar veya hassas konuşmalar gibi kişisel verileri elde etmeye çalışır. Eavesdropping saldırıları genellikle iki şekilde sınıflandırılır: Pasif ve aktif. Pasif Eavesdropping saldırısında saldırgan yalnızca ağ trafiğini gözlemler ve iletilen veriler üzerinde herhangi bir değişiklik yapmaz. Bu tür saldırılarda saldırgan, iletilen verilerde herhangi bir manipülasyon yapmadan sadece bilgi toplar. Bu bilgiler şifreler, finansal veya kişisel veriler olabilir. Aktif Eavesdropping saldırısı ise daha karışık bir saldırı türüdür ve saldırgan, ağ üzerindeki verileri toplamakla kalıp aynı zamanda ağda sahte birimler oluşturarak veya sistemdeki birimleri taklit ederek aktif bir şekilde bilgi toplar. Bu tür bir saldırıda, saldırgan kullanıcılara zararsız bir ağ cihazı gibi görünüp kullanıcılara çeşitli sorular sorarak ya da belirli verileri alarak güvenlik açıklarını istismar eder. Bu tür saldırılara örnek olarak Man in the Middle saldırıları verilebilir. Burada saldırgan, iki taraf arasında iletilen verileri hem dinler hem de manipüle eder. Eavesdropping saldırıları, şifrelenmemiş veya zayıf şifrelemeye sahip ağlarda büyük bir tehdit oluşturur. Bu tür saldırılardan korunmak için, verilerin şifrelenmesi ve güvenli iletişim protokollerinin kullanılması önemlidir (Stallings, 2017: 10,15).

Birthday Attack adlı saldırı ise kriptografik hash fonksiyonlarının zayıflıklarını hedef alır ve özellikle mesajların, yazılımların veya dijital imzaların bütünlüğünü tehdit eder. Bu saldırı "birthday paradox" olarak bilinen istatistiksel bir kavramdan kaynaklanır ve bu kavram, bir grup insan arasında aynı doğum günü paylaşan iki kişinin olma olasılığının beklenenden yüksek olduğunu ifade eder. Aynı prensip hash fonksiyonlarının çalışma mantığına da uygulanır. Bir hash fonksiyonu, verilen veri girişiyle sabit uzunlukta bir hash değeri (mesaj özeti) üretir. Ancak hash değerlerinin sayısı sınırlıdır ve çok sayıda farklı veri, aynı hash değerini üretebilir. Birthday Attack'te bir saldırgan iki farklı mesaj için aynı hash değerini bulmaya çalışır, buna çakışma yaratma denir. Bu çakışma bulunduğunda saldırgan, mesajlardan birini değiştirip alıcıya gönderebilir. Alıcı sadece hash değerlerine bakarak mesajın değiştiğini fark etmez. Bu saldırı özellikle dijital imza sistemlerinde tehlikeli oluşturabilir çünkü bir saldırgan imzalanmış bir mesajı değiştirip aynı hash değeriyle alıcıya iletebilir. Birthday Attack, zayıf hash fonksiyonları nedeniyle daha büyük tehlike oluşturur, bu yüzden güçlü ve güvenli şifreleme algoritmalarının kullanımı büyük öneme sahiptir (Chavan ve diğerleri, 2023).

Fidye zararlıları yani ransomware, genellikle kurumları hedef alarak kritik verileri şifreleyip erişilemez hale getirir. Saldırganlar, sistem açıklarını kullanarak kötü amaçlı yazılım yerleştirir ve ardından şifrelenmiş dosyaların geri verilmesi için maddi bir karşılık yani fidye talep eder. Fidyenin genellikle kripto para birimi olarak ödenmesi istenir. Bu tür saldırılar genellikle sosyal mühendislik tekniklerine dayanır; örneğin phishing e-postaları ya da güvenlik açıkları kullanılarak sisteme sızılır. Fidye zararlıları özellikle sağlık, finans ve kamu sektörlerinde büyük risk oluşturur. Çünkü şifrelenen veriler kurumların işeyişini durdurabilir ve maddi kayıplara yol açabilir. Fidye ödense bile şifreli verilerin geri alınması kesin bir olanak değildir. Bu nedenle fidye yazılımlarına karşı güçlü güvenlik önlemleri, düzenli yedeklemeler ve etkili bir siber güvenlik stratejisinin varlığı gereklidir (Threat Hunter Team, 2014).

PriceWaterhouseCoopers'ın 2015 yılına ait "The Global State of Information Security" çalışması, siber suçların her gün 117.000'den fazla saldırıya yol açacak kadar büyüdüğünü ortaya koymaktadır. Ayrıca söz konusu çalışmada siber saldırıların ve türlerinin daha da artacağı, özellikle casusluk ve siber savaşın arttığı ve saldırganların kimliklerini gizlemekte daha başarılı hale geldikleri de belirtilmiştir. Saldırıların çoğu ABD, Rusya, Birleşik Krallık, Almanya gibi ülkelerde meydana gelmektedir. Özellikle mobil saldırılar, akıllı telefonların yaygınlaşmasıyla birlikte artış göstermektedir (Bendovschi, 2015).

Ses kullanarak yapılan siber saldırı kavramı

Ses, bir titreşimin ortama periyodik etkiler yaparak işitme sistemi tarafından algılanıp değerlendirilmesi sonucu beyinde oluşan bir duyumdur. Sesin oluşum süreci üç temel unsurdan oluşur: titreşim kaynağı, titreşimlerin iletilmesini sağlayan madde ortamı ve oluşan bu titreşimleri algılayacak işitme sistemi. Bu unsurlar bir araya geldiğinde ses fiziksel olarak ortaya çıkar. Ancak ses sadece bir fiziksel olgu değildir, insan deneyimiyle de şekillenen bir algı biçimidir. İnsanlar varoluşlarından itibaren sürekli olarak sesle iç içe olduklarından ses her birey için farklı algı yaratabilir. Aynı zamanda ses, iletişim ve çevresel etkileşimler dışında, yaşamın devamlılığını sağlamak için de kritik bir rol oynar (Değirmenli, 2023).

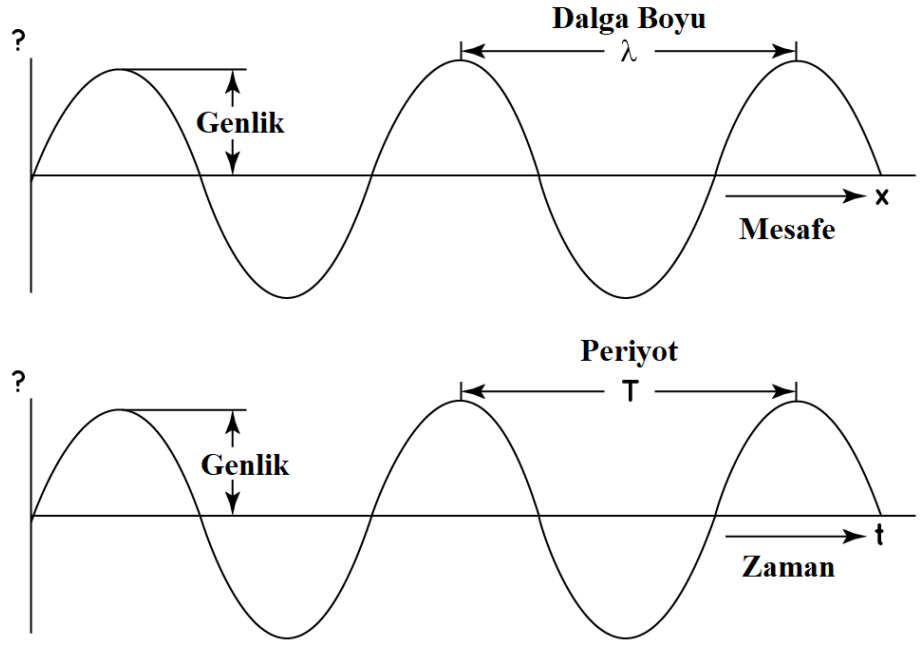
Sesin fiziksel özellikleri, sesin nasıl üretildiğinin ve nasıl algılandığının anlaşılması için önemlidir. Bu özellikler frekans, genlik, dalga boyu ve periyot gibi unsurlarla belirlenir:

Frekans, bir ses dalgasının saniyede yaptığı titreşim sayısıdır. Frekans, sesin perdesini yani tizlik-peslik algısını belirler. Frekans arttıkça ses daha tiz, azaldıkça daha pes olur. İnsan kulağı yaklaşık 20 Hz ile 20 kHz arasındaki frekansları duyabilir.

Genlik kavramı ses dalgasının denge durumundan en yüksek noktaya kadar olan mesafesidir. Genlik, sesin şiddeti veya gürlüğü ile ilişkilidir. Yüksek genlikli sesler daha yüksek, düşük genlikli sesler ise daha düşük gürültü seviyesinde duyulur (Karakuş, 2024).

Dalga boyu bir dalganın kendisini tekrar ederken kat ettiği mesafedir. Dalga boyu sesin yayılma hızına ve frekansına bağlı olarak değişir. Sesin kaynağından yayılma şekli ve ortamın özellikleri, dalga boyunu etkiler.

Periyot, bir titreşimin kendisini tamamlaması için geçen süredir. Sesin periyodu dalganın frekansına ters orantılıdır. Yani, frekans arttıkça periyot kısalır. Şekil 2.1'de sesin genlik, dalga boyu, periyot, zaman ve mesafe gibi özelliklerinin ses dalgası üzerindeki temsilinin gösterimi yapılmıştır.



Şekil 2.1. Ses dalgası üzerinde genlik, dalga boyu, periyot, zaman ve mesafe özelliklerinin gösterimi

Sesin doğadaki varlığı ise genellikle karmaşık bir yapıya sahiptir. Herhangi bir doğal ses, yalnızca bir temel frekanstan ve onun üst frekanslarından oluşur. Üst frekanslar, temel

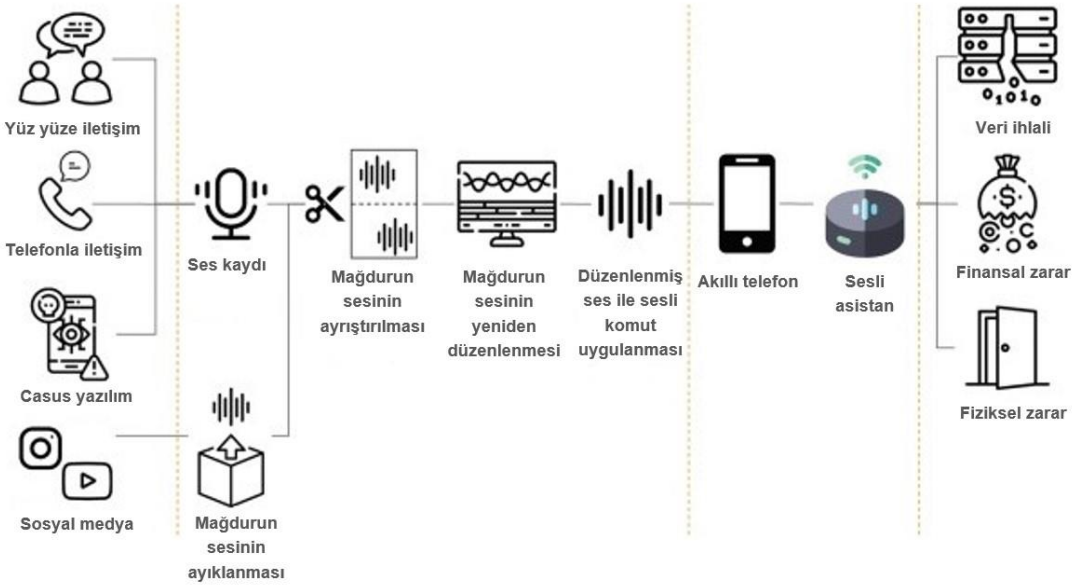
frekansın katlarıdır ve bu bileşenler sesin tınısını yani sesin rengini belirler (Bishop ve Keating, 2012). Bu durum özellikle müzikte ve ses mühendisliğinde çok önemlidir, çünkü bir enstrümanın sesini diğerinden ayırt edilmesini sağlar.

Doğal yollarla oluşan sesler karmaşıktır çünkü birden çok frekansı aynı anda içerirler. Bu sesler, işitme sistemi tarafından analiz edilerek farklı tınılar, tonlar ve uyumlar olarak algılanır. Örneğin aynı frekansa sahip iki sesin tınıları, ses kaynağının özelliklerine göre farklı olabilir. Tını, sesin ayırt edici bir özelliği olarak farklı çalgıların aynı notayı çalmalarına rağmen farklı algılanmalarını sağlar.

Ses, doğada sadece bir frekans ve genlikten oluşmaz. Her ses kaynağı, birçok farklı frekanstan oluşan karmaşık bir yapıdan meydana gelir. Bu da sesin algılanmasını, farklı çalgıların veya seslerin birbirinden ayırt edilmesini sağlar. Frekanslar, tınılar ve uyumlar, sesin temel fiziksel özellikleriyle birlikte bir araya geldiğinde, sesin zenginliği ve çeşitliliği ortaya çıkar.

Sesin bu karmaşık yapısı sadece fiziksel ve algısal boyutlarıyla değil, teknolojik gelişmelerle de yakın bir ilişki içindedir. Son yıllarda sesin dijital sistemlerdeki rolü, iletişimden güvenliğe kadar birçok alanda devrim yaratırken yeni tür tehditlerin de ortaya çıkmasına neden olmuştur. Sesli tanıma sistemleri ve sesli komutlarla yapılan etkileşimler, bu teknolojilerin güvenlik açıklarını hedef alan saldırıların temelini hazırlamaktadır.

Teknolojinin, özellikle ses teknolojisi alanındaki hızlı ilerlemesi, siber saldırılarda bir araç olarak sesin daha fazla kullanılmasına yol açmıştır. Şekil 2.2, bazı saldırıların aşamalarını göstermektedir. Çeşitli alanlarda yürütülen araştırmalar, ses teknolojilerinin siber güvenlik üzerindeki etkilerini açıklığa kavuşturmayı ve ses tabanlı saldırılarla ilişkili karmaşıklıkları ve potansiyel riskleri ortaya koymayı amaçlamaktadır. Birçok türü olmasına rağmen, en yaygın ses tabanlı siber saldırılar iki ana türe ayrılabilir: Sesli kimlik avı saldırıları (vishing) ve sesli komutlarla gerçekleştirilen sistem manipülasyonları.



Şekil 2.2. Ses teknolojisi kullanılarak gerçekleştirilen siber saldırılarda yer alan aşamalara bir örnek (Bilika ve diğerleri, 2024)

Sesli kimlik avı veya vishing, saldırganların telefon görüşmeleri veya sesli mesajlar aracılığıyla kullanıcıların kişisel verilerini çalmayı amaçladığı geleneksel kimlik avı saldırılarının sesle yönlendirilen karşılığıdır. Çalışmalar, vishing saldırıları sırasında faillerin hedef kullanıcıyla bir güven ortamı oluşturmak için tasarlanmış sosyal mühendislik tekniklerini kullandığını ve böylece kişisel verilerin yetkisiz kişiler tarafından kolayca ele geçirilmesine olanak sağladığını ortaya koymuştur (Naqvi ve diğerleri, 2023). Bu tür saldırı yöntemleri son derece ikna edicidir ve genellikle yazılım aracılığıyla belirli kişilere göre uyarlanabilir, ses analizi ve konuşma sentezi teknolojilerindeki gelişmelerden faydalanılabilir. Örneğin, yapay zekâ ve makine öğrenimindeki yenilikler, saldırganların yazılım aracılığıyla neredeyse birebir ses taklitleri üretmesine izin vererek hedef kullanıcıları aldatma olasılığını önemli ölçüde artırmıştır (Desetty ve diğerleri, 2020).

Ses tabanlı siber saldırıların bir diğer yaygın türü olan sesli komutlar aracılığıyla manipülasyonlar, sesli komutlar kullanılarak akıllı cihazların yetkisiz bir şekilde kontrol edilmesini ifade eder. Bu saldırılar, hedef cihazların mikrofonlarındaki veya sesli asistanlarındaki güvenlik açıklarından yararlanır. Akıllı ev sistemleri ve kişisel asistanlar bu saldırı tekniğinin önemli hedefleridir ve bu açıdan önemli riskler oluştururlar. Araştırmalar, bu cihazlardaki güvenlik açıklarının kötü amaçlı yazılımlar tarafından istismar edilebileceğini ve böylece kişisel ve finansal verilerin tehlikeye atılabileceğini göstermiştir

(Ansari ve diğerleri, 2022). Örneğin bir saldırgan, bu hedef akıllı telefonun sesli asistanı aracılığıyla kötü amaçlı komutlar vererek parolalar, finansal veriler, fotoğraflar, mesajlar, telefon numaraları ve kişiler gibi hedeflenen bir akıllı telefonda depolanan verileri çalabilir (McKee ve Noever, 2023).

Ses tabanlı saldırıların temel amaçları genellikle kişisel verileri çalmak, finansal bilgileri elde etmek veya hedef bilgi sistemlerini tamamen devre dışı bırakmaktır. Ses tanıma ve konuşma sentezi teknolojilerindeki gelişmeler sonucunda, kötü amaçlı yazılımların sesli komutlar veya sesli mesajlar yoluyla yayılması ve kullanıcıları etkilemesi daha kolay hale gelmiştir. Özellikle akıllı cihazların, kullanıcının bilgisi olmadan sesli komutlar aracılığıyla kötü amaçlı amaçlarla uzaktan kontrol edilebilmesi önemli güvenlik sorunları yaratmaktadır (Hussain ve diğerleri, 2021). Araştırmalar, sesli komutların akıllı cihazlara kötü amaçlı yazılım yüklemek veya sistem güvenlik açıklarından yararlanmak için sıklıkla kullanıldığını göstermektedir (Buil-Gil ve diğerleri, 2023). Böylece saldırganlar hedef kullanıcıya ve cihazına kolayca zarar verebilir ve kullanıcıdan çeşitli miktarlarda finansal çıkar elde edebilirler.

Ses taklidi ile yapılan saldırılar, sesli biyometrik sistemlerin en büyük güvenlik açığına işaret eder. Bu saldırı türünde bir saldırgan, hedefin sesini taklit ederek ses tanıma sistemlerini manipüle etmeye çalışır. Ses taklidi, bilgisayar tabanlı yazılımlar veya ses kaydetme cihazları kullanılarak yapılabilir. Saldırganlar, hedef kişinin sesini kaydederek ya da yapay zekâ algoritmalarıyla sesini benzer şekilde üreterek kimlik doğrulama sistemlerini atlatmayı amaçlarlar (Zhou ve diğerleri, 2022). Bu tür saldırılar, telefon bankacılığı ve akıllı cihazlar gibi sesle kontrol edilen sistemlerde oldukça yaygındır. Ses taklidi, biyometrik güvenlik sistemlerinin zayıf noktalarından faydalanan ciddi bir tehdit oluşturmaktadır.

Sesli komut manipülasyonu, saldırganların hedef cihazlara kötü niyetli komutlar enjekte ederek cihazları kontrol etmeye çalıştığı bir saldırı türüdür. Bu tür saldırılar, özellikle akıllı ev sistemlerinde yaygındır (Zhang ve diğerleri, 2017). Örneğin bir akıllı hoparlör ya da telefon, kullanıcıların sesli komutlarına yanıt verir. Ancak saldırganlar, sesli komutları manipüle ederek cihazlara zarar verebilirler. Saldırganlar, cihazların mikrofonunu kullanarak kötü amaçlı komutlar gönderebilir, bu da cihazların kontrolünü ele geçirmelerine yol açar. Yine örnek olarak akıllı sistemlerin kullanıldığı bir evdeki güvenlik sistemlerine sesli komutlar aracılığıyla müdahale etmek, evin güvenliğini riske atabilir.

Eavesdropping Attack yani akustik dinleme saldırısı, ağ üzerindeki iki elektronik cihaz arasında gönderilen sesli verilerin dinlenmesi, kaydedilmesi veya silinmesi yoluyla yapılan saldırılardır. Bu saldırılar, bir ağ üzerinden geçen sesli iletişimin dinlenmesini içerir ve genellikle hedefin özel bilgilerine ulaşmak amacıyla yapılır (X. Li ve diğerleri, 2016). Örneğin bir telefon görüşmesi sırasında sesli komutlarla gerçekleştirilen bir bankacılık işlemi, saldırganlar tarafından dinlenebilir ve kişisel finansal verilere erişim sağlanabilir. Bu tür saldırılar, genellikle iletişim hattındaki zayıflıklar veya güvenlik açıkları kullanılarak gerçekleştirilir.

Vishing, telefon aracılığıyla yapılan bir tür kimlik avı saldırısıdır. Saldırganlar, kurbanları güvenlik tehditleri hakkında bilgilendirecekleri bahanesiyle arar ve kişisel bilgilerini çalmaya çalışırlar. Bu tür saldırılar, sesli komutlarla kurbanı manipüle etmek amacıyla yapılır. Saldırganlar, genellikle kurbanları kandırarak kredi kartı bilgilerini veya bankacılık bilgilerini talep ederler (Fremont Federal Kredi Birliği, 2015). Telefonla yapılan bu tür dolandırıcılıklar, sesli komutlarla daha etkili hale gelir ve kullanıcıların güvenlikleri tehdit altına girer.

İngilizce olarak Acoustic Side-Channel Attacks yani akustik yan kanal saldırıları saldırganların cihazların elektromanyetik dalgalarını, işlemcilerinin seslerini veya diğer akustik yan etkilerini kullanarak bilgi edinmeye çalıştığı bir saldırı türüdür (Conti ve diğerleri, 2024). Akustik yan kanal saldırıları, cihazların işleme süreçleri sırasında çıkan ses dalgalarını veya titreşimleri analiz ederek kritik verilere ulaşmayı amaçlar. Örneğin bir bilgisayarın işlemcisinin ya da klavyesinin çıkardığı ses dalgaları, bir saldırgan tarafından toplanabilir ve işlenebilir. Bu tür saldırılar, daha ileri düzeyde donanım ve yazılım bilgisi gerektiren, sofistike saldırılardır.

Teknolojinin gelişimine paralel olarak ses kullanılarak yapılan siber saldırılar, yukarıdaki örnekler gibi birçok farklı şekilde çoğalarak evrim geçirmiştir. Yapay zekâ ve makine öğrenimi gibi alanlardaki gelişmeler, ses tanıma sistemlerinin yaygınlığını artırmış olsa da bu sistemlerin kötüye kullanılması engellenememiştir. Bu nedenle de dijital güvenlik konusu hala ciddi bir endişe kaynağı olmaktadır. Özellikle sesli biyometrik doğrulama ve sesli komut sistemleri, bu tür saldırılara karşı savunmasızdır. Sesli tanıma teknolojilerinin bu kadar yaygın hale gelmesi, saldırganların daha farklı ve birbirinden karışık yöntemler

kullanarak sesli komutlarla yapılabilecek kötü niyetli işlemleri gerçekleştirmelerine olanak tanımaktadır.

Ses tabanlı olarak yürütülen bu saldırılardan korunmak için çeşitli önlemler alınabilir. Sesli komutları şifrelemek, cihazların mikrofonlarına yönelik güvenlik duvarları oluşturmak, sesli biyometrik sistemleri güçlendirmek ve yapay zekâ tabanlı ses tanıma algoritmalarını geliştirmek bu önlemler arasında yer alır. Ayrıca üreticiler tarafından cihaz mikrofonları yalnızca güvenli ve doğrulanmış kaynaklardan gelen komutları kabul edecek şekilde tasarlanmalıdır.

2.2. Veri İhlali ve Kişisel Veri Kavramları

Veri ihlali, kişisel ve kurumsal verilerin güvenliğinin ihlal edilmesi anlamına gelir. Bu durum genellikle verilerin izinsiz erişim, ifşa, kayıp veya tahribatı ile ortaya çıkar. Bir veri ihlali bireysel kullanıcıların, şirketlerin veya devletlerin verilerinin gizliliğini, bütünlüğünü ve erişilebilirliğini tehdit edebilir. Veri ihlalleri yalnızca dijital ortamda değil, aynı zamanda fiziksel ortamda da meydana gelebilir; ancak dijital çağda siber saldırılar sonucu gerçekleşen veri ihlalleri, en yaygın ve etkili tehditler arasında yer almaktadır.

Siber saldırılar verilerin izinsiz bir şekilde ele geçirilmesi, kötüye kullanılması veya tahrif edilmesi gibi durumlara neden olabilir. Bu tür ihlaller, genellikle hedef alınan verilerin değerine ve hassasiyetine göre değişkenlik gösterir. Örneğin bir bankanın finansal verilerine yapılan saldırılarla kişisel ödeme bilgileri ve hesap numaraları sızdırılabilirken bir sağlık kuruluşunun veri tabanına yapılan saldırılar, bireylerin tıbbi geçmişlerine dair kritik verilere erişim sağlanmasına olanak tanıyabilir.

Veri ihlallerinin ciddiyeti, ihlalin boyutuna, içeriğine ve meydana gelen zararların doğasına bağlı olarak farklılık gösterebilir. Büyük çaplı veri ihlalleri, yalnızca bireysel kullanıcıları değil, aynı zamanda şirketleri, kamu kurumlarını ve devletleri de ciddi şekilde etkileyebilir. Ayrıca çoğu yasal düzenleme, veri ihlali durumlarında kurumların belirli bir süre içerisinde veri sahiplerine bilgilendirme yapmasını ve güvenlik açıklarını kapatmalarını zorunlu kılar.

Veri ihlalleri, genellikle siber suçlular tarafından, kişisel verilerin kötüye kullanılmak üzere ele geçirilmesi amacıyla gerçekleştirilir. Sonuç olarak bu tür ihlaller, güvenlik açıklarının

tespit edilmesi ve ihlali gerçekleştiren kişilerin yasal yollarla cezalandırılması gerekliliğini doğurur.

Kişisel veri

Özel hayatın gizliliği, birçok temel insan hakkıyla doğrudan ilişkili olan kişisel verilerin korunması konusu, teknolojik ilerlemelerle birlikte önemli bir tartışma konusu haline gelmiştir. Bilgi ve iletişim teknolojilerindeki hızlı değişimler, bireylerin kişilik haklarının korunması amacıyla çeşitli yasal düzenlemelerin yapılmasını zorunlu kılmaktadır (Pearce ve Platten, 1998).

Kişisel verilerin korunmasına yönelik ilk yasal düzenleme, 1970 yılında Almanya'da kabul edilmiştir. Bu düzenlemeden sonra 1973'te İsveç, 1974'te ABD, 1977'de Federal Almanya ve 1978'de Fransa'da kişisel verilere ilişkin kanunlar çıkarılmıştır. 1980 yılında Ekonomik İş birliği ve Kalkınma Örgütü (OECD) tarafından bağlayıcı nitelikte olmayan ancak üye devletler için rehber teşkil edebilecek "Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler" benimsenmiştir (Ural Uslan ve Değirmenci, 2023). OECD, bu ilkeler aracılığıyla uluslararası düzeyde özel hayatın gizliliği ve kişisel verilerin korunmasına yönelik güvence sağlamayı amaçlamaktadır.

Birleşmiş Milletler, 1985 yılında kişisel verilerin korunmasına ilişkin aldığı kararlar almış, 1990 yılında ise "Bilgisayarda İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler" düzenlemesini gerçekleştirmiştir. Bu rehber ilkeler, kişisel verilerin korunmasıyla ilgili bir mekanizma tesis edilmesini öngören ilk uluslararası belge niteliğindedir.

1981 yılında Avrupa Konseyi tarafından kişisel verilerin korunmasına ilişkin olarak Avrupa İnsan Hakları Sözleşmesi'nde yer alan hakların yetersiz olduğu görüşüyle 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi kabul edilmiştir. Bu sözleşme 1985 yılında yürürlüğe girmiştir; yalnızca üye ülkeleri değil, sözleşmeye taraf olan üçüncü ülkeleri de kapsamaktadır. Ayrıca bu sözleşme kişisel verilerin korunması alanında bağlayıcılık taşıyan tek uluslararası metin olma özelliğini taşımaktadır (Uslan ve Değirmenci, 2023).

Avrupa Birliği (AB) üyesi devletler arasındaki kişisel verilerin korunmasına ilişkin ulusal mevzuatların farklılıklar göstermesi, AB'yi verilerin korunması için belirli standartlar oluşturmaya teşvik etmiştir. Bu kapsamda AB, kişisel verilerin korunmasına yönelik çeşitli tarihlerde yasal düzenlemeler gerçekleştirmiştir. AB'nin ilk yasal adımı, 1995'te tarihinde kabul edilen Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi olmuştur. Bu direktif, kişisel verilerin korunması açısından üye devletler arasındaki mevzuat farklılıklarını sona erdirmeyi ve verilerin serbest dolaşımını sağlamayı hedeflemiştir. Ancak söz konusu direktif ihtiyaçları yeterince karşılayamayınca Avrupa Parlamentosu 2016'da Avrupa Birliği Genel Veri Koruma Tüzüğü'nü kabul etmiştir. Bu tüzük, direktifi yürürlükten kaldırarak AB üyesi tüm devletlerde bağlayıcı hale gelmiştir (Akıncı, 2017).

AB, kişisel verilerin korunması alanındaki çalışmalarıyla dikkat çekmektedir. AB üyesi devletler ile diğer devletler arasındaki kişisel verilerin korunmasında AB'nin standartlarına uyum sağlanması beklenmektedir. Türkiye'deki veri ihlallerinin giderilmesi ve Türkiye ile AB arasında uyumun sağlanması adına da ulusal mevzuatta çeşitli düzenlemeler yapılmıştır. Kişisel verilerin korunması, Türkiye Cumhuriyeti Anayasası'nın 20. maddesinde "özel hayatın gizliliği" başlığı altında düzenlenmiştir. 1982 Anayasası'nın ilk halinde kişisel verilere dair bir hüküm bulunmamakla birlikte, 2010 yılında yapılan anayasa değişikliği ile kişisel verilerin korunması hakkı 20. maddede anayasal güvence altına alınmıştır.

Kişilik hakkı perspektifinden bakıldığında 4721 sayılı Türk Medeni Kanunu'nun (TMK) kişiliği koruyan 23, 24 ve 25. maddelerinde kişisel verilerin korunması ile ilgili hükümler mevcuttur. Ayrıca 5237 sayılı Türk Ceza Kanunu'nun (TCK) 134 ile 140. maddeleri arasında "Özel Hayat ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı bölümde de kişisel verilerin korunmasına dair çeşitli düzenlemeler yapılmıştır. Daha sonra ise Türkiye'de Avrupa Birliği'ne üyelik sürecinde kişisel verilerin korunmasının oynadığı önemli rol nedeniyle kişisel verilerin korunması konusunun düzenlenmesi amacıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir.

Kişisel veri, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) madde 3/1-d'de "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Madde gerekçesinde ise kişisel verilerin sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi doğrudan tanımlayıcı bilgilerle sınırlı kalmayıp aynı zamanda kişinin fiziki, ailevi,

ekonomik, sosyal ve diğer özelliklerine ilişkin bilgilerin de kişisel veri olarak kabul edileceği belirtilmiştir. Buna göre bir kişinin belirli veya belirlenebilir olması, mevcut verilerin bir şekilde bir gerçek kişiyle ilişkilendirilmesiyle o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut içerikler taşıması ya da kimlik, vergi, sigorta numarası gibi kayıtlarla ilişkilendirilmesi durumunda bu veriler kişisel veri olarak kabul edilir.

Kişisel veriler genel olarak isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi doğrudan veya dolaylı yoldan bir kişiyi belirlenebilir kılabilen her türlü bilgi olarak tanımlanır. Örneğin telefon bankacılığı sisteminde müşterinin bankaya verdiği talimatın yer aldığı ses kaydı, kişisel veri olarak değerlendirilebilir (Kişisel Verileri Koruma Kurumu, 2025). KVKK madde 3/1-d'de yapılan tanımlamadan hareketle, kişisel veriler oldukça geniş bir yelpazeye yayılmaktadır. Yargıtay ceza daireleri de bu geniş kapsamı benimsemiş ve kişisel veri suçlarına ilişkin değerlendirmelerinde kişisel verilerin çok çeşitli örneklerini dikkate almıştır (Karakaya, 2024). Yargıtay'a göre kişisel veri kavramından kişinin yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir (Yargıtay 12.Ceza Dairesi, 2018/8144 E., 2019/8317 K. sayılı ve 10.07.2019 tarihli kararı). Ayrıca Yargıtay, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilgi kişisel veri olarak kabul edilmesi gerektiğini belirtmiştir (Yargıtay 12. Ceza Dairesi. 2018/8295 E., 2019/6858 K. sayılı ve 29.05.2019 tarihli kararı).

Özellikle geçtiğimiz yüzyılda bilim ve teknolojideki gelişmeler, topluma ve toplumsal yaşamı oluşturan unsurlara önemli yansımalar yapmış, bu da birçok bilgiyi kişisel veriye dönüştürmüştür. Bu bağlamda banka hesap numaraları, sosyal güvenlik numaraları,

vatandaşlık numaraları ve elektronik posta adreslerinin şifreleri gibi örnekler verilebilir. Kişisel verileri genel hatlarıyla iki gruba ayırmak mümkündür: Birinci grup, insanın varoluşundan kaynaklanan ve kişiliğiyle ilgili bilgileri içerirken ikinci grup, modern bilişim toplumunda insanın yer alması dolayısıyla edinilen veya çeşitli hizmetlere erişim için kullanılan bilgilerdir. Ancak bu ayrım, kişisel verilerin değeri ve korunma hakkı açısından bir fark yaratmamaktadır (Dülger, 2016).

Günümüzde kişisel veriler, teknolojinin gelişmesi ve dijitalleşmenin artması ile daha da hassas bir konu haline gelmiştir. Özellikle kişisel verilerin işlenmesi zorunluluğu bulunan kurum ve kuruluşlar için bu verilerin nasıl işleneceği ve nasıl saklanacağı büyük bir tartışma konusu olmuştur. Bu bağlamda, KVKK çerçevesinde 2017 ila 2019 yılları arasında yayınlanan uygulama yönetmelikleri, kişisel verilerin işlenmesine dair önemli düzenlemeler getirmiştir. 2019 yılında ise Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) kullanıma açılmış ve belirli işletmelere bu sisteme kaydolma ve işledikleri kişisel verilerle ilgili güncel bilgilendirme sağlama yükümlülüğü getirilmiştir. Bu sistemle birlikte, kişisel verileri işleyen üçüncü kişilerin bu verileri nasıl işleyecekleri ve nasıl saklayacakları, Kişisel Verileri Koruma Kurumu tarafından titizlikle denetlenmektedir (Karakaya, 2024).

Kişisel verilerin korunması yalnızca kurumların yükümlülüğü değildir, aynı zamanda kişilerin özel hayatlarının güvence altına alınması açısından da büyük bir öneme sahiptir. Kişisel verilerin hukuka aykırı şekilde işlenmesi ve paylaşılması, TCK kapsamında kişisel veri suçlarına neden olabilecek durumlar yaratmaktadır. Kişisel veri suçları, yalnızca işletmelerin faaliyetleriyle sınırlı kalmayıp bireysel düzeyde de işlenebilen suçlar arasında yer almaktadır. Bu nedenle kişisel verilerin korunmasına dair yasal düzenlemelere uyulması hem hukuki hem de toplumsal bir sorumluluktur.

Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği'nde Genel Veri Koruma Yönetmeliği (GDPR) gibi düzenlemeler, kişisel verilerin korunması için belirli kurallar koymakta ve bu verilerin işlenmesi, saklanması, iletilmesi ve erişilmesi süreçlerinde şeffaflık ve güvenlik önlemleri talep etmektedir.

Kişisel verilerin korunması, dijitalleşen dünyada giderek daha fazla önem kazanmaktadır. Siber saldırılar kişileri ve kurumları kişisel verilerin çalınması, izinsiz erişilmesi veya ifşa edilmesi gibi tehditlerle karşı karşıya bırakmaktadır. Bu bağlamda ses tabanlı sistemlerin

kötüye kullanılmasında olduğu gibi teknolojinin çeşitli şekillerde kötü amaçlarla kullanımı, kişisel veri güvenliğini daha da karmaşık hale getirmektedir.

Veri ihlali ve kişisel veri ilişkisi

Veri ihlali ve kişisel veri kavramları arasında doğrudan bir ilişki bulunmaktadır. Bir veri ihlali çoğu zaman kişisel verilerin sızdırılması, kaybolması veya izinsiz erişime açılması ile sonuçlanır. Özellikle ses tabanlı siber saldırılar, kişisel verilerin korunması açısından ciddi tehditler oluşturabilir. Sesli veriler, kimlik doğrulama, erişim kontrolü ve diğer güvenlik protokollerinde kullanılan önemli biyometrik verilerdir. Ses tabanlı saldırılar, genellikle sesli yanıt sistemlerini, telefon görüşmelerini veya dijital asistanları hedef alarak kişisel verilere erişim sağlamak amacı güder.

Bir sesli iletişim kaydının veya dijital ortamda iletilen sesli verilerin sızdırılması, kişisel verilerin ifşasına yol açabilir. Örneğin bir sesli görüşmenin kaydedilmesi ve bu kaydın izinsiz bir şekilde ele geçirilmesi, bireylerin özel bilgilerini tehlikeye atabilir. Bu tür ihlaller, kişisel verilerin korunması adına ciddi riskler oluşturur ve veri sahiplerinin mahremiyetinin ihlali anlamına gelir.

Veri ihlali, kişisel verilerin güvenliği açısından ciddi bir tehdit oluşturmakta ve siber saldırılar bu tehditleri daha karmaşık hale getirmektedir. Özellikle ses tabanlı saldırılar, kişisel verilerin korunmasını güçleştirirken, bireylerin dijital güvenliğini tehdit eden önemli bir unsur olarak öne çıkmaktadır. Bu bağlamda, kişisel verilerin korunmasına yönelik yasal düzenlemeler ve teknolojik önlemler, veri ihlallerini önlemek ve dijital ortamda güvenliği sağlamak adına hayati önem taşımaktadır.

KVKK ve GDPR kapsamında, veri sorumluları işledikleri kişisel verilerin güvenliğini sağlamakla yükümlüdür. Bu yükümlülüğün ihlali halinde veri ihlali meydana gelir. KVKK'nin 12. maddesi, veri sorumlusunun kişisel verilerin hukuka aykırı şekilde üçüncü kişilerce ele geçirilmesini engelleme yükümlülüğünü düzenlemektedir. Veri ihlali gerçekleştiğinde, sorumlu en kısa sürede ilgili kişiyi ve Kişisel Verileri Koruma Kurulu'nu bilgilendirmelidir.

KVKK, veri ihlalini açık bir şekilde tanımlamamakta ve türlerini sıralamamaktadır. Ancak GDPR, veri ihlalini dört kategoriye ayırmaktadır: (1) verilerin imha edilmesi, (2) değiştirilmesi, (3) yetkisiz şekilde açıklanması, (4) yetkisiz erişim sağlanması (Veri Koruma Komisyonu, 2019). Bu tür ihlaller, gizlilik, bütünlük ve erişilebilirlik ihlali olarak üç grupta incelenmektedir (Tosoni, 2020: 100, 102).

Özellikle erişilebilirlik ihlali, KVKK ve GDPR arasındaki en temel farklardan biridir. Örneğin, bir siber saldırı nedeniyle veri sorumlusunun kişisel verilere ulaşamaması, GDPR kapsamında veri ihlali sayılırken, KVKK'nin dar yorumuna göre veri üçüncü kişiler tarafından ele geçirilmediği sürece ihlal kabul edilmemektedir (Sevindi ve Ordu, 2023). Ancak, doktrinde KVKK'nin geniş yorumlanarak gizlilik, bütünlük ve erişilebilirlik ihlallerini de kapsaması gerektiği savunulmaktadır (Dülger, 2019).

Avrupa düzenlemeleriyle uyum sağlamak isteyen veri sorumlularının yalnızca üçüncü kişilerin verileri ele geçirmesi halinde değil, GDPR'de belirtilen tüm ihlal türlerinde Kurul'a bildirimde bulunması önerilmektedir.

Sonuç olarak veri ihlali ve kişisel veri arasındaki ilişki, dijital güvenlik ortamında giderek daha kritik bir konu haline gelmiştir. Özellikle ses tabanlı siber saldırılar, kişisel verilerin korunmasını zayıflatırken mahremiyetin ihlali riskini artırmaktadır. Bu bağlamda KVKK ve GDPR gibi yasal düzenlemeler, kişisel verilerin güvenliğini sağlamak adına önemli bir çerçeve sunmaktadır. Ancak KVKK'nin dar yorumuyla karşılaştırıldığında, GDPR'nin veri ihlali tanımının daha geniş bir kapsamı olduğu görülmektedir. Bu durum veri sorumlularının sadece üçüncü kişilerin verileri ele geçirmesi durumunda değil, tüm ihlal türlerinde de düzenleyici kurumlara bildirimde bulunmalarını gerektirmektedir. Dolayısıyla veri sorumlularının her iki yasal düzenlemeyi dikkate alarak daha geniş bir güvenlik stratejisi geliştirmeleri önemlidir. Türkiye'nin dijital güvenlik altyapısının güçlendirilmesi için KVKK'nin belirli aralıklarla güncellenmesi ve uluslararası standartlarla uyumlu bir yaklaşım benimsenmesi gerekmektedir. Bu sayede hem bireylerin hem de kurumların veri güvenliği daha sağlam bir temele oturtulabilir.

3. SES KULLANILARAK YAPILAN SİBER SALDIRI TÜRLERİ

Ses kullanılarak yapılan siber saldırılar hem bireylerin ve cihazların seslerinin manipüle edilmesiyle hem de cihaz ve donanımların ses dalgalarına maruz bırakılması gibi oldukça çeşitli yollarla gerçekleştirilebilir. Bu tür saldırılar kişisel verilerin, finansal bilgilerin, kamusal ve kurumsal verilerin, ticari sırların ve diğer hassas bilgilerin ele geçirilmesini amaçlar. Bu tür bilgiler hedeflenen kişi ya da kurumlar için büyük zararlara yol açabilecek potansiyele sahiptir.

Ses tabanlı siber saldırılar çeşitli türlere ayrılabilir. Bunlar arasında sesli kimlik avı (vishing), sesli komut manipülasyonu, sesli kimlik hırsızlığı, sesli mesajlaşma saldırıları ve ultrasonik ses dalgaları kullanılarak yapılan saldırılar yaygın olarak yer almaktadır. Her bir saldırı türü farklı teknikler ve yöntemlerle gerçekleştirilir ve buna bağlı olarak hedeflenen kullanıcılar, cihazlar ve bilgi sistemleri üzerinde farklı seviyelerde zararlara yol açar.

Sesli kimlik avı (vishing) genellikle telefon aracılığıyla gerçekleştirilir ve saldırganlar, hedef kişiyi manipüle ederek kişisel bilgilerini toplar. Sesli komut manipülasyonu ise sesli asistanlar ve akıllı cihazlar gibi teknolojilere yönelik bir saldırı türüdür. Bu saldırılarda kötü niyetli kişiler, cihazların sesli komutları yanlış bir şekilde algılamasını sağlamak için ses dalgalarını kullanarak istenmeyen işlemler gerçekleştirebilirler. Sesli kimlik hırsızlığı, bir kişinin sesini taklit ederek kimlik doğrulama süreçlerini atlatmayı amaçlayan saldırılardır. Sesli mesajlaşma saldırıları, hedef kişilere sesli mesajlar göndererek onları yanıltmak ya da zararlı yazılımlar yüklemek amacıyla kullanılabilir. Ultrasonik ses dalgalarıyla yapılan saldırılar ise genellikle sesin insan kulağı tarafından duyulamayan frekanslarını kullanılarak cihazlara zarar vermek, cihazların güvenlik sistemlerini aşmak veya veri sızıntılarına yol açmak için gerçekleştirilir.

Bu saldırı türlerinin her biri farklı teknik altyapılar ve araçlar kullanarak farklı hedefler üzerinde etki doğurabilir. Sesli saldırılar, özellikle dijitalleşen dünyada cihazların ve sistemlerin sesli komutlarla etkileşime girmesiyle giderek daha yaygın hale gelmiştir. Ayrıca bu saldırıların önemli bir kısmı genellikle hedefteki kişiler tarafından fark edilemeyecek şekilde gerçekleştirildiği için kullanıcılar bu konuda oldukça savunmasız durumda olmakta ve bu nedenle de çok büyük tehditler oluşabilmektedir. Her bir saldırı türü belirli bir tehdit seviyesi taşıdığı için siber güvenlik uzmanlarının bu yeni ve güncel tehditlere karşı stratejiler

geliştirmesi oldukça önemlidir. Ses kullanılarak yapılan siber saldırıların önlenmesi hem teknolojik önlemlerle hem de kullanıcı eğitimleriyle sağlanabilir.

3.1. İlgili Çalışmalar

Ses kullanılarak yapılan siber saldırılar konusu, son yıllarda hem akademik hem de endüstriyel alanda giderek daha fazla ilgi görmeye başlamıştır. Bu ilgi, ses tabanlı saldırıların dijitalleşen dünyada giderek daha büyük bir tehdit haline gelmesinden kaynaklanmaktadır. Literatürde, sesle gerçekleştirilen saldırılarla ilgili birçok farklı çalışma bulunmakta olup bu çalışmaların çoğu saldırı türlerinin tanımlanması, kullanılan tekniklerin analiz edilmesi ve saldırılara karşı alınabilecek güvenlik önlemlerinin incelenmesi üzerine odaklanmaktadır.

Giriş bölümünde, bu çalışmada yer alan literatürün seçilme süreci ve eleme kriterleri ayrıntılı bir şekilde açıklanmıştır. Ayrıca aşağıdaki her bölümde ayrı ayrı incelenecek saldırı türlerine ilişkin ayrıca literatür taraması da yapılmıştır. Bu süreçte, ses kullanılarak yapılan siber saldırılarla ilgili çalışmalar, belirli veri tabanlarından ve kaynaklardan taranarak seçilmiştir. Elde edilen çalışmaların sistematik derleme yöntemiyle bir araya getirilmesi ile literatürdeki araştırmaların eksikliklerine ışık tutmakta ve ses temelli siber saldırıların farklı yönlerine dair derinlemesine bir anlayış geliştirmeyi amaçlamaktadır. Konu ile doğrudan bağlantılı olan çalışmalar aşağıda sıralanmıştır:

- Christos Madamopoulos ve Nektarios Georgios Tsoutsos tarafından 2024 yılında yayımlanan “3D Printer Audio and Vibration Side Channel Dataset for Vulnerability Research in Additive Manufacturing” isimli çalışmada, eklemeli üretim süreçlerinin güvenliğine yönelik yan kanal saldırıları araştırılmak üzere, iki farklı 3D yazıcıdan elde edilen ses ve titreşim verileri sunulmuştur. Çalışma, Bambu Lab P1P ve A1 mini modellerinde gerçekleştirilen testlerle, yazıcıların sesli emisyonları ve titreşimleri üzerinden elde edilen verilerle 3D yazıcıların güvenlik açığının incelenmesine olanak sağlamaktadır. Veriler, iPhone uygulaması ve Teensy 4.0 sensör sistemi kullanılarak toplanmış olup sesli kayıtlar ve doğrusal ivmelenme verileri içermektedir. Çalışma, yazıcıların hareketleriyle ilgili verilerle CAD dosyaları ve yazıcılarda kullanılan .gcode ve .3mf dosyalarını da içermektedir.
- Hwankuk Kim tarafından 2024 yılında yayımlanan “5G Core Network Security Issues and Attack Classification from Network Protocol Perspective” isimli çalışmada, 5G teknolojisinin sağladığı avantajlar ve bu avantajların beraberinde getirdiği güvenlik

sorunları ele alınmıştır. Çalışmada 5G çekirdek ağına yönelik saldırı türleri, özellikle ağ protokolleri açısından sınıflandırılmış ve bu saldırıların güvenlik zafiyetleriyle ilişkisi incelenmiştir. 5G'nin sunduğu yazılım tanımlı altyapı, Internet of Things (Türkçe karşılığı “Nesnelerin interneti”, kısaltması IoT) cihazlarının bağlantısını sağlarken aynı zamanda ağın güvenliğini tehdit eden faktörlere de yol açmaktadır. Çalışma, 5G çekirdek ağı üzerinde yaşanabilecek beş ana güvenlik sorununu analiz etmekte ve bu tehditlere karşı alınabilecek önlemleri tartışmaktadır. Ayrıca 5G çekirdek ağı üzerindeki ağ protokollerine dayalı siber saldırılar sınıflandırılmış ve güvenlik açıkları detaylandırılmıştır.

- Devu Manikantan Shila, Kunal Srivastava, Paul O’Neill, Kishore Reddy ve Vincent Sritapan tarafından 2024 yılında yayımlanan "A Multi-Faceted Approach to User Authentication for Mobile Devices - Using Human Movement, Usage, and Location Patterns" isimli çalışmada, mobil cihazlar için kullanıcı kimlik doğrulama yöntemlerinin güvenliği ele alınmıştır. Çalışmada geleneksel bilgi tabanlı kimlik doğrulama yöntemlerinin yetersizlikleri ve bunların güvenlik açıkları tartışılmış, ayrıca biyometrik doğrulama yöntemlerinin de sürekli kimlik doğrulama için uygun olmadığı vurgulanmıştır. Yazarlar kullanıcıların konum, yürüyüş ve cihazla fiziksel yakınlık gibi çeşitli davranışsal verilerini kullanarak kimlik doğrulama sürecini sürekli ve müdahale gerektirmeden sağlamak amacıyla yeni bir çok yönlü kimlik doğrulama sistemi olan mAuth'ı önermektedirler. Bu sistem, mobil cihazın sensör verilerini işleyerek kullanıcının kimliğini dinamik olarak doğrulayan bir güvenlik çözümü sunmaktadır. Çalışma, mAuth sisteminin sensör verileriyle oluşturduğu dinamik güven skorlarını kullanarak kullanıcı doğrulama süreçlerini nasıl iyileştirebileceğini incelemektedir. Ayrıca mobil cihazlar üzerinde yapılacak çeşitli saldırı senaryolarıyla sistemin güvenliği test edilmiş ve elde edilen sonuçlar, önerilen yöntemin etkinliğini göstermektedir.
- Hai L. Vu, Kenneth K. Khaw ve Tsong Yueh Chen tarafından 2015 yılında yayımlanan "A New Approach for Network Vulnerability Analysis" adlı çalışmada, ağ zafiyetlerini analiz etmek için yenilikçi bir yaklaşım önerilmektedir. Çalışma, siber saldırıların daha karmaşık hale geldiğini ve ağlardaki zafiyetlerin birleşerek güvenlik tehditleri oluşturduğunu vurgulamaktadır. Geleneksel saldırı grafikleri çok büyük ve karmaşık olduğundan analiz edilmesi zor olabileceğinden bahsedilmiştir. Yazarlar saldırı grafikleri oluşturmak yerine ağdaki kritik zafiyetleri belirleyip bunları analiz ederek daha verimli bir yöntem geliştirmiştir. Çalışma, ağdaki güvenlik açıklarını tespit ederek

ses tabanlı siber saldırılara karşı alınacak önlemleri belirlemeye yönelik önemli çıkarımlar sunmaktadır.

- Mohammad Wazid, Amit Kumar Mishra, Noor Mohd ve Ashok Kumar Das tarafından 2024'te yayımlanan "A Secure Deepfake Mitigation Framework" başlıklı çalışmada, deepfake teknolojisinin toplum üzerindeki etkileri ve bu tür içeriklerin tespiti için geliştirilen güvenli bir framework ele alınmaktadır. Deepfake, yapay zekâ kullanarak ses, video ve görselleri manipüle eden bir teknolojidir. Çalışma, deepfake'lerin sesli medya içeriklerinde de önemli bir tehdit oluşturduğunu, sesli manipülasyonların toplumu yanıltma potansiyeline sahip olduğunu vurgulamakta; deepfake'lerin tespiti ve engellenmesi için geliştirdiği güvenlik framework'ünü sunmakta ve bu çözümün siber saldırılara karşı etkili olduğunu göstermektedir. Ayrıca sesli deepfake içeriklerinin tespiti ve güvenliğinin sağlanması, sesle yapılan siber saldırılara karşı kritik bir çözüm sunmaktadır.
- Swetha Gadde, J. Amutharaj ve S. Usha'nın 2023'teki "A Security Model To Protect The İsolation Of Medical Data İn The Cloud Using Hybrid Cryptography" çalışmasında, bulut ortamındaki sağlık verilerinin güvenliği için hibrit kriptografi temelli bir model önerilmektedir. Bu modelin sağlık verilerini korumak için IRS-AES şifreleme algoritması ve DNA tabanlı MECC kullanarak verilerin gizliliğini ve bütünlüğünü sağladığı belirtilmiştir. Ayrıca Huffman kodlama ve Runge-Kutta Optimizasyon (RKO) algoritması ile şifreleme süreci optimize edilmiştir. Çalışmada ses, video ve görüntü verileri üzerinden güvenlik testleri yapılmış ve şifreleme sürecinin etkinliği artırılmıştır.
- Sharmila S. P., Pratyush Shukla ve Narendra S. Chaudhari'nin 2022'deki "A Distinguished Method for Network Intrusion Detection using Random Initialized Viterbi Algorithm in Hidden Markov Model" çalışmasında, ağ saldırılarını tespit etmek için Hidden Markov Model (HMM) kullanarak geliştirilmiş bir Viterbi algoritması önerilmektedir. Bu algoritmanın rastgele başlatılmış parametrelerle çalışarak saldırıları tespit etmenin yanı sıra, gelecekteki olası saldırıları tahmin etme doğruluğunu önemli ölçüde artırdığından söz edilmiştir. Buradaki metodoloji, tespit edilen tüm durumların doğruluğunu %25.000'den fazla artırırken, mevcut durumu %2.000 ve gelecek durumu tahmin etme doğruluğunu ise %36.000'den fazla geliştirmektedir. Sesli siber saldırılar gibi karmaşık tehditlerin de bu tür gelişmiş algoritmalarla tespit edilebilir ve gelecekteki saldırılar daha doğru bir şekilde tahmin edilebileceğinden bahsedilmiştir.

Bu çalışma, ağ güvenliği ve tehdit tahminindeki yeni yolları açmakla birlikte ses tabanlı siber saldırılar için de potansiyel uygulamalar sunmaktadır.

- Fouzi Harrou, Benamar Bouyeddoub, Ying Sun ve Benamar Kadri'nin 2018'de yayımlanan "A Method to Detect DOS and DDOS Attacks based on Generalized Likelihood Ratio Test" başlıklı çalışmasında, Denial of Service (DOS) ve Distributed Denial of Service (DDOS) saldırılarını tespit etmek için Genelleştirilmiş Likelihood Oranı (GLR) testi kullanılmıştır. Çalışma, bu tür saldırıları tespit etmek için GLR yaklaşımını önererek, TCP ve ICMPv6 protokollerini hedefleyen saldırıların etkili bir şekilde tespit edilmesini sağlamaktadır. GLR testi, ağ trafiğindeki anormallikleri belirlemek için güçlü bir araçtır ve bu yöntem, siber saldırılara karşı etkili bir güvenlik çözümü sunmaktadır. Çalışmada kullanılan GLR testi, sesli saldırılara karşı da uygulanabilir çünkü sesli trafik, ağ üzerinden iletilen veriler arasında yer alır. Bu test, ağda anormallikler tespit ederek sesli verilerin manipülasyonu veya sahte ses içeriklerinin (sesli Deepfake'ler gibi) tespit edilmesine yardımcı olabilir.
- Tao Yang, Yibo Hu, Yang Li, Wei Hu ve Quan Pan'ın 2019'da yayımlanan "A Standardized ICS Network Data Processing Flow With Generative Model in Anomaly Detection" başlıklı çalışmasında Endüstriyel Kontrol Sistemleri (ICS) ağlarında güvenlik açıklarını tespit etmek için yeni bir veri işleme yöntemi önerilmektedir. Çalışma, ağ verilerinin daha standardize hale getirilmesi için bir yöntem geliştirmiştir böylece güvenlik anormalliklerinin tespiti daha verimli hale getirilmiştir. Ayrıca verilerin jenerasyonu için kullanılan bir yöntemle eğitim verisi toplanmış ve bu verilerin değerlendirilmesi için yenilikçi bir yöntem önerilmiştir. Çalışma, endüstriyel ağlarda karşılaşılan dengesiz veri problemini ele alarak anormallik tespiti için verimli bir yöntem sunmaktadır. Bu bağlamda sesle yapılan siber saldırılarla ilişkili ağ verilerinin analizi, bu tür yöntemlerle yapılabilir.
- Raju Dhakal ve Laxima Niure Kandel tarafından 2023'te yayımlanan "A Survey of Physical Layer-Aided UAV Security" başlıklı çalışmada, düşük maliyetli insansız hava araçlarının (İHA) güvenliği ele alınmaktadır. Çalışma, İHA'ların artan kullanımına paralel olarak bu araçların siber saldırılara ve fiziksel saldırılara maruz kaldığını ve güvenliklerini sağlamanın önemini vurgulamaktadır. Özellikle geleneksel kriptografik güvenlik yöntemlerinin yüksek işlem yükü gerektirdiği, bu nedenle daha hafif ve verimli fiziksel katman (PHY) tabanlı güvenlik yöntemlerine olan ilginin arttığı belirtilmektedir. Bu çalışmanın sesle ilgili bağlantısı, İHA'ların güvenliğiyle ilgili olarak sesli iletişim ve ses tabanlı tehditlerin de dahil edilmesidir. Çalışma, bu tür

saldırılara karşı fiziksel katman güvenliği yöntemlerinin önemini ortaya koyarken bu yöntemlerin sesli iletişim verilerinin güvenliği için de uygulanabilir olduğunu ima etmektedir.

- Dodda Venkatareddy, Shaik Yalavarthi Ijaz Ahamad, Sinde Venkata Saptha Girish, Tammisetti Nagendra Babu ve K. V. Narasimha Reddy'nin 2024'te yayımlanan "Adaptive Intrusion Detection in CAN-Based Vehicular Networks Using Transfer Learning for Evolving Threats" başlıklı çalışmasında, araç ağları için bir saldırı tespit sistemi (IDS) önerilmektedir. Bu sistem, Controller Area Network (CAN) tabanlı ağlarda, dinamik tehditlere karşı uyum sağlayabilen ve minimal yeniden eğitimle yeni saldırı desenlerine uyum sağlayabilen transfer öğrenmesi (TL) tekniklerini kullanmaktadır. Çalışma, gelişmiş CNN ve LSTM kombinasyonları ile donatılmış hibrit bir model kullanarak araç ağlarının güvenliğini artırmayı amaçlamaktadır, ayrıca araç ağlarının güvenliği ve siber saldırılara karşı koruma konusundaki önemine dikkat çekmektedir.
- W. Kasprzak, W. Szynkiewicz, M. Stefańczyk, W. Dudek, M. Węgierek, D. Seredyński, M. Figat ve C. Zieliński'nin 2020 yılında yayımlanan "Agent-based approach to the design of a multimodal interface for cyber-security event visualisation control" başlıklı çalışmasında, siber güvenlik olaylarını görselleştirmek ve kontrol etmek için multimodal bir insan-bilgisayar etkileşimi (HCI) arayüzü tasarlanmıştır. Bu arayüz, siber güvenlik analistlerine ağ trafiğini izlemede yardımcı olmak amacıyla sesli komutlar ve jestlerle etkileşim sunmaktadır.
- Arian Mokhtari, Niloofar Ghorbani ve Behnam Bahrak'ın 2022 tarihli "Aggregated Traffic Anomaly Detection Using Time Series Forecasting on Call Detail Records" başlıklı çalışması, mobil ağlardaki çağrı detay kayıtları (CDR) verilerini kullanarak ağ trafiğindeki anormallikleri tespit etmeyi amaçlamaktadır. Çalışma, GARCH, K-means ve sinir ağları gibi yöntemleri birleştirerek yeni bir hibrit model önermiştir. Bu model, kullanıcı davranışlarındaki olağandışı değişimleri doğru bir şekilde belirleyerek ağ trafiğinde oluşabilecek ani değişimlere karşı önceden önlem almayı sağlamaktadır. Çalışma, özellikle sesli aramalar ve SMS gibi çağrı türlerini içeren veriler üzerinde odaklanmaktadır.
- Mordechai Guri, Gabi Kedma, Assaf Kachlon, Yuval Elovici'nin 2014 tarihli "AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies" adlı çalışması, fiziksel olarak izole edilmiş ağlardan mobil

telefonlar aracılığıyla veri sızdırmak için kullanılan yeni bir tehdit modelini tanıtmaktadır. AirHopper, bir bilgisayarın ekran kartından yayılan radyo frekanslarını kullanarak bu verileri yakalayabilen FM alıcıları bulunan mobil telefonlara iletmektedir. Çalışma, özellikle FM alıcıları olan telefonların kullanılarak havadan gelen verilerin nasıl toplanabileceğini ve bu verilerin cihazdan mobil telefona nasıl aktarıldığını göstermektedir. Bu model, ciddi bir güvenlik açığı oluşturan bir tehdit olup yalnızca uzman kişiler tarafından gerçekleştirilebilecek şekilde tasarlanmıştır. Deneyler, verinin 1-7 metreye kadar iletilebildiğini ve saniyede 13-60 Bayt hızında veri transferi yapılabileceğini göstermektedir. Bu araştırma, izolasyonlu ağlardan veri sızdırmanın ne kadar karmaşık olduğunu ancak yine de Advanced Persistent Threats (APT) tarzı saldırganlar tarafından gerçekleştirilebileceğini ortaya koymaktadır. AirHopper, elektromanyetik sızıntı tehditlerini anlamamıza katkı sağlamakta ve siber savunma topluluğu için önemli bir uyarı sunmaktadır.

- Vinayak Rai, Kapil Mehta, Jatin, Dheeraj Tiwari ve Rohit Chaurasia'nın 2022 yılında yayımlanan "Automated Biometric Personal Identification: Techniques and Applications" başlıklı çalışmalarında, biyometrik güvenlik sistemlerinin kullanımı ve geliştirilmesi ele alınmaktadır. Çalışma, geleneksel güvenlik sistemlerinin zayıflıklarına karşı biyometrik tanıma sistemlerinin güvenli ve verimli bir alternatif sunduğunu vurgulamaktadır. Yazarlar parmak izi, yüz tanıma, sesli kimlik doğrulama gibi çeşitli biyometrik yöntemleri inceleyerek bunların avantaj ve dezavantajlarını tartışmıştır. Özellikle ses tanıma, kullanıcıların ses profillerini benzersiz bir biyometrik özellik olarak kullanarak güvenliği artıran bir yöntem olarak öne çıkmaktadır. Bu çalışma, biyometrik güvenliğin gelecekte daha da yaygınlaşacağı ve güvenlik alanında önemli değişikliklere yol açacağına dair önemli bulgular sunmaktadır.
- Shaobo Zhang, Yimeng Pan, Qin Liu, Zheng Yan, Kim-Kwang Raymond Choo ve Guojun Wang'ın 2022 yılında yayımlanan "Backdoor Attacks and Defenses Targeting Multi-Domain AI Models: A Comprehensive Review" başlıklı çalışmalarında, yapay zekâ (YZ) modellerine yönelik arka kapı saldırıları ve savunmaları kapsamlı bir şekilde incelenmektedir. Çalışma, YZ güvenliği üzerine yapılan araştırmaları sistematik bir şekilde ele alarak bilgisayarla görme, doğal dil işleme, ses tanıma ve zaman serisi gibi çeşitli alanlarda arka kapı saldırılarının nasıl gerçekleştirildiğini ve bu saldırılara karşı nasıl savunmalar geliştirilmesi gerektiğini tartışmaktadır.
- Imam Riadi, Rusydi Umar, Iqbal Busthomi ve Arif Wirawan Muhammad'ın 2021 yılında yayımlanan "Block-hash of Blockchain Framework Against Man-in-the-Middle

Attacks" başlıklı çalışmalarında Blockchain teknolojisinin man-in-the-middle (MITM) saldırılarına karşı nasıl bir güvenlik sağladığı incelenmektedir. Bu çalışmada, MITM saldırılarının özellikle kimlik doğrulama sürecindeki veri gizliliği açığına odaklandığı vurgulanmaktadır.

- Jie Peng ve Qing Ling'in 2020'de yayımlanan "Byzantine-Robust Decentralized Stochastic Optimization" başlıklı çalışmalarında, dağıtık bir ağ üzerindeki Byzantine saldırılarına karşı dayanıklı bir stokastik optimizasyon problemi ele alınmaktadır. Çalışmaya göre güvenilmez ajanlar hatalı veriler göndererek optimizasyonu bozar; çözüm olarak toplam varyans normu cezası ile düzenli ajanların modelleri yakın tutulurken Byzantine ajanlarının aykırı değerlerine de tolerans gösterilir. Deneyler, önerilen yöntemin dayanıklılığını ve mevcut yöntemlerden daha iyi performans gösterdiğini doğrular. Bu yöntem, sesli iletişim gibi hassas verilerin güvenliğini sağlayarak verilerin bozulmasını engeller.
- Nader Abdel Karima, Hasan Kanaker, Waleed K. Abdulraheem, Majdi Ali Ghaith, Essam Alhroob ve Abdulla Mousa Falah Alalie'nin 2024 yılında yayımlanan "Choosing the Right MFA Method for Online Systems: A Comparative Analysis" başlıklı çalışmasında, çevrimiçi sistemlerde kullanılan farklı Çok Faktörlü Kimlik Doğrulama (MFA) yöntemleri karşılaştırılmaktadır. Çalışma, Microsoft Authenticator, FIDO2 güvenlik anahtarları, SMS, sesli aramalar ve biyometrik doğrulama gibi yöntemleri güvenlik, kullanılabilirlik, maliyet ve uyumluluk açısından değerlendirmektedir. Yazarlar her MFA yönteminin avantajlarını ve dezavantajlarını belirleyerek, yüksek güvenlik gereksinimlerinde FIDO2 güvenlik anahtarları ve sertifika tabanlı doğrulamanın tercih edilmesini, yüksek kullanılabilirlik senaryolarında ise Microsoft Authenticator ve biyometrik doğrulamanın daha uygun olduğunu öne sürmektedir. Ayrıca SMS ve sesli aramalar gibi düşük güvenlikli yöntemlerden kaçınılması gerektiği vurgulanmaktadır. Bu çalışma, organizasyonların doğru MFA seçimini yapabilmesi için önemli bir kaynak sağlamaktadır.
- Da-Yu Kao'nun 2019 yılında yayımlanan "Comprehending Taiwan ATM Heist: From Cyber-attack Phases to Investigation Processes" başlıklı çalışmasında, banka sistemlerine yönelik siber saldırıların giderek daha sofistike hale geldiği vurgulanmaktadır. Çalışma, ATM tehditlerini inceleyerek, ATM soygunlarına yönelik siber suç soruşturma süreçlerini ele almaktadır. Yazar, ATM soygunlarını tespit etmek için ISO/IEC 27043:2015 standardına dayanan bir soruşturma stratejisi önermektedir. Bu strateji, siber saldırı aşamalarını ve kanıt toplama süreçlerini entegre ederek

soruşturmacıların daha etkin bir şekilde dijital kanıtları yorumlamalarına olanak tanır. Çalışma, banka ATM'lerinin güvenliğini artırmak için bilgi güvenliği farkındalığının artırılmasının önemine dikkat çekmekte, ayrıca siber suçların hızlı ve etkili şekilde önlenebilmesi için güvenlik önlemleri ve düzenlemeler önerilmektedir. Sesli aramaların benzeri tehditlerden korunması, aynı zamanda ATM sistemlerinin dijital izlerini takip etmek için kritik bir adım olarak sunulmuştur.

- Yoram Segal ve Ofer Hadar'ın 2019 yılında yayımlanan "Covert Channel Cyber-Attack over Video Stream DCT Payload (Copyright Protection Algorithm for Video and Audio Streams)" başlıklı çalışmasında, video paketleri üzerinden gerçekleştirilen siber saldırıların özellikle video verisinin yük kısmını kullanarak nasıl gerçekleştirilebileceği incelenmiştir. Bu çalışma, steganografi teknikleri kullanarak video akışlarının içerisinde kötü niyetli verilerin gizlenmesini hedefleyen bir siber saldırı yönteminin kanıtını sunmaktadır. Yazarlar, H.264 gibi video sıkıştırma protokollerinde, özellikle DCT (Discrete Cosine Transform) dönüşümüne dayalı olarak video içeriğinin yük kısmında nasıl zararlı verilerin gizlenebileceğini açıklamaktadır. Bu teknik, video izleyicilerinin küçük değişiklikleri fark etmeyecek kadar hassasiyeti düşük olduğundan kötü niyetli verilerin gizlenmesi için etkili bir yöntem olarak kullanılmaktadır. Çalışma, bu tür siber saldırılara karşı koruma önlemleri geliştirilmesi gerektiğini vurgularken aynı zamanda video izleyici güvenliğini artırmak için gelecekte yapılabilecek iyileştirmelere de dikkat çekmektedir.
- Aditi Shewale, Jayant Tumdam, Ajinkya Ladke, Jayesh Fating, Aryan Raut, and Prof. Rajesh Nakhate'ın 2023'te yayımlanan "Data Steganography Using LSB, X-OR & AES Algorithm" başlıklı çalışması, steganografi tekniklerini kullanarak veri gizleme ve güvenli iletim üzerine odaklanmaktadır. Çalışma, Least Significant Bit (LSB), XOR ve Advanced Encryption Standard (AES) algoritmalarını bir arada kullanarak verilerin güvenli bir şekilde gizlenmesini ve aktarılmasını sağlamak için geliştirilmiş bir model sunmaktadır.
- Md. Amran Siddiqui, Jack W. Stokes, Christian Seifert, Evan Argyle, Robert McCann, Joshua Neil ve Justin Carroll'ın 2019 yılında yayımlanan "Detecting Cyber Attacks Using Anomaly Detection with Explanations and Expert Feedback" başlıklı çalışmasında, büyük bilgisayar ağlarındaki siber saldırıların tespiti amaçlanmaktadır. Çalışma, Isolation Forest adı verilen bir anomali tespit tekniği kullanarak ağdaki anormallikleri tanımlar ve bu tespitlerin nedenlerini açıklayarak güvenlik analistlerinin müdahale sürecini hızlandırmayı hedefler.

- Zoe Lim Mei Yi ve Julia Juremi'nin 2023 yılında yayımlanan "Dezvent – Digitalizing Attendance System with 2FA and Face Recognition Implementation" başlıklı çalışmasında, geleneksel devamsızlık sistemlerinin verimsizliği ele alınarak yüz tanıma sistemi ve iki faktörlü kimlik doğrulama (2FA) kullanarak web tabanlı bir devamsızlık yönetim sistemi geliştirilmiştir. Bu sistem, katılımcıların sadece yüz taraması ile devamsızlıklarını kaydederek işlemi hızlı ve güvenli bir şekilde gerçekleştirmektedir. Yazarlar, yüz tanıma teknolojisi ile "buddy punching" (arkadaş yerine devamsızlık yapma) sorununu çözmeyi ve 2FA ile güvenliği artırarak, kullanıcı hesaplarını kaba kuvvet saldırılarına karşı korumayı amaçlamışlardır. Ayrıca bu sistemin çevre dostu olduğunu belirterek kâğıt kullanımını ortadan kaldırmıştır.
- Chandan Sai Chebrolu, Chung-Horng Lung ve Samuel A. Ajila'nın 2022 yılında yayımlanan "Dynamic Packet Filtering Using Machine Learning" başlıklı çalışmasında, ağ güvenliğini sağlamak için makine öğrenmesi tabanlı dinamik paket filtreleme modeli önerilmektedir. Bu çalışma, geleneksel statik kural tabanlı filtreleme yöntemlerinin yetersiz kaldığı durumlarda IP paketlerindeki çeşitli öznitelikler ve daha önce öğrenilen kurallar kullanarak daha etkili bir filtreleme yapmayı amaçlamaktadır.
- Arash Mahboubi, Khanh Luong, Hamed Aboutorab, Hang Thanh Bui, Geoff Jarrad, Mohammed Bahutair, Seyit Camtepe, Ganna Pogrebna, Ejaz Ahmed, Bazara Barry ve Hannah Gately'e ait 2024 yılında yayımlanan "Evolving Techniques in Cyber Threat Hunting: A Systematic Review" başlıklı çalışmada, siber tehdit avcılığının, geleneksel güvenlik önlemlerinin yetersiz kaldığı noktalarda proaktif bir savunma yöntemi olarak önemi vurgulanmaktadır. Çalışma, yapay zekâ (AI) ve makine öğrenimi gibi gelişmiş tekniklerin tehdit tespiti ve tahmini üzerindeki etkilerini ele almaktadır.
- Tsubasa Sasaki, Kenji Sawada, Seiichi Shin ve Shu Hosokawa'nın 2017 yılında yayımlanan "Fallback and Recovery Control System of Industrial Control System for Cybersecurity" başlıklı çalışmalarında, endüstriyel kontrol sistemleri (ICS) için siber güvenlik amacıyla bir yedekleme ve kurtarma kontrol sistemi (FRCS) önerilmektedir. Bu çalışma, siber saldırılar sonrası ICS'nin işlevselliğini korumak ve güvenli bir şekilde eski duruma döndürmek için FRCS'nin kullanılmasını hedeflemektedir. Yazarlar FCS'nin yanı sıra, ağ bağlantısı ve kontrol cihazlarının güvenli bir şekilde geri bağlanmasını sağlamak amacıyla sanal operasyon modu ve Plant Simulator kullanarak bir güvenlik değerlendirmesi yapmaktadır.

- Kim Hartmann ve Christoph Steup tarafından 2020 yılında hazırlanan “Hacking the AI - The Next Generation of Hijacked Systems” isimli çalışmada, yapay zekâ (YZ) ve makine öğrenimi (Öğrenme - ML) sistemlerine yönelik siber saldırılar ele alınmıştır. Çalışmada, YZ’nin modern toplumda giderek daha yaygın hale geldiği ve özellikle ağ güvenliği, otonom araçlar, yüz tanıma sistemleri gibi birçok kritik alanda kullanıldığı belirtilmiştir. Ancak, YZ ve ML sistemlerinin güvenlik açıklarının büyük ölçüde göz ardı edildiği ve bu sistemlere yönelik saldırıların hem gizli hem de yıkıcı etkilerinin olduğu vurgulanmıştır. Çalışma, özellikle ses ve görüntü işleme alanlarında kullanılan YZ sistemlerinin saldırıya açık olduğunu, saldırganların bu sistemleri manipüle ederek karar alma süreçlerini bozabildiğini ortaya koymaktadır. Ayrıca, YZ sistemlerinin saldırı yüzeylerinin modellenmesi ve güvenlik önlemlerinin geliştirilmesi gerektiği sonucuna ulaşılmıştır.
- Chuadhry Mujeeb Ahmed ve Aditya P. Mathur tarafından 2017 yılında yapılan “Hardware Identification via Sensor Fingerprinting in a Cyber Physical System” adlı çalışmada, siber-fiziksel sistemlerde fiziksel bileşenlere yönelik saldırıların tespitine odaklanarak sensör ölçümlerinden elde edilen gürültü desenlerini kullanarak bir donanım tanımlama yöntemi önermektedir. Çalışmada, bir referans gürültü deseni oluşturularak sensörlerin fiziksel manipülasyona uğrayıp uğramadığını belirleyen bir parmak izi yöntemi geliştirilmiştir. Ultrasonik seviye sensörleri üzerinde yapılan deneyler, önerilen yöntemin fiziksel saldırıları tespit etmede etkili olduğunu göstermektedir.
- Sharma ve Raglin tarafından 2018 yılında gerçekleştirilen “Image-Audio Encoding for Information Camouflage and Improving Malware Pattern Analysis” isimli çalışmada, kötü amaçlı yazılım analizinde görüntü-ses kodlama yöntemi ele alınmıştır. Çalışmada, görüntülerin ses sinyallerine dönüştürülerek hem bilgi gizliliğinin sağlanabileceği hem de veri yorumlanabilirliğinin artırılabileceği vurgulanmıştır. Özellikle, kötü amaçlı yazılım tespiti ve kümeleme süreçlerinde doğrusal olmayan öğrenme yöntemlerinin etkinliği incelenmiştir. 9339 kötü amaçlı yazılım örneği üzerinde yapılan değerlendirmeler, önerilen yöntemin sınıf dengesizliği ve görsel benzerlik gibi zorlukları aşmada etkili olduğunu göstermiştir.
- Rohit Tripathi, Manoj K. Shukla ve Yogesh Kumar tarafından 2021 yılında gerçekleştirilen “Intelligent Physical Access Control System Through Three-Stage Verification Using IoT” isimli çalışmada, IoT tabanlı üç aşamalı doğrulama sürecine

sahip akıllı bir fiziksel erişim kontrol sistemi ele alınmıştır. Çalışmada, güvenliği artırmak amacıyla çok aşamalı kimlik doğrulama sistemlerinin önemine değinilmiş ve özellikle ses temelli güvenlik sistemleri üzerinde durulmuştur. İnsan sesi algılayıcıları ve yapay zekâ destekli ses işleme teknikleri kullanılarak kapı kilitlerinin kontrol edilebileceği, bu sayede biyometrik verilerin daha güvenli bir doğrulama yöntemi olarak kullanılabileceği belirtilmiştir.

- Ioannis Antzoulis, MD Minhaz Chowdhury ve Shadman Latif tarafından 2022 yılında gerçekleştirilen "IoT Security for Smart Home: Issues and Solutions" isimli çalışmada, akıllı evlerde kullanılan IoT cihazlarının güvenlik açıkları ve bu açıkları gidermek için önerilen çözümler ele alınmıştır. Çalışmada, akıllı ev bileşenlerinin internet bağlantısıyla siber saldırılara açık hale geldiği ve bu saldırılardan korunmak için çeşitli güvenlik önlemlerinin değerlendirilmesi gerektiği vurgulanmıştır. Özellikle akıllı evlerde kullanılan cihazların mikrofon ve kamera gibi bileşenler aracılığıyla ses tabanlı saldırılara açık olduğu vurgulanarak, ses verilerini işleyen sistemlerde güçlü güvenlik protokollerinin uygulanmasının önemli olduğu belirtilmiştir.
- Mehrnoosh Monshizadeh, Vikramajeet Khatri, Mohammadali Varfan ve Raimo Kantola tarafından 2018 yılında gerçekleştirilen "LiaaS: Lawful Interception as a Service" başlıklı çalışma, makine öğrenmesi ve büyük veri analitiği tekniklerinin yasal dinleme (Lawful Interception - LI) süreçlerine entegrasyonunu ele almaktadır. Önerilen platform olan Lawful Interception as a Service (LiaaS), sesli ve görüntülü iletişim içeriklerinin otomatik olarak analiz edilmesini, kritik bilgilerin özetlenmesini ve belirli detayların aranabilir hale getirilmesini sağlamaktadır. Bu bağlamda, ses ve görüntü verileri üzerinde makine öğrenmesi tabanlı analizlerin gerçekleştirilmesiyle özellikle büyük ölçekli veri akışlarının hızlı ve güvenilir bir şekilde işlenebileceği belirtilmiştir. Özellikle sesli iletişimlerin analiz edilerek anahtar bilgilerin çıkarılması, ses tabanlı siber saldırıların tespit edilmesi ve büyük veri ortamında LI süreçlerinin hızlandırılması açısından LiaaS'in önemli bir katkı sağladığı sonucuna ulaşılmıştır.
- Marta Campi, Gareth W. Peters, Nourddine Azzaoui ve Tomoko Matsui tarafından 2021 yılında gerçekleştirilen "Machine Learning Mitigants for Speech-Based Cyber Risk" isimli çalışmada, ses tabanlı biyometrik güvenlik sistemlerinin siber saldırılara karşı nasıl korunabileceği incelenmiştir. Çalışmada, otomatik konuşmacı doğrulama (ASV) sistemlerinin sahte seslerin (deep fake) kullanılmasıyla karşı karşıya kaldığı siber saldırılara karşı daha dayanıklı hale getirilmesi için makine öğrenmesi tabanlı bir çözüm önerilmektedir. Yazarlar geleneksel doğrusal ve durağan varsayımlarını aşarak,

ses sinyallerini analiz etmek için Empirical Mode Decomposition (EMD) ve Mel-Frequency Cepstral Coefficients (MFCC) yöntemlerini birleştirerek sahte ses saldırılarını tespit etmek için daha etkili bir sınıflandırıcı geliştirmişlerdir. Çalışma ayrıca ses tabanlı siber saldırıların önlenmesi konusunda yeni bir yol haritası sunmakta ve sesli biyometrik güvenlik sistemlerinin daha güvenli hale getirilmesine katkı sağlamaktadır.

- Aryansh Gupta, Anwar Ali, Aditya Kumar Pandey, Ankit Kumar Gupta ve Abhinandan Tripathi tarafından 2022 yılında gerçekleştirilen “Metamorphic Cryptography using AES and LSB Method” isimli çalışmada, veri güvenliğini artırmak için AES şifreleme algoritması ile LSB tabanlı görüntü steganografi tekniği birleştirilmiştir. Çalışmada, hassas verilerin şifrelenmesinin ardından bu verilerin bir görüntü dosyasına gizlenmesi önerilmiştir. Bu sayede yalnızca yetkili kullanıcıların deşifre anahtarı ile gizli mesajı açığa çıkarması sağlanmıştır.
- Paul C. Hershey ve Charles B. Silio, Jr. tarafından gerçekleştirilen “Monitoring and Management Approach for Cyber Security Events over Complex Systems” isimli çalışmada, karmaşık sistemlerdeki siber güvenlik olaylarını izlemek ve yönetmek için yeni bir çerçeve önerilmiştir. Çalışmada farklı idari alanlarda çalışan uç kullanıcıların oluşturabileceği siber güvenlik olaylarını tespit etmenin zorlukları ve bu olaylara karşı proaktif yanıt verebilmek için gereken çapraz-idari alan mekanizmaları tartışılmaktadır.
- Urikhimbam Boby Clinton ve Nazrul Hoque tarafından 2024 yılında gerçekleştirilen "MU-IoT: A New IoT Intrusion Dataset for Network and Application Layer Attacks Analysis" isimli çalışmada, IoT ağlarının siber saldırılara karşı korunmasına yönelik yeni bir IoT ağı saldırı veri seti olan MU-IoT tanıtılmaktadır. Bu çalışma mevcut IoT veri setlerinin eksikliklerini gidermek amacıyla geliştirilmiştir ve özellikle IoT uygulama katmanı protokollerine dayalı trafik verilerini içermektedir.
- Lakshmanan Nataraj, Tajuddin Manhar Mohammed, Tejaswi Nanjundaswamy, Satish Chikkagoudar, Shivkumar Chandrasekaran ve B.S. Manjunath tarafından 2021 yılında gerçekleştirilen "OMD: Orthogonal Malware Detection using Audio, Image, and Static Features" isimli çalışmada, "ortogonal" siber savunma yaklaşımlarına dayalı yeni bir kötü amaçlı yazılım tespiti yöntemi önerilmektedir. Bu çalışmada ses, görüntü ve statik özelliklerin birleştirilmesiyle kötü amaçlı yazılımların tespiti için yeni bir yöntem geliştirilmiştir. Özellikle kötü amaçlı yazılım ikili dosyaları ses sinyalleri olarak temsil edilerek ses tanımlayıcılarının sınıflandırma işlemlerinde nasıl etkili olduğu

gösterilmektedir. Ayrıca ses tanımlayıcıları ile yapılan tahminlerin, görüntü benzerlik tanımlayıcıları ve diğer statik özelliklere dayalı tahminlerle ortogonal olduğu vurgulanmaktadır.

- Evi Elisa Ambarita, Ivan Kuncara, Augie Widyotriatmo, Anniken Karlsen, Francesco Scibilia ve Agus Hasan tarafından 2023 yılında gerçekleştirilen "On Cyber-Attacks Against Wind Farms" isimli çalışmada, rüzgâr çiftliklerinin sensör sistemlerine yönelik siber saldırılar ele alınmaktadır. Çalışmada bu tür saldırıları tespit etmek ve büyüklüğünü tahmin etmek için yeni bir yöntem önerilmektedir.
- Andrea Toma, Niccolò Cecchinato, Carlo Drioli, Giuseppe Oliva, Giovanni Ferrin, Gianluigi Sechi ve Gian Luca Foresti tarafından 2022 yılında gerçekleştirilen "Onboard Audio and Video Processing for Secure Detection, Localization, and Tracking in Counter-UAV Applications" başlıklı çalışmada, insansız hava araçları (UAV) için güvenli tespit, yer belirleme ve izleme amacıyla ses ve video işleme yöntemleri incelenmiştir. Çalışmanın amacı, UAV'lerdeki düşük güçlü hesaplama birimleri üzerinde ses ve video sinyallerini işleyerek bu araçların siber güvenliğini artırmak, gecikmeleri ve sinyal iletimindeki sorunları azaltmaktır.
- Wei Yang, Jialei Chen, Chuck Zhang ve Kamran Paynabar tarafından 2021 yılında gerçekleştirilen "Online Detection of Cyber-Incidents in Additive Manufacturing Systems via Analyzing Multimedia Signals" başlıklı çalışmada, katmanlı üretim (additive manufacturing, AM) sistemlerinde siber saldırıların tespiti için çevrimiçi bir mekanizma önerilmiştir. Bu çalışma, baskı süreci sırasında elde edilen ses ve video sinyallerini analiz ederek AM sistemlerine yönelik kötü niyetli saldırıları tespit etmeyi amaçlamaktadır. Ses sinyalleri için, spektrum grafiğindeki desen değişimlerini ve baskı sürecindeki baskın frekansları izlemek için Wasserstein metriği tabanlı bir kontrol çizelgesi önerilmektedir. Video sinyalleri için ise, ekstruderin yeniden yapılandırılmış hareket yolunu izlemek amacıyla Hausdorff metriği kullanılmıştır. Yapılan bir vaka çalışmasında, Ender 3D yazıcısı kullanılarak iç dolgu yoğunluğundaki değişikliklerin çevrimiçi olarak kolayca tespit edilebileceği gösterilmiştir.
- Norma Gutiérrez, Eva Rodríguez, Sergi Mus, Beatriz Otero ve Ramón Canal tarafından 2020 yılında gerçekleştirilen "Privacy Preserving Deep Learning Framework in Fog Computing" başlıklı çalışmada, mobil cihazların yaygın kullanımının beraberinde getirdiği siber güvenlik ve gizlilik sorunlarına çözüm sunulmaktadır. Bu çalışma, Fog

bilişim ortamlarında, kullanıcı verilerinin gizliliğini koruyarak dağıtık derin öğrenme (DL) modelleri ile veri analizi yapmayı amaçlamaktadır.

- Anuoluwapo O. Aluko, Rudiren Pillay Carpanen, David G. Dorrell ve Evans E. Ojo tarafından 2022 yılında gerçekleştirilen "Real-Time Cyber Attack Detection Scheme for Standalone Microgrids" başlıklı çalışmada bağımsız mikro ağların (MG) güvenli operasyonu, kontrolü ve kararlılığı için büyük önem taşıyan siber saldırı tespit yöntemleri ele alınmıştır. Sesli komutlarla kontrol edilen cihazlar ve sistemler, bu tür FDI saldırılarına karşı daha savunmasız olabilir. Bu nedenle, mikro ağlarda kullanılan durum tahmin yöntemlerinin ve saldırı tespit tekniklerinin geliştirilmesi, sesli siber saldırılara karşı etkili bir savunma oluşturulmasında önemli bir adım olacağından bahsedilmiştir.
- Mohd. Altamash ve Shailendra Narayan Singh tarafından 2022 yılında gerçekleştirilen "Reconnaissance of Credentials through Phishing Attacks & its Detection using Machine Learning" başlıklı çalışmada, siber suçlar arasında yer alan phishing (oltalama) saldırılarının tespitine yönelik makine öğrenimi teknikleri ele alınmaktadır. Bu çalışma, LinkedIn ve Facebook gibi popüler platformların giriş sayfalarına benzeyen sahte web siteleri kullanarak gerçekleştirilen phishing saldırılarının, kullanıcıların kişisel bilgilerini nasıl çaldığını incelemekte ve makine öğrenimi algoritmalarının phishing bağlantılarının tespitinde nasıl etkili bir yöntem sunduğunu araştırmaktadır. Ayrıca sesli iletişim ve sesli saldırılarla ilgili olarak ses kullanılarak gerçekleştirilen oltalama saldırılarının da siber güvenlik açısından önemli tehditler oluşturduğuna dikkat çekilmiştir.
- Runzhe Liu, Xin Peng, Zhanbo Sun, Zhihang Huang ve Haitao Hu tarafından 2022 yılında gerçekleştirilen "Research on Cyberattack Detection of Connected Automated Vehicles Based on Support Vector Machine" başlıklı çalışmada, bağlantılı otomatik araçların (CAVs) siber saldırılara karşı savunmasızlığı ele alınmıştır. Bu çalışma, CAV'lerin trafikteki durum bilgisini paylaşırken karşılaştıkları siber saldırılara karşı bir tespit modeli geliştirmeyi amaçlamaktadır. Araştırma, CAV'ler üzerindeki siber saldırıların trafik güvenliği ve akış parametreleri üzerindeki etkilerini nicel olarak analiz etmek için bir sayısal simülasyon platformu oluşturmuş ve destek vektör makineleri (SVM) kullanarak siber saldırıların tespitine yönelik bir model geliştirmiştir.

- Wanjia Zheng ve Kazumasa Omote tarafından 2021 yılında gerçekleştirilen "Robust Detection Model for Portable Execution Malware" başlıklı çalışmada, sürekli internete bağlı kişisel bilgisayarlar ve Nesnelerin İnterneti (IoT) cihazlarının özellikle akıllı telefonlar ve tabletler gibi cihazların zararlı yazılımlara karşı duyarlılığı ele alınmaktadır. Bu çalışma, yeni bir adversarial saldırı yöntemi olan IMAGE RESOURCE saldırısı ve bu tür saldırılara karşı dirençli bir zararlı yazılım tespit modeli önermektedir. Model, boyut indirgeme ve makine öğrenimi tekniklerini birleştirerek geliştirilmiştir. Ayrıca bu çalışmada makinelerin sesli komutlar aracılığıyla gerçekleştirebilecek saldırıların ve bu saldırılara karşı alınacak önlemleri incelenmiştir.
- Romain Dagnas, Anis Bkakria ve Reda Yaich tarafından 2023 yılında gerçekleştirilen "Robustness Assessment of Biometric Authenticators" başlıklı çalışmada, biyometrik doğrulama sistemlerinin siber saldırılara, özellikle sahtecilik saldırılarına karşı dayanıklılığı ele alınmaktadır. Biyometrik sistemlerin hassas alanlarda güvenli bir doğrulama sağlamak için yaygın olarak kullanılsa da sahtecilik saldırıları gibi siber tehditlere karşı savunmasız olduğundan söz edilmiştir. Bu çalışma, biyometrik doğrulayıcıların dayanıklılığını ölçen evrensel bir yöntem önermektedir.
- U. Hariharan, V. Dhanakoti, K. Rajkumar ve J. Jeyavel tarafından 2022 yılında gerçekleştirilen "Safeguarding E-Healthcare Documents Utilizing an Infrastructure for Advanced Keyless Signature Infrastructure Blockchain Within the Cloud" başlıklı çalışmada, elektronik sağlık kayıtlarının (EHR) güvenliği için blokzincir tabanlı anahtarsız imza altyapısı (KSI) önerilmektedir. Çalışma, merkezi depolama çözümlerinin sağlık verilerinin siber saldırılara karşı savunmasız hale gelmesine neden olduğunu ve bu nedenle merkezi olmayan bir çözümün gerekli olduğunu vurgulamaktadır. Ayrıca bu çalışma siber güvenlik tehditleri bağlamında sesli komutlarla gerçekleştirilebilecek saldırılar açısından blokzincir tabanlı güvenlik çözümlerinin potansiyelini ortaya koymaktadır.
- Sagar Calnoor Rajashekar, Reza Tourani ve Srikanth Gururajan tarafından 2020 yılında gerçekleştirilen "Secure Communications in Unmanned Aerial System Swarms" başlıklı çalışma, insansız hava sistemleri (UAS) arasındaki haberleşmenin güvenliğini sağlamak amacıyla Şifreli Metin Politikası-Öznitelik Tabanlı Şifreleme (CP-ABE) mekanizmasını önermektedir. Çalışma, UAS'lerin artan kullanım alanlarına ve bu sistemlerin siber saldırılara karşı savunmasızlığına dikkat çekmektedir. Önerilen yöntem, her UAS'in belirli özniteliklere sahip olmasına dayalı bir erişim politikası

belirleyerek güvenli veri iletimini sağlamaktadır. Çalışmada bir merkezî sunucu tarafından oluşturulan genel anahtarın tüm UAS'lerle paylaşılması ve her bir drona özel anahtarlar tahsis edilmesiyle yalnızca belirlenen erişim politikalarına uygun olan dronların şifrelenmiş mesajları çözebileceği gösterilmiştir. Yapılan testlerde sesli komutların metne çevrilerek UAS'lere iletilmesi ve yalnızca ilgili dronun komuta yanıt vermesi sağlanmıştır. Şifreleme ve şifre çözme süreçlerinin performans analizleri, erişim politikasının karmaşıklığına ve şifrelenen verinin boyutuna bağlı olarak değiştiğini ortaya koymuştur.

- Charilaos Skandylas, Narges Khakpour ve Javier Cámara tarafından 2022 yılında gerçekleştirilen "Security Countermeasure Selection for Component-Based Software-Intensive Systems" başlıklı çalışmada bileşen tabanlı yazılım yoğun sistemlerde güvenlik açıklarını analiz ederek maliyet-etkin karşı önlemlerin seçimini sağlayan bir yöntem önermektedir. Çalışmada yazılım sistemlerinin artan karmaşıklığı ve siber saldırıların sofistikasyonuna bağlı olarak manuel güvenlik önlemi belirleme süreçlerinin yetersiz kaldığı vurgulanmaktadır. Bu kapsamda araştırmacılar, HaiQ adlı bir araç kullanarak sistem mimarisine dayalı bir güvenlik analizi gerçekleştirmiş ve olasılıksal model denetleme teknikleriyle en uygun güvenlik mimarisini belirlemiştir. Mevcut yaklaşımların çoğunlukla tek bir sistem konfigürasyonu üzerinde güvenlik önlemleri sunduğunu belirten yazarlar, önerdikleri yöntemle çoklu sistem konfigürasyonlarını dikkate alarak daha kapsamlı bir güvenlik analizi sağlamaktadır. Çalışmanın bulguları, farklı bileşen kombinasyonlarının güvenlik seviyelerini değiştirdiğini ve saldırganlar için saldırı maliyetini artıran optimal karşı önlemlerin seçilmesi gerektiğini göstermektedir. Bu kapsamda siber saldırılara karşı ses tabanlı tehditlerin değerlendirildiği mevcut çalışmalara katkı sağlayabilecek sistematik bir güvenlik önlemi seçim süreci sunmaktadır.
- Ryan Heartfield, George Loukas, Anatolij Bezemskij ve Emmanouil Panaousis tarafından 2021 yılında gerçekleştirilen "Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning" başlıklı çalışmada, akıllı ev ortamlarında siber-fiziksel saldırıların tespiti için kendini yapılandırabilen bir saldırı tespit sistemi önerilmektedir. Çalışma, geleneksel saldırı tespit yöntemlerinin statik yapısı nedeniyle akıllı evlerdeki değişen cihaz konfigürasyonlarına ve yeni ortaya çıkan tehditlere karşı yetersiz kaldığını vurgulamaktadır. Bu kapsamda geliştirilen MAGPIE, gözetimsiz anomali tespit modellerinin karar fonksiyonlarını çevresel değişikliklere uyum sağlayacak şekilde otomatik olarak güncelleyebilen bir sistemdir. Sistem,

pekiştirmeli öğrenme temelli olasılıksal kümeleme mekanizması kullanarak siber ve fiziksel veri kaynaklarını birleştirerek saldırı tespit performansını artırmaktadır. Bu çalışma sesle etkinleştirilen sistemlere yönelik siber saldırılar da dahil olmak üzere, saldırıların yalnızca siber değil fiziksel etkilerini de dikkate alan bir yaklaşım sunmasıyla ses tabanlı siber saldırıların değerlendirilmesine katkı sağlayabilecek bir model oluşturmaktadır.

- Melike Erol-Kantarcı ve Hussein T. Mouftah tarafından 2021 yılında gerçekleştirilen "Smart Grid Forensic Science: Applications, Challenges, and Open Issues" başlıklı çalışmada, akıllı şebekelerin siber ve fiziksel güvenliği bağlamında adli bilişim biliminin rolü ele alınmaktadır. Çalışmada, bir siber saldırı veya doğal afet sonrasında yapılan adli analizlerin güç sistemlerinin güvenlik açıklarını ortaya çıkararak gelecekte benzer saldırıların önlenmesine ve arızaların engellenmesine katkı sağladığı vurgulanmaktadır. Ayrıca akıllı sayaçlardan ve veri toplayıcılardan elde edilen verilerin elektrik hırsızlığı gibi suçlarla ilgili adli süreçlerde delil olarak kullanılabileceği belirtilmektedir. Ses kayıtlarının doğrulama ve zaman damgalama işlemlerinde elektrik şebekesi frekansının kullanılması gibi uygulamalara da değinilmektedir.
- Gyorgy Kalmar tarafından 2019 yılında gerçekleştirilen “Smart Speaker: Suspicious Event Detection with Reverse Mode Speakers” başlıklı çalışmada, hoparlörlerin ters modda çalıştırılarak güvenlik amaçlı olay tespiti için kullanılabilirliği incelenmektedir. Çalışma, hoparlörlerin yalnızca elektrik sinyallerini sese dönüştüren cihazlar olmadığını, ters modda akustik sinyalleri elektrik sinyallerine dönüştürebildiklerini ortaya koymaktadır. Bu bağlamda, silah sesleri veya çığlık gibi şüpheli olayların algılanmasını sağlayan bir gömülü sistem önerilmektedir. Önerilen sistem, hoparlörlerin aktif olmadığı durumlarda ters modda sinyal kaydederek güvenlik izleme işlevi görmektedir.
- Naveenkumar G. Venkataswamy ve Masudul H. Imtiaz tarafından 2023 yılında gerçekleştirilen “Support Vector Machine for Person Classification Using the EEG Signals” başlıklı çalışma, geleneksel kimlik doğrulama yöntemlerinin güvenlik açıklarına karşı biyometrik tabanlı bir alternatif sunmayı amaçlamaktadır. Çalışma, bireylerin benzersiz beyin aktivitelerinden elde edilen Elektroensefalogram (EEG) sinyallerini kullanarak kimlik doğrulama gerçekleştiren bir sistem önermektedir. EEG sinyalleri, bireyin zihinsel durumu ve genetik özellikleriyle doğrudan bağlantılı olduğundan sahtecilik girişimlerine karşı yüksek güvenlik sağlamaktadır. Özellikle EEG sinyallerinin bireye özgü yapısı sayesinde sahtecilik girişimlerine karşı dayanıklı

bir kimlik doğrulama yöntemi sunması, ses tabanlı saldırılara karşı alternatif bir güvenlik mekanizması oluşturur.

- Junaid M. Qurashi, Kamal Jambi, Fathy E. Eassa, Maher Khemakhem, Fawaz Alsolami ve Abdullah Basuhail tarafından 2023 yılında yayımlanan "Toward Attack Modeling Technique Addressing Resilience in Self-Driving Car" başlıklı çalışma, otonom araçların siber saldırılara karşı güvenliğini artırmaya yönelik bir saldırı modeli geliştirmeyi amaçlamaktadır. Çalışma, otonom araçların yaygınlaşmasıyla birlikte bu sistemlerin maruz kalabileceği saldırı vektörlerini ve güvenlik açıklarını analiz ederek bu tehditlere karşı dirençli bir mimari oluşturmayı hedeflemektedir. Özellikle otonom araçlarda saldırı tespit ve tahmininde kullanılan makine öğrenmesi ve derin öğrenme teknikleri, ses tabanlı siber saldırıların analiz edilmesinde de kullanılabilecek yöntemler sunmaktadır.
- Jydrzej Bieniasz, Piotr Sapiecha, Milosz Smolarczyk ve Krzysztof Szczypiorski tarafından 2016 yılında yayımlanan "Towards Model-Based Anomaly Detection in Network Communication Protocols" başlıklı çalışma, ağ iletişim protokollerinde model tabanlı anomali tespiti yöntemlerini ele almaktadır. Çalışma, özellikle siber güvenlik alanında, ağ protokollerindeki hataları ve güvenlik açıklarını tespit etmek için model tabanlı tekniklerin nasıl kullanılabileceğini incelemektedir. Model tabanlı anomali tespiti ve ağ protokollerinde kullanılan otomatik model çıkarımı, sesle gerçekleştirilen saldırılarda da ağ trafiğini analiz ederek anomali tespiti yapılmasında uygulanabilir yöntemler sunmaktadır.
- Swadhin Thakkar, Kaustubh Shivdikar ve ChiragWarty tarafından 2017 yılında gerçekleştirilen "Video Steganography Using Encrypted Payload for Satellite Communication" başlıklı çalışma, özellikle uydu iletişimi bağlamında, şifreleme ve steganografi tekniklerini birleştirerek iletişim kanallarını güvence altına almayı hedeflemektedir. Yazarlar, güvenli şifreleme algoritmalarını steganografi teknikleriyle birleştiren yeni bir yöntem önermektedirler. Bu yöntem, şifreli mesajları video dosyalarına gizleyerek kötü niyetli kişiler tarafından iletişimin tespiti ve çözülmesini engellemeyi amaçlamaktadır. Önerilen sistem, şifreli mesajı geniş bir bant genişliğine yaymak için yayılma spektrumu (spread spectrum) tekniğini kullanarak mesajı video içeriğine görsel olarak algılanamayacak şekilde gömmektedir. Ayrıca sistemin güvenliği, veri doğrulama ve bütünlük kontrolü için bir Hash Tabanlı Mesaj Kimlik Doğrulama Kodu (HMAC) ile artırılmaktadır. Makale modern iletişim sistemlerinde

gizlilik, kimlik doğrulama, bütünlük ve inkâr edilemezlik gibi önemli güvenlik gereksinimlerine vurgu yapmaktadır.

- Hafiz Muhammad Ashja Khan ve diğer yazarlar tarafından 2021 yılında gerçekleştirilen "Voice Over Internet Protocol: Vulnerabilities and Assessments" başlıklı çalışmada, VoIP (Voice over Internet Protocol) teknolojisinin güvenlik açıkları ele alınmaktadır. Bu çalışma, VoIP sistemlerinin güvenliğini sağlamada kullanılan protokoller ve araçların etkinliğini değerlendirirken, tehditlerin yönetilmesi ve sistemlerin güvenliğini artırmaya yönelik çözüm önerileri sunmaktadır. Ayrıca, VoIP sistemlerinde güvenlik açıklarının yalnızca protokollerden değil, aynı zamanda işletim sistemleri ve uygulamalardan da kaynaklanabileceği vurgulanmaktadır. Bu araştırma, sesli iletişim sistemlerinin güvenliğiyle ilgili önemli bir katkı sağlamaktadır ve sesle yapılan siber saldırıların analizine yönelik benimsenebilecek yeni yöntemleri desteklemektedir.
- Amr El Mougy ve diğer yazarlar tarafından 2021 yılında gerçekleştirilen "Xenia: Secure and Interoperable Smart Home System with User Pattern Recognition" başlıklı çalışmada, akıllı ev sistemlerinin güvenlik ve uyumluluk zorlukları ele alınmaktadır. Çalışmada, Xenia adlı güvenli bir akıllı ev platformu sunulmakta ve akıllı ev cihazlarının yönetimi için merkezi bir sunucu üzerinden sağlanan API'lerle cihazların kontrolü yapılmaktadır. Ayrıca, cihazlar metin veya sesli komutlarla yönetilebilecek şekilde tasarlanmıştır. Xenia, cihazlar arasındaki koordinasyonu iyileştirmek için kullanıcı desenlerini otomatik olarak tespit eden bir makine öğrenimi algoritması kullanmaktadır. Çalışma, akıllı ev sistemlerinin heterojen yapısına rağmen, kullanıcı dostu bir etkileşim imkânı sunduğu gibi güvenlik konusunda da kapsamlı önlemler içermektedir.

Bu bölümde ses kullanılarak yapılan siber saldırılarla ilgili çeşitli akademik çalışmalar incelenmiş ve bu saldırı türlerinin güvenlik riskleri üzerindeki etkileri değerlendirilmiştir. Bu bölümün devamında literatürde yaygın olarak karşılaşılan saldırı türleri hem teknik özellikleri hem de yarattıkları güvenlik riskleri açısından ayrıca incelenecek ve ilgili çalışmalara dayanarak değerlendirmeler yapılacaktır. Her saldırı türü için ayrıca bir literatür taraması gerçekleştirilmiş olup ilgili bölümlerde bu tarama sonucuna ilişkin sentezlere yer verilecektir.

3.2. Vishing Saldırıları

İngilizce “phishing” olarak adlandırılan “kimlik avı saldırıları”, çeşitli tekniklerle hedefteki kişilerin ya da kurumların kredi kartı ve oturum açma bilgileri gibi gizli kişisel verilerini ele geçirmek veya hedef cihaza kötü amaçlı yazılım yüklemek gibi amaçlarla gerçekleştirilir. Phishing saldırılarının vishing ve pharming gibi bazı varyasyonları vardır. Phishing içeren klasik saldırılar, kurban kullanıcıdan hassas verileri toplamaya çalışan sahte e-postalar gönderen popüler yaygın saldırılardır. Vishing saldırısı, saldırganın gizli bilgileri ele geçirmek için telefon görüşmesi veya SMS kullandığı bir phishing saldırısı kategorisidir. Pharming saldırısı ise bir web sitesinin trafiğini başka bir sahte web sitesine yönlendiren alternatif bir kimlik avı saldırısı biçimidir. Bir pharming saldırısında kullanıcılar, saldırgan tarafından yaratılmış olan sahte web sayfasına farkında olmadan hassas bilgilerini girerler ve bu bilgiler saldırgan kimselere ulaşmış olur (Brabin ve Bojjagani, 2023).

Sesli kimlik avı dolandırıcılığı saldırıları anlamına gelen vishing “voice phishing” yani ses ve kimlik avı olarak tanımlanmaktadır (Aksakallı, 2022). Vishing, sesli iletişimle gerçekleştirilen bir dolandırıcılık yöntemidir. Bu terim, "phishing" kelimesindeki “p” harfi yerine "voice" kelimesinin ilk harfi kullanılarak "ses aldatmacası" anlamında ortaya çıkmıştır. Vishing, sosyal mühendislik dolandırıcılığına yönelik yöntemler arasında yer alırken teknolojinin sunduğu imkanlarla da desteklenmektedir. Dolandırıcılar, uluslararası internet servis sağlayıcıları (proxy) aracılığıyla kendilerine istedikleri numarayı gösterme şansına sahip olurlar. Bu dolandırıcılık yöntemi müşterilerin hesap numaraları, kredi kartı bilgileri gibi kişisel bilgilerini elde etmeyi hedefleyen e-postalar ve bu e-postalarda verilen sahte telefon numaralarını içermektedir. Kurban, bu sahte numaraları aradığında dolandırıcının daha önce hazırladığı banka sesli yanıt sistemi ya da çağrı merkezi ile karşılaşır. Bu yöntemle dolandırıcılar, kurbanın kişisel bilgilerini kolaylıkla ele geçirebilir. Olası bir senaryo ile örneklendirilirse: Ailesinin gayrimenkul işlerini yöneten Poyraz Bey, yoğun bir iş gününde sürekli çalıştığı ve güvendiği Tatlıbank'tan bir e-posta alır. Bu e-posta, hesaplarının iki gün içinde pasif hale geleceğini ve hemen 0(850) * numaralı çağrı merkezini arayarak hesaplarını aktiflestirmesi gerektiğini belirtmektedir. Tamamen Tatlıbank'tan geliyormuş gibi görünen bu e-posta, Poyraz Bey'i yanıltır. Belirtilen çağrı merkezini arayan Poyraz Bey, sahte sesli yanıt sisteminden şüphelenmeden kredi kartı bilgilerini sisteme girer. İşlemlerini tamamlayarak rahatlamış bir şekilde öğle yemeğine çıkar. Ancak kısa bir süre

sonra kart bilgilerini çaldırdığını öğrenir ve bu durum onun için yemeği zehir eder (Türkiye Bankalar Birliği, 2015).

Bu örnekte olduğu gibi vishing saldırısında saldırganlar, bir kişinin telefon numarasını kullanarak arama yapar ve hedef kişiyi dolandırmaya çalışır. Saldırganlar, hedef kişinin güvenini kazanmak için sahte bir kimlik kullanabilirler veya seslerini fiziki olarak ya da elektronik ortam yoluyla değiştirebilirler. Korku veya aceleyle hareket etme gibi durumları kullanıp kişilerin duyguları manipüle edilerek gerçekleştirilir. Bu tür saldırılar, genellikle finansal bilgileri çalmak veya kişisel bilgileri ele geçirmek için kullanılır. Saldırgan kişi hedef seçtiği kişiyi telefon numarasından arayarak banka numarası, ev adresi gibi kişisel bilgileri elde etmeye çalışmaktadır. Ayrıca vishing saldırıları son zamanlarda WhatsApp, Skype, TikTok gibi uygulamalar üzerinden ses teknolojileri ile de gerçekleştirilmektedir.

Shete ve diğerleri tarafından 2024 yılında yayınlanan "A Comparative Analysis of Cybersecurity Scams: Unveiling the Evolution from Past to Present" başlıklı makaledeki karşılaştırmalı analizde, geçmişte telefon aracılığıyla gerçekleştirilen temel vishing saldırılarının yapay zekâ destekli ses klonlama teknolojilerinin gelişmesiyle çok daha ikna edici ve tehlikeli bir hale geldiği vurgulanmaktadır. Çalışmada saldırganların hedef kişilerin sesini ya da bu kişileri yanıltabilecek farklı kişilerin seslerini gerçek veya klonlanmış şekilde taklit ederek finansal bilgiler elde etmeye çalıştığından bahsedilmiştir. Bu nedenle de söz konusu yöntemin geleneksel kimlik avı tekniklerinden daha yüksek başarı oranına sahip olduğu belirtilmiştir. Özellikle çağrı merkezleri ve bankacılık sistemlerinde kullanılan sesli doğrulama yöntemlerinin bu tür saldırılara karşı savunmasız olduğu tespit edilmiştir. Ayrıca vishing saldırılarının geçmişten günümüze evrimsel süreçte daha hedef odaklı hale geldiği ve kurbanların sosyal mühendislik teknikleriyle manipüle edilerek sahte aramalara yönlendirildiği ortaya konmuştur. Buna göre de yapay zekâ destekli vishing saldırılarının giderek artan bir tehdit oluşturduğu ve bireylerin yanı sıra kurumsal sistemler için de ciddi güvenlik açıkları doğurduğu sonucu ortaya çıkmaktadır.

Suthar ve Rughani tarafından 2020 yılında yapılan "A Comprehensive Study of VoIP Security" başlıklı çalışmada, VoIP (Voice Over Internet Protocol) sistemleri üzerinden gerçekleştirilen vishing saldırılarının nasıl organize edildiği ve saldırganların kullandığı teknikler detaylandırılmıştır. Çalışmada, vishing saldırılarının çoğunlukla Caller ID Spoofing (Arayan Kimlik Sahteciliği) yöntemiyle gerçekleştirildiği belirtilmektedir. Caller

ID Spoofing, ilk olarak arayan kişinin kimliğini gizlemek için arayan kimliği ekranına iletilen bilgileri kasıtlı olarak bozması ya da değiştirmesi ile gerçekleştirilir. Bu yöntemde saldırganlar güvenilir bir finans kurumu, resmi bir devlet dairesi veya tanınmış bir şirketin telefon numarasını taklit ederek hedef kişiyi aramakta ve hassas bilgilerini paylaşmasını sağlamaktadır. Bu sahte çağrılar, hedef kişinin sesli yanıtlarını kaydederek kimlik doğrulama sistemlerini atlatmak veya doğrudan banka bilgileri gibi kritik verileri ele geçirmek amacıyla yapılmaktadır. Bu şekilde gelen bir aramaya cevap verilirse dolandırıcılık faaliyetlerinde kullanılabilecek para veya değerli kişisel bilgileri çalmaya çalışmak için dolandırıcılık komut dosyaları da kullanılır (ABD Federal İletişim Komisyonu, 2024).

Bunun yanı sıra Man-in-the-Middle (MitM) saldırıları ile de VoIP trafiğinin ele geçirilebilir ve saldırganların iletişim akışını değiştirebilir (Suthar ve Rughani, 2020). Bu saldırılar sırasında kötü niyetli aktörler VoIP çağrılarının yönlendirilmesini manipüle ederek ya çağrıları dinlemekte ya da kullanıcıyı sahte bir çağrı merkezine yönlendirmektedir. Özellikle uçtan uca şifrelenmeyen VoIP protokollerinin bu tür saldırılara açık olduğu ve saldırganların çağrı içeriğini değiştirebilir. Çalışmada ayrıca VoIP trafiğinin analiz edilerek kullanıcıların sesli yanıtlarının yapay zekâ destekli ses klonlama araçlarıyla taklit edilebileceği ortaya konmuştur. Bu durum, kimlik doğrulama süreçlerinin yalnızca geleneksel parola ve PIN kodlarıyla değil, biyometrik doğrulama sistemleriyle de güvence altına alınması gerektiğini göstermektedir. Son olarak çalışma, vishing saldırılarına karşı alınabilecek güvenlik önlemlerine de yer vermektedir. Özellikle VoIP şifreleme protokollerinin etkin kullanımı, iki faktörlü kimlik doğrulamanın zorunlu hale getirilmesi ve anomali tespit sistemleriyle şüpheli çağrı davranışlarının analiz edilmesi gibi önlemler önerilmektedir. VoIP tabanlı vishing saldırılarının gün geçtikçe daha karmaşık hale gelmesi, hem bireylerin ve kurumların yalnızca teknik güvenlik önlemlerine hem de siber farkındalık eğitimlerine ağırlık vermesini zorunlu kılmaktadır.

Hijji ve Alam tarafından 2021 yılında gerçekleştirilen “A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions” başlıklı kapsamlı çalışmada, COVID-19 pandemisi sırasında sosyal mühendislik tabanlı siber saldırıların önemli ölçüde arttığı vurgulanmaktadır. Çalışma, özellikle vishing saldırılarının artışına dikkat çekerek saldırganların telefon aramaları yoluyla bireyleri manipüle etmek için psikolojik teknikleri nasıl kullandığını detaylandırmaktadır. Araştırmada, saldırganların Caller ID Spoofing

(Arayan Kimlik Sahteciliği) kullanarak telefon numaralarını değiştirdiği ve güvenilir görünen kaynaklar üzerinden kurbanlara ulaştığı belirtilmektedir. Çalışma ayrıca, COVID-19 sürecinde uzaktan çalışma modelinin yaygınlaşmasının vishing saldırıları için uygun bir zemin oluşturduğunu ortaya koymaktadır. Evden çalışan bireylerin iş bağlantıları veya IT destek ekipleri tarafından arandıklarını düşündükleri senaryolarla kandırıldığı, bu şekilde kurumsal sistemlere erişim sağlandığı vurgulanmaktadır. Pandemi sürecinde artan ransomware (fidye yazılımı) ve trojan saldırıları ile vishing'in bütünleşmiş şekilde kullanıldığına da dikkat çekilmektedir; saldırganlar, vishing yoluyla elde ettikleri bilgileri kullanarak daha büyük çaplı finansal dolandırıcılık ve veri ihlalleri gerçekleştirmektedir.

Hedefteki kullanıcı, bir vishing araması gerçekleştiğinde genellikle tanıdık bir kuruluşa ait olduğu düşünülen bir sesli yanıt sistemi (İngilizce olarak Interactive Voice Response, IVR) ile karşılaşır. IVR, önceden kaydedilmiş sesli mesajları kullanarak çağrıları yönlendiren bir sistemdir. Kullanıcı herhangi bir şüphe duymaz ve pasaport bilgileri, banka kartı şifreleri, tek kullanımlık şifreler gibi tüm gizli bilgilerini paylaşabilir. Vishing saldırıları yalnızca IVR sistemleri üzerinden değil, aynı zamanda doğrudan bir sosyal mühendis tarafından gerçekleştirilen birebir görüşmeler aracılığıyla da yürütülebilir. Saldırgan kendisini bir uzman, kolluk kuvveti yetkilisi veya internet servis sağlayıcısı gibi tanıtarak kurbanın güvenini kazanmaya çalışır. Dolandırıcı, kurbanın kişisel ve finansal bilgilerini, kredi kartı ve banka hesap bilgilerini ele geçirmeyi hedefler. Elde edilen bu bilgiler sayesinde saldırgan, kurbanın banka hesabına erişim sağlayarak mali kayıplara neden olabilir veya kimlik bilgilerini kullanarak farklı dolandırıcılık faaliyetlerinde bulunabilir. Bazı dolandırıcılar, kurbanı parayı başka bir banka hesabına aktarmaya veya doğrudan kendilerine teslim etmek amacıyla nakit çekmeye ikna etmeye çalışabilirler (Leonov ve diğerleri, 2021). Şekil 3.1’de vishing saldırısının yaygın türleri gösterilmiştir:

Şekil 3.1. Yaygın vishing yöntemlerine ilişkin bir diyagram (KeepNet, 2025).

Vishing saldırılarının bu kadar yaygın hale gelmiş olması, saldırganların ses taklit etme becerilerini önemli ölçüde artırmıştır. Bu durum da vishing saldırılarını daha ikna edici ve tespit edilmesi zor hale getirmiştir. Bu bağlamda vishing saldırılarında en kritik unsur olan ses iletişimi, saldırganların kimlik sahteciliği, sosyal mühendislik ve teknik manipülasyon stratejilerini bir araya getirerek gerçekleştirdiği karmaşık dolandırıcılık girişimlerinin merkezinde yer almaktadır.

Bu konuda adli bilişim çerçevesinde esas olarak üzerinde durulması gereken nokta ise saldırganın kullandığı ses ile konuşmacı tespitinin yapılmasıdır. Konuşmacı profili belirleme işleminde kişinin yaş, cinsiyet ve sağlık gibi fiziksel özelliklerinin ortaya çıkarılması amaçlanır (Kalluri ve LeBleu, 2020). Bu işlemde işitsel analizlere ek olarak adli ses inceleme yazılımının fiziksel özellikleri otomatik tespit edebilmesi ile profil belirlenir. Birden çok konuşmacıyı ayırt etme işlemi, dijital delil olarak kullanılan ses kayıtlarının incelenmesi ve bu kayıtlarda geçen konuşmalarda işitsel olarak birbirlerine benzeyen konuşmacıların seslerinin yazılım yolu ile ayrıştırılmasıdır. Birden çok konuşmacı varlığının söz konusu olduğu bir ses kaydında belirli kişiye ait sesin mevcut olup olmadığının tespiti, bu kişinin seslendirdiği zaman aralığının belirlenmesi ve ses kaydındaki konuşmacıların seslendirdiği bölümlerin ayrılması işlemleri gerçekleştirilebilmektedir. Maskelenmiş ses analizi işleminde

kaydın kalitesini bozan maskelemenin tespiti ve ses kaydında sadece konuşmanın olduğu kısımların vurgulanması gerçekleştirilir. Ses maskeleme, bir ortamda kayıt altına alınan konuşmaların yüksek müzik veya televizyon sesleriyle fiziksel maskelemeye maruz kalması olarak bilinir.

Vishing saldırılarında bir kişiye ait gerçek bir konuşma, bir kişiye ait olan ama sentetik olarak oluşturulmuş bir konuşma ya da gerçek bir kişiye ait olmayan ve sentetik olarak oluşturulan bir konuşma kullanılabilir. Bunun tespiti ise günümüzde oldukça zordur ve yeni yöntemler denenmektedir. Bu yöntemlerden birinde belirli bir telefon konuşmasının gerçekliğini belirlemek için ses özelliği analizini kullanma, insan ve robotik kaynaklar arasında ayrım yapmadır. Burada arayanın sesinin bir insan veya otomatik bir sisteme işaret eden belirgin özellikler açısından incelenmesi gerekmektedir. Örneğin, insan sesleri daha fazla perde ve ses seviyesi değişimi gösterme eğilimindedir ve bu da insan konuşmasının dinamik doğasını vurgular. Aksine, robotik sesler ise genellikle daha monoton ve tekdüze bir ton sergiler (Gamage ve diğerleri, 2023).

Vishing saldırılarında bir kişiye ait gerçek bir konuşmanın kullanılması durumunda, konuşmacının kimliğinin belirlenmesi adli ses incelemeleri ile mümkündür. Bu incelemeler ses kayıtlarının doğruluğunu ve bütünlüğünü değerlendirmek, konuşmacının kimliğini tespit etmek ve ses üzerinde yapılan olası manipülasyonları belirlemek amacıyla gerçekleştirilmektedir. Konuşmacı tespiti sürecinde otomatik ses izi eşleştirme, konuşmacı profili belirleme, formant frekanslarının analizi ve spektrum analizi gibi yöntemler kullanılmaktadır. Bu teknikler konuşmacının ses özelliklerini analiz ederek yaş, cinsiyet ve aksan gibi fiziksel ve dilsel faktörleri ortaya koyabilmektedir. Ayrıca kayıt bütünlüğü doğrulama süreçleri ile ses kaydında kesinti, düzenleme veya maskeleme olup olmadığı tespit edilebilmektedir. Maskelenmiş ses analizleri, kayıtlardaki arka plan gürültülerini filtreleyerek konuşmanın daha net hale getirilmesini sağlarken gerçek zamanlı ses analizleri anlık konuşmaları değerlendirerek kimlik doğrulama süreçlerinde kullanılabilmektedir (Korkmaz ve Boyacı, 2018).

Gerçek bir kişiye ait olan bir ses ile gerçek olmayıp sentetik olarak oluşturulmuş bir konuşma söz konusu ise burada ses klonlamadan söz edilmelidir. Ses klonlaması, bir yapay zekâ programının gerçek bir kişinin konuşma tarzını taklit ederek onun belirli ve benzersiz olan sesini kopyaladığı bir işlemdir. Yapay zekâ ve makine öğrenimindeki gelişmeler sayesinde

bu teknik, bir kişinin sesinin son derece doğru bir şekilde kopyalanmasına olanak tanımış ve popülerlik kazanmıştır. Bu ilerlemeler, daha gerçekçi bir biçimde sentetik seslerin üretilmesini mümkün kılmakta, bu süreç hem olumlu hem de olumsuz sonuçlar doğurabilmektedir. Bu işlem için kullanılan programlar, verilerdeki karmaşık kalıpları belirleme yeteneğine sahip yapay sinir ağlarına dayanmaktadır. Bir sesi klonlamak amacıyla öncelikle klonlanacak kişiden büyük miktarda ses verisi ile ilgili programın eğitilmesi gerekmektedir, sağlanan veri ne kadar fazla olursa klonlama o kadar yüksek doğrulukla gerçekleşir. Program eğitildikten sonra ilgili kişiye benzeyen yeni ses klipleri üretebilir. Bu da ilgili program tarafından temel frekans, hece süresi ve tonlama gibi ses parametrelerinin değiştirilmesiyle sağlanır.

Ses klonlama teknolojilerinin gelişimi, sentetik medya ve deepfake uygulamalarını da beraberinde getirmiştir. Deepfake terimi, yapay zekâ destekli medya üretim tekniklerini tanımlamak için kullanılan bir kavram olup genellikle kişilerin ses veya görüntülerinin sahte biçimde üretilmesini ifade etmektedir. Derin öğrenme algoritmalarını temel alan bu teknoloji, belirli bir kişinin yüz hareketlerini ve ses tonunu taklit edebilen sentetik içerikler üretmek için büyük veri kümelerinden yararlanmaktadır. Deepfake ses klonlama teknikleri, bir kişinin sesini analiz ederek o kişiye ait yeni, ancak gerçekte söylenmemiş konuşmalar oluşturulmasını mümkün kılmaktadır. Bu süreç, kişinin özgün ses özelliklerini çıkaran derin sinir ağları kullanılarak gerçekleştirilmekte ve son derece gerçekçi sonuçlar üretebilmektedir.

Deepfake ses klonlama teknolojileri, özellikle kimlik hırsızlığı ve sosyal mühendislik saldırıları için yeni ve tehlikeli bir araç haline gelmiştir. Gerçekçi bir şekilde oluşturulmuş sentetik sesler hedef alınan kişinin yöneticisi, banka temsilcisi veya devlet yetkilisi gibi kritik rollerdeki kişileri taklit ederek kurbanı yanıltmasına olanak sağlamaktadır. Günümüzde yalnızca birkaç dakikalık ses kaydı ile oldukça gerçekçi klonlar oluşturulabilirken yeni algoritmalar üç saniyelik bir ses kaydıyla bile taklit işlemini gerçekleştirebilmektedir. Deepfake teknolojisinin vishing saldırılarında kullanımı, kimlik avı yöntemlerini daha karmaşık hale getirmekte ve geleneksel saldırılara kıyasla tespit edilmesini zorlaştırmaktadır. Örneğin bir e-ticaret şirketinde çalışan bir kişi, yöneticisinin sentetik sesiyle yapılan bir çağrıyı gerçek sanarak oturum açma bilgilerini paylaşabilir. Benzer şekilde sosyal medya platformlarında paylaşılan ses kayıtları veya sesli mesajlar, saldırganlar tarafından ele geçirilip kullanılarak hedef kişiye ait sahte telefon görüşmeleri

oluşturulabilir. Bu tür saldırılar, yalnızca yüksek profilli kişilerle sınırlı kalmayıp herkesin potansiyel hedef haline gelmesine yol açmaktadır.

Bununla birlikte deepfake içeren vishing saldırılarının hala belirli zorlukları bulunmaktadır. Geleneksel kimlik avı yöntemleri, geniş ölçekli saldırılar için daha elverişli olurken deepfake destekli vishing genellikle daha fazla planlama ve teknik bilgi gerektirmektedir. Bu nedenle güvenlik sistemlerinin deepfake içeren vishing saldırılarını tespit edebilecek mekanizmalarla donatılması ve bireylerin bu tür tehditlere karşı bilinçlendirilmesi büyük önem taşımaktadır (Bateman, 2020).

Forbes'in 2019 yılına ait bir haberine göre Mart 2019'da İngiltere merkezli bir enerji şirketi, deepfake ses teknolojisi kullanılarak gerçekleştirilen nitelikli bir CEO dolandırıcılığı saldırısına maruz kaldı ve 243.000 ABD doları kaybetti. Wall Street Journal'dan edinilen bilgilere göre ise saldırganlar, Almanya merkezli ana şirketin CEO'sunun sesini yapay zekâ destekli ses üretim yazılımı kullanarak taklit etti. Saldırganlar, İngiltere'deki şirketin CEO'sunu arayarak kendilerini ana şirketin yöneticisi gibi tanıttı ve acil bir banka havalesi talep etti. Para, Macaristan'daki sahte bir tedarikçiye transfer edildikten sonra Meksika'ya ve ardından farklı hesaplara yönlendirilerek dolandırıcıların kimliklerinin tespit edilmesi zorlaştırıldı. Saldırganlar, ilk başarılı işlemden sonra ikinci bir transfer talebinde bulundu ve önceki ödemenin iade edildiğini iddia etti. Ancak geri ödeme gerçekleşmediği için İngiltere'deki CEO talebi reddetti. Üçüncü aramada dolandırıcılar bir başka ödeme yapılmasını talep etti, ancak bu kez arama Avusturya'dan yapıldığı için şüphe uyandırdı ve dolandırıcılık girişimi fark edildi. Bu olay, deepfake teknolojisinin sosyal mühendislik saldırılarında nasıl kötüye kullanılabileceğini göstermektedir. Geleneksel kimlik avı (phishing) ve iş e-postası sahtekarlığı gibi yöntemlerin hala yaygın olarak kullanıldığı belirtilse de yapay zekâ tabanlı deepfake saldırılarının tespit edilmesini daha zor hale getirdiği görülmektedir. Özellikle büyük ölçekli finansal işlemler gerçekleştiren kurumların, çalışanlarını bu tür saldırılar konusunda bilinçlendirmesi ve güvenlik önlemlerini artırması gerekmektedir. Kritik ödemeler öncesinde telefonla veya farklı bir iletişim kanalı üzerinden ek doğrulama yapılması, anormal banka bilgisi değişikliklerine karşı dikkatli olunması ve kimlik doğrulama süreçlerinin güçlendirilmesi önerilmektedir. Ayrıca yapay zekâ destekli güvenlik sistemleri kullanılarak e-posta yazım tarzı analizleri gibi tekniklerle dolandırıcılık girişimleri tespit edilebilir. Bu tür önlemler, deepfake içeren vishing saldırılarının önlenmesi açısından kritik önem taşımaktadır.

ABD Kent Eyalet Üniversitesi'nin vishing saldırılarına yönelik olarak önerilen önlemler şunlardır:

- Bilinmeyen bir arayan, bir vishing dolandırıcısı olabilir. En güvenlisi, arayanın sesli mesaj bırakmasına izin vermektir. Sesli mesaj daha sonra dinlenerek arayanın güvenilir olup olmadığına karar verilebilir.
- Bir dolandırıcı, arayan kimliğini taklit edebilir ve aramalarını güvenilir bir kaynaktan geliyormuş gibi gösterebilir. Güvenilir olduğu düşünülen bir aramayı cevaplandıysa ve alışılmadık sorular sorulduğu fark edildiyse derhal telefon kapatılmalıdır.
- Eğer bir arayan, cihaz üzerinde kontrol sahibi olmasını sağlayacak bir işlem yapılmasını istiyorsa bunu yapmasına izin verilmemelidir. Bunu yapmak, cihazdaki hassas bilgilerin savunmasız hale gelmesine neden olabilir.
- Arayanın gerçekten iddia ettiği kişi olduğundan emin olunmalıdır. Arama yapmak için kullanılan numara kontrol edilmeli ve onların zaten bilmesi gereken sorulara cevap verilmesi isteniyorsa dikkatli olunmalıdır.
- Telefon numaranısı güvenilir olmayan kaynaklarla paylaşılmamalı; aksi halde numara, dolandırıcıların eline geçebilir. Ayrıca telefon üzerinden şifre gibi hassas bilgiler paylaşılmamalı. Eğer arayanın bir dolandırıcı olduğu düşünülüyorsa konuşma yapılmamalı ya da tuşlara basarak yönlendirmelere uyulmamalı.
- Bir dolandırıcı, hızlı hareket edilmezse bazı sonuçlarla karşılaşılacağını iddia edebilir. Bu sonuçlar, bir ödülü kaybetmekten hapse girmeye kadar değişebilir. Eğer gerçekçi olmayan bir aciliyet hissedilirse büyük olasılıkla bir vishing dolandırıcılığı ile karşı karşıya gelinmiş olduğundan söz edilebilir.

Sonuç olarak vishing saldırıları, gelişen ses taklit teknolojileri ve siber güvenlik alanındaki zayıflıklar nedeniyle daha da karışık hale gelmektedir. Sosyal mühendislik tekniklerinin gücü, saldırganların hedeflerini manipüle etme ve kişisel verileri elde etme yeteneklerini artırmaktadır. Bu nedenle hem bireylerin hem de organizasyonların ses tabanlı saldırılara karşı daha bilinçli ve savunmalı olmaları gerekmektedir. Gelecekte ses tanıma sistemlerinin güçlenmesi, yapay zekâ ve makine öğrenimi tekniklerinin bu tür saldırıları tespit etme konusunda önemli bir rol oynamasına olanak sağlayacaktır. Ancak bu teknolojilerin gelişimiyle yeni güvenlik açıklarının ortaya çıkması da kaçınılmazdır. Buna göre proaktif güvenlik önlemleri ve sürekli eğitim, vishing gibi sosyal mühendislik saldırılarına karşı etkili

savunma stratejilerinden olacaktır. Vishing'in geleceği hem teknolojik gelişmelerle hem de kullanıcıların farkındalıklarıyla şekillenecektir.

3.3. Sesli Kimlik Hırsızlığı

Sesli Kimlik Hırsızlığı, saldırganların sesli iletişim yoluyla bireylerin ses verilerini izinsiz olarak ele geçirerek kimliklerini taklit etme veya dolandırıcılık amaçlı kullanma eylemidir. Sesli kimlik hırsızlığı kavramı, telekomünikasyon teknolojilerinin yaygınlaşmasıyla birlikte ortaya çıkmıştır. İlk olarak sesli kimlik doğrulama sistemleri kullanılmaya başlandığında bu sistemlerin güvenlik açıkları araştırılmaya başlanmıştır. 2000'li yıllarda telefon tabanlı dolandırıcılık vakaları artış gösterirken 2010'lu yıllarda yapay zekâ ve makine öğrenmesi tekniklerinin gelişimiyle ses klonlama yöntemleri saldırganlar tarafından daha etkin bir şekilde kullanılmaya başlanmıştır.

Bu tür bir saldırıda, saldırganlar ses örneklerini analiz ederek hedef kişinin kimliğini doğrulayan sistemleri yanıltabilir veya sosyal mühendislik teknikleriyle kurbanlarını manipüle edebilirler. Özellikle yapay zekâ tabanlı ses sentezi ve deepfake teknolojilerinin gelişmesi, sesli kimlik hırsızlığının giderek daha da yaygınlaşmasına neden olmuştur. Bu saldırılar, kurbanların güvendiği bir kişiyle etkileşimde olduğu yanılsaması yaratılarak ve kurbanın genellikle kamu kurumlarına duyduğu doğal güveni istismar ederek gerçekleştirilir. Saldırganlar genellikle kurbanları kişisel bilgilerini saldırganla paylaşmaları için kandırmak amacıyla kamu veya finans kurumlarını, kamu görevlilerini, halk üyelerini veya sosyal medya platformlarının temsilcilerini taklit eder (AT&T Cybersecurity, 2017). Bu manipülasyon, vishing saldırılarında olduğu gibi, kurbanın tanıdık isimlere güvenme konusundaki psikolojik yatkınlığını etkili bir şekilde istismar ederek saldırganların kötü niyetli hedeflerine ulaşmasını kolaylaştırır.

Sesli kimlik avı veya vishing, sesli kimlik hırsızlığı ile yakından ilişkilidir ancak ondan farklıdır. Çizelge 3.1'de vishing ve sesli kimlik hırsızlığı arasındaki temel farklar gösterilmiştir:

Çizelge 3.1. Genel olarak vishing ve sesli kimlik hırsızlığı arasındaki temel farklar

Saldırı Türü	**Vishing (Voice Phishing)**	**Sesli Kimlik Hırsızlığı (Voice Identity Theft)**
Tanım	Telefon veya sesli mesaj yoluyla sosyal mühendislik teknikleri kullanarak kurbanlardan hassas bilgiler elde etmeye çalışan bir dolandırıcılık yöntemi.	Bireylerin ses örneklerini ele geçirerek kimlik doğrulama sistemlerini aldatma veya dolandırıcılık amacıyla kullanma yöntemi.
Amaç	Kurbanı kandırarak şifre, kredi kartı bilgileri, kimlik bilgileri gibi hassas verileri ele geçirmek.	Kişinin sesini taklit ederek biyometrik sistemleri aşmak veya kurbanın yerine geçerek dolandırıcılık yapmak.
Teknikler	• Saldırganın güvenilir bir kişi (banka temsilcisi, polis, devlet görevlisi vb.) gibi davranması. • Aciliyet hissi yaratarak kurbanı hızlıca harekete geçirmeye zorlama. • Sahte çağrı merkezi numaraları kullanma.	• Yapay zekâ tabanlı ses klonlama ve deepfake teknolojileri. • Kayıtlı ses örneklerini kullanarak kimlik doğrulama sistemlerini aşma. • Biyometrik ses tanıma sistemlerine karşı saldırılar gerçekleştirme.
Teknoloji Kullanımı	Genellikle düşük seviyede teknik beceri gerektirir. Telefonla ikna edici konuşma becerisi temel yeterliliktir.	Yapay zekâ, makine öğrenmesi ve ses sentezi teknolojileri gibi daha sofistike teknikler içerir.
Saldırının Hedefi	İnsan faktörüne odaklanır. Kurbanın psikolojik manipülasyon yoluyla kandırılması amaçlanır.	Teknolojik sistemler hedef alınır. Biyometrik kimlik doğrulama mekanizmaları aşılmaya çalışılır.
Örnek Durumlar	• Kurbanın bankasından arandığını sanarak kredi kartı bilgilerini paylaşması. • Vergi dairesi çalışanı gibi davranarak sahte bir ceza bildirimi yapma. • Teknik destek birimi gibi davranarak hesap bilgilerini isteme.	• Banka veya devlet kurumlarının sesli kimlik doğrulama sistemlerinin ele geçirilmesi. • Yapay zekâ ile oluşturulan sahte seslerin dolandırıcılıkta kullanılması. • Telefon görüşmelerinde taklit edilen sesle, kurbanın yerine geçerek işlemler yapma.
Önleme Yöntemleri	• Şüpheli telefon aramalarına karşı dikkatli olunmalı. • Kişisel bilgileri paylaşmadan önce arayanın kimliği doğrulanmalı. • Telefon numarasının gerçekten ilgili kuruma ait olup olmadığı kontrol edilmeli.	• Ses biyometrisi kullanılan sistemlerde ek güvenlik önlemleri (çok faktörlü kimlik doğrulama) alınmalı. • Hassas konuşmaların kaydedilmesini önlemek için güvenli iletişim yöntemleri tercih edilmeli. • Yapay zekâ destekli sahte ses tespit sistemleri kullanılmalı.

Vishing, doğrudan bir kişiyi kandırarak hassas bilgilerini ele geçirme stratejisine dayanırken sesli kimlik hırsızlığı daha çok ses biyometrisini ele geçirerek kişinin yerine geçmeyi hedefler. Vishing saldırılarında saldırganlar genellikle sosyal mühendislik teknikleri kullanarak hedeflerinden şifreler, kredi kartı bilgileri veya kişisel veriler toplamaya çalışır. Buna karşılık sesli kimlik hırsızlığı, daha çok biyometrik kimlik doğrulama sistemlerini aşmayı ve kurbanın sesini taklit ederek yasa dışı işlemler yapmayı amaçlar. Ayrıca sesli kimlik hırsızlığı saldırısı, sesli iletişimlerde ve sistemlerde savunmasız olan yeni hesaplar

açma veya mevcut hesaplar üzerinden dolandırıcılık yapma gibi dolandırıcılık faaliyetlerinde çalınan kişisel olarak tanımlanabilir bilgilerin kullanımını da içerir (Kayser ve diğerleri, 2024).

Vishing'te olduğu gibi sesli kimlik hırsızlığı saldırılarında da genellikle saldırganın tanıdık veya güvenilen bir kişi gibi davranması ile karşılaşılır. Bu tür saldırılarda saldırgan, tanıdık veya güvenilen bir kişiden kaydedilen ses örneklerini veya sentezlenmiş konuşmayı da kötüye kullanabilir. Saldırganların bu tür saldırılarda kullandıkları yaygın taktiklerden biri, güven kazanmak için kurumsal kurumlardan veya bireylerden bilgi kullanmaktır. Bu yöntem, saldırganlar daha önceki araştırmalar veya sosyal medya aracılığıyla topladıkları belirli ayrıntıları dahil ettiklerinde daha da etkili hale gelir ve bu da finansal verilerin veya hatta kimlik bilgilerinin saldırganların eline geçmesine yol açabilir (Hussain ve diğerleri, 2021). "Güvenlik doğrulaması" bahanesiyle kişisel verileri talep etme gibi teknikler, kurbanın verilerini koruma içgüdüsünü istismar ederek saldırganın kritik bilgilere erişme amacını kolaylaştırır.

Ayrıca burada değerlendirilmesi gereken diğer bir nokta ise sesli kimlik hırsızlığı ve sesli kimlik dolandırıcılığı arasındaki farktır. Sesli kimlik hırsızlığı bir bireyin kişisel bilgilerinin veya ses verilerinin izinsiz olarak ele geçirilmesi ve kullanılmasını ifade eder; bu durum, genellikle kişisel bilgilere erişim sağlayarak bireyin kimliğini kopyalamak veya başka bir birey gibi hareket etmek amacıyla gerçekleştirilir (ABD Genel Hizmetler İdaresi, 2023). Sesli kimlik hırsızlığının en yaygın biçimleri arasında telefon aramaları, yapay zekâ destekli ses klonlama ve sosyal medya gibi platformlardan ses kayıtlarının ele geçirilmesi bulunmaktadır. Sesli kimlik dolandırıcılığı (voice identity fraud), bir başkasının kimliği kullanılarak maddi veya sosyal kazanç elde etmeye yönelik süreçleri kapsar (Avustralya Bilgi Komisyonu Ofisi, 2023). Bu dolandırıcılık, genellikle sesli aramalar yoluyla gerçekleştirildiği için vishing süreçleri ile de ilişkili olabilir. Ancak sesli kimlik hırsızlığından farklı olarak dolandırıcılık aşamasında hırsızlık yoluyla elde edilen bilgiler aktif olarak kullanılır. Sesli kimlik dolandırıcılığına saldırganların gerçek kişilerin ses verilerini kullanarak kredi veya kredi kartı başvurularında bulunabilmesi, başkalarının seslerini kullanarak yasa dışı gelir elde edilmesi, sesli yanıtlama sistemleri aldatılarak yetkisiz erişim sağlanması, yapay zekâ ile gerçek kişilerin seslerinin kopyalanması ve dolandırıcılık aramalarında bu seslerin kullanılması gibi örnekler de verilebilir. Çizelge

3.2'de sesli kimlik hırsızlığı ve sesli kimlik dolandırıcılığı arasındaki yukarıda sayılan farklılıklar gösterilmiştir:

Çizelge 3.2. Sesli kimlik hırsızlığı ve sesli kimlik dolandırıcılığı arasındaki farklılıkları gösteren çizelge

Saldırı Türü	**Sesli Kimlik Hırsızlığı**	**Sesli Kimlik Dolandırıcılığı**
Tanım	Bir kişinin ses verilerinin izinsiz olarak ele geçirilmesi.	Ele geçirilen ses verilerinin dolandırıcı amaçlarla kullanılması.
Amaç	Bilgileri saklamak, gelecekte kullanmak veya satmak.	Kimlik bilgileri finansal kazanca dönüştürmek.
Yöntem	Telefon dinleme, sosyal medya, yapay zekâ destekli ses toplama.	Sahte aramalar, deepfake teknolojisi, sosyal mühendislik taktikleri.
Zamanlama	Bilgiler ele geçirildikten sonra dolandırıcılığın başka bir aşamada gerçekleştirilmesi.	Kimlik hırsızlığından hemen sonra veya aynı anda gerçekleştirilmesi.
Örnek Durumlar	Ses kaydının izinsiz ele geçirilmesi.	Ses kaydı kullanılarak banka hesabından para çekilmesi.

Sesli kimlik hırsızlığı saldırıları genellikle sosyal mühendislik ilkelerine dayalı daha kapsamlı manipülasyonları içerir. Saldırganlar, hedeflerinin hızlı bir şekilde harekete geçmesini sağlamak için psikolojik baskı uygulayarak bir korku veya aciliyet duygusu yaratırlar. Böylece kurban, yaşadığı olayın bir yanılsama olduğunu fark etmeden zarar görür. Örneğin saldırganlar, hemen harekete geçilmezse kurbanın banka hesabının bloke edileceğini iddia edebilir ve yeterli düşünmeden kişisel verileri hızla paylaşmaya zorlayabilir (Siddiqi ve diğerleri, 2022).

Bireyler arasında farkındalık yaratmak, sesli kimlik hırsızlığını önlemede büyük önem taşır. Mağdurlar, bilinmeyen numaralardan gelen aramalara karşı dikkatli olmalı ve şüpheli yaklaşımlarla kişisel bilgi taleplerini değerlendirmelidir. Arayanın kimliğini resmi kanallar aracılığıyla doğrulamak veya kişisel verileri hemen paylaşmamak gibi basit adımlar, bu saldırılara kurban gitme riskini önemli ölçüde azaltabilir. Finans kuruluşları ayrıca, çok faktörlü kimlik doğrulama ve arayan doğrulama sistemleri gibi dolandırıcılık girişimlerini önlemeyi amaçlayan kullanıcı eğitim programları ve teknolojik önlemler yoluyla kamuoyunun farkındalığını artırabilir.

Sonuç olarak sesli kimlik hırsızlığı saldırıları, yaygın olarak kullanılan ve giderek dijitalleşen bir ortamda büyük bir tehdit oluşturan sosyal mühendislik ve psikolojik manipülasyonun oluşturduğu risklerden birine örnektir.

SkyNews'in 2024 yılına ait bir haberine göre Hollywood yıldızı Scarlett Johansson, yapay zekâ tarafından piyasaya sürülen bir sohbet robotunun sesinin kendisine ürkütücü derecede benzer olması sebebiyle hukuki yollara başvurdu. Johansson, şirketin yeni sohbet robotu için seslendirme teklifi aldığını ancak kişisel nedenlerle bu teklifi reddettiğini belirtti. Sohbet robotunu geliştiren firma ise Johansson'un sesinin kullanılmadığını ve bu durumun bir taklit amacı taşımadığını savunsa da Johansson, şirketin kurucusunun niyetinin açık olduğunu iddia etti. Johansson, sesinin nasıl üretildiği konusunda netlik sağlamak amacıyla ilgili firmaya iki hukuki mektup gönderdiğini belirtti. "Kendi benliğimizin, eserlerimizin ve kimliğimizin korunması" konusunun günümüzde önem arz ettiğini vurguladı. İlgili firma bu sesin Johansson'un sesine benzemediğini ve bu durumun kasıtlı olmadığını öne sürerek sohbet robotunun sesini kullanmayı duraklattıklarını duyurdu. Bu olay, yapay zekânın ses taklitleri üzerinden bireylerin hakları ve kimliği üzerindeki etkilerini sorgulayan tartışmaları yeniden gündeme getirdi (SkyNews, 2024). Özellikle tanınan ve bilinen kişilerin seslerinin ele geçirilmesinin kolaylığı, sesli kimlik hırsızlığının yaygınlaşmasına ve bu şekilde etik kullanımı ya da bireylerin rızası olmaksızın verilerinin sömürülmesi konularında önemli bir örnek teşkil etmektedir.

Sesli kimlik hırsızlığına karşı alınabilecek güvenlik önlemleri, bireysel farkındalığın artırılmasının yanı sıra biyometrik kimlik doğrulama sistemlerinin daha dayanıklı hale getirilmesini de içermelidir. Öncelikle, ses biyometrisi ile kimlik doğrulama yapılan sistemlerde çok faktörlü kimlik doğrulama (MFA) kullanımı zorunlu hale getirilmelidir. Bu sayede yalnızca ses tanıma değil, ek bir doğrulama katmanı (örneğin SMS ile gönderilen tek kullanımlık şifreler veya fiziksel güvenlik anahtarları) gereklilik haline gelerek saldırı riskleri azaltılabilir. Ayrıca canlılık algılama (liveness detection) teknolojileri, bir kişinin ses kaydının mı yoksa gerçek zamanlı konuşmasının mı kullanıldığını ayırt edebilir. Derin öğrenme tabanlı sahte ses tespit sistemleri, sahte veya yapay zekâ destekli klonlanmış sesleri analiz ederek anormal desenleri tespit edebilir. Kurumlar açısından büyük ölçekli şirketlerin ve finans kuruluşlarının tehdit istihbaratı sistemlerini güncel tutarak sürekli olarak sesli kimlik saldırılarına karşı korunma stratejileri geliştirmesi gerekmektedir. Güvenlik eğitim

programları, çalışanların ve müşterilerin vishing ve sesli kimlik hırsızlığı saldırılarını erken tespit etmelerine yardımcı olabilir.

3.4. Fiziksel Ses Taklidi ile Gerçekleştirilen Saldırılar

Fiziksel ses taklidi, insanların seslerini benzeterek gerçekleştirilen dolandırıcılık ve siber saldırılarının giderek daha yaygın hale geldiği bir yöntemdir. Bu tür saldırılar, sesli iletişimin güvenlik açısından zayıf noktalarına dayanmaktadır. Ses taklidi, sosyal mühendislik saldırılarında yaygın olarak kullanılan bir tekniktir ve genellikle telefon dolandırıcılıklarından, kimlik hırsızlığından finansal sahtekarlıklara kadar çok çeşitli kötü niyetli amaçlarla kullanılır.

Fiziksel ses taklidi, genellikle bireylerin seslerini insan eliyle veya düşük teknoloji araçlarla benzetme sürecini içerir. Buradaki temel fark, yapay zekâ ve derin öğrenme tekniklerinin aksine doğal ses taklidinin daha manuel bir süreçle gerçekleştirilmesidir. Taklitçilerin sesin tonunu, hızını, aksanını ve vurgularını doğru bir şekilde kopyalamaları sahtekarlıkların başarı oranını artırır. Bunun sonucunda hedef kişi veya kurumlar genellikle sesin gerçek olduğuna inanarak yanıltılabilir.

Ses taklidiyle gerçekleştirilen saldırılarda, en yaygın yöntemlerden biri Bölüm 3.2'de anlatılan "vishing" adlı telefon dolandırıcılığıdır. Saldırganlar, genellikle bilinen bir sesle iletişime geçerek kurbanlarını kişisel bilgilerini, şifrelerini veya finansal bilgilerini paylaşmaya ikna etmeye çalışır. Ayrıca sesli komutlarla güvenlik protokollerinin aşılması da mümkündür, örneğin telefonla yapılan aramalarda bankalar veya kamu hizmetleri gibi kurumlardan gelen "gerçek" sesli komutların taklit edilmesiyle güvenlik sistemleri saldırganlar tarafından yanıltılarak aşılabilir.

Fiziksel ses taklidinin günümüzde YZ destekli tekniklerle (örneğin derin öğrenme algoritmalarıyla) daha da gelişmesiyle bu tür saldırılar daha da detaylanmış ve gelişmiştir. Ancak fiziksel yani manuel ses taklidi yine de birçok dolandırıcılıkta etkili bir yöntem olmaya devam etmektedir. Gerçekleştirilen dolandırıcılık teknikleri arasında kurbanların telefonla iletişimde oldukları sesi doğru bir şekilde taklit etmek, sık kullanılan sesli güvenlik sorularını yanıtlamak veya yanlış bir kimlik sunmak yer alır.

Fiziksel ses taklidi, sosyal mühendislik saldırılarının bir aracı olarak kullanıldığında, saldırganlar genellikle kurbanlarının güvenini kazanmak için sesli iletişim kurarlar. Bu saldırı türü insanların sesleriyle ilişkilendirdiği güven duygusundan yararlanarak kurbanların tedbir almasını engellemeye çalışır. Bu kapsamda sesli kimlik hırsızlığı ve dolandırıcılık, geleneksel kimlik sahtekarlığından daha tehlikeli hale gelebilir, çünkü kurbanlar sesi tanıdık ve güvenilir bulurlar.

Sesin sahipliği kavramı ise bireyin kimliği ve mahremiyeti açısından önemli bir mesele olarak ele alınmaktadır. Tarih boyunca, sesin bir bireye ait olduğu fikri mitolojiler ve halk hikayelerinde işlenmiş ancak modern teknolojik gelişmelere kadar gündelik hayatta pek sorgulanmamıştır. Örneğin Yunan mitolojisinde Echo ve Narcissus hikayesi veya Andersen'in Küçük Deniz Kızı masalı, sesin zorla alınmasının birey üzerinde yarattığı psikolojik etkileri gösteren anlatılar arasındadır. Ancak günümüzde ses verileri, bireylerin izni olmaksızın toplanmakta, ticari veya devlet güdümlü amaçlarla kullanılmakta ve siber suçlular tarafından kötüye kullanılabilmektedir. Bu durum yalnızca bireysel mahremiyet açısından değil, aynı zamanda demokratik süreçlerin güvenliği ve kamu güvenilirliği açısından da ciddi tehditler oluşturmaktadır.

Sesin tanımlanması konusunda dilbilimciler dahi ortak bir görüşe varamamaktadır. Genel olarak insan sesi, vokal traktın (sesin üretim yolu) ürettiği ses dalgaları olarak tanımlansa da bu tanım konuşma seslerinin yanı sıra refleksif ve istemsiz sesleri de içermektedir. Ses sadece dilbilimsel açıdan anlam taşıyan konuşma seslerinden ibaret değildir; duygusal tepkileri ifade eden çığlıklar, kahkahalar, iç çekmeler gibi unsurlar da bireyin kimliğini belirleyen özellikler arasındadır. Sesin sahipliği meselesi bireyin mahremiyeti ve güvenliği açısından kritik bir konudur. Ses verileri kötü niyetli aktörler tarafından ele geçirilerek kimlik sahtekarlığı ve sosyal mühendislik saldırılarında kullanılabilir. Yapay zekâ destekli ses üretim teknolojileri, bireylerin kimliğini taklit etmeyi mümkün kılmakta ve bu durum biyometrik güvenlik sistemlerini risk altına sokmaktadır. Bu nedenle sesin hukuki ve etik açıdan sahipliğinin belirlenmesi, ses temelli siber saldırılarla mücadelede önemli bir adımdır.

Ses taklitçiliği ve aksan değişimi, dil bilimi ve nörobilim açısından da oldukça önemli bir konudur. Günlük hayatta uluslararası ortaklarla çalışan, farklı kökenlerden insanlarla aynı toplulukta yaşayan veya profesyonel olarak ses taklitçiliği yapan bireyler için aksan, sürekli kullanılan ve karşılaşılan bir olgudur. Frontiers in Human Neuroscience dergisindeki bir

editoryal yazıda belirtildiği gibi "Konuşma dili aksansız var olamaz." Dil ediniminde taklit önemli bir rol oynar. Çocuklar ana dillerini öğrenirken hem kelimeleri hem de dilin ritmini ve vurgu özelliklerini taklit ederler. Yetişkinler için ise ikinci bir dili aksansız konuşmak zorlaşır. Taklit ayrıca eğlence amaçlı da kullanılır. Taklit sanatçılarının başarılı olabilmesi için hedefledikleri kişinin konuşma biçimini, ritmini ve belirgin ses özelliklerini dikkatlice incelemeleri gerekir. Aksan, dilin gelişimi açısından kritik bir unsurdur. Scientific American'a göre yeni aksanlar, izole edilmiş konuşmacı gruplarının kelimeleri telaffuz etme biçimlerinde neredeyse algılanamaz değişiklikler yapmasıyla ortaya çıkar. Bu küçük farklılıklar zamanla yeni dillerin doğmasına yol açabilir.

Aksan edinimi doğum öncesi dönemde başlar. Journal of Voice and Speech, Language, and Hearing'de yayımlanan Katherine Wermke'nin iki çalışması, bebeklerin ağlama şekillerinin bile aksan taşıdığını göstermektedir. Almanca ve Mandarin Çincesi konuşan ailelerden gelen bebekler incelendiğinde, tonal diller konuşulan evlerde büyüyen bebeklerin ses perdelerinin daha yüksek olduğu görülmüştür. Bu bulgular, bebeklerin daha doğmadan aksan, tonlama ve perde farklılıklarını öğrendiğini göstermektedir.

Aksan değişimi, bireylerin sosyal çevresine ve izolasyon düzeyine bağlı olarak farklı şekillerde gerçekleşir. Linguistic Society of America tarafından yapılan bir araştırmada Big Brother UK adlı reality show'un katılımcılarının aksanları incelenmiştir. Araştırmacılar, katılımcıların konuşmalarında günlük küçük dalgalanmalar olduğunu, ancak uzun vadede belirgin bir aksan değişikliği yaşanmadığını tespit etmiştir. Üç ay boyunca kapalı bir ortamda sürekli etkileşim halinde olmalarına rağmen katılımcılar aynı aksanı benimsememiştir. Bu da göstermektedir ki aksan değişimi, bireyin maruz kaldığı dile sürekli temas etmesiyle hemen gerçekleşmez; aksine kişisel, nörolojik ve sosyal faktörlerden etkilenir.

Aksanların doğrudan değişmemesi, ses taklitçilerinin nasıl farklı aksanlar edinebildiği sorusunu gündeme getirir. University of California at San Francisco araştırmacılarına göre, bireyin ana dili ile sonradan öğrendiği diller arasında nöroplastisite ve stabilite arasında bir denge bulunmaktadır. Beynin öğrenmeye açık yapısı yeni aksanların benimsenmesini sağlarken mevcut aksanın korunmasını da garanti eder.

Ancak aktörlerin ve ses taklitçilerinin yeni aksanlar edinmesi beyin kimyasındaki değişimlerle değil, doğrudan mimikri yani taklitçilik ile gerçekleşir. Live Science'a göre ses

taklitçileri, ana dili konuşan bireyleri dinleyerek ve onları mekanik olarak taklit ederek aksanları öğrenir. Ses koçları, oyuncuların ağızlarını farklı şekillerde hareket ettirmelerini sağlayarak belirli sesleri üretmelerine yardımcı olur. Bu süreç yalnızca kelimelerin nasıl telaffuz edildiğini öğrenmekle kalmaz, aynı zamanda konuşma ritmi ve kalıplarının da özümsenmesini içerir.

Vantrilokluk, sesin kaynağını değiştirerek başka bir yerden geliyormuş gibi gösteren bir konuşma tekniği olarak tanımlanır. Genellikle bir ses taklidi sanatçısının (vantrilok) kukla ile sahne performansı sergilediği bu teknik, tarihsel süreçte hem eğlence hem de kehanet amacıyla kullanılmıştır (Ramati ve Abeliovich, 2022). Kelime kökeni Yunanca engastrimythos terimine dayanmakta olup Latinceye ventriloquist olarak çevrilmiştir. Connor (2000), bu terimi sesin konuşan kişinin dışından geldiği illüzyonunu yaratmaya yönelik bir ifade biçimi olarak tanımlamaktadır.

Teknolojik gelişmelerle birlikte sesin manipülasyonu yeni bir boyut kazanmış ve algoritmik vantrilokluk kavramı ortaya çıkmıştır. Dijital asistanlar (örneğin Siri ve Alexa), kullanıcılarla insan benzeri konuşmalar gerçekleştirebilmek için önceden programlanmış yanıtlar üretmekte ve sesi bir yapay zekâ aracı olarak kullanmaktadır (Ramati, 2024).

Drenten ve Psarras (2021), sosyal medyanın bu yeni vantrilokluk biçimi için önemli bir alan sunduğunu çünkü seslerin kökenlerinden bağımsız olarak yeniden üretilebildiğini vurgulamaktadır. Algoritmik vantrilokluk, insan sesi ile yapay üretim arasındaki sınırları bulanıklaştırarak kimlik, mahremiyet ve otantiklik kavramlarını yeniden tartışmaya açmaktadır.

Vantrilokluk, sesi bir kaynaktan farklı bir yerden geliyormuş gibi gösterme sanatıdır ve tarih boyunca eğlence, kehanet ve hatta tıbbi bağlamlarda kullanılmıştır. Ancak günümüzde bu kavram, yalnızca sahne sanatlarıyla sınırlı kalmayıp sesin manipülasyonu bağlamında geniş bir perspektife oturmuştur. Algoritmik vantrilokluk ile yapay zekâ destekli ses taklidi teknolojileri gündeme gelse de fiziksel yani manuel ses taklidi yani bireylerin bilinçli olarak başkalarının seslerini taklit etmesi halen geçerliliğini koruyan bir durumdur. Özellikle dolandırıcılık, kimlik sahtekarlığı ve sosyal mühendislik saldırıları bağlamında manuel ses taklidi çeşitli riskler barındırmaktadır.

Manuel ses taklidi bireylerin doğrudan kendi ses tellerini, ağız yapısını ve nefes kontrolünü kullanarak bir başkasının sesini mümkün olduğunca aslına uygun bir şekilde taklit etmesi sürecidir. Bu beceri, doğuştan gelen bir yetenek olabileceği gibi sistemli bir eğitim süreciyle de geliştirilebilir. Profesyonel ses sanatçıları, taklit yeteneklerini geliştirirken hem kulaklarını hem de seslerini eğiterek belirli ses frekanslarını, vurgu sistemlerini ve konuşma ritimlerini kopyalamayı öğrenirler.

Ses taklidini etkileyen faktörler arasında konuşmacının ses perdesi, tonu, vurgulama biçimi, ağız ve boğaz yapısı ile nefes kontrolü yer almaktadır. Profesyonel ses sanatçıları, hedefledikleri kişinin ses rengini, aksanını, konuşma hızını ve belirli kelimeleri nasıl vurguladığını dikkatlice analiz ederek taklit sürecini en doğal hale getirmeye çalışırlar. Bu süreçte kullanılan teknikler arasında şunlar yer almaktadır:

- Dikkatli dinleme: Taklit edilecek sesin detaylarına odaklanarak belirli kalıpların ve frekansların analiz edilmesi.
- Fonetik analiz: Sesin nasıl şekillendirildiğini anlamak için kelimelerin telaffuz biçimlerinin incelenmesi.
- Ağız ve nefes kontrolü: Konuşmacının dudak, dil ve çene hareketleriyle birlikte nefes tekniğinin taklit edilmesi.
- Tekrar ve pratik: Sesin doğal hale gelmesi için sürekli alıştırma yapılması.

Ses taklidi yeteneği genel olarak ses sanatçıları, aktörler ve mizahçılar tarafından eğlence ve gösteri amaçlı olarak kullanılmaktadır. Ancak manuel ses taklidinin kötüye kullanımı da mümkündür ve özellikle dolandırıcılık ile kimlik sahtekarlığı gibi siber suçlar bağlamında önemli bir güvenlik riski oluşturmaktadır. Siber saldırganlar, hedefledikleri kişilerin sesini taklit ederek sosyal mühendislik saldırıları gerçekleştirebilmekte, özellikle finansal dolandırıcılık ve kurumsal güvenlik ihlallerinde manuel ses taklidinden faydalanmaktadırlar.

Bu tür saldırılar, genellikle telefon üzerinden gerçekleştirilen sosyal mühendislik teknikleriyle ilişkilidir ve hedef kişinin güvenini kazanarak hassas bilgilere erişmeye yöneliktir. Siber saldırganlar, ses taklidi kullanarak kimlik doğrulama süreçlerini atlatabilir, özel bilgileri ele geçirebilir veya kurbanları manipüle edebilir.

- Vishing (Voice Phishing) Saldırıları: Vishing, geleneksel phishing saldırılarının sesli versiyonudur ve genellikle telefon görüşmeleri aracılığıyla gerçekleştirilir. Saldırgan,

hedeflediği kişinin sesini taklit ederek bir banka yetkilisi, müşteri temsilcisi veya şirket yöneticisi gibi davranarak hassas bilgilere erişmeye çalışır. Özellikle büyük şirketlerde çalışan yöneticileri hedef alan bu saldırılar, finansal işlemleri yönlendirmek veya veri sızdırmak amacıyla kullanılmaktadır.

- CEO Dolandırıcılığı (Whaling Attack): Bu tür saldırılar, özellikle şirket çalışanlarını ve yöneticilerini hedef alır. Saldırgan, şirket CEO'sunun veya yöneticisinin sesini taklit ederek finansal işlemleri yönlendirme girişiminde bulunur. Büyük ölçekli firmalarda bir yöneticinin sekreterine veya muhasebe departmanına telefon ederek acil bir para transferi talep etmek gibi yöntemler kullanılabilir.
- Siyasi Manipülasyon ve Medya Manipülasyonu: Ses taklitçiliği, siyasi manipülasyon amacıyla da kullanılabilir. Örneğin bir siyasetçinin sesi taklit edilerek sahte bir telefon görüşmesi gerçekleştirilebilir ve bu kayıt kamuoyuyla paylaşılabilir. Manipüle edilen bu kayıtlar, hedeflenen kişinin itibarını zedeleyebilir ve kamuoyunda yanlış algılar oluşturabilir.
- Kişisel ve Kurumsal Veri Hırsızlığı: Saldırganlar, hedef kişinin arkadaşlarını, ailesini veya iş arkadaşlarını arayarak onların güvenini kazanabilir ve özel bilgilere ulaşabilir. Özellikle bankacılık sistemlerinde, müşteri kimlik doğrulama süreçlerinde sesli onay sistemlerinin kullanıldığı durumlarda saldırganlar manuel ses taklidi yaparak bu sistemleri aşmaya çalışabilir.

Manuel ses taklidi yoluyla gerçekleştirilen saldırılar, bireyler ve kurumlar açısından ciddi güvenlik riskleri taşıdığından bu tür saldırıları önlemek için hem bireysel hem de kurumsal düzeyde bazı önlemler alınmalıdır:

- Çok faktörlü kimlik doğrulama kullanımı: Sadece sesli onaya dayanan sistemler yerine ek güvenlik önlemleriyle kimlik doğrulama sağlanmalıdır.
- Eğitim ve farkındalık programları: Öğrenciler, çalışanlar ve yetkili kimseler ses taklidiyle gerçekleştirilen sosyal mühendislik saldırılarına karşı bilinçlendirilmelidir.
- Gelişmiş ses tanıma teknolojileri: Sesin biyometrik özelliklerini analiz eden ve yapay taklitleri ayırt edebilen güvenlik sistemleri geliştirilmelidir.
- Şüpheli çağrılara karşı prosedürler: Özellikle finansal işlemlerle ilgili talepler telefonla geldiğinde ek doğrulamalar yapılmalıdır.

Sonuç olarak fiziksel yani manuel ses taklidi, yalnızca bir sanat ve eğlence biçimi olmanın ötesine geçerek siber güvenlik tehditleri arasında önemli bir yer edinmiştir. Vantrilokluk ve ses taklitçiliği, tarih boyunca insanları eğlendiren ve merak uyandıran bir yetenek olarak görülse de modern dünyada bu yeteneğin kötü niyetli kullanımı giderek artmaktadır. Bu bağlamda teknolojik ilerlemelerle birlikte manuel ses taklidi ve onun potansiyel tehditleri üzerine daha fazla araştırma yapılması ve güvenlik önlemlerinin geliştirilmesi büyük bir önem taşımaktadır.

3.5. Deepfake Teknolojisi ile Gerçekleştirilen Saldırılar

Teknolojinin dünya çapında giderek daha fazla kullanılması ve yayılmasıyla yapay zekânın alt dalları olan makine öğrenimi ve derin öğrenme de daha karmaşık uygulamalar ve araçlarla insanlığın karşısına çıkmaktadır. Bu gelişmeler özellikle Metinden Konuşmaya (İngilizce olarak Text to Speech) teknolojisi açısından önemli bir potansiyel sunmaktadır. TTS teknolojisi, metni yapay insan sesine dönüştürerek sohbet robotu oluşturma ve sanal asistanlar gibi birçok uygulamada kullanılmaktadır. Ancak bu teknolojinin en büyük sınırlamalarından biri, üretilen seslerin genellikle doğal olmayan ve robotik tınılara sahip olmasıdır. Bu sorunun üstesinden gelmek amacıyla geliştirilen Ses Klonlama (Voice Cloning) teknolojisi, belirli bir kişinin sesini klonlayarak daha doğal ses örnekleri oluşturmayı mümkün kılmaktadır. Bununla birlikte bu tür teknolojilerin gelişmesiyle ses ve video manipülasyonları da giderek yaygınlaşmış, "deepfake" olarak adlandırılan içerikler üretilmeye başlanmıştır. Önceleri yalnızca uzmanlar tarafından erişilebilen bu teknoloji, artık herkesin kullanımına açık hale gelmiş ve toplumda teknolojiye karşı bir güvensizlik ortamı oluşmasına neden olmuştur (Amezaga ve Hajek, 2022).

Deepfake, ilk kez 2017 yılında Reddit'te "deepfakes" adlı bir kullanıcının bu web sitesinde farklı bir aktörün yüzüyle sahte bir video göndermesiyle ortaya çıkmıştır. Bu yeni teknolojinin ortaya çıkmasıyla portre hakları, itibar hakları ve telif hakları gibi kişisel haklar ile işletmelere zarar veren çeşitli ekonomik ve itibari zararlar doğuran yasal zorluklar da kaçınılmaz hale gelmiştir. Ayrıca bir politikacının veya hükümetin Deepfake ile yapılan uydurma bir videosunun yayınlanması medya krizine, sosyal istikrarsızlığa ve ulusal istikrarsızlığa neden olabilecektir (Hamza ve diğerleri, 2022).

Deepfake, yapay zekâ teknolojileri kullanılarak geliştirilen veya değiştirilen ve otantik olarak kabul edilmesi amaçlanan sentetik bilgi veya materyalleri ifade eder. Bunlar ses, video, resim ve metin sentezini içerir (Shaaban ve diğerleri, 2023). Resim 3.1'de temsili bir görsel üzerinde bir saldırganın medya sentezi ile deepfake içeriği oluşturması gösterilmiştir:

Resim 3.1. Bir saldırganın deepfake içeriği oluşturması sürecine ilişkin temsili bir görsel

Deepfake teknolojisi bir kişinin yüz ifadelerini, hareketlerini, sesini ve tonunu taklit etmeyi öğrenmek için büyük veri örneklerini analiz eden sinir ağlarına dayanır. Bu süreç, iki farklı kişinin görüntülerini ya da yüzlerini değiş tokuş etmek için derin öğrenme algoritmalarını da kullanmayı gerektirir (Westerlund, 2019). Temel mantık, derin öğrenme algoritmalarının temel bileşeni olan bir dizi yapay sinir ağını, aktör ve hedef yüzlerin çok çeşitli örnekleri üzerinde eğitmektir. Yeterli eğitimle bu sinir ağları, her bir yüzün özelliklerini sayısal olarak temsil edebilecektir. Böylece tek yapılması gereken, aktörün yüzünü hedefle eşleştirmek için sinir ağlarını yeniden yapılandırmaktır (Dickson, 2020).

Deepfake teknolojisinin gelişimiyle yüz ve ses değişim süreçleri daha karmaşık ve gerçekçi hale gelmiştir. Özellikle çekişmeli üretici ağlar (İngilizce olarak generatif adversarial networks, kısaltması GANs) ve dönüştürücü tabanlı modeller gibi ileri düzey derin öğrenme algoritmaları, sahte görsel ve işitsel içeriklerin daha hızlı ve doğal bir şekilde üretilmesine olanak tanımaktadır (Goodfellow ve diğerleri, 2014). Bu süreçte makine öğrenimi modelleri yalnızca yüz özelliklerini değil aynı zamanda mikro ifadeleri, göz kırpma oranlarını ve doğal

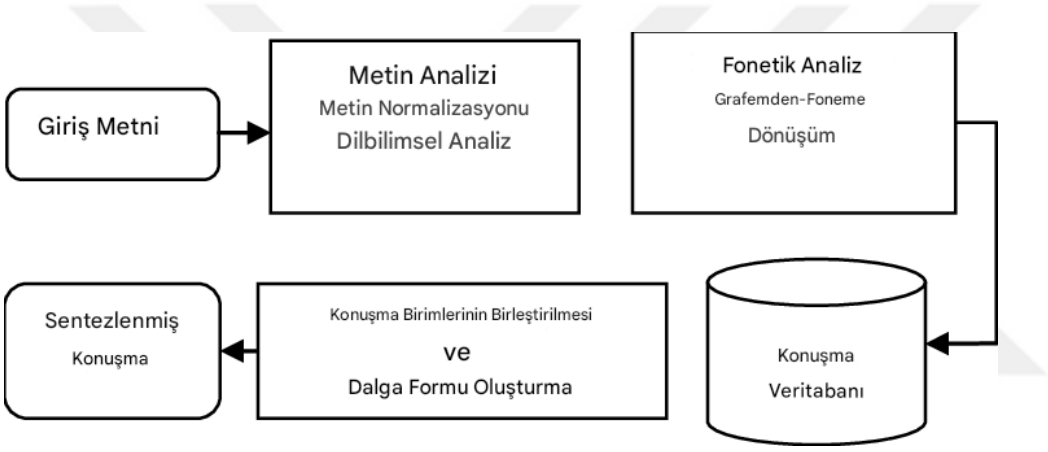
konuşma akışını da taklit edebilmekte; böylece yapay olarak üretilen içeriğin tespit edilmesini daha da zorlaştırmaktadır (Y. Li ve diğerleri, 2018). Bununla birlikte bu teknolojinin artan yaygınlığı ve erişilebilirliği, sahte içeriklerin kötüye kullanım potansiyelinin giderek hızlanmasını beraberinde getirmektedir.

İdeal bir yüz ve ses değişimini gerçekleştirebilmek için yüzlerin ve ortamların farklılıklarının daha iyi anlaşılması amacıyla çok çeşitli verilere ihtiyaç vardır. Bu noktada deepfake teknolojisi için kullanılmak istenen yüz hakkında ayrıntılı bir görüntü hafızası oluşturulmalıdır. Kaynak görüntüyü hedef görüntüyle senkronize etmek veya hedefin hareketlerini, jestlerini ve mimiklerini kaynak görüntüye göre yönlendirmek için derin öğrenme algoritmaları hedefin her bir hareketini hafızasında tutar. Bu nedenle gerçeğe yakın ve hipergerçekçi sahte videolar üretebilmek için kaynak kişinin, hedefin mümkün olan tüm açılardan çekilmiş çok sayıda görüntü ve ses kaydına sahip olması gerekir. Aksi takdirde gerçeklik algısının oluşturulabilme başarısı, algoritmadaki veri miktarının azalmasıyla birlikte düşecektir. Ayrıca deepfake video üretim sürecinde hedef her zaman bir hareketli görüntü olmayabilir; derin sinir ağları donuk kareler üzerinde de kullanılabilmektedir.

Deepfake teknolojisi, gerçeği manipüle etmede yalnızca görüntü verileri üzerinde işlem yapmakla kalmaz, aynı zamanda gerçeğin işitsel yansıtıcısı olan ses unsurlarında da derin sinir ağlarından faydalanır. Birinin sesini taklit etmek için ses çözücü kodlama süreci, görüntü öğrenimiyle benzer uzun ve detaylı bir süreçtir. Bu süreçte taklit edilecek hedef kişinin ağız hareketleri, vurgulamaları ve tonlamaları gibi belirleyici özelliklerini elde edebilmek için yine oldukça fazla veriye ihtiyaç duyulmaktadır. (Elitaş, 2022).

Bu kapsamda deepfake teknolojisi yalnızca görsel içeriklerin üretilmesiyle sınırlı kalmayıp ses sahtekarlığı (voice spoofing) ve ses klonlama (voice cloning) teknikleri ile de önemli bir tehdit unsuru haline gelmiştir. Sesli deepfake teknolojisi, belirli bir kişinin sesini taklit etmek için yapay zekâ ve derin öğrenme tekniklerini kullanarak sahte ses kayıtları üretme sürecidir (Kreuk ve diğerleri, 2020). Burada öncelikle hedef kişinin konuşma örnekleri toplanır ve bir ses modeli eğitilir. Gelişmiş sinir ağları, hedef kişinin ses tonunu, vurgularını, kelime aralarındaki duraksamalarını ve hatta nefes alıp vermesini dahi analiz ederek orijinal sese son derece yakın bir taklit oluşturabilir (L. Zhang ve diğerleri, 2021).

Sesli deepfake üretiminde yaygın olarak kullanılan yöntemlerden biri, metinden sese dönüşüm (Text to Speech, TTS) tabanlı sistemlerdir. Bu sistemlerde hedef kişinin sesiyle eğitilmiş bir model, herhangi bir metni bu kişinin konuşuyormuş gibi sentezleyebilir (Huang ve diğerleri, 2022). Alternatif olarak konuşma dönüştürme (İngilizce olarak Voice Conversion, kısaltması VC) teknikleri de kullanılabilir. Bu teknikler, bir kaynak konuşmacının sesini alarak hedef kişinin sesiyle eşleşecek şekilde dönüştürür. Özellikle SV2TTS (Speaker Verification to Text to Speech) gibi modern yaklaşımlar, yalnızca birkaç saniyelik ses kaydına dayanarak yüksek doğrulukta sahte sesler üretebilmektedir (Jin ve diğerleri, 2023). Şekil 3.2'de deepfake ile sentezlenmiş ses üretimine ilişkin bir şemaya yer verilmiştir:



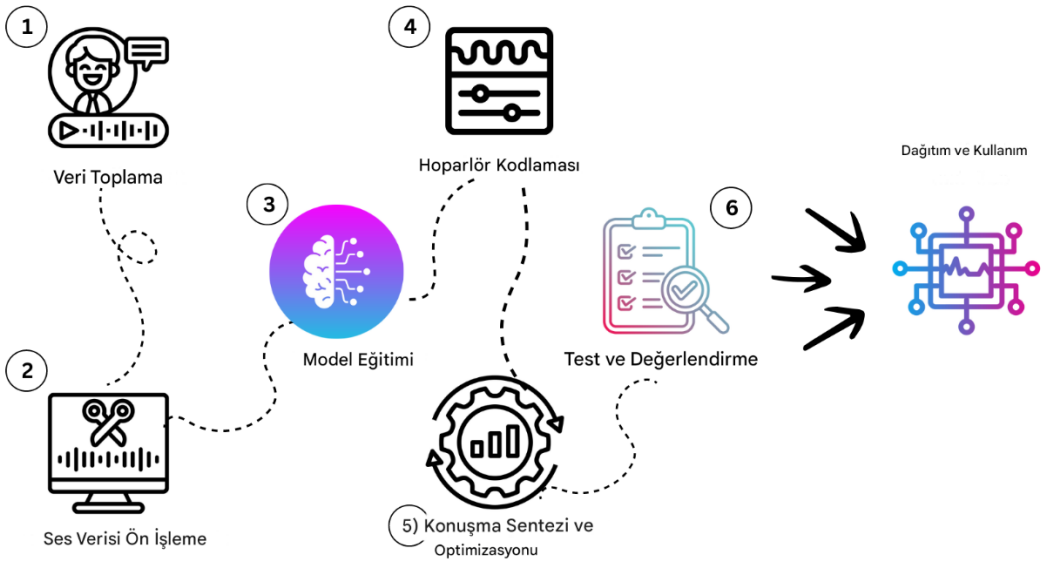
Şekil 3.2. Deepfake ile ses üretimine ilişkin bir şema (Mache, 2015)

Deepfake ile ses üretimi, yalnızca hedef kişinin sesinin birebir taklit edilmesini sağlamaz; aynı zamanda hedef kişinin sesini belirli duygularla veya farklı tonlamalarla yeniden üretme imkânı sunar. Örneğin bir politikacının sesini kullanarak onun hiç söylemediği bir konuşmayı yapıyormuş gibi göstermek mümkündür (F. Wu ve diğerleri, 2021). Aynı zamanda yapay zekâ destekli ses klonlama sistemleri, birden fazla sesi birleştirerek tamamen yeni ve sentetik bir ses de oluşturabilir (Xie ve diğerleri, 2020).

Son yıllarda yapılan çalışmalar, bu tür sahte seslerin insan kulağı tarafından ayırt edilmesinin giderek zorlaştığını göstermektedir. Yapılan deneylerde eğitimli dinleyiciler dahi deepfake ses kayıtlarını gerçek insan seslerinden ayırt etmekte zorlanmaktadır (Y. Tian ve diğerleri, 2023). Bunun temel sebebi, sinir ağlarının sesin mikro düzeydeki özelliklerini analiz ederek doğal ve akıcı konuşmalar üretebilmesidir. Bu durum, kimlik doğrulama sistemleri ve güvenlik uygulamaları için ciddi bir risk oluşturmaktadır. Bu nedenle deepfake ses

sahtekarlığının artan kullanımı siber güvenlik, dolandırıcılık ve bilgi güvenliği ihlalleri açısından önemli tehditler oluşturmaktadır. Özellikle kimlik sahtekarlığı ve finansal dolandırıcılık alanlarında deepfake destekli saldırılar giderek yaygınlaşmaktadır (Nguyen ve diğerleri, 2021). Yapılan araştırmalar, bu teknolojinin sahte sesli komutlarla bankacılık sistemlerine erişim sağlamaktan sosyal mühendislik saldırılarını daha ikna edici hale getirmeye kadar geniş bir yelpazede kötüye kullanılabileceğini göstermektedir (Tolosana ve diğerleri, 2020). Bu durum hem bireysel kullanıcılar hem de büyük kuruluşlar için ciddi bir güvenlik açığı oluşturmaktadır.

Deepfake teknolojisinin gelişimiyle bu teknoloji, çeşitli saldırı türlerinde ve kötü amaçlı kullanım senaryolarında giderek daha fazla yer edinmeye başlamıştır. Özellikle siber güvenlik, dezenformasyon ve dolandırıcılık bağlamında derin öğrenme tabanlı bu manipülasyon tekniklerinin kullanımı, bireyler ve kurumlar için önemli tehditler oluşturmaktadır (Chesney ve Citron, 2019). Şekil 3.3'te gelişen teknoloji sonucu meydana gelen türleri ile sesli deepfake oluşturma çemberine ait bir görsele yer verilmiştir:



Şekil 3.3. Sesli deepfake oluşturma çemberi (BotTalk, 2023)

Siber saldırganlar, deepfake teknolojisini kullanarak kimlik avı (phishing) ve sosyal mühendislik saldırılarını daha etkili ve zarar verici hale getirebilmektedirler. Geleneksel kimlik avı saldırılarında saldırganlar, sahte e-postalar veya mesajlar kullanarak kurbanlarını kandırırken deepfake tabanlı saldırılarda ses ve görüntü manipülasyonu da devreye

girmektedir. Özellikle deepfake ses klonlama teknikleriyle üst düzey yöneticilerin sesleri taklit edilerek çalışanlardan hassas bilgilerin alınması veya büyük meblağlarda para transferi yapılması sağlanabilmektedir (Mirsky ve Lee, 2021). 2019 yılında bir şirketin CEO'sunun sesi deepfake teknolojisiyle klonlanarak şirketin yöneticilerinden 243.000 dolarlık para ele geçirilerek bir dolandırıcılık gerçekleştirilmiştir (West, 2019).

Deepfake teknolojisinin fidye yazılımlarıyla (ransomware) entegre edilerek kullanılması da yeni tehditler arasında yer almaktadır. Saldırganlar, hedef kişilerin sahte görüntülerini ve ses kayıtlarını oluşturup bu materyalleri kullanarak mağdurları şantajla tehdit edebilmektedirler (Westerlund, 2020). Bu durum da bireylerin kişisel mahremiyetine yönelik ciddi bir tehdit oluşturmaktadır.

Deepfake teknolojisinin en yaygın kötüye kullanım alanlarından biri de yanlış bilgi yayma (disinformation) ve medya manipülasyonudur. Sosyal medya platformlarında yayılan sahte videolar, kamuoyunu yönlendirmek ve belirli politik veya ekonomik çıkarlar doğrultusunda algı oluşturmak amacıyla kullanılmaktadır (Vaccari ve Chadwick, 2020). Özellikle seçim dönemlerinde deepfake teknolojisi, sahte konuşmalar veya manipüle edilmiş görüntülerle kamuoyunu yanıltıcı içerikler üretmek için kullanılmaktadır. Örneğin 2020 ABD Başkanlık seçimlerinde deepfake teknolojisinin dezenformasyon kampanyalarında kullanılabileceği yönünde ciddi endişeler ortaya çıkmıştır (Garfinkel, 2022).

Ayrıca medya kuruluşları ve gazeteciler de deepfake teknolojisi nedeniyle ciddi tehditlerle karşı karşıya kalmaktadır. Geleneksel medya, manipüle edilmiş içerikleri tespit etmek için yeni doğrulama yöntemleri geliştirmek zorunda kalırken deepfake ile üretilmiş sahte haberlerin tespiti giderek zorlaşmaktadır (Agarwal ve diğerleri, 2019). Bu nedenle deepfake tespit algoritmalarının geliştirilmesi büyük önem taşımaktadır.

Biyometrik kimlik doğrulama sistemleri, güvenlik açısından önemli bir katman sağlasa da deepfake teknolojisinin gelişimiyle birlikte bu sistemlerin güvenilirliği sorgulanmaya başlanmıştır. Özellikle yüz tanıma sistemlerine yönelik gerçekleştirilen deepfake saldırıları, kimlik doğrulama süreçlerini riske atmaktadır (Dang ve diğerleri, 2020). Yapılan araştırmalar, deepfake ile üretilmiş yüz görüntülerinin birçok biyometrik sistem tarafından gerçek olarak algılanabildiğini göstermektedir (Jain, 2024).

Benzer şekilde ses biyometrisi de deepfake teknolojisiyle tehdit altındadır. Bankacılık ve finans sektöründe yaygın olarak kullanılan ses tanıma sistemleri, deepfake ses klonlama yöntemleriyle aşılabilmektedir (Tolosana ve diğerleri, 2020). Bu durum, finansal işlemlerde dolandırıcılık riskini artırmakta ve ses biyometrisine dayalı güvenlik önlemlerinin yeniden değerlendirilmesini gerektirmektedir.

Deepfake teknolojisinin yaygınlaşmasıyla birlikte, bireylerin ve toplumların medya içeriklerine olan güveni giderek azalmaktadır. İnsanlar, gördükleri veya duydukları içeriğin gerçek olup olmadığını sorgulamak zorunda kalmaktadırlar. Bu durum, dijital çağda bilgi güvenilirliğini zedeleyerek "gerçeklik krizi" (reality crisis) olarak adlandırılan bir olguyu ortaya çıkarmaktadır (Rini, 2020).

Ayrıca deepfake teknolojisi psikolojik ve sosyal boyutlarıyla da ele alınmalıdır. Deepfake mağdurları, kişisel ve mesleki itibarlarının zarar görmesi nedeniyle travma yaşayabilmekte, bu da sosyal mühendislik saldırılarının etkisini artırmaktadır (Chesney ve Citron, 2019). Bu nedenle bireylerin dijital okuryazarlık düzeylerinin artırılması ve deepfake içerikleri ayırt edebilme yeteneklerinin geliştirilmesi büyük önem taşımaktadır.

Deepfake saldırılarını önlemek ve tespit etmek için çeşitli yöntemler geliştirilmiştir. Bunlar arasında yapay zekâ destekli deepfake tespit sistemleri, blok zinciri tabanlı doğrulama mekanizmaları ve eğitim programları yer almaktadır (Verdoliva, 2020). Özellikle Convolutional Neural Networks (CNN) ve Recurrent Neural Networks (RNN) gibi derin öğrenme tabanlı algoritmalar, deepfake içeriklerinin tespitinde yaygın olarak etkin şekilde kullanılmaktadır (Afchar ve diğerleri, 2018).

Ayrıca hükümetler ve teknoloji şirketleri deepfake teknolojisinin kötüye kullanımını engellemek için çeşitli yasal ve teknik önlemler almaktadır. Avrupa Birliği ve ABD, deepfake içeriklerin belirlenmesi ve yayılmasını önlemek amacıyla çeşitli yasal düzenlemeler getirmiştir (Maras ve Alexandrou, 2019).

Sesli deepfake konusunda aşağıda detaylandırılan derin öğrenme yöntemleri, teknik süreçler, saldırı yöntemleri ve savunma mekanizmaları bu konunun temelini oluşturmaktadır:

- Derin öğrenme ve yapay sinir ağları: Sesli deepfake'ler, genellikle derin öğrenme algoritmalarına dayanır. Özellikle Generative Adversarial Networks (GANs) ve

Variational Autoencoders (VAEs) gibi yöntemler, sahte seslerin üretilmesinde yaygın olarak kullanılır. GAN'lar bir "üretici" ağ ve bir "ayırıcı" ağ arasında rekabetin olduğu bir sistemle çalışır. Üretici ağ, sahte sesler üretirken, ayırıcı ağ bu seslerin gerçek mi yoksa sahte mi olduğunu belirlemeye çalışır. Bu iki ağ arasındaki mücadele, sahte seslerin giderek daha gerçekçi hale gelmesini sağlar.

- Teknik süreç ve veri kümesi: Sesli deepfake üretiminde geniş veri kümeleri kullanılır. Bu veri kümeleri farklı konuşma tarzlarını, aksanları, duygusal tonları ve diğer ses özelliklerini içerir. Derin öğrenme modelinin doğru bir şekilde çalışabilmesi için çok büyük miktarda ses verisi gereklidir. Bu veriler sesin doğru şekilde analiz edilmesi ve taklit edilmesi için model tarafından öğrenilir. Bu model sesin pitch, tonlama, hız, akustik özellikler gibi öğelerini detaylı şekilde öğrenir.
- Ses sentezleme teknikleri: Ses sentezlemede WaveNet gibi modeller sıklıkla kullanılır. WaveNet, her bir ses dalgasını tahmin ederek doğal ve akıcı sesler üretmeye olanak tanır. Bu model, belirli bir ses parçasını her bir ses dalgasının frekansını ve genliğini öğrenerek yeniden üretebilir. Bunun yanı sıra Text to Speech (TTS) ve ses klonlama teknolojileri de deepfake sesler üretmek için kullanılır. TTS, yazılı metni sesli hale getirmek için kullanılırken, Voice Cloning bir kişinin sesini taklit etmek için özel olarak eğitilir.
- Saldırı yöntemleri: Sesli deepfake saldırıları genellikle sesli kimlik doğrulama sistemlerine karşı yapılır. Bu sistemler, bir kişinin kimliğini doğrulamak için ses özelliklerini kullanır (örneğin, bankacılık sistemleri). Ancak deepfake teknolojisiyle üretilen sesler, bu tür sistemleri yanıltabilir. Bu sebeple sesli kimlik doğrulama sistemleri güvenlik açıklarına sahip olabilir.
- Sesli kimlik hırsızlığı ve manipülasyon: Sesli deepfake teknolojisi, sesli kimlik hırsızlığını gerçekleştirmek için oldukça yaygın kullanılır. Saldırganlar, bir kişinin sesini deepfake aracılığıyla taklit ederek telefonla dolandırıcılık yapabilir ya da sosyal mühendislik saldırıları gerçekleştirebilir. Bu durum, özellikle bir kişinin sesinin çok yaygın kullanıldığı ve kolay tanınabilir olduğu durumlarda büyük bir tehdit oluşturur. Örneğin bir yöneticinin sesini taklit ederek şirketteki çalışanlardan gizli bilgileri çalmak mümkündür.
- Gelişen savunma teknikleri: Sesli deepfake tespiti için çeşitli savunma teknikleri geliştirilmiştir. Bu yöntemler arasında sesin doğal akışını inceleyen algoritmalar, sinyal işleme yöntemleri ve sesin "kötü" bölümlerini tespit etmeye yönelik makineler

yer alır. Ayrıca, sesin bazı biyometrik özellikleri, örneğin ses frekansları, mikrofon türü ve konuşma hızı gibi unsurlar analiz edilerek sahte seslerin tespiti sağlanabilir.

Sesli deepfake saldırıları, derin sinir ağları (Deep Neural Networks, DNNs) kullanılarak gerçekçi ve insan kulağı tarafından ayırt edilmesi zor olan sahte ses kayıtları oluşturma sürecini içerir. Bu süreç genel olarak üç ana adımdan oluşmaktadır: Veri toplama ve ön işleme, model eğitimi ve ses sentezi.

Veri toplama ve ön işleme:

Sesli deepfake üretiminde en kritik aşamalardan biri, hedef kişinin ses verisini elde etmek ve bu veriyi makine öğrenimi algoritmalarına uygun hale getirmektir.

Veri Kaynakları: Ses verisi, hedef kişinin konuşmalarından alınan açık kaynak verilerden (örneğin, YouTube konuşmaları, telefon kayıtları, röportajlar) veya kayıtlı özel veri setlerinden elde edilebilir.

Örnekleme Frekansı (Sampling Rate): Standart insan sesi genellikle 16kHz veya 44.1kHz frekansta işlenir. Daha yüksek örnekleme oranları (örneğin 48kHz) daha ayrıntılı bir sentezleme sağlar.

Mel-Frekans Kepstral Katsayıları (MFCCs): Sesin temel bileşenlerini çıkarmak için MFCC özellik çıkarımı yapılır. Bu yöntem, insan kulağının algıladığı frekans bileşenlerini ayırt ederek sesin daha gerçekçi modellenmesini sağlar.

Ön işleme sürecinde uygulanan işlemler:

- Gürültü temizleme ve filtreleme (Low-pass filtering, Gaussian noise removal)
- Ses normalizasyonu (Amplitude normalization)
- Zaman-frekans dönüşümleri (Fourier transform, Wavelet transform)
- Zarf analizi (Envelope extraction)

Bu işlemler, verinin deepfake modeline uygun hale getirilmesini sağlar.

Model eğitimi ve ses klonlama algoritmaları

Sesli deepfake saldırılarında iki temel derin öğrenme yöntemi kullanılır: Metinden Konuşmaya (Text to Speech, TTS) Modelleri ve Konuşma Dönüştürme (Voice Conversion, VC) Modelleri.

Metinden Konuşmaya (Text to Speech, TTS) Modelleri, belirli bir kişinin ses özelliklerini taklit etmek için eğitilmiş özel sinir ağları kullanır. Bu sistemler genellikle üç ana bileşenden oluşur:

- Akustik Model (Acoustic Model): Tacotron 2 veya FastSpeech gibi modeller, metni ses dalgasına dönüştürmek için kullanılır. Bu modeller, sembolik dil girdisini alarak Mel spektrogramları üretir. Örneğin Tacotron 2 modelinde WaveNet veya Griffin-Lim algoritması kullanılarak sentezleme yapılır.
- Ses Kodlayıcı (Vocoder): Üretilen Mel spektrogramlarını gerçekçi ses dalgalarına dönüştürmek için WaveNet, Parallel WaveGAN veya HiFi-GAN gibi modeller kullanılır.
- Duygusal ve Prosodik Manipülasyon: TTS modellerine prosodi bilgisi (tonlama, hız, vurgu) eklendiğinde, sahte ses duygusal tonlamalarla çok daha gerçekçi hale getirilebilir.

Konuşma Dönüştürme (Voice Conversion, VC) Modelleri ise bir kişinin sesini kaynak ses verisiyle eşleştirerek sahte bir ses üretir.

- Speaker Verification to Text to Speech (SV2TTS): SV2TTS, sadece 5-10 saniyelik bir ses kaydından hedef kişinin ses özelliklerini çıkararak herhangi bir metni o kişinin sesiyle söyleyebilir. Üç aşamalıdır: Speaker Encoder hedef kişinin ses kimliğini çıkarır, Synthesizer mel spektrogram üretir, Vocoder ses dalgalarına dönüştürür.
- AutoVC ve StarGAN-VC: Kaynak ses sinyalini zaman-frekans dönüşümleriyle hedef sese eşleştirerek dönüştürür. StarGAN-VC gibi modeller, farklı dillerde konuşan kişilerin bile seslerini dönüştürebilir.

Ayrıca ses klonlama sürecinde kullanılan bazı temel algoritmalar şunlardır:

- WaveNet (Google) yüksek kaliteli ses üretimi,

- WaveGlow (NVIDIA) gerçek zamanlı ses sentezi,
- StyleGAN-VC ise sesin duygusal tonlamasını değiştirmek için kullanılır.

Saldırı senaryoları ve güvenlik açıkları

Sesli deepfake saldırıları çeşitli alanlarda kullanılabilir:

- Kimlik doğrulama sistemlerini atlatma: Bankalar ve güvenlik sistemlerinde kullanılan ses biyometrisi tabanlı kimlik doğrulamalarını aşmak için deepfake sesler üretilebilir. Örnek: "Lütfen kimliğinizi doğrulamak için adınızı söyleyin." Deepfake ile üretilen sahte bir ses kaydı bu komutu yanıtlayabilir.
- Sosyal mühendislik ve dolandırıcılık: Bir yöneticinin sesinin kopyalanarak çalışanlardan banka havalesi veya gizli bilgi talep etmesi sağlanabilir. Örnek: "Bu dosyaları hemen şu adrese gönderin, acil bir durum var."
- Dezenformasyon ve manipülasyon: Politikacıların seslerinin taklit edilerek yanlış açıklamalar yapmaları sağlanabilir. Örnek: "Başkan şu an itibarıyla istifa ettiğini duyurdu."

Saldırıların gerçekleştirildiği bazı teknikler şunlardır:

- Adversarial Attacks: Düşman ağırlıklı eğitim (adversarial training) ile güvenlik sistemleri kandırılır.
- Data Poisoning: Yapay zekâ sistemleri yanlış veriyle eğitilerek manipüle edilir.
- Low-Latency Real-Time Deepfake: Bu teknikte gerçek zamanlı konuşmaları taklit eden düşük gecikmeli deepfake modelleri kullanılarak kişilerin ve kurumların manipülasyon edilmesi süreci kolaylaştırılmaktadır.

Sesli deepfake saldırıları, makine öğrenimi ve sinyal işleme tekniklerinin birleşimiyle oluşturulan oldukça detaylı ve karışık siber saldırılardır. Gerçek zamanlı deepfake üretimi giderek daha erişilebilir hale gelmektedir; bu da finans, güvenlik ve medya alanlarında ciddi güvenlik riskleri yaratmaktadır. Bu risklere ilişkin bazı güvenlik önlemleri aşağıda verilmiştir:

- Anormal durumlara duyarlı ses biyometrisi sistemleri geliştirilmelidir.

- Konuşmacı değişkenliğini (speaker variability) tespit eden derin öğrenme modelleri güçlendirilmelidir.
- Ses sinyallerinin spektrogram analiziyle manipülasyon izleri araştırılmalıdır.
- GAN tabanlı saldırılara karşı tersine mühendislik (reverse engineering) yöntemleri geliştirilmelidir.

Deepfake teknolojisi, gelişmiş yapay zekâ modellerinin sunduğu yenilikler sayesinde ses ve video manipülasyonlarını giderek daha gerçekçi hale getirmekte ve siber güvenlik tehditleri açısından önemli bir risk faktörü oluşturmaktadır. Çalışmanın bu bölümünde deepfake teknolojisi kullanılarak gerçekleştirilen ses tabanlı saldırılar detaylı şekilde ele alınmış, bu saldırıların bireyler, kurumlar ve ulusal güvenlik üzerindeki etkileri tartışılmıştır.

Özellikle finansal dolandırıcılık, kimlik avı (phishing), sosyal mühendislik saldırıları, yanlış bilgilendirme ve biyometrik güvenlik açıkları gibi alanlarda deepfake teknolojisinin kullanımı giderek yaygınlaşmaktadır. Saldırganlar, deepfake ile ses klonlama tekniklerini kullanarak üst düzey yöneticilerin veya bireylerin seslerini taklit etmekte, bu yolla şirketlerden hassas bilgileri ele geçirmekte ve büyük ölçekli mali kayıplara neden olmaktadırlar (Mirsky ve Lee, 2021).

Deepfake saldırılarının en tehlikeli yönlerinden biri, birçok mevcut güvenlik sisteminin bu tür tehditlere karşı yeterli koruma sağlayamamasıdır. Özellikle ses biyometrisine dayalı kimlik doğrulama sistemleri, deepfake ile üretilmiş ses kayıtlarını gerçek seslerden ayırt etmekte zorlanmaktadır. Yapılan araştırmalar, GANs tabanlı deepfake modellerinin sadece birkaç saniyelik bir referans ses kaydı kullanarak yüksek doğrulukta sahte sesler üretebildiğini ortaya koymuştur (Nguyen ve diğerleri, 2021). Bu durum, sesle kimlik doğrulama sistemlerini hedef alan saldırıların sayısının artmasına neden olmaktadır.

Deepfake saldırılarının siyasi ve sosyal manipülasyon açısından da ciddi sonuçları bulunmaktadır. Sahte videolar ve ses kayıtları, toplumsal algıyı yönlendirmek ve kamuoyunu manipüle etmek amacıyla kullanılmaktadır. Ukrayna Devlet Başkanı'nın deepfake kullanılarak hazırlanmış sahte teslimiyet konuşması, uluslararası düzeyde yanlış bilgilendirme kampanyalarının bir örneği olarak gösterilmektedir (Vaccari ve Chadwick, 2020). Bu tür saldırılar yalnızca bireyleri değil, ulusal güvenliği ve kamu düzenini de tehdit etmektedir.

Bu kapsamda çalışmanın bu bölümü deepfake teknolojisiyle gerçekleştirilen saldırıların etkilerini analiz etmiş ve bu saldırılara karşı alınabilecek önlemleri değerlendirmiştir. Deepfake tespit sistemleri ve çok faktörlü kimlik doğrulama yöntemleri gibi çeşitli güvenlik önlemleri geliştirilmekte olsa da saldırganların bu teknolojileri hızla uyarlaması nedeniyle mevcut çözümler yetersiz kalmaktadır.

Bu bölüm, aşağıdaki temel sonuçları ortaya koymaktadır:

- Deepfake tabanlı sosyal mühendislik saldırıları, büyük ölçekli finansal dolandırıcılıklara yol açmakta ve mevcut sesli kimlik doğrulama sistemlerinin güvenilirliğini sarsmaktadır.
- Ses biyometrisi gibi geleneksel kimlik doğrulama yöntemleri deepfake teknolojileriyle aşılabilmekte, bu da bankacılık ve kamu güvenliği sistemlerini tehdit etmektedir (Tolosana ve diğerleri, 2020).
- Deepfake ses ve video içerikleri siyasi amaçlarla yanlış bilgi yaymak için kullanılmakta, bu da seçim süreçlerinden kamu güvenliğine kadar geniş bir alanda risk oluşturmaktadır (Chesney ve Citron, 2019).
- Yapılan araştırmalar, mevcut deepfake tespit sistemlerinin yeni nesil sahte içerikleri tespit etmekte zorlandığını ve bu sistemlerin sürekli olarak güncellenmesi gerektiğini göstermektedir (Y. Tian ve diğerleri, 2023).

Bundan sonraki çalışmalar, deepfake saldırılarına karşı daha dayanıklı kimlik doğrulama sistemlerinin geliştirilmesi, tespit mekanizmalarının hassasiyetinin artırılması ve deepfake içeriğinin yayılmasını önlemek için yasal düzenlemelerin güçlendirilmesi gibi alanlara odaklanmalıdır. Özellikle yeni nesil yapay zekâ tabanlı tespit sistemleri (örneğin multimodal analiz ve Graph Attention Networks gibi yöntemler), bu saldırılara karşı savunmada önemli bir rol oynayabilir (Verdoliva, 2020).

3.6. Sesli Asistanlar Aracılığıyla Gerçekleştirilen Saldırılar

Sesli asistanlar, kullanıcıların sesli komutlar aracılığıyla dijital cihazlarla etkileşim kurmasına olanak tanıyan doğal dil işleme (NLP), makine öğrenimi ve yapay zekâ teknolojilerinin bir birleşimi olarak ortaya çıkmıştır. Bu sistemler kullanıcıların sorularına yanıt verme, hatırlatıcı ayarlama, cihaz kontrolü sağlama ve bilgi sunma gibi işlevleri yerine getirebilmektedir.

Sesli asistan teknolojisinin kökleri, 1950'li yıllara kadar uzanmaktadır. 1952 yılında Bell Labs tarafından geliştirilen Audrey isimli ilk ses tanıma sistemi, yalnızca bir kullanıcının sesinden İngilizce rakamları (0-9) tanıyabilmekteydi (Paay ve diğerleri, 2020). Bu gelişme, ses tanıma alanında atılan ilk adım olarak kabul edilmiş ve sonraki yıllarda yapılan çalışmalara öncülük etmiştir.

1970'li ve 1980'li yıllarda ses tanıma teknolojileri üzerinde yapılan çalışmalar hız kazanmış, örneğin IBM (International Business Machines, Türkçe adıyla Uluslararası İş Makineleri) tarafından geliştirilen Shoebox adlı sistem 16 kelimeyi tanıyabilen bir model olarak öne çıkmıştır (Nassif ve diğerleri, 2019). 1997 yılında IBM, tüketici pazarına yönelik olarak ViaVoice adlı ses tanıma yazılımını piyasaya sürmüştür. ViaVoice, kullanıcıların sesle metin yazmasına olanak tanıyarak kişisel bilgisayarlar üzerinde sesli etkileşim çağını başlatmıştır (IBM, 1997). Ancak bu dönemde sesli sistemlerin sınırlı doğruluk oranı, yüksek maliyeti ve işlem gücü gereksinimleri, teknolojinin yaygınlaşmasını engellemiştir.

1990'ların sonlarında internetin yaygınlaşmasıyla birlikte sanal asistan kavramı daha fazla ilgi görmeye başlamış olsa da o dönemlerde geliştirilen karakterler sesli asistanlardan ziyade grafik tabanlı yardımcılar olarak karşımıza çıkmıştır. Örneğin, 1997 yılında Microsoft tarafından tanıtılan Clippy, Microsoft Office kullanıcılarına yazılı içerik önerileri sunmayı amaçlayan bir animasyon karakteridir ve herhangi bir sesli tanıma yeteneğine sahip değildir (Bederson ve Shneiderman, 2003: 1, 432).

Sesli asistan teknolojisinin günümüzdeki halini almasındaki en önemli dönüm noktalarından biri, Apple'ın 2011 yılında tanıttığı Siri olmuştur. Siri, gelişmiş doğal dil işleme algoritmaları kullanarak kullanıcıların karmaşık sesli komutlarını anlayabilen, bağlam temelli yanıtlar verebilen bir yapay zekâ sistemidir (Lee ve diğerleri, 2012). Siri'nin başarısı Amazon'un 2014 yılında Alexa adlı sesli asistanını ve Google'ın 2016 yılında Google Assistant'ı geliştirmesine öncülük etmiştir (Hoy, 2018). Özellikle Alexa, akıllı ev cihazları ile entegrasyon yeteneği sayesinde kullanıcıların yaşam tarzlarını değiştirmiş; Google Assistant ise Google sistemine entegre edilerek dijital asistan teknolojisinin geniş kitlelerce benimsenmesini sağlamıştır.

Bunun yanı sıra sesli asistan teknolojisinin yaygınlaşması yalnızca bireysel kullanımla sınırlı kalmamış; kurumsal, sektörel ve yerleşik sistemlere entegre edilerek farklı kullanım

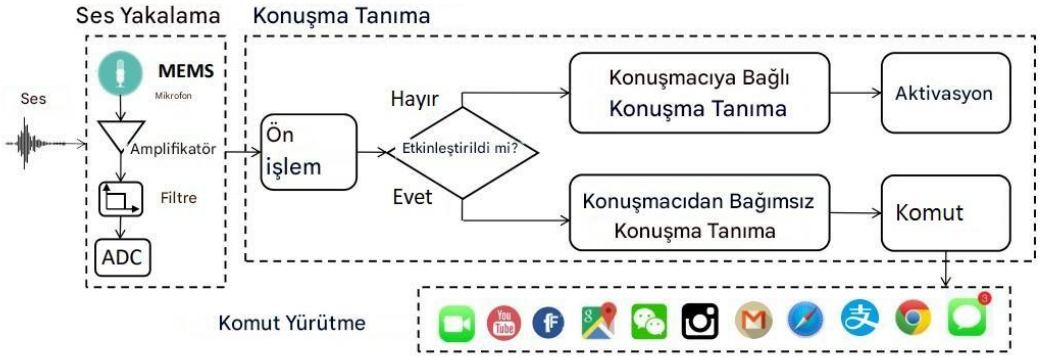
alanlarını da kapsayacak şekilde çeşitlenmiştir. Nitekim sesli asistanlar, işlevlerine ve kullanım ortamlarına göre çeşitli kategorilere ayrılmaktadır. Literatürde bu kategorilendirme genellikle mobil tabanlı sesli asistanlar, akıllı ev ve IoT cihazlarıyla bütünleşmiş sesli asistanlar ve kurumsal uygulamalar için geliştirilen sesli asistanlar şeklinde yapılmaktadır (Hoy, 2018; Nassif ve diğerleri, 2019). Mobil tabanlı sesli asistanlar, genellikle akıllı telefon ve tablet gibi taşınabilir cihazlarda yer alan, kişisel bilgiye erişimi kolaylaştıran uygulamalardır. Siri, Google Assistant ve Samsung'un 2017 yılında tanıttığı Bixby bu kategoriye örnek olarak gösterilebilir. Bu asistanlar, kullanıcıların kısa mesaj gönderme, hatırlatıcı kurma, arama yapma gibi gündelik işlevleri sesli komutlarla gerçekleştirmelerine olanak tanımaktadır.

Akıllı ev teknolojilerinin gelişimiyle birlikte, sesli asistanlar ev otomasyon sistemlerine entegre edilmiş ve bu bağlamda akıllı hoparlör tabanlı asistanlar ön plana çıkmıştır. Amazon Echo cihazları ile Alexa, Google Home ile Google Assistant ve Apple HomePod ile Siri, bu kategori altında değerlendirilmektedir (Lopatovska ve Williams, 2018). Bu tür cihazlar yalnızca bilgi sorgulama değil aynı zamanda ışıklandırma, güvenlik sistemleri, ev termostatı gibi cihazların sesli komutlarla kontrol edilmesine olanak sağlamaktadır. Ayrıca bazı bankacılık hizmetleri, müşteri ilişkileri yönetimi (CRM) uygulamaları ve çağrı merkezi çözümleri için geliştirilen kurumsal sesli asistanlar da önemli bir kullanım alanı oluşturmuştur. Örneğin IBM'nin Watson Assistant platformu, özellikle müşteri destek süreçlerinde insan müdahalesine ihtiyaç duyulmaksızın otomatik yanıt sistemleri kurmayı mümkün kılmaktadır (IBM, 2020).

Tüm bu kategorilerin ortak noktası, kullanıcı deneyimini kolaylaştırma amacı taşısa da farklı kullanım senaryoları, beraberinde farklı güvenlik ve gizlilik risklerini gündeme getirmiştir. Özellikle akıllı ev cihazlarında kullanılan sesli asistanlar, sürekli açık mikrofon yapısı sebebiyle çevresel sesleri sürekli dinlemekte ve bu durum, potansiyel ses tabanlı saldırılar için bir zemin oluşturmaktadır. Kurumsal uygulamalarda ise sesli asistanların hassas müşteri verilerine erişim sağlayabilmesi, bu verilerin üçüncü taraflarca kötüye kullanılma ihtimalini artırmaktadır.

Günümüzde sesli asistanlar, yalnızca bilgi edinme aracı olmaktan çıkarak alışveriş yapma, ev otomasyon sistemlerini kontrol etme, bankacılık işlemleri gerçekleştirme gibi oldukça karmaşık görevleri yerine getirebilecek düzeye ulaşmıştır. Ancak bu gelişim, beraberinde

ciddi güvenlik ve gizlilik risklerini de getirmiştir. Sesli asistanlar, sürekli olarak çevredeki sesleri dinleyen mikrofonlara dayanarak çalıştıkları için ses tabanlı siber saldırılara açık hale gelmişlerdir. Sesli asistanların ve komutların manipüle edilmesi akıllı evleri, sesle etkinleştirilen sanal asistanları ve diğer sesle kontrol edilen teknolojik sistemleri hedef alan önemli ve güncel bir siber güvenlik tehdididir. Bu sistemlerin modern yaşamda kullanımı (Amazon'a ait Alexa, Google'a ait Google Asistan ve Apple'a ait Siri gibi sesle etkinleştirilen kişisel asistanlardan sesle etkinleştirilen akıllı ev sistemlerine kadar) yaygınlaştıkça bu sistemlerin istismar edilme ve güvenlik ihlallerine maruz kalma potansiyeli de artmaktadır. Bu sistemler, ses dalgalarının frekansına, tonuna ve genliğine göre insan konuşmasını sentezleyebilen ve buna yanıt olarak çeşitli eylemler üretebilen ses tanıma teknolojisine dayanmaktadır (Naqvi ve diğerleri, 2023). Ancak mevcut ses tanıma teknolojileri bazı güvenlik açıkları sunmaktadır. Saldırganlar ayrıca yetkisiz sesli komutları yürütmek, özel bilgilere erişmek veya diğer kötü amaçlı eylemleri yürütmek için bu güvenlik açıklarını farklı şekillerde manipüle edebilirler. Bu nedenle sesli komut manipülasyonu yalnızca önemli bir güvenlik endişesi değil aynı zamanda birden fazla cihaz ve kullanıcı hesabı bağlandıkça büyüyen bir risktir. Bu saldırılar akıllı cihazların ses tanıma özelliğine odaklanır. En yaygın teknik, saldırganların önceden kaydedilmiş ses örneklerini kullandığı ve sesle etkinleştirilen akıllı bir cihaza komutlar vermek için bir hedefin sesini taklit ettiği ses sahteciliğidir. Bu teknikte, saldırgan kurbanın sesini kaydeder ve kapıları açmak veya yetkisiz satın almalar yapmak gibi bazı eylemleri gerçekleştirmek için kaydedilen sesi geri oynatır (Ansari ve Nazir, 2022). Şekil 3.4'te basit bir sesli komutu manipülasyonu saldırısının aşamalarına yer verilmiştir:



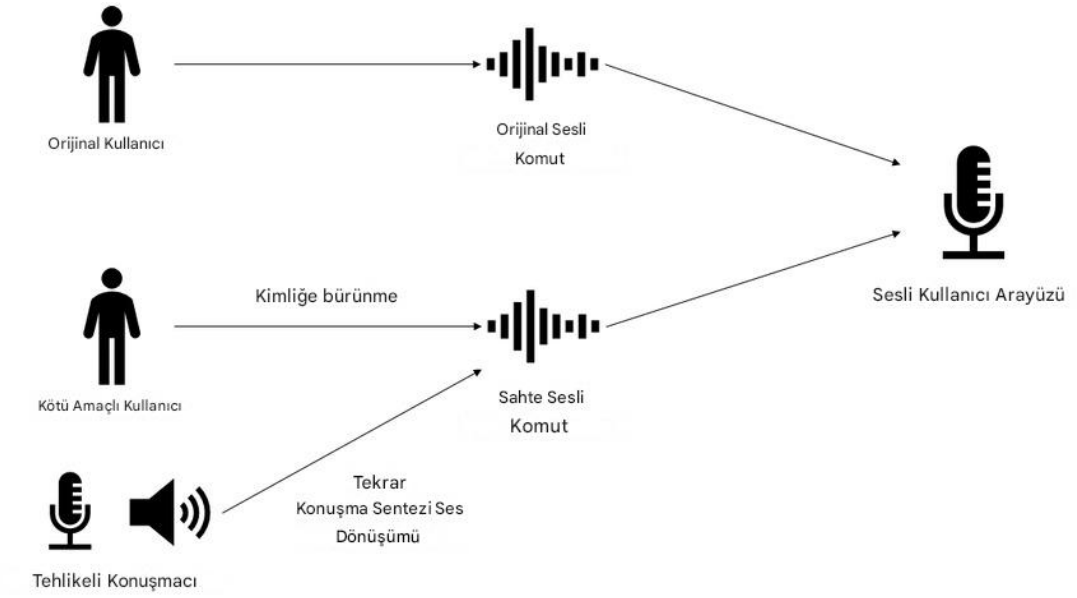
Şekil 3.4. Basit bir sesli komutu manipülasyonu saldırısının aşamaları (Zhang ve diğerleri, 2017)

Bu saldırılar genel olarak iki ana kategori altında sınıflandırılabilir: Ses Tanıma Manipülasyonu ve Yetkisiz Ses Komutları Gönderme.

Ses Tanıma Manipülasyonu, bir saldırganın hedef kullanıcının sesini taklit ederek veya kaydedip tekrar oynatarak sesli asistana komut vermesini içermektedir. Bu tür saldırılar, kullanıcının biyometrik ses verisinin kötüye kullanılması yoluyla asistanın yanıltılmasına ve kişisel bilgilerin ele geçirilmesine neden olabilir (Zhang ve diğerleri, 2017). Özellikle Voice Replay Attack ve Voice Spoofing Attack gibi yöntemler, sesli asistanların kimlik doğrulama mekanizmalarını aşmak için sıklıkla kullanılmaktadır.

Yetkisiz Ses Komutları Gönderme saldırılarında ise kullanıcıya ait olmayan bir ses kaynağı, asistanın komutlarını tetiklemek amacıyla kullanılır. Bu saldırı türü çoğunlukla çevresel sesler, medya yayınları ya da gizli ses sinyalleri aracılığıyla gerçekleştirilir. En dikkat çekici örneklerden biri, 2017 yılında gerçekleştirilen DolphinAttack çalışmasıdır. Bu çalışmada araştırmacılar, insan kulağının duyamayacağı 20 kHz üzerinde frekanslarla sesli asistanlara komut göndermeyi başarmışlardır (Zhang ve diğerleri, 2017). Benzer şekilde, 2018 yılında yapılan CommanderSong saldırısında, müzik dosyalarının içerisine gizlenmiş sesli komutlarla asistanların kontrol edilebileceği gösterilmiştir (Carlini ve Wagner, 2018).

Şekil 3.5’te temel bir diyagramda gösterilen bu saldırı türleri, kullanıcıların finansal verilerinin ele geçirilmesi, kişisel bilgilerinin açığa çıkması, cihaz kontrolünün kötü niyetli kişilerin eline geçmesi gibi sonuçlara yol açabilmektedir. Örneğin, bir saldırgan, evde açık bırakılan bir akıllı hoparlöre dışarıdan sesli komut göndererek kapı kilidini açabilir, online alışveriş yapabilir veya kişisel takvim bilgilerine erişebilir.



Şekil 3.5. Sesli asistanların ve komutların manipülasyonuna ilişkin genel diyagram (Hayashi ve Ruggiero, 2022)

Bu saldırı türünün meydana getirdiği tehditler karşısında hem kullanıcılar hem de geliştiriciler tarafından çeşitli önlemlerin alınması gerekmektedir. Bu önlemler arasında şunlar öne çıkmaktadır:

- Ses biyometrisi: Sesli asistanların yalnızca kayıtlı kullanıcının sesine tepki vermesi için gelişmiş ses biyometrik doğrulama sistemlerinin kullanılması.
- Komut doğrulama: Kritik komutlar için sesli asistanların ek bir doğrulama mekanizması (PIN kodu, mobil bildirim onayı) talep etmesi.
- Sesli komutların filtrelenmesi: Çevresel seslerden veya medya yayınlarından gelen olası saldırı komutlarının algılanmaması için algoritmalar geliştirilmesi.
- Kullanıcı bilinçlendirme: Kullanıcıların cihazlarının mikrofon ayarlarını kontrol etmeleri, yalnızca güvenli ağlar üzerinden asistan kullanmaları ve sesli komut geçmişlerini düzenli olarak temizlemeleri.

Ayrıca sesli asistan üreticilerinin sistemlerin sürekli dinleme modunda kaydedilen verileri şeffaf bir biçimde yönetmesi, belirli süre sonunda otomatik olarak silmesi ve bu verilerin üçüncü taraflarla paylaşımına izin vermemesi gerekmektedir. Bu risklere rağmen sesli asistanların modern yaşamı kolaylaştıran önemli teknolojik araçlar olduğu kaçınılamaz bir gerçektir. Ancak bu sistemlerin açık mikrofon altyapısına dayanması, onları ses tabanlı siber

saldırılar için potansiyel bir hedef haline getirmektedir. Saldırı yöntemlerinin çeşitlenmesi ve karmaşıklaşması, sesli asistanların güvenliği konusundaki farkındalığın artırılmasını ve teknik önlemlerin geliştirilmesini zorunlu kılmaktadır. Bu bağlamda sesli asistanlar aracılığıyla gerçekleştirilen ses tabanlı saldırıların sürekli olarak izlenmesi, analiz edilmesi ve etkili savunma stratejilerinin geliştirilmesi büyük önem taşımaktadır.

Sesli asistan teknolojilerinin kullanıcı deneyimini kolaylaştırma potansiyeli beraberinde önemli güvenlik açıklarını da getirmiştir. Bu açıklar, özellikle sesli komutların kötü niyetli kişiler tarafından manipüle edilmesi suretiyle gerçekleştirilen ses tabanlı siber saldırılar bağlamında dikkat çekmektedir. Resim 3.2'de sesli komutlar aracılığıyla manipüle edilen bir akıllı hoparlör dolayısıyla meydana gelen bir saldırı türü gösterilmiştir:

Resim 3.2. Bu örnekte sesli komutlar aracılığıyla manipüle edilen bir akıllı hoparlör dolayısıyla meydana gelen bir saldırı sonucu maddi zarar gerçekleşmiştir (Zhang ve diğerleri, 2019).

Sesli asistanlar aracılığıyla gerçekleştirilen saldırılar, temelde sistemin ses tanıma, doğal dil işleme ve komut yürütme mekanizmalarını hedef alarak kullanıcıların gizliliklerini ihlal etmeyi, yetkisiz erişim sağlamayı veya dolaylı yoldan maddi zarara yol açmayı amaçlamaktadır. Söz konusu saldırıların en yaygın yöntemlerinden bazıları şunlardır:

- Ses komutlarının manipülasyonu (command injection attacks): Sesli asistanlar tarafından algılanan komutların manipüle edilmesi, bu teknolojiye yönelik en yaygın

saldırı yöntemlerinden biridir. Bu tür saldırılar, genellikle iki ana teknikle gerçekleştirilir: Dolaylı ses enjeksiyonunda saldırgan, hedef kullanıcının ortamında sesli komut yayınlayarak cihazın bu komutu algılamasını sağlar; televizyondan, radyodan veya başka bir hoparlörden önceden kaydedilmiş veya sentetik olarak üretilmiş komutlar oynatılır ve özellikle "wake word" (örneğin, “Hey Siri”, “Alexa”) kullanıldıktan sonra kritik komutlar iletillir. Araştırmalar, bu yöntemin düşük seviyeli gürültü ortamlarında başarı oranının oldukça yüksek olduğunu göstermektedir (Zhang ve diğerleri, 2017). Ultrasonik komut enjeksiyonu (dolphinattack) ise Zhang ve arkadaşları tarafından 2017 yılında gerçekleştirilen bir çalışmada insan kulağının duyamayacağı 20 kHz üzerindeki ultrasonik frekanslarda sesli komutların gönderilerek sesli asistanların tetiklenebileceğini ortaya konularak meydana getirilmiştir. Bu saldırı türü, mikrofonların mekanik hassasiyetlerinden faydalanarak asistanın algılayabileceği ancak kullanıcı tarafından duyulamayacak komutların gönderilmesini sağlar (Zhang ve diğerleri, 2017).

- Ses taklidi (voice spoofing) ve sentetik ses saldırıları: Ses taklidi saldırıları, bir hedef kullanıcının ses özelliklerinin taklit edilerek sistemin kandırılmasına dayanır. Bu tür saldırılar aşağıdaki tekniklerle gerçekleştirilmektedir:
- Fiziksel ses taklidi: Saldırgan hedef kullanıcının ses tonunu, aksanını ve telaffuz biçimini taklit ederek sesli asistanı yanıltabilir. Bu yöntem manuel taklit becerisi gerektirse de özellikle hedef kişinin sesinin sıkça kamuya açık mecralarda yer aldığı durumlarda mümkündür (W. Wu ve diğerleri, 2015).
- Ses klonlama ve deepfake tabanlı saldırılar: Gelişmiş makine öğrenimi ve derin sinir ağı tabanlı ses sentezleme teknikleri, yalnızca birkaç dakikalık ses örneği kullanılarak herhangi bir kullanıcının sesini dijital ortamda klonlamayı mümkün kılmaktadır (Kurita ve diğerleri, 2020). Özellikle Tacotron, WaveNet gibi TTS modelleri ve Voice Conversion (VC) teknikleri kullanılarak sesli asistanlara hedef kullanıcının sesiyle komut gönderilebilir.
- Gizli komut yerleştirme (hidden voice commands): Bu saldırı yöntemi, sesli komutların insan kulağı tarafından algılanamayacak şekilde doğal seslerin içine gömülmesi esasına dayanır. Örneğin müzik veya arka plan gürültüsü içerisine yerleştirilen komutlar, sesli asistanın komut yürütme mekanizması tarafından algılanabilirken kullanıcı tarafından fark edilmez (Carlini ve diğerleri, 2016). Bu

teknik özellikle reklam videoları, YouTube içerikleri veya sosyal medya platformları aracılığıyla geniş çaplı saldırılara imkân sağlamaktadır.

- Sesli kimlik doğrulama sistemlerinin yanıltılarak atlatılması: Bazı sesli asistanlar, yalnızca tanımlı bir kullanıcının sesini algıladığında işlem gerçekleştiren kimlik doğrulama mekanizmalarına sahiptir. Ancak bu sistemler çeşitli yöntemlerle aşılabilmektedir: Ses kayıtlarının kullanımı ile saldırgan, hedef kullanıcının daha önceki konuşmalarından elde ettiği ses kayıtlarını kullanarak asistanı kandırabilir. Bu saldırı, özellikle sosyal medyada, podcastlerde veya telefon konuşmalarında ses kaydına maruz kalan kişilere yöneliktir. Adversarial ses örnekleri kullanımı da yaygındır. Makine öğrenimi tabanlı sesli asistanların zafiyetlerinden biri adversarial örnekler karşısındaki kırılganlıklarıdır. Bu saldırı türünde ses dalgasına küçük, insan kulağının algılayamayacağı seviyede gürültü (perturbation) eklenerek modelin yanlış komut algılaması sağlanır (Yakura ve Sakuma, 2018).
- Yan kanal saldırıları (side-channel attacks): Sesli asistanlara yönelik gelişmiş saldırı tekniklerinden biri de yan kanal saldırılarıdır. Bu yöntem, cihazın sesli yanıtlarından, işlem süresinden veya mikrofon hassasiyetinden faydalanarak sistem hakkında bilgi toplama esasına dayanır. Örneğin bir saldırgan, cihazın yanıt süresini analiz ederek cihazın kilitli olup olmadığını veya belirli bir uygulamanın açık olup olmadığını çıkarabilir (Apthorpe ve diğerleri, 2019).

Bu noktada özellikle sesli asistan teknolojisinin akıllı ev sistemleri (smart home technologies) ve akıllı hoparlörler (smart speakers) ile entegre edilmesi, saldırı alanını daha da genişletmiş ve ses tabanlı saldırıların etki alanını artırmıştır. Akıllı ev sistemleri; aydınlatma, ısıtma-soğutma, güvenlik kameraları, kapı kilit sistemleri, ev içi ağ kontrolü gibi işlevleri sesli komutlar aracılığıyla yönetmeye olanak tanımaktadır. Bu teknolojik kolaylık, saldırganların yalnızca bilgi güvenliğini değil, aynı zamanda fiziksel güvenliği tehdit eden saldırılar gerçekleştirmesine zemin hazırlamaktadır.

Özellikle smart speaker cihazlarının sürekli açık mikrofon modunda çalışıyor olması, ortamda fark edilmeden komut dinleme ve uygulama kapasitesini mümkün kılmaktadır. Bu durum, saldırganların fiziksel ortam dışında bulunarak çeşitli iletim kanalları (örneğin TV, radyo, video içerikleri veya Bluetooth bağlantısı) aracılığıyla sesli komutları cihazlara iletebilmesine olanak sağlamaktadır. Literatürde bu saldırılar, genellikle Remote Acoustic Injection Attacks veya Proximity-Based Attacks başlıkları altında incelenmektedir (Cheng

ve diğerleri, 2020). Saldırganların akıllı ev sistemlerini hedef alarak gerçekleştirdiği başlıca saldırı teknikleri şu şekilde özetlenebilir:

Öncelikle, akıllı kilit sistemlerinin (smart lock systems) hedef alındığı saldırılarda, saldırgan ortamda bulunmaksızın, önceden kaydedilmiş veya klonlanmış bir ses örneği ile "kapıyı aç" komutunu cihaz üzerinden iletebilir. Bu tür saldırılar özellikle sesli kimlik doğrulamanın pasif ve zayıf olduğu sistemlerde yüksek başarı oranına sahiptir. Ayrıca saldırganlar ev içi ağ (home network) yönetim komutlarını manipüle ederek bağlı IoT cihazlarını devre dışı bırakabilir, internet bağlantısını kesebilir veya güvenlik kameralarının kontrolünü ele geçirebilir.

Bir diğer riskli durum, akıllı ev otomasyon senaryolarının (smart home automation scenarios) kötüye kullanılmasıdır. Çoğu kullanıcı, sesli asistanlarına önceden tanımlı görev zincirleri atamakta; örneğin "evden çıkıyorum" komutuyla ışıkların kapanması, alarmın devreye alınması gibi işlevleri eşleştirmektedir. Saldırgan gizli bir ses komutu yerleştirerek bu otomasyon zincirlerini manipüle edebilir, alarm sistemini devre dışı bırakabilir veya enerji yönetim sistemlerini kontrolsüz şekilde çalıştırarak maddi zarar verebilir.

Smart speaker cihazlarının Bluetooth veya Wi-Fi üzerinden yetkisiz şekilde ele geçirilmesi (unauthorized device pairing) de saldırı tekniklerinden biridir. Saldırgan, cihazla aynı ağ üzerinde bulunduğunda veya Bluetooth sinyal aralığına girdiğinde hedef hoparlöre doğrudan bağlantı kurarak sesli komut iletme girişiminde bulunabilir. Bu teknik özellikle kullanıcıların cihaz ayarlarını varsayılan güvenlik düzeyinde bırakmaları durumunda başarıyla uygulanabilmektedir (Ren ve diğerleri, 2019).

Bununla birlikte son yıllarda literatürde dikkat çeken bir diğer saldırı yöntemi, siber-fiziksel saldırılar (cyber-physical attacks) kapsamında değerlendirilen sesli asistanlar üzerinden enerji şebekesi, güvenlik alarmı gibi kritik altyapıların dolaylı şekilde hedef alınmasıdır. Örneğin akıllı prizler, termostatlar veya aydınlatma sistemleri sesli komutlarla aşırı yük alarak cihaz arızasına veya yangın riskine yol açabilecek şekilde yönlendirilebilir (Truong ve diğerleri, 2021).

Bu saldırıların en tehlikeli noktalarından biri de çoğu zaman kullanıcı tarafından algılanamayacak şekilde gerçekleştirilmeleridir. Özellikle çoklu komut zincirleri (command

chaining) tekniği ile birden fazla komut, tek bir sesli komut içerisinde zincirleme olarak iletilebilmekte ve böylece saldırgan yalnızca bir etkileşimle birçok cihaz üzerinde işlem gerçekleştirebilmektedir. Bu saldırı türü, güvenlik açıklarının birden fazla cihazda zincirleme olarak sömürülmesine neden olmakta ve saldırının tespit edilmesini daha da zorlaştırmaktadır.

Son olarak akıllı ev sistemlerinin genellikle bulut tabanlı çalışması saldırganların yalnızca fiziksel ortamda değil, uzaktan da sesli asistan altyapısına yönelik saldırılar gerçekleştirmesini mümkün kılmaktadır. Sesli komutların bulut üzerinden işlenmesi sürecinde, veri iletim kanalları üzerinde yapılan man-in-the-middle (MitM) saldırıları, yetkisiz komut enjeksiyonu için potansiyel bir yöntem oluşturmaktadır. Buna göre sesli asistan teknolojisinin akıllı ev sistemleri ve smart speaker cihazlarıyla entegrasyonu, kullanıcı konforunu artırmakla birlikte, çok katmanlı ve geniş ölçekli siber saldırılara açık bir ekosistem yaratmıştır. Bu sistemler aracılığıyla gerçekleştirilen ses tabanlı saldırılar yalnızca dijital güvenlik risklerini değil, aynı zamanda fiziksel güvenlik tehditlerini de beraberinde getirmektedir. Bu nedenle sesli asistan tabanlı sistemler için hem yazılım hem de donanım düzeyinde çok katmanlı güvenlik önlemlerinin geliştirilmesi çok kritik bir öneme sahiptir.

Bunun yanı sıra son yıllarda sesli asistan teknolojilerine yönelik gerçekleştirilen saldırı yöntemleri arasında arka kapı saldırıları (Backdoor Attacks) ve yapay zekâ odaklı saldırılar (AI-driven Attacks) da dikkat çekmektedir. Bu saldırılar, klasik komut enjeksiyonu yöntemlerinden farklı olarak sistemin makine öğrenimi altyapısını hedef almakta ve daha gelişmiş saldırı yöntemleri oluşturmaktadır.

Arka kapı saldırıları (Backdoor Attacks), makine öğrenmesi tabanlı sistemlerin eğitim aşamasında kötü niyetli aktörler tarafından sisteme kasıtlı olarak gizli tetikleyiciler yerleştirilmesiyle gerçekleştirilen bir saldırı türüdür. Bu teknik genellikle sesli asistanların ses tanıma ve doğal dil işleme modellerine yönelik uygulanmaktadır. Saldırgan, modelin eğitimi sırasında belirli bir ses paterni, belirli bir tonlama veya özel bir kelime dizisi içeren gizli bir tetikleyici ekler. Model, bu tetikleyici ile karşılaştığında, normal şartlarda vermeyeceği bir yanıt veya komut dizisini yerine getirir (K. Liu ve diğerleri, 2018). Bu saldırıların en tehlikeli yanı sistemin olağan kullanımında herhangi anormal bir duruma neden olmaması, yalnızca saldırganın özel tetikleyiciyi kullanması durumunda

etkinleşmesidir. Örneğin bir saldırgan, sesli asistan modeline eğitim verisi sırasında fark edilmeden "önemsiz" gibi görünen bir kelime kombinasyonunu backdoor olarak yerleştirebilir. Son kullanıcı, bu tetikleyici ifadeyi fark etmeden söylediğinde asistan gizlice bir bankacılık işlemi başlatabilir veya bağlı bir akıllı cihazı devre dışı bırakabilir.

Öte yandan sesli asistan sistemlerine yönelik bir diğer gelişmiş saldırı kategorisi, AI-driven attacks olarak adlandırılan ve yapay zekâ tarafından otomatikleştirilmiş saldırılardır. Bu saldırı türünde saldırgan manuel bir müdahaleden ziyade, makine öğrenimi, derin öğrenme veya doğal dil işleme tekniklerini kullanarak otomatik saldırı stratejileri geliştirir. Literatürde özellikle Adversarial Example Attacks başlığı altında incelenen bu tekniklerde, sesli asistanın algılayamayacağı veya kullanıcı tarafından duyulamayacak şekilde manipüle edilmiş ses örnekleri oluşturulur. Bu örnekler insan kulağı tarafından anlaşılmaz olsa da sesli asistanın algoritmaları tarafından geçerli bir komut olarak algılanacak şekilde tasarlanır (Carlini ve Wagner, 2018). Örneğin müzik dosyasına gömülü düşük frekansta bir komut, kullanıcı farkında olmadan akıllı ev sistemini devre dışı bırakabilir.

AI-driven saldırıları yalnızca komut enjeksiyonuyla sınırlı değildir. Saldırganlar, yapay zekâ algoritmalarını kullanarak sesli asistan kullanıcılarının ses örneklerini analiz edebilir, kişisel kullanım alışkanlıklarını modelleyebilir ve sosyal mühendislik saldırılarını optimize edebilirler. Özellikle voice profile reconstruction (ses profili yeniden inşası) teknikleriyle kullanıcıların sesli kimlik doğrulama sistemleri hedef alınabilmekte ve saldırganlar sahte ses profilleri oluşturarak kimlik doğrulama süreçlerini atlatabilmektedir (J. Zhang ve diğerleri, 2021).

Yapay zekâ destekli saldırıların bir diğer boyutu ise otomatik komut zinciri üretimidir. Bu teknikte, saldırganlar doğal dil işleme tabanlı sistemler aracılığıyla sesli asistan için etkili olabilecek yüzlerce potansiyel komut zincirini otomatik olarak üretir, test eder ve başarı oranı yüksek olanları saldırıda kullanır. Bu durum, manuel saldırı denemelerine kıyasla saldırganlara çok daha geniş bir saldırı yüzeyi sunmaktadır.

Özetle backdoor attacks ve AI-driven attacks, sesli asistan teknolojilerinin güvenlik mimarisi açısından yalnızca donanımsal veya basit yazılımsal önlemlerle önlenmesi mümkün olmayan, model seviyesinde ele alınması gereken ileri düzey saldırı kategorileridir. Bu tür saldırıların tespit edilmesi, sistem performansına etki etmeden önleyici savunma

mekanizmalarının geliştirilmesi halen araştırma literatüründe önemli bir çalışma alanı olarak varlığını sürdürmektedir.

Webrazzi'nin 2019 yılına ait bir haberine göre Japonya ve Michigan Üniversitesi'nden araştırmacılar, lazer ışığı kullanarak sesli asistanları hackleme yöntemini keşfettiler. Bu saldırı, U.S. Defense Advanced Research Projects Agency (DARPA) tarafından finanse edilen bir araştırma kapsamında gerçekleştirildi. Araştırmacılar, saldırganların sesli komutları söylemeden yalnızca lazer ışınları ile sesli asistanları hackleyebileceklerini gösterdiler. Lazer ışınları, mikrofonun diyaframına yansıyarak ses dalgalarına benzer titreşimler yaratmış ve cihaz, bu titreşimleri sesli komut olarak algılamıştır. Araştırmalara göre lazer ışıkları ile sesli asistanlar 110 metreye kadar uzaktan kontrol edilebilmiştir. Ayrıca saldırganlar lazer ışığını 70 metre uzaklıktaki bir çan kulesinden bir cihazın mikrofonuna yönlendirerek sesli asistanı kontrol edebilmişlerdir. Araştırmada gerekli ekipmanın düşük bir maliyetle temin edilebileceği, hatta uzun mesafeli saldırılar için kullanılan telefoto lensin yalnızca 600 dolara kadar çıkabileceği belirtilmiştir. Bu tür bir saldırı ev güvenliği, online hesaplar ve diğer hassas verilere erişim için büyük bir tehdit oluşturabilir. Bu olay, sesli asistanların güvenlik açıklarını ve lazer tabanlı saldırılarla yapılan potansiyel siber saldırıları gözler önüne sermektedir.

Zhang ve diğerlerinin 2018 tarihli ve "Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home" başlıklı çalışmasında sanal asistan sistemlerine (ilgili çalışmada İngilizce olarak Virtual Personal Assistant şekilde kullanılmıştır ve kısaltması VPA olarak belirtilmiştir) yönelik Voice Squatting Attack (VSA) ve Voice Masquerading Attack (VMA) olarak adlandırılan iki yeni saldırı türü tanımlanmıştır. VSA, sesli asistanların uygulama çağırma yöntemlerindeki zaaflardan yararlanarak kullanıcının yanlışlıkla kötü niyetli bir beceriyi çalıştırmasını sağlamaktadır. Örneğin "Alexa, Capital One'ı aç" şeklinde verilen bir komut, eğer saldırgan tarafından "Capital One Please" adlı kötü amaçlı bir beceri oluşturulmuşsa sistemin yanlış yönlendirilmesine sebep olabilir. VMA ise kullanıcı ile VPA arasındaki etkileşimi manipüle ederek saldırganın kendisini meşru bir uygulama veya VPA hizmeti gibi göstermesine olanak tanımaktadır. Bu saldırılar sonucunda kullanıcıların hassas bilgilerinin ele geçirilmesi, yanlış yönlendirilmesi veya saldırgan tarafından yanıltılması mümkün hale gelmektedir. Araştırmada Amazon Echo ve Google Home kullanıcılarıyla gerçekleştirilen bir anket çalışması, kullanıcıların doğal dil kullanımı nedeniyle VSA saldırılarına karşı savunmasız

olabileceğini ortaya koymuştur. Ayrıca saldırının gerçek dünyada uygulanabilirliğini değerlendirmek amacıyla Alexa platformu üzerinde çeşitli kötü niyetli beceriler yayınlanarak test edilmiştir. Çalışma kapsamında 2699 kullanıcının saldırıya maruz kaldığı ve toplamda 21308 komutun işlendiği tespit edilmiştir. Bu bulgular, VSA ve VMA saldırılarının yalnızca teorik bir tehdit olmadığını aksine gerçek dünyada geniş çaplı etkilere sahip olabileceğini göstermektedir. Bununla birlikte araştırmacılar bu güvenlik açıklarını ilgili platform sağlayıcıları olan Amazon ve Google ile paylaşmış ve risklerin azaltılması için çeşitli çözümler önermiştir. Önerilen çözümler arasında sesli becerilerin çağrılma isimlerini analiz eden bir filtreleme sistemi geliştirilmiş ve potansiyel olarak benzer seslere sahip beceriler tespit edilmiştir. Yapılan testlerde Alexa platformundaki 19670 özel beceriden 4718'inin bu tür saldırılara açık olduğu belirlenmiştir. Ayrıca VMA saldırılarını tespit edebilmek için bağlam duyarlı bir dedektör (context-sensitive detector) geliştirilmiş ve bu sistemin %95 doğruluk oranına sahip olduğu gösterilmiştir. İlgili çalışma, VPA sistemlerinin güvenliğine yönelik ilk kapsamlı güvenlik analizlerinden biri olup ses tabanlı saldırıların ciddiyetini ve potansiyel etkilerini gözler önüne sermektedir. Ancak bu alandaki güvenlik açıklarının tamamen kapatılması için daha fazla araştırmaya ihtiyaç duyulmaktadır. Sesli asistanların kullanıcı kimlik doğrulama mekanizmalarının güçlendirilmesi, sesli komutların güvenliğinin artırılması ve saldırı tespit sistemlerinin daha da geliştirilmesi gerekmektedir. Gelecekte yapılacak çalışmaların ses tabanlı sistemlerin hem güvenlik hem de kullanılabilirlik açısından daha dengeli bir yapıya kavuşturulmasına katkı sağlaması beklenmektedir.

Sonuç olarak sesli asistanlar ve akıllı hoparlörler, kullanıcı deneyimini iyileştiren ve günlük yaşamı kolaylaştıran teknolojiler olmasına rağmen çok katmanlı güvenlik risklerini de beraberinde getirmektedir. Bu sistemler hem yazılım hem de donanım seviyesinde çeşitli saldırı tekniklerine açıktır. Bluetooth veya Wi-Fi üzerinden yetkisiz erişim sağlanması, siber-fiziksel saldırılar, adversarial yapay zekâ saldırıları ve lazer tabanlı manipülasyon teknikleri gibi farklı yöntemlerle sesli asistanlara yönelik tehditlerin sürekli olarak geliştiği gözlemlenmektedir. Özellikle, makine öğrenmesi tabanlı saldırılar, klasik güvenlik önlemleriyle tespit edilmesi zor olan yeni tehdit türleri ortaya çıkarmaktadır. Arka kapı saldırıları (Backdoor Attacks), adversarial saldırılar ve otomatik komut zincirleri, ses tanıma ve doğal dil işleme sistemlerini istismar ederek saldırganlara geniş bir saldırı yüzeyi sunmaktadır. Bu durum, güvenlik önlemlerinin yalnızca erişim kontrolü ve şifreleme teknikleriyle sınırlı kalmaması gerektiğini göstermektedir. Makine öğrenimi modellerinin

güvenliğini sağlamak için adversarial eğitim yöntemleri, anormal durum tespiti ve model bütünlüğünü koruyacak önleyici mekanizmalar geliştirilmelidir (K. Liu ve diğerleri, 2018; Carlini ve Wagner, 2018).

Ayrıca saldırganların yalnızca yazılım açıklarını değil, donanım seviyesinde yer alan güvenlik zafiyetlerini de istismar edebileceği unutulmamalıdır. Lazer tabanlı saldırılar gibi fiziksel etkileşim gerektirmeyen yöntemlerin ortaya çıkması, sesli asistan güvenliğinin yalnızca sanal tehditlerle sınırlı olmadığını ve fiziksel güvenlik önlemlerinin de kritik bir bileşen olduğunu göstermektedir. Gelecekte mikrofonların fiziksel koruma önlemleri ile güçlendirilmesi ve ışık bazlı saldırılara karşı dirençli hale getirilmesi için yeni donanım çözümleri geliştirilmelidir (Sugawara ve diğerleri, 2020).

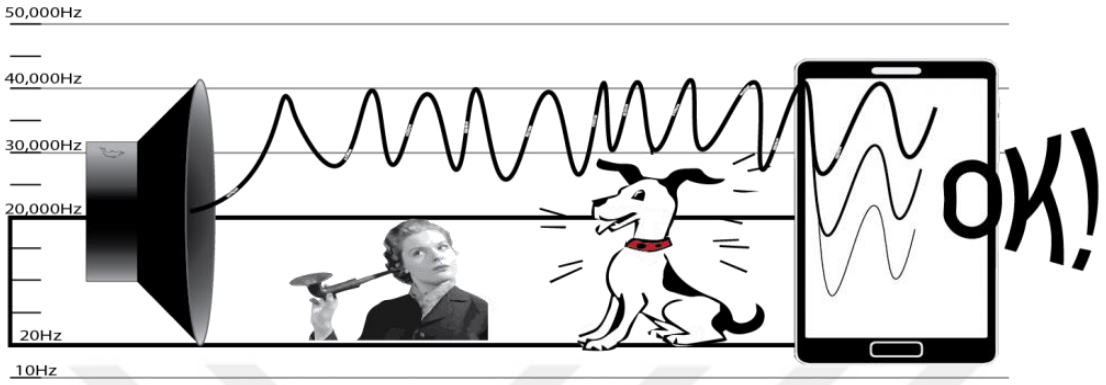
Bu kapsamda sesli asistanların güvenliğini artırmak için çok yönlü güvenlik stratejileri benimsenmelidir. Kullanıcı farkındalığının artırılması, güçlü kimlik doğrulama mekanizmalarının uygulanması, komut filtreleme sistemlerinin geliştirilmesi ve yapay zekâ tabanlı anomali tespit sistemlerinin entegre edilmesi gibi önlemler, saldırı risklerini azaltmada etkili olabilir. Ancak bu önlemlerin uygulanabilmesi için hem teknoloji sağlayıcılarının hem de son kullanıcıların bilinçli ve aktif olarak hareket etmeleri gerekmektedir.

Yeni nesil saldırı tekniklerine karşı koruma sağlamak için akademik çalışmaların ve endüstri iş birliklerinin güçlendirilmesi büyük önem taşımaktadır. Özellikle, sesli asistanlar için geliştirilen güvenlik çözümlerinin, dinamik tehdit ortamına uyum sağlayacak şekilde sürekli olarak güncellenmesi ve geliştirilmeye devam edilmesi gerekmektedir.

3.7. Ultrasonik Ses Dalgalarıyla Yapılan Saldırılar ve DolphinAttack

Ultrasonik ses dalgalarıyla gerçekleştirilen saldırılar, sesle etkinleştirilen akıllı sistemlerin güvenlik açıklarından yararlanan en sofistike siber saldırı türlerinden biridir. Bu saldırılar, genellikle insan işitme aralığının üzerindeki yüksek frekanslı ses dalgalarını (20 kHz'in üzerinde) kullanarak kullanıcıların fark edemeyeceği (Resim 3.3'te örnek bir grafik verilmiştir) komutlar gönderir. Özellikle "DolphinAttack" olarak adlandırılan yöntem, saldırganların akıllı telefonlar, akıllı hoparlörler ve sanal asistanlar gibi sesle kontrol edilen cihazların ses algılama mekanizmalarını manipüle ederek kullanıcıların bilgisi olmadan

yetkisiz komutlar vermelerine olanak tanır (Yan ve diğerleri, 2022). Bu tür saldırılar kullanıcıların kişisel bilgilerini, finansal işlemlerini ve özel verilerini tehlikeye atabilecek ciddi güvenlik riskleri doğurmaktadır.



Resim 3.3. İnsan kulağının duyabildiği ve duyamadığı frekans aralıklarını karşılaştırmalı olarak betimleyen görsel. (Serene-Risc Smart Cybersecurity Network, 2017)

Ultrasonik ses tabanlı saldırılar, akustik dalgaların manipülasyonu ile meydana getirilir; kökeni askeri ve güvenlik alanlarında gerçekleştirilen akustik silah araştırmalarına dayanmaktadır. Ses dalgalarının tahrip edici etkileri üzerine yapılan araştırmalar, ultrasonik dalgaların sesli komut sistemlerinde nasıl kullanılabileceğine dair ipuçları sunmuştur (Yan ve diğerleri, 2022). Günümüzde bu teknikler sivil alanlarda özellikle IoT (Internet of Things) ve yapay zekâ destekli cihazlara yönelik tehditler şeklinde kendini göstermektedir.

2017 yılında Zhejiang Üniversitesinden araştırmacılar tarafından geliştirilen DolphinAttack, ses kontrollü cihazların insan kulağının duyamayacağı yüksek frekanslı ses dalgalarıyla manipüle edilebileceğini gösteren ilk geniş çaplı saldırı modeli olmuştur (Zhang ve diğerleri, 2017). Bu çalışmanın ardından araştırmacılar benzer prensipleri kullanarak daha gelişmiş ve detaylandırılmış saldırı yöntemleri geliştirmiştir.

DolphinAttack, sesli komutları ultrasonik taşıyıcılar üzerine modüle ederek insan kulağı tarafından duyulamayan ancak hedef cihazın mikrofonları tarafından algılanabilen sinyaller oluşturur. Aynı zamanda DolphinAttack, AM modülasyonu ile sesli komutlar giren bir saldırıdır (Roy ve diğerleri, 2017). Bu saldırı, akıllı telefonlara yerleştirilen MEMS ve ECM mikrofonlarının doğrusal olmayan çıkışlarından yararlanmaktadır (Kune ve diğerleri, 2013). Mikrofon devrelerinin doğrusal olmamasından yararlanarak modüle edilmiş düşük frekanslı sesli komutlar başarıyla demodüle edilir, geri kazanılır ve ses tanıma sistemleri tarafından

yorumlanır. Bu saldırı özellikle Siri, Google Now, Alexa ve diğer popüler sesli asistanları hedef alabilir (Alchekov ve diğerleri, 2023). Bu saldırının başarılı olabilmesi için iki temel bileşen gereklidir:

- Ultrasonik ses dalgalarının üretilmesi: Saldırganlar, ultrasonik ses üretebilen özel donanım ve yazılımlar kullanarak insan kulağıyla algılanamayan sinyaller üretir.
- Ses tanıma sistemlerinin manipüle edilmesi: Bu sinyaller, hedef cihazın mikrofonu tarafından algılandığında, ses tanıma sistemleri tarafından geçerli komutlar olarak işlenir (Xia ve diğerleri, 2023). Bu saldırı yöntemi, özellikle mobil bankacılık uygulamaları ve akıllı ev sistemleri gibi kritik güvenlik gereksinimleri olan alanlarda ciddi riskler oluşturmaktadır.

DolphinAttack yönteminde sesli komutlar ultrasonik taşıyıcılarla (örneğin f> 20 kHz) modüle edilerek duyulmazlık sağlanmıştır. Mikrofon devrelerinin doğrusal olmayan özelliklerinden yararlanarak modüle edilen düşük frekanslı sesli komutlar başarıyla demodüle edilebilir, geri kazanılabilir ve daha da önemlisi sesli komut tanıma sistemleri tarafından anlaşılabilir. DolphinAttack, popüler sesli komut tanıma sistemlerinde test edilmiştir; bunlar arasında Siri (Resim 3.4'te Siri'ye yönelik bir saldırı örneği yer almaktadır), Google Now, Samsung S Voice, Huawei HiVoice, Cortana ve Alexa yer almaktadır. Duyulamayan sesli komutların enjeksiyonu ile Siri'nin FaceTime araması başlatması, Google Now'ın telefonun uçak moduna geçmesi ve hatta bir Audi otomobilinin navigasyon sisteminin manipüle edilmesi gibi birkaç deney niteliğinde saldırı gerçekleştirilmiştir. Ayrıca donanım ve yazılım savunma çözümleri önerilmiştir. DolphinAttack, desteklenen vektör makineleri (SVM) kullanılarak seslerin sınıflandırılmasıyla tespit edilebileceği doğrulanmış ve sesle kontrol edilebilir sistemlerin duyulamayan sesli komut saldırılarına karşı dayanıklı olacak şekilde yeniden tasarlanması gerektiği vurgulanmıştır.

Resim 3.4. Siri'ye ve akıllı ev sistemlerine yönelik bir saldırı örneği (Xia ve diğerleri, 2023)

Ultrasonik ses dalgalarıyla yapılan saldırılar DolphinAttack'ın yanı sıra SurfingAttack, sabit sürücülere yönelik saldırılar ve Near Inaudiable Ultrasonic Attacks gibi diğer alt bölümlerde incelenecek olan farklı saldırı şekilleriyle de gerçekleştirilir. Bu kısımda konu bütünlüğü sağlanabilmesi için DolphinAttack haricindeki bu saldırı türlerinden genel olarak bahsedilmiştir.

2020 yılında tanımlanan "SurfingAttack", ultrasonik dalgaları katı yüzeyler aracılığıyla ileterek sesli asistanları uzaktan kontrol etmeyi amaçlar (Xia ve diğerleri, 2023). Örneğin bir masanın altına gizlenmiş bir ultrasonik dönüştürücü, masanın yüzeyi boyunca yönlendirilmiş ultrasonik dalgalar göndererek masanın üzerindeki bir akıllı telefonun sesli asistanını etkinleştirebilir. Bu yöntemle saldırganlar cihazlara fiziksel olarak dokunmadan komutlar gönderebilirler.

Ultrasonik ses tabanlı saldırılar yalnızca sesli asistanları değil, sabit disk sürücülerini (HDD) de hedef alabilir. Yapılan çalışmalar, belirli frekanstaki ultrasonik dalgaların HDD bileşenlerinde titreşim oluşturarak okuma/yazma işlemlerini bozabileceğini ve sistem çökmesine yol açabileceğini göstermiştir (Yan ve diğerleri, 2022). Bu tür saldırılar özellikle veri merkezleri ve kurumsal bilgi sistemleri için önemli bir tehdit oluşturmaktadır.

Near Inaudible Ultrasonic Attacks (NUIT) ise hedef cihazın kendi hoparlörünü kullanarak saldırıyı gerçekleştiren karmaşık bir yöntemdir. Bu saldırı tekniğinde cihazın hoparlörü

aracılığıyla yayılan ultrasonik sinyaller, yine aynı cihazın mikrofonu tarafından algılanarak saldırganın belirlediği komutların çalıştırılmasına neden olabilir (Xia ve diğerleri, 2023). Bu durum da saldırganların bir cihazın sesli asistanını uzaktan kontrol etmelerine ve yetkisiz işlemler gerçekleştirmelerine olanak tanır.

Bu tür saldırılar, siber güvenlik alanında giderek daha fazla ilgi görmekte olup özellikle cihazların fiziksel temas gerekmeksizin kontrol edilebilmesi nedeniyle büyük bir tehdit oluşturmaktadır. Ultrasonik saldırıların etkinliği kullanılan frekans aralıklarına, hedef cihazın mikrofon hassasiyetine ve ortam koşullarına bağlı olarak değişkenlik gösterebilir. Ayrıca saldırganlar bu yöntemi gizli dinleme, yetkisiz komut yürütme ve kritik sistemlere zarar verme gibi çeşitli amaçlar için kullanabilirler. Dolayısıyla bu saldırıların potansiyel etkilerini anlamak ve güvenlik açıklarını tespit etmek, savunma mekanizmalarının geliştirilmesi açısından büyük önem taşımaktadır.

Ultrasonik saldırılara karşı genel korunma yöntemleri donanımsal ve yazılımsal olarak ikiye ayrılmaktadır:

- Donanımsal önlemler: Mikrofonların ultrasonik ses dalgalarına karşı duyarlılığını azaltan filtreler geliştirilmelidir, akıllı cihazlara fiziksel engelleyici mekanizmalar eklenmelidir.
- Yazılımsal önlemler: Ses tanıma sistemleri, insan kulağının algılayamayacağı frekanslardaki sesleri tespit edebilecek algoritmalarla güncellenmelidir, kullanıcı kimlik doğrulaması için biyometrik ses izleri ve çok faktörlü kimlik doğrulama mekanizmaları eklenmelidir (Alchekov ve diğerleri, 2023), cihaz üreticileri sesle etkinleştirilen cihazların yazılımlarını düzenli olarak güncellemelidir.

Zhang ve diğerlerinin 2017 tarihli ve “DolphinAttack: Inaudible Voice Commands” başlıklı çalışmasında DophinAttack’a yönelik olarak bazı savunma stratejileri önerilmiştir. Bunlardan ilki mikrofon iyileştirmesidir. Bu savunma türüne göre duyulmaz sesli komutların temel nedeni, mikrofonların 20 khz üzerindeki frekansta sesleri algılayabilmesidir. Ancak ideal bir mikrofonun böyle sesleri algılamaması gerekir. Günümüzdeki çoğu MEMS mikrofonu, 20 khz üzerindeki frekansları algılayabilmektedir. Bu yüzden mikrofonların tasarımında ultrasonik frekanslarda sinyalleri baskılayacak iyileştirmeler yapılmalıdır. Bu çalışmada yapılan deneylere göre iPhone 6 Plus’ın mikrofonu, duyulamayan komutlara karşı

oldukça dayanıklıdır. Önerilen diğer savunma stratejisi ise duyulmaz sesli komut iptalidir. Bu stratejiye göre de eski tip mikrofonlarla ultrasonik frekanslardaki modüle edilmiş sesli komutları algılayıp iptal etmek için bir modül eklenebilir. Bu modül, modülasyon özellikleri gösteren ultrasonik frekanslardaki sinyalleri tespit edip bunları demodüle ederek ana sinyale (baseband) dönüştürür. Böylece sesli komutlar iptal edilebilir. Bu işlem mikrofonun normal işleyişini etkilemez, çünkü mikrofon duyulabilir sesler ile ultrasonik gürültüler arasında bir ilişki kurmaz. Yazılım tabanlı savunma, modüle edilmiş sesli komutların özgün özelliklerini analiz ederek bunları gerçek sesli komutlardan ayırır. DolphinAttack saldırısını tespit etmek için sesin 500 ile 1000 Hz arasındaki yüksek frekans aralığı incelenebilir. Bu frekans aralığındaki farkları kullanarak, yazılım tabanlı bir sınıflandırıcı (örneğin destek vektör makineleri) kullanılarak kaydedilmiş ve geri kazanılmış sesler arasında %100 doğru tespit yapılabilir. Bu yöntem, yazılım tabanlı savunma stratejisinin DolphinAttack'ı tespit etme konusunda oldukça etkili olduğunu gösterir. DolphinAttack'ın tamamen ortadan kaldırılması oldukça zorlu bir süreçtir hatta donanım seviyesinde değişiklikler gerektirdiği için bu tamamen mümkün olmayabilir.

Zhang ve diğerlerinin 2021 tarihli ve "EarArray: Defending against DolphinAttack via Acoustic Attenuation" başlıklı çalışmasında, ek bir donanıma veya donanım değişikliğine ihtiyaç duymadan bu tür saldırıları tespit edebilen ve saldırganın yönünü belirleyebilen hafif yapılı bir yöntem olan EarArray tasarlanmıştır. Temel olarak duyulamayan sesli komutlar ultrasonik dalgalar üzerine modüle edilmekte olup bu dalgalar duyulabilen seslere kıyasla doğal olarak daha hızlı sönümlenmektedir. İlgili çalışmada akıllı cihazların dahili mikrofonları aracılığıyla komut ses sinyalleri incelenmiştir, yapılan deneyler sonucu EarArray'ın sönümleme oranını tahmin edebilmekte ve böylece saldırıları tespit edebilmekte olduğuna ulaşılmıştır. Çalışmada, duyulabilen sesler ve ultrasonik seslerin bir ses kaynağından bir sesli asistana (örneğin bir akıllı hoparlöre) yayılımı modellenmiş ve yöntemin temel ilkesi ile uygulanabilirliği ortaya konmuştur. EarArray, özel olarak tasarlanmış iki mikrofon dizisi kullanılarak uygulanmış ve gerçekleştirilen deneyler sonucunda duyulamayan sesli komutları %99 doğrulukla tespit edebildiği, saldırganın yönünü %97,89 doğrulukla belirleyebildiği gösterilmiştir.

Llyod ve diğerlerinin 2023 tarihli ve "Mitigating Inaudible Ultrasound Attacks on Voice Assistants With Acoustic Metamaterials" başlıklı çalışmasında, sesli asistanlara yönelik ultrasonik saldırıları önlemek için akustik metamaterial filtreler kullanarak fiziksel bir

savunma yöntemi sunulmaktadır. Ultrasonik komutlar, insan kulağı tarafından duyulamamasına rağmen akıllı hoparlörler tarafından algılanabilir ve kötü niyetli amaçlarla kullanılabilir. Bu tür saldırıları engellemek için geliştirilen metamaterial filtreler, belirli frekanslardaki ses dalgalarını modüle ederek mikrofonun bu sinyalleri algılamasını engeller. Çalışmada sert plakalar ve yerel rezonans gösteren deliklerden oluşan bir kompozit metamaterial filtre tasarlanmış ve bir Amazon Echo Dot üzerinde test edilmiştir. Deney sonuçları, filtrelerin normal sesli komutları etkilemeden ultrasonik saldırıları başarıyla engellediğini göstermektedir. Ayrıca bu filtreler küçük boyutlu olup akıllı hoparlörlere kolayca monte edilebilmektedir. Metamaterial filtrelerin üretimi için SLA 3D baskı yöntemi kullanılmış ve deneyler sonucunda filtrelerin etkinliği doğrulanmıştır. Farklı açılar ve mesafelerde yapılan testlerde filtreler olmadan akıllı hoparlörün ultrasonik saldırılarla tetiklendiği, ancak filtreler eklendiğinde saldırıların tamamen engellendiği gözlemlenmiştir. İlgili çalışmada yazılım tabanlı savunmalara kıyasla düşük maliyetli ve donanıma müdahale gerektirmeyen mekanik bir çözüm sunulmaktadır. Ayrıca söz konusu çalışmada metamaterial filtrelerin tasarımı kolayca özelleştirilebilir, farklı frekans bantlarına uyarlanabilir ve çeşitli sesli asistanlara entegre edilebilir olduğundan da bahsedilmiştir.

Huang ve diğerlerinin 2020 tarihli ve “A defense scheme of voice control system against DolphinAttack” başlıklı çalışması, DolphinAttack saldırısına karşı sesli kontrol sistemlerini korumaya yönelik bir savunma yöntemi önermektedir. DolphinAttack, sesli kontrol sistemlerinin mikrofonlarındaki ses frekansı tanımlama zafiyetlerini hedef alan bir saldırı modelidir. Bu saldırı, sesli komutu ultrasonik taşıyıcıya modüle ederek komutların insan kulağı tarafından duyulmadan ses tanıma sistemi tarafından doğru bir şekilde çözülmesini sağlar. DolphinAttack, akıllı cihaz kullanıcılarının mülkiyet hakları ve gizliliği üzerinde büyük bir tehdit oluşturur. İlgili çalışmada, DolphinAttack’a karşı korunmak için yazılım ve donanım kombinasyonu kullanan kesik döngü kimlik doğrulamasına dayalı bir güvenlik güçlendirme yöntemi önerilmektedir. Bu güvenlik çözümüne göre ikinci kimlik doğrulaması eklenerek bilinmeyen bazı zayıflıklar azaltabilir. Saldırgan veya kullanıcı ses tanıma sistemini uyandırıp komut verdiğinde sistem yüksek güvenlik seviyesiyle ikinci kimlik doğrulaması yapmaya zorlanır. Komut, ikinci kimlik doğrulamasını geçerse yürütülür; geçemezse bu komut iptal edilir ve kullanıcıya rapor gönderilir. Bu güvenlik güçlendirmesi, DolphinAttack nedeniyle yaşanabilecek gizlilik sızıntısı ve diğer potansiyel zararların risklerini önemli bir ölçüde azaltmaktadır. Söz konusu çalışmanın amacı, sesli kontrol sistemlerine yönelik olası saldırıları engellemeye yönelik pratik çözümler geliştirmektir.

DolphinAttack'ın mikrofonları, 20kHz'in üzerindeki ultrasonik frekansları algılayabilen cihazlarla gerçekleştirilebileceği belirtilmiştir. Çalışmada bu tür saldırılara karşı yazılım tabanlı çözümler, sesli komutların doğru şekilde sınıflandırılmasını sağlayarak bu tür saldırılara karşı savunma yapmaktadır. Ancak donanım tabanlı çözümlerin her mikrofonu değiştirmek gerektiği için uygulamada zorluklar yarattığından da bahsedilmiştir.

Ultrasonik ses dalgaları, PIN tabanlı kimlik doğrulama sistemleri gibi güvenlik protokollerini de hedef alarak önemli bir tehdit oluşturur. X. Liu ve diğerlerinin 2021 tarihli ve "UltraPIN: Inferring PIN Entries via Ultrasound" başlıklı çalışmasına göre UltraPIN, bu tür bir saldırının örneğidir ve kullanıcıların PIN girişlerini tahmin etmek için ultrasonik ses dalgalarından faydalanan bir yöntem olarak öne çıkmaktadır. Bu saldırı, akıllı telefonlar aracılığıyla gerçekleştirilebilir. Saldırgan, telefonunun hoparlörlerinden insan kulağının duymadığı ultrasonik sinyaller gönderirken mikrofonlar aracılığıyla çevredeki akustik sinyalleri kaydeder. Bu kaydedilen sinyaller, parmak hareketlerinin izini sürmek ve PIN girişi hakkında bilgi çıkarmak için işaret işleme teknikleriyle analiz edilir. Düşük enerjili ve gürültülü ultrasonik sinyallerden yüksek kaliteli özellikler çıkarılabilmesi, saldırının etkinliğini artırır. Bu çalışmada örnek olarak yürütülen bir UltraPIN saldırısında üç denemede %75 oranında başarı sağlanmış ve PIN girişleri tahmin edilmiştir. Bu tür bir saldırı PIN girişlerinin yalnızca fiziksel olarak gözlemlenmesiyle elde edilebilecek bilgilerle sınırlı kalmaz, aynı zamanda ses dalgalarının akustik yansıması ve frekansları üzerinden de bilgi çıkarılabilir. Bu nedenle ultrasonik ses dalgalarıyla gerçekleştirilen saldırıların ortaya çıkardığı güvenlik açıkları, bu tür tehditlerin daha yakından incelenmesini gerektirmekte ve sonuç olarak PIN tabanlı sistemlerin güvenliğinin yeniden değerlendirilmesine zemin hazırlamaktadır. Bu durum, daha güvenli kimlik doğrulama yöntemlerinin benimsenmesi ihtiyacını da ön plana çıkarmaktadır.

Sonuç olarak ultrasonik ses dalgalarıyla gerçekleştirilen saldırılar, modern sesle kontrol edilen cihazların güvenliğini ciddi şekilde tehdit eden oldukça karmaşık bir siber saldırı türü olarak dikkat çekmektedir. DolphinAttack, SurfingAttack, HDD'ye yönelik ultrasonik saldırılar ve Near Inaudible Ultrasonic Attacks (NUIT) gibi teknikler, ses algılama ve tanıma sistemlerini manipüle ederek saldırganların cihazlara yetkisiz erişim sağlamalarına olanak tanımaktadır. Bu saldırılar özellikle mobil cihazlar, akıllı ev sistemleri ve IoT cihazları gibi yaygın teknolojilerde önemli güvenlik açıkları oluşturarak kullanıcıların kişisel bilgileri ve hassas verileri üzerinde büyük riskler doğurmaktadır.

Söz konusu saldırıların etkinliğini ve potansiyel tehlikelerini göz önünde bulundurulduğunda yalnızca yazılım temelli savunma stratejilerinin yetersiz kaldığı, aynı zamanda donanım tabanlı önlemlerin de önem kazandığı açıkça görülmektedir. Donanım seviyesinde mikrofon iyileştirmeleri, ultrasonik sinyalleri engelleyen akustik metamaterial filtreler ve sesli komutları tespit etmeye yönelik gelişmiş algoritmalar gibi önlemler, bu tehditlere karşı önemli savunmalar sunmaktadır. Ayrıca sesli komut tanıma sistemlerinde yapılan iyileştirmeler ve biyometrik doğrulama mekanizmalarının entegrasyonu, bu tür saldırılara karşı koruma sağlamak adına etkili bir çözüm önerisi sunmaktadır.

Öte yandan bu tür saldırıların daha karmaşık hale gelmesiyle güvenlik uzmanlarının ve cihaz üreticilerinin tehditlerin farkında olmaları ve daha güvenli sistemler tasarlamaları gerekmektedir. Teknolojik gelişmelerin hızına paralel olarak ultrasonik saldırıların tespit edilmesi, sınıflandırılması ve önlenmesi için sürekli olarak yeni savunma mekanizmalarının geliştirilmesi hayati önem taşımaktadır. Ayrıca kullanıcıların bu tür saldırılara karşı farkındalık seviyelerinin artırılması ve güvenlik pratiklerinin güçlendirilmesi, dijital güvenliğin sağlanmasında kritik rol oynamaktadır. Günümüzde ultrasonik ses dalgalarıyla gerçekleştirilen saldırılar, güvenlik alanında ciddi bir tehdit olarak kalmaya devam etmekte ve bu tehditlere karşı alınacak önlemler, dijital dünyadaki güvenlik açığının kapanmasında önemli bir yer tutmaktadır.

3.8. NUIT Tekniği ile Yapılan Saldırılar

Near-Ultrasound Inaudible Trojan (NUIT) saldırıları, ultrasonik ses dalgalarını kullanarak sesle kontrol edilen cihazlara izinsiz erişim sağlamaya yönelik gelişmiş bir siber saldırı tekniğidir. İlk olarak ultrasonik ses dalgalarının güvenlik açıklarını tetikleyebileceğine dair çalışmalar, yukarıdaki kısımda da belirtildiği gibi, 2017 yılında gerçekleştirilen DolphinAttack araştırmasıyla gündeme gelmiştir. Bu çalışmada insan kulağının algılayamayacağı frekansta iletilen ses dalgalarının akıllı asistanlar ve sesli komut sistemleri tarafından bir kullanıcı komutu olarak algılanabileceği gösterilmiştir. Daha sonraki araştırmalar, bu saldırıların gelişmiş modülasyon teknikleriyle daha da karmaşık hale getirilebileceğini ortaya koymuş ve özellikle 2023 yılında Xia, Chen ve Xu tarafından yapılan çalışmalar, NUIT saldırılarının sistematik olarak nasıl gerçekleştirilebileceğini detaylandırmıştır (Xia ve diğerleri, 2023).

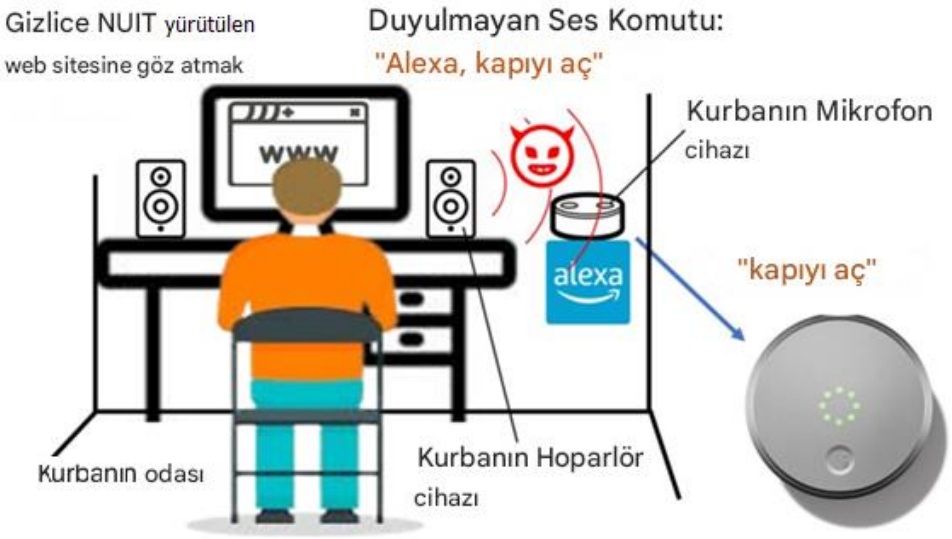
NUIT saldırıları zaman içinde sadece akıllı telefonlar ve sesli asistanlar gibi tüketici cihazlarını değil aynı zamanda akıllı ev sistemleri, otomobiller ve hatta endüstriyel IoT cihazlarını da hedef alabilecek şekilde genişlemiştir. Bu evrimleşme, saldırı yöntemlerinin giderek daha detaylı ve karışık hale gelmesine, güvenlik açıklarının daha fazla alana yayılmasına neden olmuştur. Dolayısıyla NUIT saldırılarının gelişimini anlamak, bu tehditlere karşı etkili savunma mekanizmaları geliştirmek açısından kritik bir öneme sahiptir.

Near-Ultrasound Inaudible Trojan (NUIT), sesli asistanlar ve akıllı cihazlar gibi sesle etkileşimli sistemlere yönelik önemli bir güvenlik tehdidi oluşturan bir akustik saldırı tekniğidir. NUIT, insan kulağının algılayamayacağı yüksek frekanslı ultrasonik ses dalgaları kullanarak cihazlara zarar verici komutlar göndermeyi amaçlar. Bu saldırılar, geleneksel akustik saldırı yöntemlerinden farklı olarak yazılım ve donanım katmanlarında etkili olan güvenlik açıklarını hedef alır (G. Chen ve diğerleri, 2023). NUIT saldırıları, iki ana kategoriye ayrılır: NUIT-1 ve NUIT-2. NUIT-1'de, bir cihaz hem saldırı kaynağı hem de hedef olarak kullanılır. Örneğin bir akıllı telefonun hoparlörü aracılığıyla yayılan ultrasonik sinyaller, telefonun mikrofonu tarafından algılanarak kötü niyetli komutları çalıştırabilir. NUIT-2 ise bir cihazın hoparlöründen yayılan ultrasonik sinyallerin yakınındaki bir cihaz tarafından algılanması yoluyla gerçekleşir. Bu tür bir saldırı, fiziksel olarak yakın cihazlar arasında yapılabilir ve pratikte daha büyük tehditler oluşturur (BleepingComputer, 2023).

Xia ve diğerlerinin 2023 tarihli ve “Near-Ultrasound Inaudible Trojan (NUIT): Exploiting Your Speaker to Attack Your Microphone” başlıklı çalışması, Near-Ultrasound Inaudible Trojan (NUIT) adlı yeni saldırı sınıfını tanıtmaktadır. NUIT, sesli komutları kullanarak, özellikle akıllı cihazların sesli komut sistemlerine (İngilizce olarak Voice Control System, kısaltması VCS) saldırmayı hedefleyen, duyulamayan saldırılar gerçekleştirebilen bir yöntemdir. NUIT'in iki farklı türü vardır: NUIT-1 ve NUIT-2. NUIT-1, saldırganın aynı cihazda bulunan mikrofonu ve VCS’yi, cihazın hoparlörünü kullanarak hedef almasıyla gerçekleşir. NUIT-2 ise saldırganın bir cihazdaki hoparlörü kullanarak başka bir cihazdaki mikrofonu ve VCS’yi hedef alması durumudur. Çalışma, NUIT saldırılarının başarılı bir şekilde gerçekleştirilebilmesi için karşılaşılan üç ana zorluğu ele almaktadır. İlk zorluk ticari hoparlörlerin sınırlı bant genişliğidir. Bu durum NUIT saldırılarının başarılı olabilmesi için önemli bir engel teşkil eder. Saldırganlar, bu sorunu aşmak için özel bir modülasyon tekniği kullanmaktadır. İkinci zorluk ise VCS cihazlarının otomatik olarak ses seviyesini kısmalarıdır. Cihazlar, sesli komutları aldıktan sonra hoparlörlerini kapatarak sonraki

komutları daha net bir şekilde duyabilmeyi amaçlar. Ancak bu durum, saldırının gerçekleşmesini engeller. Bu engel, zamanlama ve tepki süresi ile aşılabilir. Üçüncü zorluk ise saldırıların sessiz yanıtlarla gerçekleştirilmesidir. NUIT saldırılarının sesli yanıtlar vermemesi gerekmektedir. Bunun için bazı cihazların yanıt mekanizmaları test edilerek sesi duymadan komut verebilen saldırılar geliştirilmiştir. Söz konusu çalışma, bu üç zorluğu aşmak için kullanılan yöntemleri detaylı bir şekilde sunmakta ve NUIT saldırılarının etkili olabileceğini göstermektedir. Ayrıca NUIT saldırılarının bazı cihazlarda (örneğin iPhone 6 Plus) başarılı olamayabileceği belirtilmiştir. Bunun nedeni, bu cihazın mikrofonundaki zayıf doğrusal olmayan özelliklerdir. Mikrofonun düşük kazançlı ses amplifikatörü, NUIT saldırılarına karşı direncin artırılmasına neden olmaktadır. Ancak bu durumun cihazların güvenliğini artırmak için ideal bir çözüm olmadığı, çünkü mikrofonun zayıf doğrusal olmayan özelliklerinin yasal kullanımda da sorunlara yol açabileceği vurgulanmaktadır. Son olarak ilgili çalışmada NUIT saldırılarına karşı savunma önerileri sunulmuştur. Savunma mekanizmaları, saldırının başarılı olduğu durumlarda mikrofonun NUIT sinyallerini tespit etmesini sağlamaya yönelik bir yazılım çözümünü içermektedir. Bu yazılım, simülasyonlar kullanılarak değerlendirilmiş ve sonuçlar savunma sisteminin sıfır yanlış pozitif ve sıfır yanlış negatifle çalıştığını göstermektedir. Bu savunma yöntemi, VCS cihazlarının fiziksel özelliklerinden yararlanarak NUIT saldırılarının tespit edilmesini sağlamaktadır.

NUIT'in güvenlik riskleri arasında yetkisiz komut yürütme, kimlik doğrulama sistemlerinin atlatılması ve kritik altyapıların tehlikeye girmesi yer alır. Resim 3.5'te gerçekleştirilme şekline ilişkin bir örneğe yer verilen sesli asistanlar aracılığıyla gerçekleştirilen bu saldırılar, kullanıcıların izni olmadan cihazlarını kontrol etmelerine ve özel bilgilerini sızdırmalarına olanak tanır (G. Chen ve diğerleri, 2023). Saldırganlar, sesli asistanları kullanarak, IoT cihazları gibi akıllı ev sistemlerini açabilir veya kapatabilir, alarm sistemlerini devre dışı bırakabilir. Bunun yanı sıra, NUIT saldırıları, gizliliğin ihlal edilmesine ve cihazların kötü amaçlı yazılımlar tarafından ele geçirilmesine yol açabilir. Bu tehditlere karşı etkili güvenlik önlemleri, sesli asistanların güvenliğini sağlamak için kritik öneme sahiptir.



Resim 3.5. NUIT saldırısının gerçekleştirilmesine ilişkin bir örnek (Xia ve diğerleri, 2023)

NUIT saldırıları, hedef sistemin ya da cihazın mikrofonuna insan kulağı tarafından algılanamayan ultrasonik sinyaller enjekte edilmesi yoluyla gerçekleştirilir. Bu sinyaller, cihazın yerleşik ses tanıma sistemleri tarafından geçerli komutlar olarak algılanarak saldırganın çeşitli kötü niyetli eylemlerini gerçekleştirmesine olanak tanır. Örneğin, Resim 3.5'teki gibi, bir saldırgan akıllı bir hoparlörü kullanarak akıllı kilitleri açabilir, finansal işlemler başlatabilir veya bağlı cihazları kontrol edebilir.

NUIT saldırıları, ultrasonik dalgalar aracılığıyla sesli komutların gizlice iletilmesini sağlayan birçok teknik kullanır:

- Modülasyon ve demodülasyon: Ultrasonik sinyaller, konuşma benzeri desenler halinde modüle edilerek hedef cihaza iletilir. Cihazın mikrofonu bu sinyalleri yakalayıp demodüle ettiğinde bunları geçerli bir kullanıcı komutu olarak algılayabilir.
- Sinyal enjeksiyonu: Ultrasonik ses dalgaları, mikrofona doğrudan veya ortam yansımaları aracılığıyla iletilerek saldırı gerçekleştirilir.
- Algoritmik açıklardan yararlanma: Cihazların ses tanıma sistemlerinde ultrasonik frekansları normal konuşmalardan ayırt edemeyen algoritmalar bulunmaktadır. Saldırganlar bu zafiyetten yararlanarak cihazları istismar edebilir.

NUIT saldırılarının en tehlikeli yönlerinden biri, saldırının tamamen fark edilmeden gerçekleşebilmesidir. Kullanıcı, cihazının saldırıya uğradığını fark etmeden önemli güvenlik ihlallerine maruz kalabilir. Bu saldırılar şu riskleri beraberinde getirir:

- Yetkisiz erişim ve veri hırsızlığı: Saldırganlar, ultrasonik komutlar ile kullanıcı kimlik bilgilerini ele geçirebilir.
- Fiziksel güvenliğin tehlikeye girmesi: Akıllı kapı kilitlerinin açılması gibi saldırılar, fiziksel güvenliği tehdit edebilir.
- Kurumsal tehditler: Özellikle hükümet binaları, araştırma laboratuvarları ve finans kuruluşları gibi hassas bölgelerde saldırganlar kritik altyapıları hedef alabilir.
- Kimlik doğrulama sistemlerinin atlatılması: Sesle kimlik doğrulama sistemleri, bu tür saldırılara karşı hassastır ve saldırganlar sistemleri yetkisiz erişim için kullanabilir.

NUIT saldırılarının etkilerini en aza indirmek için çeşitli güvenlik önlemleri alınmalıdır:

- Gelişmiş filtreleme teknikleri: Cihaz mikrofonları, ultrasonik frekansları otomatik olarak filtreleyebilecek şekilde tasarlanmalıdır.
- Anormal durumları algılama algoritmaları: Sesli asistanlar, normal konuşma ile saldırıya yönelik ultrasonik komutları ayırt edebilecek yapay zekâ tabanlı sistemler ile desteklenmelidir.
- Kriptografik ses kimlik doğrulama: Kullanıcı ses imzalarının şifrelenerek doğrulanması, yetkisiz erişimleri engelleyebilir.
- Sesli komutlara ilişkin ekstra güvenlik katmanları: Özellikle finansal işlemler gibi kritik eylemler için ek doğrulama mekanizmaları (örneğin iki faktörlü kimlik doğrulama) uygulanmalıdır.
- Kullanıcı farkındalığının artırılması: Kullanıcılar, ultrasonik saldırıların farkında olmalı ve cihazlarını düzenli olarak kontrol etmelidir.

NUIT saldırıları, gelişen teknolojinin etkisiyle gelecekte daha da karışık hale gelerek akıllı cihazların güvenliğini ciddi şekilde tehdit edebilir. Bu nedenle üreticilerin güvenlik protokollerini sürekli olarak güncellemeleri ve kullanıcıların bilinçli hareket etmeleri kritik öneme sahiptir.

McKee ve Noever'ın 2023 tarihli ve "NUANCE: Near Ultrasound Attack on Voice Assistants" başlıklı çalışması, insan kulağı tarafından duyulamayan ancak mikrofonlar tarafından algılanabilen 16 kHz ila 20 kHz aralığındaki ultrasonik ses dalgaları kullanılarak gerçekleştirilen Near-Ultrasound Inaudible Trojan (NUIT) saldırılarını ele almaktadır. Araştırmacılar, NUIT saldırılarının temel mekanizmasını, uygulanabilirliğini ve bu tür saldırılara karşı olası savunma yöntemlerini incelemiştir. İlgili çalışmada saldırı mekanizması incelenmiştir. Buna göre NUIT saldırıları, ultrasonik dalgalar aracılığıyla sesli asistanlara gizli ve yetkisiz komutlar göndererek sistemleri manipüle etmeyi amaçlar. Bu saldırılarda insan kulağının algılayamayacağı frekansları kullandığından kullanıcıların herhangi bir anormal durum fark etmesi neredeyse imkansızdır. Araştırmada, saldırının başarıyla uygulanabilmesi için ses sinyalinin yüksek frekansta modüle edilmesi, hedef cihazın mikrofonunun bu sinyalleri algılaması ve sesli komut olarak işlemesi, saldırının fiziksel temas veya kullanıcı etkileşimi olmadan gerçekleşmesi gerektiği vurgulanmaktadır. Araştırmacılar çeşitli akıllı hoparlörler, akıllı telefonlar ve sesli asistanlar üzerinde NUIT saldırılarını test etmiş ve bu saldırının özellikle sürekli açık mikrofonlara sahip cihazlarda son derece etkili olduğunu göstermiştir. Çalışmada, saldırının başarı oranı, mesafe ve çevresel koşullara bağlı olarak değişse de çoğu modern mikrofon tarafından ultrasonik sinyallerin algılandığı kanıtlanmıştır. Ayrıca ilgili çalışmada NUIT saldırılarını önlemek amacıyla güvenlik önlemleri de önerilmektedir. Frekans filtreleme algoritmaları, mikrofon girişlerine entegre edilerek ultrasonik komutların engellenmesi; kimlik doğrulama mekanizmaları, sesli asistanlara gelen komutların yalnızca kayıtlı kullanıcılara ait olduğunun doğrulanması; donanım düzeyinde iyileştirmeler ve mikrofon üreticilerinin yalnızca insan kulağı tarafından algılanabilen frekans aralığında çalışan cihazlar geliştirmesi bu önerilerden bazılarıdır.

Yan ve diğerlerinin 2022 tarihli ve "A Survey on Voice Assistant Security: Attacks and Countermeasures" başlıklı çalışması ise NUIT saldırılarının teknik detaylarını ve güvenlik açıklarını derinlemesine inceleyerek saldırının nasıl gerçekleştirildiğini ve modern sesli komut sistemlerine yönelik risklerini analiz etmektedir. Söz konusu çalışmaya göre NUIT saldırıları, ilk olarak 2023 yılında akademik literatürde detaylı bir şekilde ele alınmış ve özellikle sesli asistanlar, akıllı hoparlörler ve mobil cihazlara yönelik ciddi bir tehdit olarak tanımlanmıştır. Saldırganlar, hoparlörler üzerinden mikrofonlara gizli komutlar göndermek için ultrasonik dalgaları kullanarak sistemlerin fark edilmeden manipüle edilmesini sağlamaktadır. NUIT saldırılarının gerçekleştirilmesi için gereken aşamalar da çalışmada

tanımlanmıştır. İlk olarak sinyal üretimi aşamasında saldırgan ultrasonik frekansta modüle edilmiş bir ses sinyali üretir, daha sonra sinyal hoparlörler veya belirli bir yönlendirme tekniği ile hedef mikrofonlara iletilir, hedef cihazın mikrofonu bu ultrasonik sinyalleri tanır, insan sesi olarak yorumlar ve son olarak cihaz sahte sesli komutları işleyerek belirtilen eylemleri gerçekleştirir. Bu mekanizma saldırganların yetkisiz olarak sesli asistanları kullanmasına, kapıları açmasına, ödemeler yapmasına veya kişisel verilere erişmesine olanak tanımaktadır. Araştırmada NUIT saldırılarının geniş çapta uygulanabilir olduğu ve modern mikrofon teknolojisinin bu tür saldırılara karşı yeterli koruma sunmadığı gösterilmiştir. Özellikle gizli ve tespit edilemez saldırılar, kullanıcıların saldırının gerçekleştiğini fark edememesi; finansal ve veri güvenliği tehditleri, sesli komutlarla banka işlemlerinin manipüle edilmesi; kurumsal güvenlik açıkları, büyük ölçekli organizasyonlarda kullanılan akıllı hoparlörler ve IoT cihazlarının risk altında olması öne çıkmaktadır. Yan ve diğerleri, NUIT saldırılarını önlemek için birkaç yöntem önermektedir: Sesli komut doğrulama, sesli asistanların her komutu doğrulaması için ek kimlik doğrulama mekanizmalarının uygulanması, donanım ve yazılım filtreleri, mikrofonların insan sesiyle ultrasonik sinyalleri ayırt edebilecek şekilde tasarlanması, kullanıcı farkındalığı, cihaz kullanıcılarının ultrasonik saldırılar konusunda bilinçlendirilmesi ve güvenlik önlemlerinin artırılması önerilen yöntemlerdendir.

DolphinAttack ve Near-Ultrasound Inaudible Trojan (NUIT) saldırıları, akıllı cihazlar ve sesli asistanlar gibi sesle etkinleştirilen sistemlere yönelik sofistike tehditler oluştursa da her biri farklı saldırı yöntemleri ve teknikler kullanmaktadır. DolphinAttack, ultrasonik ses dalgalarını kullanarak cihazların mikrofonlarına sesli komutlar iletmekte ve böylece cihazları kontrol altına almaktadır. Bu saldırı, insan kulağının duyamayacağı frekansta ses sinyalleri göndererek akıllı telefonlar, akıllı hoparlörler ve akıllı ev sistemleri gibi cihazlara komutlar verilmesini sağlar (Zhang ve diğerleri, 2017). Bu teknikte karşılaşılan ana zorluk, bu tür sinyallerin fark edilememesi ve ses filtrelerini kolaylıkla aşabilmesidir, bu da kullanıcıların farkında olmadan cihazlarının saldırgan tarafından kontrol edilmesine yol açabilir.

Buna karşın NUIT, elektromanyetik dalgalar kullanarak benzer bir amaca ulaşır, ancak kullandığı teknik tamamen farklıdır. NUIT, sesli komutları doğrudan cihazın mikrofonuna göndermek yerine elektromanyetik darbelerle cihazların elektronik sistemlerine müdahale eder. Bu saldırı, özellikle sesli asistanlar ve sesli komutla etkinleştirilen cihazlar için bir

tehdit oluşturur. NUIT'in belirgin farkı, elektromanyetik sinyallerle saldırı yapması ve doğrudan sesle iletilen komutlar yerine elektronik bileşenlere etki etmesidir (G. Chen ve diğerleri, 2023). Bu tür bir saldırının tespit edilmesi, kullanılan elektromanyetik dalgaların izlenmesi gerektiğinden oldukça zordur ve genellikle özel donanım gereksinimlerini beraberinde getirir.

NUIT'in temel farklarından bir diğeri de bu saldırının yalnızca sesli komutlarla sınırlı kalmaması ve internet üzerinden uzaktan gerçekleştirilmesi olmuştur. Guenevere Chen ve ekibi tarafından geliştirilen bir NUIT saldırısı, popüler akıllı cihazlar ve sesli asistanlara yönelik uzaktan, sessiz bir saldırı yöntemi olarak dikkat çekmektedir (G. Chen ve diğerleri, 2023). Örneğin bir kullanıcı, bir YouTube videosu izlerken kötü amaçlı bir NUIT saldırısı, video veya ses dosyasındaki sinyalleri kullanarak cihazın mikrofonunu hedef alabilir ve cihazın sesli asistanını aktif hale getirebilir. Bu durum, saldırganların kullanıcıların cihazlarını fiziksel müdahale olmadan, sadece sesli komutlar aracılığıyla kontrol etmelerine imkân tanımaktadır. Özellikle NUIT saldırısının başarılı olabilmesi için cihazın ses seviyesi yeterince yüksek olmalı ve saldırı komutlarının süresi 77 milisaniyeyi aşmamalıdır. Bu da NUIT'in oldukça hızlı ve etkili bir şekilde saldırı gerçekleştirmesini sağlar (G. Chen ve diğerleri, 2023).

Her iki saldırı türü de sesli asistanları hedef alır, ancak DolphinAttack ultrasonik dalgalarla cihazların mikrofonlarını manipüle ederken NUIT elektromanyetik sinyalleri kullanarak daha geniş bir cihaz yelpazesinde etki gösterebilir. Ayrıca NUIT'in internet üzerinden uzaktan gerçekleştirilebilmesi, onu daha karmaşık ve tespit edilmesi zor bir tehdit haline getirir. NUIT, kullanıcıların cihazlarını, özellikle de sesli asistanlarını, çok daha sessiz bir şekilde ele geçirebilir ve bu da saldırıların fark edilmesini daha da zorlaştırır. Sonuç olarak her iki saldırı türü de önemli güvenlik açıkları yaratmakta ancak NUIT'in uzaktan erişim yetenekleri ve elektromanyetik müdahale kullanımı, onu benzersiz ve özellikle tespit edilmesi çok daha zor bir tehdit haline getirmektedir.

Sonuç olarak Near-Ultrasound Inaudible Trojan (NUIT) saldırıları, sesle etkileşime giren cihazların güvenliğini ciddi şekilde tehdit eden gelişmiş bir saldırı tekniği olarak karşımıza çıkmaktadır. Uluslararası araştırmalar, özellikle son yıllarda NUIT saldırılarının kullanım alanlarının arttığını ve bu tür tehditlerin akıllı cihazlar, sesli asistanlar ve IoT sistemlerinde yaygınlaşarak daha büyük güvenlik risklerine yol açtığını göstermektedir. NUIT’in temel

özelliklerinden biri, saldırıların insan kulağının algılayamayacağı ultrasonik frekanslarla gerçekleştirilmesi ve cihazların ses tanıma sistemlerine zarar vererek kullanıcının fark etmeden kötü niyetli komutları işleme almasını sağlamasıdır. Bu saldırılar, cihazlara fiziksel müdahaleyi gerektirmeden uzaktan ve gizlice gerçekleştirilebilir, bu da güvenlik protokollerinin yetersiz kaldığı durumlarda ciddi ve büyük zararlar meydana getirebilir.

Saldırıların etkisini azaltmak için çeşitli savunma önlemleri önerilmektedir. Mikrofonlarda ultrasonik sinyalleri filtreleyebilecek sistemlerin entegrasyonu ve sesli komutlara ek güvenlik katmanları eklenmesi ve kullanıcı farkındalığının artırılması, bu tehditlere karşı korunmada önemli rol oynamaktadır. Ancak NUIT saldırılarının hızla evrilmesi, güvenlik önlemlerinin sürekli olarak güncellenmesini ve gelişen saldırı tekniklerine karşı hazırlıklı olunmasını gerektirmektedir. Bu bağlamda üreticilerin ve kullanıcıların NUIT gibi tehditlere karşı daha etkili ve güncel çözümler geliştirmesi elzemdir.

3.9. SurfingAttack Saldırıları

Ses tabanlı akıllı cihazlar, günlük yaşamın ayrılmaz bir parçası haline gelmiş olup bu teknolojik ilerlemeler beraberinde yeni siber güvenlik tehditlerini de getirmiştir. Sesle çalışan IoT cihazlarının hızla yaygınlaşmasıyla birlikte, ses tabanlı saldırılar ciddi bir güvenlik riski haline gelmiştir. Gong ve diğerleri (2019), ses tabanlı saldırıları dört ana kategoriye ayırmaktadır: Temel ses kaydı saldırıları, işletim sistemi seviyesindeki saldırılar, makine öğrenmesi seviyesindeki saldırılar, donanım seviyesindeki saldırılar.

Makine öğrenmesi seviyesindeki saldırılar, otomatik konuşma tanıma (ASR) sistemlerini hedef alarak ASR sistemleri tarafından anlaşılabilen ancak insanlar tarafından kolayca fark edilemeyen saldırı komutları kullanır. Donanım seviyesindeki saldırılar ise insan sesi yerine sentetik analog sinyallerin tekrarlanmasına dayanır. Örneğin Kasmi ve Esteves (2015), kulaklık kablolarına kasıtlı elektromanyetik girişim uygulayarak akıllı telefonlara sesli komut enjekte eden bir saldırı yöntemi sunmuştur. Son yıllarda ortaya çıkan ve donanım seviyesindeki bir saldırı türü olan "SurfingAttack" tekniği, sesli asistanlar ve diğer ses tabanlı sistemlerin güvenlik açıklarını hedef alan gelişmiş bir siber saldırı yöntemi olarak dikkat çekmektedir. Bu saldırı, ultrasonik ses dalgalarını kullanarak akıllı cihazların MEMS (Micro-Electro-Mechanical Systems) mikrofonları aracılığıyla kullanıcıdan bağımsız olarak komutlar almasını sağlamaktadır.

SurfingAttack, siber güvenlik literatüründe ilk olarak Yan ve arkadaşları (2020) tarafından tanımlanmıştır. Araştırmalar, MEMS mikrofonlarının insanların duyamayacağı yüksek frekanslı ses sinyallerine tepki verebildiğini göstermiştir. Bu durum, saldırganların akıllı cihazlarla kullanıcı farkında olmadan etkileşime girebileceğini ortaya koymuştur.

Son zamanlarda araştırmacılar, ses ve ultrasonik ses dalgalarına dayalı saldırı yöntemleri geliştirmiştir. Bolton ve diğerleri (2018), özel olarak tasarlanmış ultrasonik ses tonlarının sabit disk sürücülerini (HDD) bozarak işletim sistemlerini çökerttiğini göstermiştir. Trippel ve diğerleri (2017) ise MEMS ivmeölçerlerin akustik rezonans enjeksiyonları yoluyla manipüle edilebileceğini kanıtlamıştır. Bunun yanı sıra ultrasonik ses dalgaları kullanılarak sesle kontrol edilen sistemlere yönelik saldırılar gerçekleştirilmiştir. Ancak ultrasonik ses dalgalarının doğrusal yayılım özelliği ve ultrasonik ses hoparlörlerinin kolay tespit edilebilir şekilde bir boyuta sahip olması nedeniyle bu tür saldırıların uygulanması çok sınırlıdır. Yine de bu tür saldırılar, gizlilik ve güvenlik açısından çok daha büyük riskler oluşturmaktadır.

Başlangıçta ultrasonik ses tabanlı saldırılar kısa mesafelerle sınırlıyken ve çevresel faktörlerden kolayca etkilenirken zamanla geliştirilen yöntemler sonucunda daha etkili hale gelmiştir. 2017 yılında tanıtılan DolphinAttack, ultrasonik frekanslar kullanarak sesli asistanları hedef almış ancak yalnızca hava yoluyla iletilen sinyallerle çalışabilmiştir (Zhang ve diğerleri, 2017). SurfingAttack ise 2020 yılında geliştirilmiş olup katı malzemeler üzerinden yayılan ultrasonik dalgaları kullanarak daha uzun mesafelerde ve doğrudan görüş hattı gerektirmeden etkileşim kurabilen bir yöntem olarak öne çıkmıştır (Yan ve diğerleri, 2020).

SurfingAttack saldırısında kullanılan yönlendirilmiş dalga teknolojisi, tahribatsız muayene (NDT) ve yapısal sağlık izleme (SHM) gibi alanlarda uzun süredir kullanılmaktadır. Yönlendirilmiş dalga testinde (GWT), dayanıklı katı yapılar boyunca enerji kaybı olmadan uzun mesafelere yayılabilen akustik dalgalar kullanmaktadır. Bu yöntem çelik borular, demir yolu rayları ve metal kompozit yapıların incelenmesi gibi alanlarda yaygın olarak uygulanmaktadır.

Yan ve diğerlerinin 2020 tarihli “SurfingAttack: Interactive Hidden Attack on Voice Assistants Using Ultrasonic Guided Waves” başlıklı çalışmasında, farklı iletim ortamları bağlamında yeni bir saldırı türü olarak tanımlanan SurfingAttack’ın teknik ve operasyonel

özellikleri detaylı biçimde ele alınmıştır. Bu saldırı türü, sesle kontrol edilen cihaz ile saldırgan arasında birden fazla turdan oluşan bir iletişim kurulmasına olanak tanımakta ve doğrudan görüş açısı gerektirmeden daha uzun mesafelerden saldırı gerçekleştirilmesini mümkün kılmaktadır. SurfingAttack, duyulamayan ses saldırılarının etkileşim döngüsünü tamamlayarak SMS doğrulama kodlarının ele geçirilmesi, kullanıcı farkında değilken sahte aramalar yapılması gibi çeşitli yeni saldırı senaryolarının uygulanabilmesine neden olmaktadır. İlgili çalışmada, SurfingAttack'ın gerçekleştirilmesi için aşılması gereken birtakım teknik zorluklara da yer verilmiştir. Öncelikle katı malzemeler üzerinden etkili bir SurfingAttack saldırısı gerçekleştirebilmek adına, sinyalin çok yönlü iletimini mümkün kılacak şekilde özel olarak tasarlanması gerekmiştir. İkinci olarak bu yeni saldırı yöntemi, fiziksel olarak yakın bulunan bir kullanıcıyı fark ettirmeden birkaç iletişim turunu tamamlayabilme kapasitesine sahiptir. Bu durum, sesle kontrol edilen cihazların genellikle yalnızca insanlar tarafından kullanılmak üzere tasarlanmış olması nedeniyle önemli bir mühendislik zorluğu oluşturmaktadır. Çalışmada, söz konusu saldırı modelinin oluşturduğu güvenlik tehdidinin azaltılmasına yönelik potansiyel savunma yöntemleri ve deneysel bulgular da sunulmuştur. Bununla birlikte çalışmada katı malzemelerin iletim ortamı olarak kullanılması yoluyla duyulamayan ultrasonik saldırılar gerçekleştirmenin fizibilitesi araştırılmıştır. Bilindiği kadarıyla bu çalışma, yönlendirilmiş dalga teknolojisinden yararlanarak sesli asistanları hedef alan ilk saldırı yöntemini sunmaktadır. Hava yolu ile iletilen sinyal tabanlı diğer saldırı yöntemleriyle karşılaştırıldığında SurfingAttack saldırısı, ses sinyallerini malzeme içerisine gizleyerek gerçekleştirilmesiyle daha önce mümkün olmayan saldırı senaryolarının hayata geçirilmesine olanak tanımaktadır. Çalışmada yapılan örnek bir saldırıda, ultrasonik yönlendirilmiş dalga enerjisi kullanılarak sadece 0.75W güçle yaklaşık 30 fit (yaklaşık 9 metre) uzunluğundaki bir masa boyunca saldırının başarıyla gerçekleştirilebildiği gösterilmiştir. Sesle kontrol edilen cihazların insan-bilgisayar etkileşimi temelinde çalışır, bu saldırı türünde saldırganın cihazla minimum ses seviyesinde karşılıklı etkileşime girerek örneğin SMS doğrulama kodlarını ele geçirmesi veya sahte telefon görüşmeleri gerçekleştirmesi mümkün hale gelmektedir. Sonuç olarak söz konusu çalışmada SurfingAttack saldırısının gerçekleştirilmesine yönelik teknik detaylar kadar bu yeni tehdit türüne karşı geliştirilebilecek savunma mekanizmaları üzerine çeşitli tartışmalara da yer verilmiştir. Bu sayede hem donanımsal hem de yazılımsal düzeyde saldırının önlenmesine yönelik çözüm önerileri geliştirilerek sesle çalışan sistemlerin güvenliği açısından önemli bir katkı sunulmuştur.

SurfingAttack genellikle yüksek frekansta modüle edilen ultrasonik ses sinyallerinin MEMS mikrofonlarına iletilmesiyle gerçekleştirilir. MEMS mikrofonları, ses dalgalarını elektriksel sinyallere dönüştüren küçük mekanik-elektrik sistemleridir ve çoğu modern akıllı cihazda bulunmaktadır. Ancak, bu mikrofonlar 16 kHz - 100 kHz frekans aralığında da sinyalleri algılayabilmektedir. Bu saldırı tekniği genellikle aşağıdaki adımları takip eder:

- Ultrasonik sinyal üretimi: Saldırgan, piezoelektrik dönüştürücüler veya yüksek frekanslı hoparlörler aracılığıyla ultrasonik sinyaller üretir.
- Modülasyon: Üretilen ultrasonik sinyal, hedef cihaza iletilecek bir komut içerir. Örneğin bir sesli asistanın belirli bir komutu algılaması sağlanabilir.
- Yansıtma ve yönlendirme: Ultrasonik sinyaller, masa, cam veya ahşap gibi sert yüzeyler üzerinden yönlendirilerek hedef cihaza ulaştırılır.
- Sinyalin mikrofon tarafından algılanması: MEMS mikrofonları, gelen sinyali sesli bir komut olarak algılar ve işlemciye iletir.
- Komutun uygulanması: Akıllı cihaz, saldırganın verdiği komutu çalıştırarak belirlenen işlemi gerçekleştirir. Örneğin bir saldırgan, bir masanın altına gizli bir piezoelektrik dönüştürücü yerleştirerek masanın üzerindeki bir akıllı telefonun sesli asistanını etkinleştirebilir ve cihaz sahibinin haberi olmadan arama yapma, mesaj okuma veya ödeme işlemleri gerçekleştirme komutları verebilir (Lakshmanan, 2020).

SurfingAttack ayrıca ciddi güvenlik riskleri de barındırmaktadır. Başlıca tehditler şunlardır:

- Yetkisiz erişim: Kullanıcıların bilgisi dışında cihazlarının kontrol edilmesine yol açabilir ve kişisel verilerin ele geçirilmesine sebep olabilir.
- Finansal riskler: Saldırgan, kullanıcının ödeme bilgilerine erişerek yetkisiz para transferleri veya alışverişler yapabilir.
- Kurumsal güvenlik açıkları: Şirket içi iletişim sistemleri ve konferans odalarındaki akıllı cihazlar manipüle edilebilir.
- Gizlilik ihlalleri: Kullanıcının sesi taklit edilerek yapılan komutlarla özel görüşmeler kaydedilebilir veya üçüncü taraflarla paylaşılabilir.

SurfingAttack gibi saldırılara karşı korunmak için geliştiriciler ve kullanıcılar çeşitli önlemler almalıdır:

- Ultrasonik sinyal algılama: Cihazlar, insan sesiyle uyumsuz olan ultrasonik sinyalleri tespit eden gelişmiş sinyal işleme algoritmaları ile donatılmalıdır.
- Frekans filtreleme: MEMS mikrofonları, yalnızca insan kulağının algılayabileceği frekans aralığında çalışacak şekilde tasarlanmalıdır.
- İki faktörlü kimlik doğrulama (2FA): Özellikle finansal işlemler için ek güvenlik adımları zorunlu hale getirilmelidir.
- Mikrofon hassasiyet kontrolleri: Cihazlar, çevresel faktörlere göre mikrofon hassasiyetini ayarlayabilmeli ve belirli durumlarda mikrofon erişimini sınırlandırmalıdır.
- Kullanıcı farkındalığı: Kullanıcılar, sesli asistanların güvenli kullanımına yönelik bilinçlendirilmeli ve açık alanlarda veya bilinmeyen cihazlarla sesli komut kullanımını sınırlandırmalıdır.

Son yıllarda yapay zekâ ve doğal dil işleme alanındaki gelişmeler, insan-bilgisayar etkileşiminde sesin temel bir yöntem haline gelmesini sağlamıştır. Siri, Alexa, Google Assistant gibi sesli asistanlar ve sesle kontrol edilen askeri gemiler gibi yeni nesil teknolojiler bu gelişmelerin sonucudur. Ancak araştırmacılar yakın zamanda bu sistemlerin duyulamayan frekanslarda yapılan sinyal enjeksiyonlarına karşı savunmasız olduğunu göstermiştir. Mevcut çalışmaların çoğu, genellikle doğrudan görüş hattı içinde ultrasonik hoparlörler kullanarak tek bir komut göndermeye veya hoparlör dizileri ile saldırının menzilini genişletmeye odaklanmaktadır. Ancak hava dışında, ses dalgaları titreşimin mümkün olduğu diğer malzemeler aracılığıyla da yayılabilir. Bu şekilde SurfingAttack, ses tabanlı akıllı cihazların güvenliğini tehdit eden güncel bir saldırı yöntemi olarak öne çıkmaktadır.

SurfingAttack, DolphinAttack ve NUIT ile kıyaslandığında sesli cihazlara yönelik gerçekleştirilen ses tabanlı saldırılar arasında kendine özgü birkaç önemli fark sunmaktadır. Her üç saldırı türü de sesli cihazlara, özellikle sesli asistanlara müdahale etmeyi amaçlasa da kullandıkları teknikler ve etki alanları farklıdır. DolphinAttack, ultrasonik ses dalgaları kullanarak sesli cihazlara komutlar gönderen bir saldırıdır. İnsan kulağının duymadığı frekansta sesler göndererek cihazların mikrofonlarını manipüle eder (Zhang ve diğerleri,

2017). Ancak DolphinAttack genellikle daha kısa mesafelerde etkili olur ve çevresel faktörlere duyarlıdır. Diğer yandan NUIT, elektromanyetik dalgaları manipüle ederek cihazlarla etkileşim kurar ve özel donanım gerektirir. NUIT, elektromanyetik alanları hedef alarak cihazları kontrol etmeyi sağlar ancak daha fazla teknik bilgi ve ekipman gerektiren bir saldırıdır. SurfingAttack ise bu iki saldırı türünden farklı olarak özellikle MEMS mikrofonlarını hedef alır ve yüksek frekanslı ultrasonik dalgalar kullanarak cihazları kontrol eder (Yan ve diğerleri, 2020). Bu saldırı, çok daha geniş bir etki alanına sahip olmasının yanı sıra doğrudan cihazla temasa gerek duymadan katı yüzeyler üzerinden yansıtılan sinyallerle etkili hale gelir. SurfingAttack daha uzun mesafelerde ve hatta yansıyan ses dalgalarıyla bile başarılı olabilen bir saldırıdır, bu da onu DolphinAttack ve NUIT'ten ayıran en önemli özelliktir. Özetle SurfingAttack, ultrasonik dalgaların yüksek frekansları ve MEMS mikrofonlarının özelliklerini kullanarak daha geniş mesafelerde ve daha karmaşık ortamlarda başarılı olabilirken DolphinAttack ve NUIT daha kısa mesafeler ve daha teknik altyapılarla sınırlıdır. Bu da SurfingAttack'ın daha güçlü ve zarar verme potansiyeli daha yüksek bir tehdit oluşturduğunu gösterir.

Sonuç olarak SurfingAttack sesle çalışan akıllı cihazların güvenliğini ciddi şekilde tehdit eden çok yeni bir saldırı türüdür. Ultrasonik yönlendirilmiş dalgaların kullanılmasıyla bu saldırı, doğrudan görüş açısı gerektirmeden ve kullanıcı farkında olmadan akıllı cihazlarla etkileşime girilmesine olanak tanımaktadır. MEMS mikrofonlarının yüksek frekanslı sesleri algılama kapasitesinin kullanılması, saldırganlara bu tür cihazlarla gizli bir şekilde etkileşim kurma fırsatı sunmaktadır. Çalışmalar SurfingAttack gibi tehditlerin önlenmesi için hem donanım hem de yazılım düzeyinde güvenlik önlemlerinin önemini vurgulamaktadır. Özellikle ultrasonik sinyalleri algılayabilen gelişmiş sinyal işleme algoritmalarının cihazların sadece insan kulağına duyulabilir frekansta çalışacak şekilde tasarlanmasının ve mikrofon hassasiyet kontrollerinin devreye sokulmasının önemine dikkat çekilmektedir. Ayrıca kullanıcı farkındalığının artırılması, bu tür saldırılara karşı savunmada kritik bir faktör olarak öne çıkmaktadır. Teknolojinin hızla gelişen doğası, yeni saldırı yöntemlerini beraberinde getirmekte ve siber güvenlik stratejilerinin de bu hızla evrilmesi gerektiğini ortaya koymaktadır. Sonuç olarak sesli asistanlar ve diğer sesle kontrol edilen sistemlerin güvenliği, sadece yazılımsal değil aynı zamanda donanım bazlı önlemlerle de sağlanmalıdır. Bu bağlamda hem geliştiriciler hem de kullanıcılar, güvenlik açıklarını azaltmak için güncel yaklaşımlar geliştirmeli ve bu teknolojilerin güvenli kullanımı sağlanmalıdır.

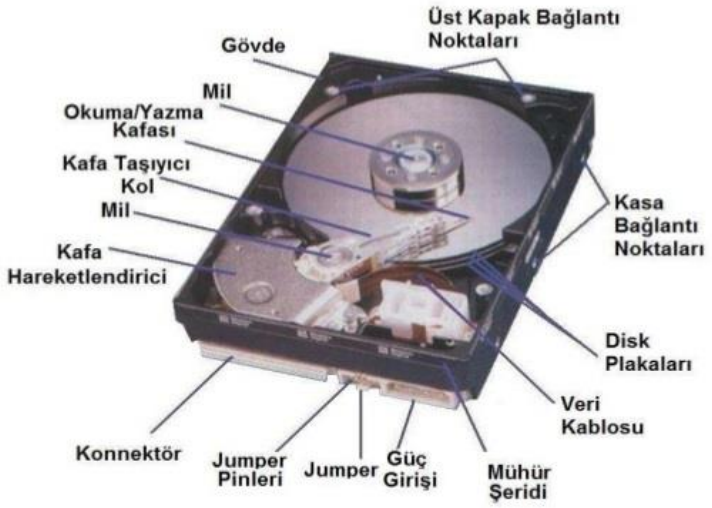
3.10. HDD Üzerine Yapılan Ultrasonik Ses Tabanlı Saldırılar

Hard disk sürücüleri (HDD), bir diğer adıyla sabit disk sürücüleri, sürücü ünitesine kalıcı olarak sabitlenmiş olan sert bir manyetik disktir ve veri depolamak amacıyla kullanılmaktadır (ABD Ticaret Bakanlığı Ulusal Standartlar ve Teknoloji Enstitüsü, 2014). Her diskin yüzeyi, manyetik alan etkisine sahip manyetik bantla kaplanmıştır. Disk plakaları, manyetik olmayan alüminyum ya da cam gibi malzemelerden imal edilmektedir.

Disklerin yüzeyine oldukça yakın bir konumda yer alan yazma ve okuma kafaları bulunur. Her kafada, magnetorezistif (MR) bir algılayıcı yer alır. Yazma ve okuma kafası, diskin yüzeyinden geçerken MR algılayıcısında direnç değişimi meydana gelir. Bu analog direnç değişikliği, sayısal verilere dönüştürülerek işlenir.

Hard disklerde sabit hızda dönen disklerin bağlı olduğu bir iğne bulunmaktadır. Diskler arasında ve yüzeyde hareket eden yazma ve okuma kafaları ortak bir kola bağlıdır. Bu taşıyıcı kol, kafaların yay şeklinde hareket etmesini sağlayarak dönen disklerin tüm yüzeylerinin taranmasını mümkün kılar. Böylece her bir kafa, karşılık geldiği diskin neredeyse tamamını tarayabilir.

Diskleri döndüren iğnenin hareketleri, yazma ve okuma kafalarını hareket ettiren taşıyıcı kolun hareketleri ve yazma-okuma işlemi, elektronik kontrol kartı tarafından denetlenir. Resim 3.6'da hard disk ve yapısı gösterilmiştir.



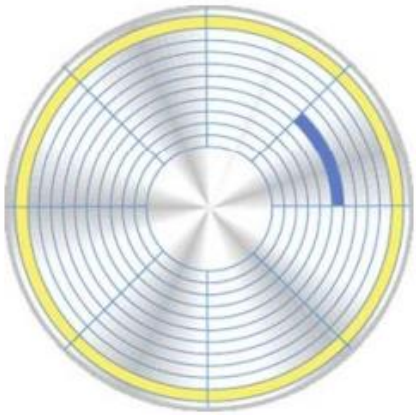
Resim 3.6. Bir hard diskin iç yapısı (Teknocityblog, 2016)

Bir sabit diskin veri kapasitesini artırmak için disk sayısı artırılabilir, her bir diske iki yazma ve okuma kafası karşılık gelir. Böylece diskler çift taraflı kullanılabilir hale gelir.

Yazma ve okuma kafalarını taşıyan hareketli kol, son derece hızlı bir şekilde hareket eder; bu kol, kenardan merkeze ve tekrar başlangıç noktasına gelme hareketini saniyede 50 kez gerçekleştirebilir. Bu işlem, yüksek hızlı doğrusal bir motorla gerçekleştirilir. Sabit disk plakaları da aynı şekilde hızlı bir şekilde döner.

Sabit diskler, kapasiteleri ve devir sayıları ile tanımlanır. Sabit disklerin kapasiteleri, en küçük anlamlı bilgi birimi olan Byte'ın üst katlarıyla ifade edilirken devir sayısı RPM (Rotation Per Minute – dakika başına dönüş sayısı) birimi ile belirtilir ve sabit disk plakalarının dakikada gerçekleştirdiği dönüş sayısını ifade eder. 1990'lardan günümüze kadar 3600rpm, 5400rpm, 7200rpm ve 10000rpm dönüş hızına sahip sabit disk sürücüleri üretilmiştir. Yüksek rpm değerine sahip diskler daha fazla ısındığından içerisine monte edilecek kasada hava sirkülasyonunun ideal şekilde sağlanması büyük önem taşır.

Disk plakaları son derece hassas bir yapıya sahiptir. Üzerinde toz, tüy, nem veya buhar gibi kirletici unsurların kesinlikle bulunmaması gerekir. Yazma ve okuma kafası ile disk yüzeyi arasında gözle görülemeyecek kadar ufak bir boşluk vardır, bu nedenle bu boşluğa yabancı maddelerin girmemesi kritik öneme sahiptir. Aksi takdirde bu bölgede yer alan bilgiler ve bunlarla ilişkili daha büyük veri kümeleri okunamayabilir. Eğer yazma ve okuma kafası herhangi bir nedenle (örn. sallantı veya düşme) disk yüzeyine temas ederse ilgili alan hasar görür ve bu durumda "bad sector" olarak adlandırılan ölü bölgeler oluşabilir (Resim 3.7).



Resim 3.7. Disk üzerinde iz (track) ve kesim (sector) oluşturulması (T.C. Millî Eğitim Bakanlığı, 2007)

Fiziksel kusurlar nedeniyle oluşan ölü bölgelerin kurtarılması mümkün değildir. Disk plakalarında bad sector sayısının artması, sabit diske işletim sistemi kurulumunu engelleyebilir veya disk performansını önemli ölçüde yavaşlatabilir.

Bir sabit disk kullanılmadan önce mutlaka formatlanması gerekir. Formatlama, sabit diskin üzerine yazılacak bilgilerin nerelere ve hangi standartlara göre kaydedileceğini belirleme sürecidir. Formatlanmamış bir sabit diske, anlamlı bilgi kümeleri yazmak mümkün değildir.

Sabit disklerde veriler, iz (track) ve kesim (sector) adı verilen alanlarda depolanır. Resim 3.7'de izler sarı, sektörler ise mavi renkle gösterilmiştir. Her bir sektör belirli bir byte sayısını (örneğin, 256 byte ya da 512 byte) tutar. İşletim sistemi düzeyinde ya da disk sürücüsünün kendisinde, bu sektörler küme (cluster) adı verilen gruplara ayrılır. Sektörler ve izler, düşük seviyeli formatlama işlemiyle plakalar üzerinde oluşturulur. Her bir sektörün başlangıç ve bitiş noktaları da plakaya yazılır. Düşük seviye formatlama işlemi, sabit diskin byte bloklarını tutabilecek şekilde hazırlanmasını sağlar. Bu işlemden sonra yüksek seviyeli formatlama gerçekleştirilir ve burada sektörlere FAT (File Allocation Table – Dosya Ayırma Tablosu) gibi dosya depolama yapıları yazılır (T.C. Millî Eğitim Bakanlığı, 2007). Böylece sabit disk, üzerine dosya yazma işlemleri için hazır hale gelir.

Sabit disk sürücüleri (Hard Disk Drives - HDD), modern bilgisayar sistemlerinin veri depolama mimarisinin temel taşlarından biri haline gelmiştir. Bu teknolojinin temelleri 1950'li yıllarda IBM tarafından atılmıştır. IBM mühendislerinden Reynold B. Johnson, bilgisayarlarda doğrudan erişimli bir depolama aygıtına duyulan ihtiyaçtan yola çıkarak ilk sabit disk sürücüsünü geliştirmiştir. 1956 yılında tanıtılan IBM 350 Disk File, IBM 305 RAMAC sistemine entegre edilmiş ve bu sistemle birlikte veri depolamada yeni bir çağ başlatmıştır (Record Nations, 2024).

Başlangıçta bu diskler, dışsal birimler olarak konumlandırılmış ve oldukça büyük fiziksel boyutlara sahipti. Veri saklama kapasitesi sınırlı olmasına rağmen, manyetik bant teknolojisine kıyasla daha hızlı veri erişimi sağlamaları nedeniyle tercih edilmişlerdir. İlk sabit diskler birden fazla manyetik "plaka" içeriyor ve iklim kontrollü ortamlarda çalıştırılıyordu. Bu nedenle ilk nesil sabit diskler, özellikle kurumsal veri merkezlerinde kullanılmaya uygun bir altyapı gerektiriyordu (McLoughlin, 2011: 1, 512).

1980’li yıllarda kişisel bilgisayarların yaygınlaşmasıyla birlikte sabit disk sürücülerinin ev kullanıcılarına yönelik versiyonları geliştirilmeye başlandı. Apple, 1983 yılında ProFile adlı ilk harici sabit disk modelini piyasaya sürdü. Ancak bu model geniş çaplı başarı elde edemedi ve birçok üretici, veri saklama birimlerini dahili sürücülere entegre etmeye yöneldi. Bu yaklaşım, özellikle 1980’lerin sonları ve 1990’ların başlarında sabit disklerin standart bir donanım bileşeni haline gelmesini sağladı (Record Nations, 2024).

1994 yılında, yedi büyük teknoloji şirketinin ortaklığıyla Universal Serial Bus (USB) teknolojisinin geliştirilmesi, harici sabit disk sürücülerinin yeniden ön plana çıkmasına neden oldu. Bu dönemde geliştirilen sürücüler, USB portları aracılığıyla bilgisayarlara bağlanabiliyor ve taşınabilir veri depolama ihtiyaçlarına etkin çözümler sunuyordu. Günümüzde ise hem harici hem de dahili sabit diskler yüksek kapasiteleri ve gelişmiş veri aktarım hızları ile dijital dünyada temel bir rol oynamaktadır.

Özellikle cam tabanlı disk plakalarının geliştirilmesi, termal genleşmeye karşı daha dayanıklı sürücüler üretilmesini mümkün kılmış, bu da sabit disklerin güvenilirliğini ve ömrünü artırmıştır (McLoughlin, 2011: 1, 512). Modern sabit disklerde kullanılan okuma ve yazma kafaları, medya yüzeyine mikron seviyesinde yakınlıkta "uçmakta" ve hiçbir fiziksel temas olmaksızın veri aktarımı gerçekleştirmektedir. Bu yapı "Winchester" sürücüler olarak bilinen ve günümüzün temel HDD teknolojisini oluşturan disk tiplerinin temelini teşkil etmektedir.

Sonuç olarak sabit disk teknolojisi, 1950’li yıllardaki büyük ve hantal yapısından, bugün milyonlarca gigabayt veriyi taşınabilir bir şekilde barındırabilen kompakt ve verimli sistemlere evrilmiştir. Bu evrim, yalnızca teknolojik ilerlemeyi değil, aynı zamanda bilgiye erişim biçimimizin dönüşümünü de temsil etmektedir.

Bu teknolojik ilerlemeler sabit disklerin sadece depolama kapasitesi açısından değil, aynı zamanda işleyiş dinamikleri bakımından da daha karışık ve hassas hale gelmesine neden olmuştur. Özellikle mikron düzeyinde çalışan okuma ve yazma kafalarının disk yüzeyiyle temassız çalışması, mekanik hassasiyetin üst düzeye taşınmasını beraberinde getirmiştir. Bu durum, sabit disk sürücülerini yalnızca elektromanyetik ya da fiziksel temas kaynaklı tehditlere değil aynı zamanda dışsal çevresel faktörlere karşı da savunmasız hale getirmiştir. Yapılan deneysel çalışmalar, HDD’lerin yapısal rezonans noktalarına yakın frekanslarda

maruz bırakıldıklarında, okuma-yazma sürecinde ciddi bozulmalar ve veri kayıpları yaşanabildiğini göstermektedir (Shahrad ve diğerleri, 2018). Bu tür bulgular, sabit disk teknolojisinin evrimiyle birlikte ortaya çıkan yeni güvenlik açıklarını ve bu sistemlerin ses tabanlı saldırılar gibi beklenmedik tehditlere karşı ne derece savunmasız olduğunu gözler önüne sermektedir.

Son yıllarda yapılan çalışmalar, sabit disk sürücülerinin (HDD) yalnızca fiziksel temasla değil, aynı zamanda belirli akustik koşullar altında da zarar görebileceğini ortaya koymuştur. Bu saldırıların temelinde HDD'lerin mekanik yapılarının ve özellikle okuma ve yazma kafalarının ses frekanslarına karşı duyarlılığı yatmaktadır. Özellikle ultrasonik frekans aralığında (20 kHz üzeri) yayılan yüksek frekanslı ses dalgaları, HDD'lerin normal çalışmasını sekteye uğratabilmekte hatta veri kayıplarına veya sistem çökmesine yol açabilmektedir (CNNTürk, 2018).

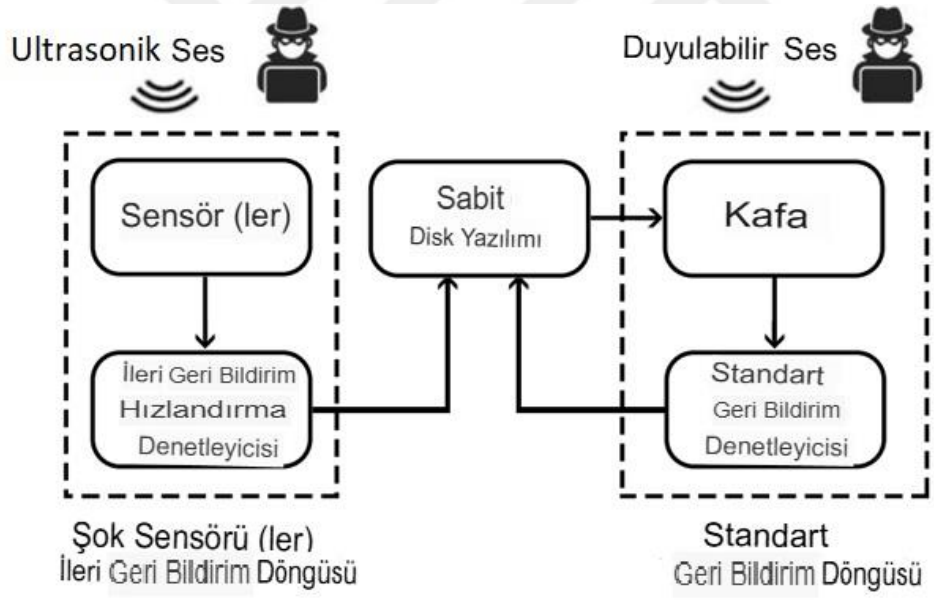
HDD'lerde veri, dönen plakalar üzerinde hareket eden okuma ve yazma kafaları aracılığıyla işlenmektedir. Bu sistem, özellikle yüksek hassasiyet gerektiren bir yapı içerdiğinden dış kaynaklı mekanik titreşimlere karşı oldukça hassastır. Ultrasonik saldırılar bu noktada devreye girer; belirli frekanstaki ses dalgaları, kafaların izlediği izleme yollarını bozarak diskin kafa konumlama sisteminin hata vermesine neden olur. Bu durum diskte geçici veya kalıcı arızalara, sistem çökmelerine ve veri bütünlüğünün bozulmasına neden olabilir (BilgiGüvende, 2018).

Araştırmacılar insan kulağına duyulamayan sonik ve ultrasonik sinyallerin, hedef bir bilgisayarın yerleşik hoparlöründen veya hedef cihazın yakınındaki bir hoparlörden ultrasonik sesler yayarak sabit disk sürücülerine (HDD) fiziksel zarar verebileceğini göstermiştir. Benzer bir araştırma, 2017 yılında Princeton ve Purdue Üniversitesinden bir grup araştırmacı tarafından yapılmış ve akustik rezonans adı verilen bir fiziksel fenomeni kullanarak HDD'ler üzerinde hizmet reddi (DoS) saldırısı gerçekleştirilmiştir. HDD'ler dışsal titreşimlere maruz kaldığı için araştırmacılar, özel olarak tasarlanmış akustik sinyallerin HDD'nin iç bileşenlerinde önemli titreşimler yaratabileceğini ve bu titreşimlerin HDD'ye dayanan sistemlerin başarısızlığına yol açabileceğini göstermiştir.

Modern HDD'ler, akustik rezonans nedeniyle kafa çarpması (head crash) durumunu önlemek amacıyla şok sensörlü ileri besleme denetleyicileri kullanmaktadır. Bu sensörler, hareketi

algılayarak veri okuma ve yazma işlemleri sırasında kafa konumlandırma doğruluğunu artırır. Ancak Michigan Üniversitesi ve Zhejiang Üniversitesinden bir grup araştırmacı, yayımladıkları yeni bir makalede sonik ve ultrasonik seslerin şok sensörlerinde yanlış pozitiflere yol açtığını, bunun da sürücünün başını gereksiz yere park etmesine sebep olduğunu belirtmişlerdir.

Akustik dalgalar, HDD'nin kafa düzeneğini ve şok sensörünü titreştirerek veri akış kaybına ve fiziksel hasara yol açar. Modern HDD'ler, kafanın konumunu ayarlamak için sensörle çalışan ileri beslemeli denetleyiciler kullanır. Bolton ve diğerlerinin 2018 tarihli ve "Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems" başlıklı çalışması ultrasonik titreşimin HDD kafasının konumu için yanlış pozitifleri tetiklediğini, duyulabilir tonların kafayı titreştirdiğini ve bunun da kötü konumlandırmaya neden olduğunu bulmuştur (Şekil 3.6).



Şekil 3.6. HDD'ye yönelik ses tabanlı saldırıların basamakları (Bolton ve diğerleri, 2018)

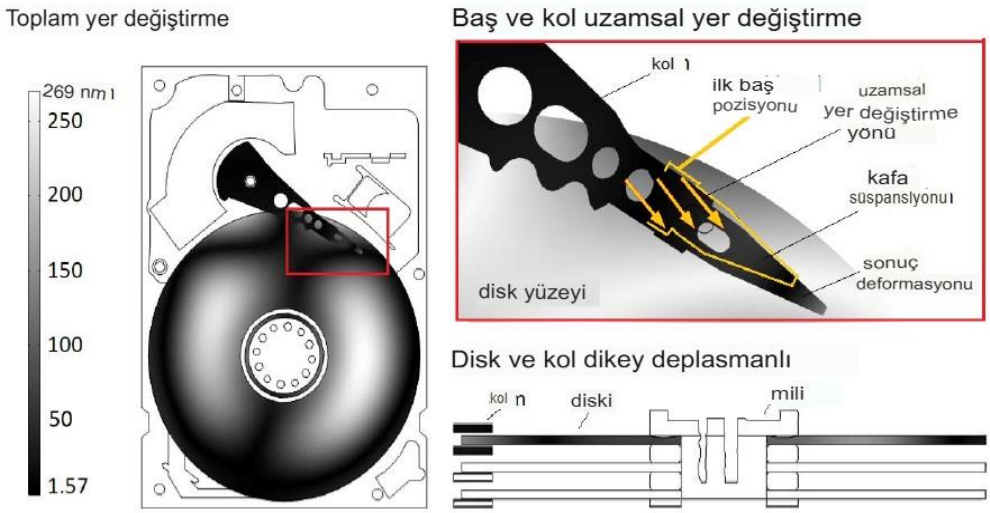
Bu disk sürücüsünün güvenlik açığını kullanarak araştırmacılar, saldırganların CCTV (Kapalı Devre Televizyon) sistemleri ve masaüstü bilgisayarlarındaki HDD'ler üzerinde başarılı saldırılar gerçekleştirebileceğini göstermiştir. Araştırmada "Bir saldırgan, sabit disk sürücüsü güvenlik açıklarını kullanarak bir dizüstü bilgisayarın yerleşik hoparlörü üzerinden Windows'u çökertmek ve denetim sistemlerinin video kaydını yapmasını engellemek gibi sistem seviyesinde sonuçlar doğurabilecek saldırılar gerçekleştirebilir." şeklinde bir sonuca ulaşmıştır.

Bu tür saldırılar, hedef sistemin kendi yerleşik hoparlörlerinden veya yakındaki harici bir hoparlörden kullanıcıyı kötü amaçlı bir sesi çalmaya kandırarak gerçekleştirilebilir. Deneysel kurulumda araştırmacılar Seagate, Toshiba ve Western Digital markalarına ait çeşitli HDD'ler üzerinde akustik ve ultrasonik müdahaleleri test etmiş ve ultrasonik dalgaların sadece 5-8 saniye içinde hatalar oluşturduğunu bulmuşlardır.

Bununla birlikte 105 saniye veya daha uzun süren ses müdahaleleri, video gözetim cihazındaki stok Western Digital HDD'sinin titreşimin başlangıcından itibaren cihaz yeniden başlatılana kadar kayıt yapmayı durdurmasına yol açmıştır. Bolton ve diğerlerinin çalışmasında bir kurban kullanıcı, saldırıya uğrayan sistemin fiziksel olarak yakınında değilse bile bir saldırganın herhangi bir frekansı kullanarak sistemi hedef alabileceğinden bahsedilmiştir. Ayrıca bu çalışmaya göre sistemin canlı kamera yayını, saldırının varlığına dair herhangi bir gösterge sunmaz, ayrıca sistem çevredeki ses hakkında herhangi bir bilgi sunmaz; bu nedenle, bir kurban kullanıcı sistemin fiziksel olarak yakınında değilse bile bir saldırgan sesli sinyaller kullanarak tespit edilmeden bir saldırı gerçekleştirebilir. Araştırmacılar çalışmada Windows ve Linux işletim sistemleriyle çalışan masaüstü ve dizüstü bilgisayarlarda da HDD'leri kesintiye uğratmayı başarmışlardır, bir Dell XPS 15 9550 dizüstü bilgisayarını 45 saniye içinde dondurmuş ve 125 saniyede çökertmişlerdir. Bu saldırı, dizüstü bilgisayarın yerleşik hoparlörü üzerinden kötü amaçlı bir sesin yürütmesi sağlanarak gerçekleştirilmiştir. Araştırma ekibi, bu tür saldırıları tespit etmek veya engellemek için bazı savunma yöntemleri önermiştir. Bunlar arasında firmware güncellemesi olarak dağıtılabilecek yeni bir denetleyici, şok sensörünün ultrasonik tetiklenmesini tespit ederek gereksiz baş parkını engelleyen bir sensör füzyon yöntemi ve sinyali zayıflatmak için gürültü sönümleyici malzemeler bulunmaktadır (Bolton ve diğerleri, 2018).

2018 yılında yapılan farklı bir araştırma ise yalnızca belirli frekanslardaki ses dalgalarının HDD sistemlerinde sistematik bozulmalara yol açabileceğini kanıtlamıştır. Örneğin HDD üzerine 2.5 ile 3.5 kHz arasında değişen frekanslarda ses titreşimleri uygulandığında okuma ve yazma sürecinin tamamen durdurulabildiği, bunun sonucunda işletim sisteminin çöktüğü gözlemlenmiştir (Threatpost, 2018). Bu tür saldırılar kötü niyetli kişiler tarafından bir güvenlik açığı olarak değerlendirildiğinde fiziksel erişim olmaksızın donanım düzeyinde saldırılar gerçekleştirilebileceğini göstermektedir.

Resim 3.8'de 5 kHz frekansında bir akustik sinyal saldırısı sırasında HDD başlık montajı ve disk yüzeyinin yer değiştirmesini gösteren COMSOL simülasyonu (solda üst görünüm, sağ altta yan kesit, sağ üstte okuma ve yazma başlığının yer değiştirmesi) gösterilmiştir.



Resim 3.8. HDD başlık montajı ve disk yüzeyinin yer değiştirmesini gösteren bir görsel (Bolton ve diğerleri, 2018)

Bu görsel üzerinde disk yüzeyindeki yer değiştirmeye dikkat edilmelidir (merkezi izler boyunca maksimum dikey yer değiştirme yaklaşık 156 nm ve başlık süspansiyonunun maksimum yatay yer değiştirmesi yaklaşık 8 nm. Bu durum, 50 nm genişlik dikkate alındığında, 7.5 nm okuma ve 5 nm yazma hata eşiklerini aşmaktadır.

Bu saldırıların özellikle güvenlik kameraları gibi sürekli kayıt yapan cihazlarda tehlike arz ettiği de belirtilmektedir. Bazı durumlarda saldırı, cihazın sabit diskine zarar vererek video kayıtlarının durmasına ve veri kaybına neden olabilmektedir. Bu da güvenlik açısından ciddi bir tehdit oluşturmakta ve saldırının tespitini zorlaştırmaktadır. Çünkü saldırının fiziksel bir iz bırakmaması, olay sonrası adli analizlerde tanımlanmasını güçleştirmektedir (İnternet Protokolü Video Marketi - IPVM, 2018).

The Hacker News tarafından bildirilen bir başka senaryo ise saldırıların hedefli şekilde kullanılabileceğini ortaya koymaktadır. Örneğin önemli sistem dosyalarının bulunduğu bölgelere denk gelen titreşimler, sistemin çökmesine ve işletim sistemi kaynaklı hatalara

neden olabilir. Bu durum sadece bireysel kullanıcılar için değil, aynı zamanda kritik altyapıların işleyişi için de risk teşkil etmektedir (The Hacker News, 2018).

Özetle HDD'ler üzerinde gerçekleştirilen ultrasonik saldırılar, donanımsal güvenliğe yönelik geleneksel yaklaşımların ötesinde bir tehdit kategorisine işaret etmektedir. Bu saldırıların başarılı olabilmesi için karmaşık yazılımlar yerine yalnızca uygun frekans aralıklarında çalışan ses kaynakları yeterlidir. Bu da saldırının düşük maliyetli ve kolay uygulanabilir olması nedeniyle ileriye dönük olarak daha yaygın bir tehdit haline gelme potansiyeli taşıdığını göstermektedir. Bu saldırılar, bilgisayar sistemine fiziksel temas gerektirmeden yalnızca ses dalgaları yoluyla HDD'nin çalışmasını sekteye uğratmayı amaçlamaktadır. Bu tür saldırılarda kullanılan temel yöntem, HDD içerisinde hareketli parçalara sahip olan okuma ve yazma kafasının konumlandırma sistemini hedef almaktır. Ultrasonik frekanstaki ses dalgaları, aktüatör motorlarının titreşim frekanslarıyla rezonansa girerek kafanın izlediği konumlama yolunu bozabilmekte ve bunun sonucunda veri erişimi başarısızlıkla sonuçlanabilmektedir.

Zhang ve arkadaşları (2008) tarafından gerçekleştirilen deneysel çalışmalarda, belirli frekans aralıklarındaki (örneğin 2.4 kHz ile 20 kHz arasında) ultrasonik seslerin HDD'lerde arıza meydana getirebildiği gösterilmiştir. Bu deneylerde HDD'ye yönlendirilen ses dalgalarının kafanın titreşimlerine neden olduğu, bu titreşimlerin de veri okuma ve yazma süreçlerini engellediği ortaya konmuştur. Örneğin saldırı sırasında dosya transferlerinin durduğu, sistemin hata mesajları verdiği ve bazı durumlarda işletim sisteminin çökmesine kadar giden etkilerin gözlendiği raporlanmıştır. Bu bulgular, HDD'lerin ses temelli saldırılara karşı ciddi ölçüde kırılgan olduğunu ortaya koymaktadır.

HDD'lere yönelik ultrasonik saldırılar özellikle "acoustic resonance" fenomeninden yararlanmaktadır. Rezonans frekansı, bir cismin doğal titreşim frekansıdır ve dışarıdan bu frekansla verilen ses dalgaları, cismin titreşimini şiddetlendirir. HDD'lerde bulunan metalik ve mekanik parçaların belirli rezonans frekanslarında titreşim üretmeleri mümkündür. Bu rezonans, HDD'nin mekanik dengesini bozarak okuma ve yazma hatalarına neden olur. Literatürde, bu saldırıların hedeflediği modellerin farklı rezonans frekanslarına sahip olabileceği ve dolayısıyla saldırı için kullanılacak frekansın cihaz modeline özel olarak belirlenmesi gerektiği belirtilmiştir.

Güvenlik açısından bakıldığında bu tür saldırıların en büyük tehlikesi, doğrudan fiziksel erişim gerektirmemesi ve bir ortamda bulunan ses sistemleri veya hoparlörler gibi masum görünen cihazlar aracılığıyla gerçekleştirilebilmesidir. Örneğin bir müzik dosyası ya da video içeriğine gömülen zararsız gibi görünen ultrasonik sinyaller, HDD üzerinde kalıcı arızalara neden olabilir. Bu durum özellikle veri merkezleri, kritik altyapılar ve gözetim sistemleri gibi yüksek güvenlik gereksinimi taşıyan ortamlarda ciddi tehditler oluşturmaktadır.

İlk olarak Guri ve diğerleri (2017) ortaya konulan bu tür saldırılar, HDD'nin iç mekanizmasını hedef alarak cihazın işlevselliğini kesintiye uğratmayı amaçlamaktadır. Çalışmada, ultrasonik ses dalgalarının sürücünün okuma ve yazma kafasında rezonansa yol açabileceği ve bu durumun da diskin üzerinde doğru konumlandırmayı bozarak veri erişimini engelleyebileceği deneysel olarak gösterilmiştir.

Bu tür saldırılar, özellikle HDD'nin servo sistemine de müdahale ederek kafanın doğru iz üzerinde hareket etmesini engeller. Saniyede 20.000 Hz'nin üzerindeki frekanslarda (insan kulağının duyamayacağı aralıkta) yayınlanan ses dalgaları, cihazın iç yapısında rezonans yaratmakta ve fiziksel parçalarda kontrol kaybına neden olmaktadır. Bunun sonucunda işletim sistemleri "disk hatası", "veri okunamıyor" gibi uyarılar verirken sistem performansında ciddi düşüşler ve bazı durumlarda sistem çökmesi yaşanabilmektedir.

Guri ve diğerlerinin gerçekleştirdiği deneylerde, HDD'nin yaklaşık 1 metre mesafeden maruz kaldığı ultrasonik dalgaların yalnızca birkaç saniye içinde veri erişimini durdurabildiği gösterilmiştir. Bu saldırı yöntemi herhangi bir sistemsel zafiyet ya da yazılım açığına dayanmadığı için geleneksel güvenlik mekanizmaları tarafından tespit edilmesi oldukça zordur. Ayrıca saldırının fiziksel olması, uzaktan gerçekleştirilebilmesi ve herhangi bir sisteme doğrudan temas gerektirmemesi bu yöntemi özellikle tehlikeli kılmaktadır. Geliştirilen bu saldırı modeli, hem siber güvenlik araştırmalarında fiziksel kanalların kullanımı açısından dikkat çekici bir örnek oluşturmakta hem de donanımsal düzeyde yeni nesil güvenlik önlemlerinin gerekliliğini gözler önüne sermektedir. Bu bağlamda, sabit disklerin akustik izolasyonu, sürücü donanımında rezonans frekanslarına karşı dayanıklı yapıların geliştirilmesi ve fiziksel alanlara yönelik siber güvenlik politikalarının oluşturulması gibi çok katmanlı savunma stratejileri ön plana çıkmaktadır (Kwong ve diğerleri, 2019).

Alfredo Ortega tarafından 2017 yılında yayınlanan “Turning hard disk drives into accidental microphones” başlıklı çalışmada, sezyum buharı tabanlı atom saatleri ile HDD'lerin rezonans frekanslarının etkileşimi araştırılmış ve belirli frekans aralıklarındaki ses dalgalarının HDD içindeki okuma ve yazma kafasını bozulmaya uğrattığı gösterilmiştir. Burada karşılaşılan bu bozulma, cihazın veri okuyamamasına, hatalı veri yazmasına veya işletim sisteminin çökmesine neden olmuştur.

Benzer şekilde, Seagate ve Western Digital gibi önde gelen üreticilerin bazı HDD modelleri üzerine yapılan analizlerde, 2–9 kHz aralığında değişen düşük ultrasonik frekansların bile HDD'yi yanıltabildiği gözlemlenmiştir (Bolton ve diğerleri, 2018). Bu bulgular, HDD üreticilerinin elektromekanik parça tasarımında bu tür saldırı vektörlerini göz önünde bulundurması gerektiğini ortaya koymuştur.

Bu saldırıların potansiyel etkileri oldukça geniştir. Örneğin sunucu odalarında çalışan HDD’ler, dışarıdan görünür bir hasar izi bırakmadan yalnızca ses dalgaları ile devre dışı bırakılabilir. Bu durum kritik sistemlerin kesintiye uğramasına, hizmet aksaklıklarına ve potansiyel veri kaybına yol açabilir. Sonuçlar sadece veri kaybı ile sınırlı kalmaz, aynı zamanda sistem güvenliği ve veri bütünlüğü üzerinde de ciddi tehditler oluşturabilir. Bu tür saldırıların önlenmesi, sadece donanım odaklı önlemlerle değil aynı zamanda yazılım tabanlı çözümlerle de mümkün olacaktır.

Önleme yöntemleri arasında akustik izolasyon, HDD kasalarının rezonansı engelleyecek şekilde tasarlanması ve ultrasonik sinyalleri algılayabilecek sensör sistemlerinin entegre edilmesi gibi hem fiziksel hem de yazılımsal önlemler yer almaktadır. Bununla birlikte bu konuda hala yeterince farkındalık bulunmamakta ve sanayi düzeyinde standart güvenlik önlemleri bu tür saldırıların olasılıklarını yeterince hesaba katmamaktadır.

Ultrasonik saldırıların tespiti ve önlenmesi için çeşitli fiziksel ve yazılımsal önlemler önerilmektedir. Fiziksel önlemler arasında HDD’lerin dış seslere karşı izole edilmesi, kasalara ses emici malzemeler yerleştirilmesi ve rezonansa giren bileşenlerin mekanik olarak güçlendirilmesi gibi yöntemler yer alır. Yazılımsal olarak ise HDD’nin beklenmedik davranışları sürekli izlenerek anormal durumların tespiti yapılabilir. Ayrıca gelecekteki depolama teknolojilerinin tasarımında, akustik güvenlik tehditlerine karşı dayanıklılığı artıracak mühendislik çözümlerinin dikkate alınması büyük önem taşımaktadır.

Akustik dalgaların HDD üzerindeki fiziksel etkileri, disklerin normal çalışma işlevlerini bozarak veri kaybı ve sistem hatalarına yol açabilir. Özellikle duyulabilen seslere ait ses dalgaları, okuma ve yazma başlıkları ile disk yüzeylerini titreştirerek disklerin verimli çalışmasını engelleyebilirken ultrasonik ses dalgaları, HDD'nin şok sensörlerini etkileyerek başlıkların hatalı bir şekilde yerleşmesine neden olabilmektedir. Bu tür saldırılar sadece fiziksel değil, aynı zamanda operasyonel sistemler üzerinde de geri döndürülemeyen zararlara yol açma potansiyeline sahiptir.

Sistem düzeyinde HDD'nin düzgün çalışmaması, işletim sistemlerinin çökmesine veya uygulamaların beklenildiği gibi çalışmamasına sebep olabilir. Gerçekleştirilen testlerde, bir dizüstü bilgisayarın hoparlöründen yayılan ses dalgalarının yazma işlemlerini engellediği gözlemlenmiştir. Akustik müdahaleler, özellikle yüksek desibel seviyelerine sahip seslerin varlığında verilerin bütünlüğünü tehdit edebilecek bir risk taşımaktadır.

Bu tür saldırıları minimum düzeye indirebilmek için savunma mekanizmalarının geliştirilmesi büyük önem arz etmektedir. Akustik dalgaların etkisini azaltmak amacıyla gürültü azaltıcı malzemeler ve sensör füzyonu gibi stratejiler önerilmektedir. Bu yöntemler, HDD'nin başlıklarını koruyarak verimli bir şekilde çalışmaya devam etmesini mümkün kılabilir. Ayrıca yeni geri bildirim kontrol sistemleri ile ultrasonik saldırılara karşı etkili çözümler geliştirmek, bu tür siber saldırılara karşı güçlü bir savunma hattı oluşturmaya katkıda bulunacaktır.

Ultrasonik ses dalgalarıyla gerçekleştirilen farklı saldırı türlerinin hedef sistemleri, kullandıkları yöntemler, teknik işleyişleri ve oluşturdukları güvenlik tehditleri dikkate alındığında bu tür saldırıların kapsamlı bir şekilde sınıflandırılması gerekliliği ortaya çıkmaktadır. Çizelge 3.3'te, literatürde öne çıkan ve bu bölümde incelenen dört farklı ultrasonik ses tabanlı saldırı türü sistematik biçimde karşılaştırılmış ve bu saldırıların özellikleri temel bileşenler üzerinden analiz edilmiştir:

Çizelge 3.3. Ultrasonik ses dalgalarıyla gerçekleştirilen siber saldırı türlerinin genel karşılaştırması

Saldırı Türü	**DolphinAttack**	**NUIT**	**SurfingAttack**	**HDD Saldırıları**
Yöntem	Ultrasonik ses dalgaları ile ses tanıma sistemlerinin manipülasyonu.	Elektromanyetik müdahaleler ile elektronik sistemlerin etkilenmesi.	MEMS mikrofonlarının yüksek frekanslı ultrasonik dalgalarla hedef alınması.	Ultrasonik ses dalgaları ile mekanik bileşenlerin fiziksel olarak zarar görmesi.
Hedef Sistem	Sesle çalışan sistemler (ör. akıllı telefonlar, akıllı ev sistemleri).	Sesle çalışan sistemler (ör. akıllı telefonlar, akıllı ev sistemleri).	Akıllı cihazlar (ör. akıllı telefonlar, akıllı hoparlörler).	Sabit disk sürücüleri (HDD).
Temel Özellik	İnsan kulağının duyamayacağı frekanstaki sinyallerle ses filtrelerinin atlatılması.	Elektromanyetik sinyallerin yönlendirilerek kötü amaçlı komut iletiminin sağlanması.	MEMS mikrofonlar üzerinden cihazlara fiziksel temas olmadan komut gönderilmesi.	Yüksek frekanslı ses ile HDD'nin iç parçalarının doğrudan zarar görmesi.
Başlıca Zorluklar	Duyulamaz frekans nedeniyle tespit edilmesi zordur.	Tespiti için özel donanım gerektirir.	Uzun mesafede çalışabilir, yansıtılma yoluyla etkili olabilir, fark edilmesi zordur.	İnsan kulağının algılayamayacağı frekansta gerçekleştiği için fark edilmesi güçtür.

3.11. Kriptografi ve Steganografi Yöntemi ile Gerçekleştirilen Ses Tabanlı Saldırılar

Kriptografi, çeşitli verilere yetkisiz kişilerin erişmesini engellemek amacıyla bilgi gizleme ve koruma tekniklerinin bütününü ifade eder. Bu bilim dalı, mesajların yalnızca yetkili alıcılar tarafından anlaşılabilir hale getirilmesini sağlamak için matematiksel algoritmalar ve anahtar sistemleri kullanır. Kriptografi veri bütünlüğü, kimlik doğrulama, gizlilik ve inkâr edilemezlik gibi güvenlik ilkeleri kapsamında temel bir rol oynamaktadır (Stallings, 2017: 10, 15).

Kriptografinin tarihi, M.Ö. 1900'lü yıllarda Antik Mısır'a kadar uzanmaktadır. İlk örneklerden biri, Mısır hiyerogliflerinde karşılaşılan sembolik yazım biçimidir. Ancak sistematik olan kriptografik uygulamalar, Antik Yunan döneminde özellikle Sezar Şifresi (Caesar Cipher) gibi temel yer değiştirme algoritmalarıyla başlamıştır (Singh, 1999: 1, 23). Kriptografinin en erken biçimleri arasında alfabenin belirli sayıda kaydırılması esasına dayanan Sezar şifrelemesi yer almaktadır. Bu yöntemde örnek olarak "BABA" kelimesi, üç harf kaydırılarak "EDED" şeklinde yazılır. Sezar şifresi, basit yapısı nedeniyle kolayca kırılabilir ve harf frekansı analizi yapılarak şifreli metindeki harflerin yerlerine neyin geçtiği tespit edilebilir (Birer, 2022).

Tarihte kriptografinin kaderini değiştiren önemli bir olay, İskoçya Kraliçesi Mary'nin gönderdiği şifreli mesajın İngiliz ajanları tarafından çözülmesidir. Kraliçe Mary, 1587 yılında Sör Anthony Babington ile olan yazışmasında sembollere dayalı bir şifreleme yöntemi kullanmış, ancak şifredeki sembollerin tekrar sıklığı dikkatle incelenerek bu mesaj çözülebilmiş ve sonuç olarak Kraliçe Mary ile Babington idam edilmiştir (Birer, 2022).

Sezar şifresi gibi sabit kaydırmalı yöntemler yerine, 16. yüzyılda Blaise de Vigenère tarafından tanıtılan ve çok alfabeli yer değiştirme kullanan Vigenère şifresi, kriptografide bir dönüm noktası olmuştur. Bu yöntem, bir anahtar sözcük yardımıyla metindeki her harfi farklı şekilde şifreler. Aynı harf için farklı şifreli karakterler kullanıldığından frekans analizi yapmak zorlaşır ve bu yöntem 300 yıl boyunca kırılmaz kabul edilmiştir. Ancak 1863'te Friedrich Kasiski tarafından geliştirilen analiz yöntemi ile bu şifre de kırılmıştır (Birer, 2022).

20. yüzyılda ise kriptografi, elektromekanik cihazlarla yeni bir boyut kazanmıştır. Bu dönemin en dikkat çekici örneği, Almanya tarafından geliştirilen Enigma makinesidir. Enigma, şifreli mesajlarda her bir harfi farklı bir harfe dönüştürerek oldukça karmaşık bir yapı sunmuştur. Ancak Alan Turing ve ekibinin sistematik çalışmaları ve operatör hatalarını avantaja çevirmeleri sonucunda Enigma şifresi kırılmıştır. Özellikle her mesajın "Heil Hitler" ile bitmesi ya da Enigma'nın hiçbir harfi kendisiyle eşleştirmemesi gibi sabit kalıplar, çözüm sürecinde önemli ipuçları sağlamıştır (Birer, 2022).

II. Dünya Savaşı sonrasında bilgisayarların yaygınlaşması ile kriptografi, askerî veya devletsel bir alan olmaktan çıkarak bireysel güvenlik ihtiyaçlarına da hizmet eden bir disiplin haline gelmiştir. Bu değişim, daha güvenli ve sistematik şifreleme yöntemlerinin geliştirilmesini zorunlu kılmıştır. Modern kriptografik sistemlerde yalnızca şifreleme yöntemini değil, şifreleme anahtarlarının rastgeleliğini ve öngörülemezliğini sağlamak da temel öncelik haline gelmiştir. Özellikle rastgele sayı üretimindeki güvenlik açıkları (örneğin Netscape'in SSL protokolü ya da WEP protokolündeki açıklıklar) güvenlik sistemlerinin bütünlüğünü zayıflatmıştır. Bu nedenle günümüzde güçlü şifreleme sistemleri, rastgele oluşturmaya dayalı anahtar üretimini, tek yönlü fonksiyonları ve hesaplama karmaşıklığını esas alarak inşa edilmektedir.

Modern kriptografi ise 1970’li yıllarda özellikle Whitfield Diffie ve Martin Hellman tarafından geliştirilen açık anahtarlı kriptografi (public key cryptography) ile yeni bir boyut kazanmıştır (Diffie ve Hellman, 1976). Bu dönemde Rivest, Shamir ve Adleman tarafından geliştirilen RSA algoritması günümüzde hala yaygın biçimde kullanılan bir şifreleme yöntemidir (Rivest ve diğerleri, 1978).

İletişim güvenliği açısından genellikle iki bireyin yalnızca birbirleriyle paylaşabildikleri, dış müdahaleye kapalı bir kanal üzerinden iletişim kurması amaçlanır. Ancak günümüzde iletişim, çoğunlukla internet ve telefon gibi üçüncü tarafların erişimine açık kanallar üzerinden yürütülmektedir. Bu bağlamda kriptolojinin temel amacı, açık iletişim kanallarında yapılan veri alışverişinin güvenliğini sağlamaktır. Kriptoloji gizlilik, bütünlük ve kimlik doğrulama gibi temel güvenlik unsurlarına odaklanarak bu unsurların gerçekleşmesini sağlamak amacıyla çeşitli protokollerin kullanılmasını gerektirir. Bir kriptografik sistemin güvenliği kullanılan şifreleme algoritmaları, donanım ve yazılım bileşenleri ile tasarlanan güvenlik modeline dayanır. Bu model, sistemde yer alan tarafların

hangi tür anahtar bilgilerine sahip olacağını belirler. Temel olarak iki tür güvenlik modeli öne çıkmaktadır: Simetrik (paylaşılan anahtarlı) ve asimetrik (açık anahtarlı) modeller.

Simetrik kriptografide hem gönderici hem de alıcı aynı gizli anahtarı kullanarak veri şifreleme ve çözme işlemlerini gerçekleştirir. Bu nedenle güvenli iletişim başlamadan önce tarafların bu gizli anahtarı güvenli bir şekilde paylaşmaları gerekmektedir. Şifreleme algoritması, açık metni verilen anahtar aracılığıyla şifreli (anlamsız) bir metne dönüştürür. Bu modelde mesajın içeriğinin değiştirilmediğini doğrulamak amacıyla genellikle Mesaj Kimlik Kodu (MAC) adı verilen bir kontrol etiketi de şifreli mesaja eklenir. Bu etiket, şifreli metin ve anahtar birlikte kullanılarak oluşturulur ve mesajın bütünlüğünü garanti altına alır.

Simetrik şifreleme algoritmaları hızlı, verimli ve düşük işlemci gereksinimi nedeniyle sıklıkla tercih edilir. Ancak bu yöntemde anahtar paylaşımı büyük bir güvenlik açıklarına yol açabilir. Anahtarın kötü niyetli üçüncü şahıslar tarafından ele geçirilmesi durumunda tüm iletişim deşifre edilebilir. Ayrıca saldırganlar, şifreli metnin uzunluğundan yola çıkarak orijinal metin hakkında tahminlerde bulunabilir veya iletişimde bulunan taraflar hakkında elde ettikleri ek bilgilerle şifreyi çözmeye çalışabilirler.

Asimetrik kriptografi ise 1970'li yıllarda geliştirilen ve açık anahtar kriptografisi olarak da adlandırılan bir şifreleme yöntemidir. Ralph Merkle'in öncülük ettiği bu yaklaşım Whitfield Diffie ve Martin Hellman tarafından geliştirilerek 1976 yılında Diffie-Hellman anahtar değişim protokolüyle dünyaya duyurulmuştur. Asimetrik modelde her kullanıcının bir açık ve bir gizli anahtarı bulunur. Açık anahtar herkesle paylaşılabilirken gizli anahtar sadece sahibinde bulunur. Gönderici, alıcının açık anahtarını kullanarak mesajı şifreler ve bu mesaj yalnızca alıcının gizli anahtarı ile çözülebilir. Bunun yanı sıra mesajın özgün bir kaynaktan geldiğini doğrulamak için dijital imza mekanizması da kullanılabilir. Bu işlemde gönderici mesajın bir kısmını kendi gizli anahtarıyla şifreler, alıcı ise bu bölümü göndericinin açık anahtarı ile doğrular. Bu doğrulama, mesajın gerçekten belirtilen kişi tarafından gönderildiğini garanti altına alır. RSA (Rivest-Shamir-Adleman) algoritması, asimetrik şifreleme alanında en yaygın kullanılan yöntemlerden biridir. RSA'da kullanılan anahtar uzunlukları genellikle 1024, 2048 veya 4096 bit şeklindedir. Günümüzde 2048 bit ve üzerindeki anahtarlar, artan işlem gücüne karşı daha güvenli kabul edilmektedir. Asimetrik kriptografi özellikle internet güvenliğinde sıkça kullanılan TLS (Transport Layer Security) gibi protokollerin temelini oluşturur.

Hash fonksiyonları, değişken uzunluktaki bir veriyi sabit uzunlukta bir özet (hash) değerine dönüştüren algoritmalardır. Bu özet değeri, veri üzerinde yapılan en küçük değişiklikleri bile tespit edebilecek şekilde tasarlanmıştır. Hash fonksiyonları deterministik olarak çalışır, yani aynı veri her zaman aynı hash değerine sahiptir. Bu fonksiyonlar internetten indirilen dosyaların bütünlüğünü doğrulamak veya parola gibi hassas bilgilerin veri tabanlarında saklanmasını sağlamak amacıyla sıkça kullanılırlar.

Parola güvenliğinde hash algoritmalarının yanı sıra "salt" adı verilen rastgele bir veri ile parolanın birlikte işlenmesi yoluyla hash değeri oluşturulur. Böylece aynı parolaya sahip farklı kullanıcılar için farklı hash değerleri elde edilerek güvenlik seviyesi artırılır. MD5, SHA-1, SHA-2, SHA-3, bcrypt ve BLAKE3 gibi algoritmalar yaygın olarak kullanılan hash fonksiyonları arasında yer almaktadır. Ancak MD5 ve SHA-1 gibi eski algoritmalar, günümüzde çeşitli zayıflıkları nedeniyle önerilmemektedir.

Blok şifreleme, verileri sabit uzunlukta bloklara ayırarak her bir bloğu ayrı ayrı şifreleyen bir şifreleme yöntemidir. Bu yöntem sayesinde açık metin, belirli bir anahtar yardımıyla aynı uzunlukta şifreli metinlere dönüştürülür. Daha sonra, aynı anahtar kullanılarak bu şifreli metinlerin tekrar orijinal açık metne dönüştürülmesi mümkündür. Günümüzde en çok kullanılan blok şifreleme algoritmalarından biri AES (Advanced Encryption Standard)'dir. AES, DES (Data Encryption Standard)'in zayıflıkları nedeniyle yerini almış ve 128 bit blok uzunluğu ile 128, 192 ve 256 bitlik anahtar uzunluklarına olanak tanıyan esnek bir yapı sunmuştur.

Kuantum kriptoloji, kuantum fiziğinin prensiplerine dayalı olarak geliştirilen yeni nesil bir şifreleme yaklaşımıdır. Bu alandaki ilk fikirlerden biri 1968 yılında Stephen Weisner tarafından ortaya atılmış ve kuantum para kavramı ile literatüre girmiştir. Kuantum kriptolojinin temelinde kuantum süperpozisyonu ve kuantum dolanıklık gibi kavramlar yer alır. Süperpozisyon, bir parçacığın aynı anda birden fazla durumda bulunabilmesi anlamına gelirken dolanıklık, iki parçacığın birbirinden ne kadar uzakta olurlarsa olsunlar eş zamanlı etkileşim halinde olabilmeleri durumudur.

Kuantum kriptolojinin en bilinen uygulamalarından biri olan Kuantum Anahtar Dağıtımı (QKD), özellikle BB84 protokolü ile tanınır. Bu protokol sayesinde iki taraf arasında gizli bir anahtar fiziksel olarak aktarılmadan kuantum bitleri (qubit) üzerinden güvenli bir şekilde

paylaşılabilir. Kuantum sistemlerde yapılan her ölçüm işlemi sistemin durumunu değiştirdiği için dış müdahaleler anında fark edilebilir. Bu nedenle kuantum kriptoloji, klasik şifreleme sistemlerine göre daha yüksek bir güvenlik seviyesi sunar. Ancak halihazırda kuantum teknolojilerinin sınırlı gelişmişliği nedeniyle pratikte kullanım alanları sınırlıdır.

Kriptografi, geleneksel olarak metin tabanlı iletişim güvenliğinde kullanılsa da günümüzde ses sinyalleri üzerinde de uygulanmaktadır. Özellikle ses verilerinin şifrelenmesi, VoIP (Voice over IP) gibi teknolojilerde iletişimin gizliliğini sağlamak için kritik bir öneme sahiptir. Ancak bu teknolojinin siber saldırılar için kötüye kullanımı da söz konusu olabilir. Örnek olarak sesli iletilere zararlı yazılımlar veya komutlar kriptografik yollarla gizlenebilir, bu da ses tabanlı saldırıların bir türü olarak değerlendirilmektedir.

VoIP (Voice over IP), internet protokolü (IP) ağları üzerinden sesli iletişim ve multimedya oturumlarının iletilmesi için kullanılan bir yöntem ve teknoloji grubudur. Sistem terminal ekipmanları, geçitler, ağ yönetimi gibi öğeleri barındırır. Geleneksel telefon ağı ses iletimini devre anahtarlama yöntemiyle gerçekleştirirken VoIP, ses sinyallerini kodlayıp sıkıştırarak ve ardından TCP/IP standardı ve diğer özel işleme ile ses verilerini paketleyerek iletim platformu olarak IP paket anahtarlama ağını kullanır. Daha sonra ses verisi, bağlantısız UDP protokolü ile iletilir. Veriler çözümlendikten sonra orijinal ses sinyali tekrar eski haline getirilir ve sesin internet üzerinden iletilmesi sağlanır.

Steganografi, bir mesajın varlığını gizlemeyi amaçlayan bilgi saklama yöntemidir. Bu yöntem bilgiyi görünüşte zararsız bir taşıyıcı (örneğin bir resim, metin ya da ses dosyası) içine gömerek iletilmesini sağlar. Steganografi, kriptografinin aksine mesajın içeriğini gizlemekten ziyade mesajın varlığını dahi fark edilmez kılmayı hedefler (Johnson ve diğerleri, 2001).

Tarihsel olarak steganografinin izleri Antik Yunan'a kadar uzanır. Herodot'un "Tarihler" adlı eserinde, bir kölenin kafasındaki saçlar tıraş edildikten sonra derisine gizli bir mesaj kazındığı, saçlar yeniden uzadığında ise mesajın taşındığı anlatılmaktadır. Orta Çağ'da da görünmez mürekkepler ve minyatür yazılar gibi yöntemlerle steganografi uygulanmıştır (Kahn, 1996).

Modern dönemde ise steganografi dijital ortamlarda kullanılmak üzere yeniden şekillenmiştir. Özellikle dijital medya dosyalarında (görüntü, ses, video) bilgi gizleme yöntemleri, bilgisayar güvenliği ve dijital adli bilişim alanlarında büyük ilgi görmektedir.

Günümüzde steganografi, dijital ortamda daha karmaşık yöntemler kullanılarak uygulanmaktadır. Resim, video, ses ve müzik dosyaları gibi çoklu ortam verilerinin içerisine gözle veya kulakla algılanamayacak şekilde gizli mesajlar saklanabilmektedir. Bu işlemler, verinin kalitesini bozmadan ve insan algısının fark edemeyeceği şekilde gerçekleştirilir. Örneğin sayısal bir imgedeki piksel değerlerinde gözle görülmeyecek kadar küçük değişiklikler yapılabilir ve bu değişikliklerle gizli bilgiler saklanabilir. Ayrıca ses ve müzik dosyaları içinde de benzer şekilde değişiklikler yapılabilir (Karabat, 2010).

Steganografi, özellikle güvenli iletişim gereksinimlerinde önemli bir rol oynar. Bununla birlikte steganaliz adı verilen yöntemler, saklanan gizli bilgilerin ortaya çıkarılmasına yönelik matematiksel analizler sunar. Bu teknikler, gizli haberleşmeleri tespit etmek ve yasadışı kullanımları önlemek amacıyla güvenlik açısından büyük önem taşır (Karabat, 2010).

Steganografi, gizli mesajların veya bilgilerin doğal görünümlü ortamlar içinde saklanarak yalnızca doğru alıcı tarafından anlaşılmasını sağlar. Latincede "steganos" kelimesi "görünmeyen", steganografi ise "gizlenmiş yazı" anlamına gelir (Bilgin, 2013). Bu yöntem, bilgi iletimi sırasında mesajın varlığının gizlenmesine odaklanır. Alıcı, yalnızca doğru anahtar bilgisine sahipse mesajı çözebilir. Kriptografiden farklı olarak steganografide verinin varlığının gizlenmesi esastır, şifreleme algoritması esas değildir.

Birleşmiş Milletler'in İnsan Hakları Evrensel Beyannamesi'ne göre, her birey düşünce ve ifade özgürlüğüne sahiptir. Ancak bu özgürlükler başkalarına zarar vermemelidir. Günümüzde bu düzenlemeye paralel olarak iletişim ve bilgi alışverişi sıklıkla izlenmektedir. Kriptografik veriler doğal dil yapısından sapmalar gösterdiği için daha dikkat çekebilir. Bu sebeple, verinin varlığını gizleyen steganografi daha güvenli bir seçenek olarak öne çıkar.

Steganografik bir algoritmanın başarısı üç ana özelliğe dayanır: Değişimin fark edilmemesi, saklanabilir veri miktarı ve dayanıklılık. Bu teknikler, veri saklamanın görsel veya duyusal olarak fark edilmeden yapılmasını sağlar. Ancak veri miktarının artması, algılanabilir

değişikliklere neden olabilir. Bu denge, steganografinin getirdiği en büyük zorluklarından biridir.

Steganografi teknikleri, kullanılan yönteme göre farklı türlere ayrılabilir. Bunlar arasında teknik steganografi (bilimsel yöntemlere dayalı gizleme teknikleri), dilsel steganografi (doğal dilde yazılarak gizlenmiş mesajlar), açık kodlar (gizli anlamı olan yazılar) ve jargon kodları yer alır. Bu kodlar, sadece belirli bir grup tarafından anlaşılabilir ve mesajın çözülmesi için özel bir anahtar gerektirir.

Steganografinin kötü amaçlarla kullanımına örnek olarak suçluların gizli mesajlarını iletmek için kullandığı yöntemler verilebilir. Bunun yanı sıra iyi amaçlarla da kullanılır, örnek olarak dijital filigranlar, yazar haklarını korumak için içeriklere gizlice yerleştirilebilir. Steganografi, mesajları saklamak için resimler ve ses dosyaları gibi dijital taşıyıcılar kullanır. Bu taşıyıcılar üzerinden gizli bilgileri iletmek, çeşitli şifreleme ve kodlama yöntemleri gerektirir (Alabdali ve Alzahrani, 2021).

Steganografi, çeşitli araçlarla tespit edilebilse de mesajları gizleyen araçlar gönderen, alıcı ve kullanılan ortam açısından çok büyük tehditler yaratabilir. Pasif bir saldırı, iletişimi ve ortamı gözlemleyerek gizli mesajı çözmeyi amaçlar. Teknolojinin ilerlemesiyle steganografi uygulamaları daha karmaşık hale gelmiş ve gizliliği sürdürmek zorlaşmıştır.

Steganografi, farklı tekniklerle yapılabilir. Bunlar arasında değiştirmeye dayalı yöntemler, işaret işlemeye dayalı yöntemler, istatistiksel yöntemler ve diğer alternatif yaklaşımlar yer alır. Bu yöntemler, veriyi taşıyan medya üzerinde dikkat çekmeyen değişiklikler yaparak mesajın gizliliğini korur.

Çeşitli akademik çalışmalar, steganografinin farklı medya türlerinde nasıl uygulanabileceğini incelemiştir. Resim, ses ve metin dosyalarındaki veri saklama yöntemleri detaylı şekilde ele alınmıştır. 2000'li yıllardan sonra LSB (Least Significant Bit) gibi yöntemler, resim ve ses dosyalarına veri saklamak için yaygın olarak kullanılmaktadır. Bu yöntemlerin geliştirilmesi, steganografinin daha güvenli ve etkili bir şekilde uygulanmasını sağlamıştır.

Steganografi bilgi güvenliğini sağlamak için yeni dönemde kullanılan bir yöntemdir, ancak diğer birçok şey gibi çift taraflı etkileri vardır. Bir yandan özellikle politik, finansal ve diğer alanlarda gizli ve özel bilgilerin güvenli ve güvenilir iletimini sağlar; diğer yandan bazı suçlular için yanlış veya hatta kötü niyetli amaçlar için çeşitli fırsatlar sunar. Örneğin steganografi, bilgisayar virüslerini çeşitli multimedya taşıyıcılarına gizleyerek güvenlik duvarları ve antivirüs yazılımlarını aşmak ve sabotaj faaliyetleri yürütmek için kullanılabilir. Steganografinin kötüye kullanılması, devletin ve toplumun güvenliğini zayıflatarak illegal bilgilerin yayılmasına yol açabilir ve bu da insanların hayatları ve malları için potansiyel tehditler oluşturur. Bu nedenle, steganografi teknolojisine karşı bir önlem olarak steganaliz teknolojisi, araştırmacılardan giderek daha fazla ilgi görmektedir (H. Tian ve diğerleri, 2015).

Steganaliz, steganografinin bir karşıt teknolojisidir. Hedefi, gizli bilgilerin varlığını keşfetmek ve hatta gizli iletişimi ortadan kaldırmaktır. Steganaliz, steganografinin suç amaçlı kullanılmasını çözme konusunda önemli bir teknolojidir (Baidu, 2021). Steganaliz teknolojisinin geliştirilmesi, steganografinin yasadışı kullanımını engellemeye yardımcı olabilir ve kişisel verilerin kaybını önlemek, yasadışı verileri ortaya çıkarmak, şiddeti engellemek ve ardından kamu güvenliği ile toplumsal istikrarı sağlamak için önemli bir rol oynayabilir. Steganaliz araştırmaları, mevcut steganografinin eksikliklerini ortaya çıkarabilir ve steganografinin güvenliğinin değerlendirilmesini sağlayabilir. Bu durum, mesaj gizleme yöntemlerinin geliştirilmesi ve iyileştirilmesi için oldukça faydalı bir tekniktir.

Steganografi günümüzde ses, görüntü, video ve metin gibi iletim medyalarında yaygın olarak kullanılmaktadır. Farklı taşıyıcı türleri, kendilerine özgü bilgi gizleme algoritmalarına sahiptir. Çünkü insan organları, özellikle de kulaklar, seslerdeki ince değişikliklere duyarlı değildir (Praetorius, 2015); bu nedenle insanlar, orijinal taşıyıcı (gizli bilgi içermeyen taşıyıcı) ile gizli taşıyıcı (gizli bilgi içeren taşıyıcı) arasındaki farkı duyusal olarak tespit edemezler ve gizli iletişimi fark edemezler. Kriptografi teknolojisinden farklı olarak steganografi teknolojisi, yerleştirilen bilgilerin konumunu ve yöntemini gizleyerek daha güvenilir ve güvenli bir bilgi iletimi yöntemi sağlar, böylece bilgiler üçüncü taraflar tarafından tespit edilemez (Khari ve diğerleri, 2019). Kriptografi teknolojisi, iletilen şifreli metnin belirgin bir şekilde "ihlal" hissi vermesine yol açar ve bu durum, saldırganların dikkatini çekme ihtimalini artırır. Bir kez fark edildiğinde saldırganlar, şifreli metni yok etmek için brute force gibi çeşitli araçlar ve yöntemler kullanabilir; bu da gizli iletişimin

riskli yönünü artırır. Kısacası kriptografi teknolojisi, gizli iletişimin içeriğini gizlerken steganografi teknolojisi gizli iletişimin "davranışını" gizler, bu da steganografi teknolojisinin daha fazla gizlilik ve güvenlik sağladığı anlamına gelir (Antonio ve diğerleri, 2019). Çizelge 3.4, steganografi ve kriptografi arasındaki farkları beş açıdan karşılaştırmaktadır (Z. Wu ve diğerleri, 2021):

Çizelge 3.4. Steganografi ve kriptografi karşılaştırması (Z. Wu ve diğerleri, 2021)

Teknik	**Amaç**	**Güvenlik İlkesi**	**Analiz Türü**	**Teknik Yöntem**	**Uygulama Alanı**
Steganografi	Gizli iletişim	Gizlilik ve doğrulama	Steganaliz	Alan ve dönüştürme alanları, model tabanlı, ses, video, görüntü	Sesli, video ve görüntü
Kriptografi	Veri koruma	Veri bütünlüğü, kimlik doğrulama, inkâr edilemezlik	Kriptanaliz	Transpozisyon, yer değiştirme, akış şifresi, blok şifresi	Dosya

Dijital ses steganografisi, bir ses dosyası içerisine duyulamayacak düzeyde bilgi saklamayı mümkün kılar. Bu yöntemler özellikle LSB (Least Significant Bit) algoritmaları ile gerçekleştirilmekte olup sesin duyusal bütünlüğünü bozmazken içerik eklemeye olanak tanır (Mazurczyk ve diğerleri, 2016: 1, 296). Saldırganlar bu tür yöntemlerle sesli asistanlara komutlar gizleyebilir, gizli mesajlar iletebilir ya da güvenlik sistemlerini manipüle edebilirler. Bu kapsamda steganografi yalnızca bir güvenlik aracı değil, aynı zamanda potansiyel bir siber saldırı vektörü olarak da değerlendirilmektedir.

Kriptografi ve steganografi, güvenlik alanında kritik öneme sahip iki ayrı tekniktir ve sesli iletişimde bu tekniklerin uygulanması, siber güvenlik tehditlerinin çeşitliliğini arttırmaktadır. Ses tabanlı saldırılar, özellikle sesli verinin şifrelenmesi veya gizlenmesi durumunda daha karmaşık ve zor tespit edilebilir hale gelmektedir. Kriptografi, verilerin güvenli bir şekilde iletilmesini sağlamak için matematiksel algoritmalar kullanırken

steganografi, verilerin gizliliğini sağlamak amacıyla verinin içerisine gizli bilgilerin yerleştirilmesini sağlar (Pekerti ve diğerleri, 2024). Ses tabanlı saldırılarda bu iki yöntem, saldırganların iletişim süreçlerini gizlemelerine ve siber saldırıları daha etkili hale getirmelerine olanak tanır.

Sesli veri sesli asistanlar, telefon görüşmeleri, çevrim içi toplantılar gibi birçok dijital ortamda yaygın olarak kullanılmaktadır. Ses verilerinin güvenliği, özel bilgilerin korunması ve kişisel mahremiyetin sağlanması açısından oldukça kritik bir öneme sahiptir. Kriptografi, sesli verilerin şifrelenmesini sağlayarak bu verilerin yalnızca yetkili kişiler tarafından erişilmesini temin eder (Pekerti ve diğerleri, 2024). Kriptografi yöntemleri, sesli iletilerin içeriğini gizleyerek dinlemelere karşı koruma sağlar. Öte yandan steganografi, sesli veriler içinde gizli bilgilerin saklanmasıyla ilgilidir. Bu yöntemle ses verisinin görünürde herhangi bir değişiklik olmadan içine şifreli mesajlar yerleştirilebilir (Pekerti ve diğerleri, 2024).

Bu iki yöntem sesli veri ile ilişkilendirildiğinde, bir yandan sesli saldırıların gizliliğini artırırken diğer yandan saldırıların tespit edilmesini daha da zorlaştırır. Pekerti ve diğerleri (2024), sesli verilerin güvenliğini sağlamak için steganografinin popüler bir teknik olduğunu ve özellikle yüksek sistem verimliliği sağladığını belirtmektedir. Kriptografi ise daha güçlü güvenlik sağlamak için sesli iletilerin şifrelenmesi noktasında önemli bir rol oynamaktadır (Pekerti ve diğerleri, 2024).

Sesli iletişimde güvenliğin sağlanmasında kriptografi ve steganografinin birlikte kullanımı, saldırganlar için olduğu kadar savunma mekanizmaları için de güçlü bir kombinasyon oluşturmaktadır. Özellikle VoIP gibi düşük bant genişliğine sahip, gerçek zamanlı ses iletimi içeren teknolojilerde geleneksel şifreleme yöntemleri bazı sınırlılıklara sahip olabilirken steganografi bu sınırlamaları aşmak ve gizli iletişimi sürdürmek için kullanılabilmektedir (Z. Wu ve diğerleri, 2021). VoIP tabanlı sesli iletişimde steganografik yöntemler, ses paketlerinin yük kısmına ya da iletişim protokollerinin başlık alanlarına gizli veri yerleştirilerek gerçekleştirilmektedir. Bu yöntem yalnızca iletilen mesajın değil, mesajın varlığının da fark edilmesini zorlaştırmaktadır (Z. Wu ve diğerleri, 2021).

Sesli veriler üzerinde gerçekleştirilen steganografi uygulamaları, genellikle duyulamayacak düzeyde küçük değişiklikler yaparak gerçekleştirilir. Bu bağlamda sabit kod kitapları (Fixed Codebook - FCB), doğrusal tahmin katsayıları (LPC) ve uyarlanabilir kod kitapları (ACB)

gibi ses kodlama yapılarına müdahale edilerek veri gizlenmesi mümkün hale gelmektedir. Bu teknikler, insan kulağının algılayamayacağı farklılıklardan faydalanarak gizli verinin ses içine gömülmesini sağlar (Z. Wu ve diğerleri, 2021). Ancak bu tür bir bilgi gizleme yalnızca güvenli iletişim değil, aynı zamanda saldırganlar tarafından yasa dışı veri aktarımı amacıyla da kullanılabilmektedir. Bu durum, kriptografik güvenlik önlemlerinin yanı sıra steganaliz tekniklerinin de gelişmesini zorunlu kılmaktadır.

Öte yandan modern kriptografi özellikle üçlü güvenlik ilkesini (gizlilik, bütünlük ve kimlik doğrulama) uygulama konusunda vazgeçilmezdir. Sesli verilerde uygulanan kriptografik algoritmalar, bu üç ilkenin uygulanması için kolaylık sağlasa da uygulama sürecinde siber saldırıların hedefi de olabilmektedir (Pekerti ve diğerleri, 2024). Bununla birlikte, kriptografik iletilerin doğası gereği ilgi çekici olabilmesi, bu verilerin daha kolay hedef haline gelmesine yol açabilmektedir. Bu noktada, steganografinin "iletişim davranışını gizleyen" yapısı, kriptografiyle birlikte kullanıldığında daha kapsamlı bir güvenlik stratejisi sunar (Z. Wu ve diğerleri, 2021).

Gelişen tehdit ortamında sesli iletişimi hedef alan saldırılar, her geçen gün daha detaylandırılabilir hale gelmektedir. Bu kapsamda sesli iletilere yönelik hem steganografik hem de kriptografik koruma mekanizmalarının birlikte uygulanması, çok katmanlı bir savunma yaklaşımını mümkün kılmaktadır. Sesli veri güvenliğinin sağlanmasında bu yöntemlerin bir arada değerlendirilmesi, yalnızca iletişim gizliliğini değil aynı zamanda mesajın bütünlüğünü ve kaynağının doğruluğunu da teminat altına alır. Ancak bu güçlü kombinasyonun kötüye kullanım ihtimali de unutulmamalıdır. Dolayısıyla bu alanlarda geliştirilen savunma teknolojileri kadar saldırı tespit sistemlerinin de ilerletilmesi büyük önem taşımaktadır.

Sonuç olarak kriptografi ve steganografi, sesli iletişimin korunmasında tamamlayıcı güvenlik katmanları sunmaktadır. Kriptografi içerik güvenliğini, steganografi ise iletişimin varlığını gizlemeyi amaçlayarak, bir arada kullanıldıklarında sesli veri üzerinde üst düzey bir koruma sağlamaktadır. Ancak bu tekniklerin kötü niyetli aktörlerce kullanılabilmesi, onları potansiyel saldırı araçları haline de getirmektedir. Bu nedenle, sesli iletişimde hem güvenliği sağlayan hem de saldırıları tespit edebilen bütünsel çözümler geliştirmek bilgi güvenliği alanında stratejik bir öncelik haline gelmiştir. Gelecekte yapay zekâ destekli tespit

sistemleri, kuantum kriptografi ve gelişmiş steganaliz teknikleri bu alanda önemli gelişmelerin önünü açacaktır.

3.12. Akustik Dinleme Saldırıları

Akustik dinleme, modern teknolojik cihazlar üzerinden bilgi sızdırmaya yönelik geliştirilen saldırı türlerinden biri olmakla birlikte, tarihsel kökleri 20. yüzyılın ortalarına dayanmaktadır. Özellikle Soğuk Savaş döneminde, akustik temelli gözetleme yöntemleri istihbarat örgütleri tarafından yoğun biçimde kullanılmıştır. Bunun en bilinen örneklerinden biri, 1945 yılında Sovyetler Birliği'nin ABD Moskova Büyükelçiliği'ne hediye ettiği ve içerisinde "The Thing" adı verilen pasif bir dinleme cihazı barındıran ahşap arma olayıdır. Bu cihaz, herhangi bir güç kaynağına ihtiyaç duymaksızın çevredeki yüksek frekanslı radyo dalgalarını kullanarak ortam seslerini yansıtabilen bir özelliğe sahiptir (Levy, 2001: 1, 368). Bu olay, elektronik olmayan ancak frekans temelli çalışan ilk akustik yan kanal saldırılarından biri olarak kabul edilmektedir.

Bilgisayar çağında ise akustik dinleme saldırıları, özellikle elektromekanik yazıcılar ve klavyeler gibi cihazlardan yayılan seslerin analiz edilmesiyle gelişmiştir. 2004 yılında Asonov ve Agrawal tarafından gerçekleştirilen bir çalışmada, bilgisayar klavyesinde yazılan karakterlerin ses frekanslarına göre %96 oranında doğru tahmin edilebildiği gösterilmiştir (Asonov ve Agrawal, 2004). Bu çalışma, akustik yan kanal saldırılarının teoriden pratiğe geçişini sağlamış ve saldırganların yalnızca ortam seslerini dinleyerek şifre ya da metin bilgilerini elde edebileceğini kanıtlamıştır.

Son yıllarda ise akustik dinleme saldırılarının odağı sesli asistanlar, akıllı telefonlar ve dizüstü bilgisayarlar gibi mikrofon donanımına sahip cihazlara yönelmiştir. Özellikle 2019 yılında Kwong ve arkadaşları tarafından yayımlanan çalışmada, sabit disklerin içerisindeki mekanik titreşimlerin, mikrofon gibi kullanılabileceği ve çevredeki sesleri algılayabileceği gösterilmiştir (Kwong ve diğerleri, 2019). Bu gelişme yalnızca ses kaydı yapan cihazların değil, sıradan donanım bileşenlerinin bile siber saldırılar için kullanılabileceğini ortaya koyarak akustik dinleme saldırılarının kapsamını genişletmiştir. Buna paralel olarak Panda ve arkadaşları da PIN girişlerinin tuş seslerinden yola çıkarak sesin oldukça yüksek doğrulukla analiz edilebileceğini kanıtlamıştır (Panda ve diğerleri, 2020).

Akustik dinleme saldırılarının tarihçesi, sesin fiziksel özelliklerinden faydalanarak bilgi toplama girişimlerinin uzun süredir var olduğunu göstermektedir. Günümüzde ise bu saldırılar, siber güvenlik alanında ses tabanlı yan kanal tehditlerinin en gelişmiş örneklerinden biri olarak değerlendirilmektedir.

Akustik dinleme saldırıları (acoustic eavesdropping attacks), ses tabanlı siber saldırıların gelişen ve giderek daha karmaşık hale gelen bir türüdür. Bu saldırılar, geleneksel ağ dinleme veya fiziksel cihaz erişimi gerektiren yöntemlerden farklı olarak çevredeki ses dalgalarını analiz ederek bilgi elde etme esasına dayanır. Günümüz teknolojilerinde yaygınlaşan mikrofon tabanlı cihazlar özellikle akıllı telefonlar, dizüstü bilgisayarlar, sesli asistanlar ve IoT tabanlı sistemler bu tür saldırılar için potansiyel hedef haline gelmiştir (F. Wu ve diğerleri, 2021). Bu cihazların çoğu, sesli komutlara tepki verebilmek için sürekli olarak dinleme modunda çalışmaktadır. Bu durum, kullanıcı farkında olmadan çevredeki konuşmaların tuş vuruşlarının ya da diğer akustik sinyallerin toplanmasını mümkün kılmaktadır (Pekerti ve diğerleri, 2024).

Akustik dinleme saldırılarının temel amacı, çevredeki sesli verilerden hassas bilgileri çıkarmaktır. Bu bilgiler şifreler, PIN numaraları, kimlik bilgileri veya özel konuşmalar gibi çok önemli düzeyde gizlilik barındıran kişisel verileri de içerebilir. Bu saldırılar, genellikle iki farklı strateji ile gerçekleştirilir: Kötü amaçlı yazılımlar aracılığıyla cihaz mikrofonlarının ele geçirilmesi ve fiziksel akustik ses yansımalarının analiz edilmesi.

İlk yöntemde, bir cihaza sosyal mühendislik teknikleriyle (örneğin oltalama bağlantıları veya sahte uygulamalar) sızılarak cihazın mikrofonuna uzaktan erişim sağlanır. Bu sayede saldırganlar, cihazın kullanılmadığı anlarda bile ortam seslerini kaydedebilir ve özel konuşmaları, telefon görüşmelerini veya tuş vuruşlarını izleyip dinleyebilir (F. Wu ve diğerleri, 2021). Bu tür saldırıların saptanması oldukça güçtür çünkü kullanılan mikrofon cihazın orijinal parçasıdır ve genellikle sistem tarafından mikrofonun sürekli dinleme modunda olması normal bir durum olarak kabul edilir.

İkinci ve daha karışık olan yöntem ise ses dalgalarının fiziksel yüzeylerden yansımasını analiz etmeye dayalıdır. Bu teknikle saldırganlar, belirli konumlara yerleştirdikleri mikrofonlar veya ses kaydedici cihazlar aracılığıyla duvarlardan, masalardan veya çevredeki objelerden yansıyan sesleri toplayarak tuş vuruşlarının ses desenlerini analiz edebilirler.

Araştırmalar, düşük arka plan gürültüsü bulunan ortamlarda tuş sesi tabanlı metin çıkarımının oldukça başarılı olduğunu göstermektedir (Panda ve diğerleri, 2020).

Akustik saldırılar yalnızca sesli asistanlara ya da mikrofonları hedef almaya yönelik değildir. Ultrasonik frekansları kullanan gelişmiş saldırı türleri de mevcuttur. DolphinAttack adı verilen yöntemle 20 kHz üzerindeki insan kulağının duyamayacağı frekanslarda sesli komutlar gönderilerek cihazlara komutlar iletilebilir ya da sesli kayıt yapılabilir (Kwong ve diğerleri, 2019). Bu durum, fiziksel bir müdahale olmaksızın sesli sistemlerin manipülasyonunun gerçekleştirilmesini mümkün kılar.

Bu tür saldırıların tespit edilmesi zor olduğundan savunma mekanizmalarının da çok katmanlı ve detaylı olması gerekmektedir. Kullanıcıların öncelikle cihaz ayarlarını düzenli olarak gözden geçirmesi, kullanılmayan mikrofonların devre dışı bırakılması ve yalnızca güvenilir uygulamalara mikrofon erişimi verilmesi önerilmektedir. Ayrıca iletişimlerin uçtan uca şifrelenmiş platformlar üzerinden gerçekleştirilmesi, olası veri sızıntılarını önleyebilecek önemli bir tekniktir (Pekerti ve diğerleri, 2024).

Özellikle kamu kurum ve kuruluşları gibi büyük verisel zararların meydana gelebileceği ortamlarda bu saldırı türünden korunabilmek için fiziksel güvenlik önlemlerinin alınması büyük bir önem taşır. Örneğin sesin dış ortama iletilmesini engelleyen özel ses yalıtım sistemleri, karıştırıcı (jammer) cihazlar veya yankı bastırıcı teknolojiler, hassas ortamlarda ek koruma sağlayabilir (F. Wu ve diğerleri, 2021). Ayrıca kullanıcıların ses güvenliğine yönelik bilinçlendirilmesi ve farkındalık eğitimi hem bireysel hem de kurumsal düzeyde bilgi güvenliğinin sağlanmasında belirleyici rol oynamaktadır.

Mikrofon temelli cihazların yaygınlaşması, bu tür saldırıların daha görünmez olmasına ve etkili bir şekilde meydana gelmesine yol açmıştır. Gerek kötü amaçlı yazılımlar aracılığıyla cihaz mikrofonlarının ele geçirilmesi gerekse fiziksel yansımalarla ses analizinin yapılması, bireysel kullanıcılar ve kurumlar açısından yeni tehditlerin var olabileceğini ortaya koymaktadır. Ancak bu saldırılara karşı alınacak teknik, fiziksel ve davranışsal önlemler, güvenliği artırmak için etkili savunma katmanları oluşturacaktır.

Bu noktada ayrıca akustik temelli olan ve keylogger adı verilen saldırılar, dijital güvenlik alanında önemli bir tehdit olarak öne çıkmaktadır. Geleneksel keylogger yazılımlarından

farklı olarak akustik saldırılar, fiziksel ortamda gerçekleşen ses dalgaları aracılığıyla veri toplamayı hedefler. Klavye tuşlarına basıldığında her tuş, belirli frekansta ses dalgaları yayarak bu seslerin doğru analiz edilmesi ile saldırganlar kullanıcıların yazdığı metinleri elde edebilirler. Akustik temelli keylogger'lar, özellikle hassas bilgilerin girildiği ortamlarda ciddi bir güvenlik riski oluşturmakta ve geleneksel yazılımsal önlemlerin bu tür saldırılara karşı yetersiz kalmasına neden olmaktadır. Bu bağlamda akustik saldırıların tespitine yönelik yeni tekniklerin geliştirilmesi büyük önem taşımaktadır.

Bhardwaj ve Goundar'ın 2020 yılında yayımlanan "Keyloggers: Silent Cyber Security Weapons" başlıklı çalışmasında keylogger'lar, bilgisayar sistemlerinde kullanıcıların tuş vuruşlarını gizlice kaydeden kötü amaçlı yazılımlar olarak tanımlanmaktadır. Bu yazılımlar, genellikle trojan türündeki zararlı yazılımlar aracılığıyla hedef sistemlere yerleştirilir ve kullanıcının fark etmeden faaliyet göstermeye devam eder. Keylogger'lar, çoğunlukla sosyal mühendislik saldırıları veya kötü amaçlı bağlantılarla yayılarak kullanıcıların kişisel bilgilerini, parola ve kredi kartı bilgileri gibi hassas verileri ele geçirmeyi amaçlar. Yazılım, kullanıcıların tuş vuruşlarını kaydederek verileri şifreleyip saldırganlara gönderir ve bu süreçte sistemin kaynaklarını yasal programlar ile paylaşarak tespit edilmesini zorlaştırır. Böylece keylogger'lar, hedef bilgisayar üzerindeki kullanıcı faaliyetlerini izleyerek ciddi güvenlik açıklarına neden olabilmektedir. Çizelge 3.5'te keylogger kullanım örneklerine yer verilmiştir:

Çizelge 3.5. Keylogger kullanım örnekleri (Bhardwaj ve Goundar'ın 2020)

Kullanım Amacı	Kullanım Türü	Açıklama
Pozitif	**Ebeveyn İzleme**	Çocukların ve öğrencilerin internet gezinme alışkanlıkları ve etkinliklerini kontrol ederek siber farkındalıklarını sağlamak ve zararlı etkinliklerden kaçınmalarını temin etmek.
	Çalışan Verimliliğini Artırma	Çalışanların sosyal medya veya verimsiz sitelerde harcadığı zamanı kontrol etmek. Ancak, bu süreç, çalışanların izni ve gizlilik ile ilgili uygun politikalar çerçevesinde yapılmalıdır.
	Yazı Araştırmaları	Yapılan araştırmalar, keylogger'ların bilişsel yazma süreçleri (akıcılık ve akış) ile ikinci dil öğrenme üzerine yapılan çalışmalarda verimli bir araç olarak kullanıldığını ortaya koymuştur.
	Etik Hacking	Kullanıcı sistemlerini kasıtlı olarak istismar ederek güvenlik açıklarını değerlendirme ve penetrasyon testleri yapma, ardından gelecekteki tehditleri azaltmak için düzeltmeler yapma.
	Adli Soruşturmalar	Kurumsal, hükümet ve askeri casusluk faaliyetlerinde, siber suç soruşturmaları için dijital analizler yapma ve ihlalleri tespit etme.
Negatif	**Bilgi Toplama**	Hedef sistemin klavyesindeki her tuş vuruşunu kaydetmek ve her türlü hassas bilgiyi (ödeme kartı verileri, sosyal güvenlik numaraları, ehliyet bilgileri, iki faktörlü kimlik doğrulama kodları, parolalar, e-posta ve banka bilgileri vb.) çalmak.
	Ekran Kaydı	Hedef sistemde görsel izleme yaparak dosya oluşturma, güncelleme veya kopyala-yapıştır işlemlerini izlemek ve düzenli aralıklarla ekran görüntüleri göndererek takip etme.
	Kimlik Hırsızlığı	Kişisel tanımlayıcı bilgilerin toplanmasının ardından, ekonomik ve finansal dolandırıcılık faaliyetleri gerçekleştirme. Son zamanlarda büyük çapta bu tür olaylar meydana gelmiştir.

Akustik temelli keylogger saldırıları, geleneksel yazılımsal keylogger tekniklerinden farklı olarak klavye tuşlarına basıldığında oluşan ses dalgalarını analiz ederek yazılan bilgilerin elde edilmesini amaçlayan siber saldırı yöntemlerindendir. Bu tür saldırıların temeli, her bir tuşun karakteristik bir ses frekansı ve yankılanma biçimi yaratması ilkesine dayanır. Bu akustik imzaların analiz edilmesiyle saldırganlar, kullanıcıların klavyede ne yazdığını yüksek doğrulukla tahmin edebilirler.

Bu tür saldırıların ilk dikkat çeken akademik örneklerinden biri, Berkeley Üniversitesi'nden Asonov ve Agrawal tarafından 2004 yılında yayımlanan çalışmadır. Bu araştırmada, tuş vuruşlarının ses kayıtlarının analiz edilerek yazılan metnin büyük ölçüde tahmin edilebileceği gösterilmiştir. Araştırmacılar, tuşların farklı frekanslarda ses çıkardığını ve bu seslerin sınıflandırma algoritmaları ile ayırt edilebildiğini ortaya koymuşlardır (Asonov ve Agrawal, 2004).

Zamanla bu teknik gelişmiş ve yapay zekâ destekli modellerin uygulanmasıyla sonuçların doğruluk oranı artmıştır. Özellikle 2009 yılında Vuagnoux ve Pasini tarafından gerçekleştirilen bir çalışmada, yalnızca elektromanyetik sızıntıların değil aynı zamanda tuşların çıkardığı sesin de etkili bir şekilde kullanılabileceği gösterilmiştir (Vuagnoux ve Pasini, 2009). Bu gelişmelerle birlikte, akustik keylogger'lar hem siber güvenlik topluluklarında hem de istihbarat alanında dikkat çeken bir tehdit haline gelmiştir.

Sonraki yıllarda akustik sinyallerin analizinde makine öğrenmesi algoritmaları kullanılmaya başlanmış; özellikle Support Vector Machine (SVM), Hidden Markov Models (HMM) ve son dönemde derin öğrenme temelli sistemlerle tuş sesleri aracılığıyla karakter tahmininde yüksek başarılar elde edilmiştir. Örneğin 2020 yılında Panda ve arkadaşları tarafından gerçekleştirilen bir çalışmada, PIN girişlerinin akustik sinyallerle başarılı biçimde tahmin edilebildiği gösterilmiştir; bu çalışmada davranışsal akustik emisyonlar analiz edilmiş ve doğruluk oranı %90’a yaklaşmıştır (Panda ve diğerleri, 2020).

Salas-Nino ve diğerlerinin 2023 yılında yayımlanan "The Evolution of Keylogger Technologies: A Survey from Historical Origins to Emerging Opportunities" başlıklı çalışmasında, keylogger teknolojilerinin tarihsel gelişimi ayrıntılı biçimde ele alınmakta ve bu teknolojilerin günümüzde siber güvenlik açısından halen ciddi tehditler oluşturduğu vurgulanmaktadır. Çalışmada, 1970’li yıllarda Sovyetler Birliği tarafından ABD

elçiliklerinde kullanılan ve IBM Selectric daktilolarını hedef alan “Selectric bug” adlı elektromekanik keylogger’dan başlayarak günümüzde yazılım tabanlı, donanım destekli ve hatta yapay zekâ ile güçlendirilmiş modern saldırı tekniklerine kadar geniş bir yelpazede keylogger teknolojilerinin evrimi incelenmiştir. Özellikle 2000’li yıllardan sonra form-grabbing, JavaScript tabanlı, API yakalayıcı ve kernel düzeyine sızabilen yazılımların ortaya çıkması ile keylogger’ların yalnızca fiziksel değil aynı zamanda çok katmanlı dijital saldırı araçlarına dönüştüğü gösterilmektedir. Bu bağlamda saldırganlar artık sadece tuş vuruşlarını değil, mikrofonlar üzerinden toplanan akustik verileri de analiz ederek tuş seslerinden anlamlı bilgiler çıkarabilmekte, bu da keylogger’ları akustik dinleme saldırılarının önemli bir parçası haline getirmektedir. Salas-Nino ve arkadaşları, bu tür saldırıların kurumsal sistemleri de hedef alabileceğine dikkat çekerek özellikle kamuya açık cihazlarda ve kurumsal ağlarda anti-keylogger çözümlerinin öneminin altını çizmektedir (Salas-Nino ve diğerleri, 2023).

Akustik keylogger saldırılarının başarılı olabilmesi için mikrofonun kapalı konumda olması oldukça önemlidir. Mikrofonun klavyeye olan uzaklığı, çevresel gürültü, kullanılan klavyenin mekanik ya da membran yapıda olması ve ortamın akustiği gibi birçok değişken, saldırının etkinliğini doğrudan etkiler. Bu saldırılar genellikle şu adımlarla gerçekleştirilir:

- Ses toplama: Klavye yakınında bulunan bir mikrofonla tuş sesleri kaydedilir.
- Özellik çıkarımı: Her tuşun çıkardığı seslerden frekans, süre ve genlik gibi akustik özellikler çıkarılır.
- Sınıflandırma: Elde edilen özellikler, önceden eğitilmiş bir makine öğrenmesi modeli ile analiz edilerek hangi tuşun basıldığı tahmin edilir.
- Metnin meydana getirilmesi: Sıralı olarak elde edilen tuş tahminleri bir araya getirilerek yazılan metin oluşturulur.

Bu teknik özellikle ofis ortamları, açık alanlar veya çevresel gürültünün düşük olduğu ortamlarda yüksek doğrulukla çalışmaktadır. Ancak modern akustik işleme teknikleri ile gürültülü ortamlarda da tatmin edici sonuçlar elde etmek mümkün hale gelmiştir.

M. Chen ve diğerlerinin 2022 yılında yayımlanan "Behavicker: Eavesdropping Computer-Usage Activities through Acoustic Side Channel" başlıklı çalışmasında, bilgisayar kullanım aktivitelerinin akustik yan kanal üzerinden dinlenebilme olasılığına dair önemli bir araştırma

sunulmuştur. Bu çalışma, kullanıcıların klavye ve fare etkileşimlerinden yayılan ses sinyallerini tespit ederek akustik yan kanal üzerinden bilgisayar kullanım aktivitelerini izlemeyi amaçlamaktadır. Geleneksel eylem tanıma yöntemlerinden farklı olarak Behavicker sistemi, kullanıcının bilgisayar başındaki etkileşimlerini yüksek seviyede tanıyabilmek için çok ölçekli bir öğrenme şeması kullanmaktadır. Çalışmada klavye tuşlarına basma, sol tıklama, sağ tıklama, orta tıklama ve kaydırma gibi temel etkileşim olaylarının tanınmasıyla bilgisayar kullanım aktiviteleri doğru bir şekilde sınıflandırılmakta ve deneyler, bu yöntemin %88,3 doğruluk oranıyla etkileşim olaylarını ve %82,7 doğruluk oranıyla bilgisayar kullanım aktivitelerini tanıyabildiğini göstermektedir. Bu bulgular, akustik yan kanal saldırılarının kullanıcının bilgisayar aktivitelerini izleme ve bu aktivitelerden kişisel bilgi elde etme açısından ciddi bir tehdit oluşturabileceğini ortaya koymaktadır.

Y. Chen ve diğerlerinin 2024 yılında yayımlanan “A survey of acoustic eavesdropping attacks: Principle, methods, and progress” başlıklı çalışmasında akustik dinleme saldırıları, bilgi güvenliğini tehdit eden en kritik yan kanal saldırılarından biri olarak ele alınmıştır. Çalışma mikrofon, sensör ve diğer akustik algılayıcılar aracılığıyla ses sinyallerinin toplanarak işlenmesiyle hassas verilerin elde edilmesine dayanan akustik dinleme tekniklerinin temel ilkelerini, tarihsel gelişimini ve uygulama senaryolarını kapsamlı şekilde analiz etmektedir. Ayrıca çalışmada akustik dinleme saldırıları üç ana kategori altında sınıflandırılmaktadır: Hareket sensörüne dayalı (motion sensor-based), optik sensöre dayalı (optical sensor-based) ve radyo frekans temelli (RF-based) saldırılar. Hareket sensörlü yaklaşımlar, ses dalgalarının neden olduğu titreşimleri ivmeölçerler gibi sensörlerle algılayarak sesli bilgiyi yeniden yapılandırmaya çalışırken optik sensörlü saldırılar, lazer veya ışık kaynakları aracılığıyla yüzey titreşimlerini ölçerek ses verisini geri kazanmaktadır. RF-temelli yöntemler ise sesin neden olduğu elektromanyetik değişimleri radyo dalgaları yoluyla analiz ederek akustik bilgiye ulaşmayı amaçlamaktadır. Bu saldırı türlerinin avantajları, zorlukları ve gerçek dünyadaki uygulanabilirlikleri çeşitli açılardan karşılaştırılmış; özellikle müdahalesizlik (non-intrusiveness), makine öğrenmesine olan bağımlılık, hareketli kaynakları tespit edebilme, opak yalıtkanlar üzerinden işlem yapabilme gibi kriterler üzerinden değerlendirilmiştir. Makale, ayrıca bu teknolojilerin sesin doğruluğu ve enerji verimliliği gibi açılardan optimize edilmesi gerektiğini vurgularken akustik yan kanal saldırılarına karşı daha etkin savunma stratejileri geliştirilmesine yönelik bir araştırma çerçevesi sunmaktadır. Bu bağlamda çalışma hem sesli verilerin gizliliği açısından hem de

gelecekteki güvenlik protokollerinin tasarımı bakımından önemli bir başvuru kaynağı niteliği taşımaktadır.

Akustik dinleme saldırılarının başarısı, kullanılan donanımın frekans algılama kapasitesine, veri işleme hassasiyetine ve enerji verimliliğine bağlı olarak artmaktadır. Modern sistemler, düşük enerji tüketimiyle uzun süreli dinleme imkânı sunmakta ve bu durum söz konusu saldırıları daha yaygın ve kalıcı etkilere sahip olabilecek bir tehdit haline getirmektedir. Saldırıların etkinliğini artıran bir diğer faktör, özellikle sesli komutlarla çalışan cihazların sürekli dinleme modunda olmasıdır; bu durum, kullanıcı farkında olmadan verilerin izinsiz şekilde toplanmasına zemin hazırlar. Buna göre sesli veri güvenliği yalnızca dijital önlemlerle değil, aynı zamanda fiziksel güvenlik protokolleriyle de desteklenmeli; sensör optimizasyonu, ses şifreleme ve çevresel akustik yalıtım gibi stratejilerle korunmalıdır.

Mikrofon tabanlı cihazların ve sesle etkileşimli teknolojilerin yaygınlaşmasıyla fiziksel ortamlardaki ses sinyalleri, dijital analizlere açık hale gelmiş; bu durum, bireysel gizliliğin ve kurumsal veri güvenliğinin yeni bir tehdit boyutuyla karşı karşıya kalmasına neden olmuştur. Akustik dinleme yalnızca mikrofon erişimiyle sınırlı kalmamakta, aynı zamanda ultrasonik frekanslar aracılığıyla gerçekleştirilen ve insan kulağının algılayamayacağı düzeyde olan saldırılarla daha karmaşık hale gelmektedir. Özellikle akustik temelli keylogger teknikleri, yazılı içeriklerin ya da şifrelerin yalnızca tuş seslerinden elde edilebilmesini mümkün kılmakta ve geleneksel güvenlik mekanizmalarını etkisiz kılmaktadır. Bu tehditlerin tespiti, genellikle düşük ses seviyelerinde gerçekleştirilmesi ve çevresel gürültüye entegre edilebilmesi nedeniyle son derece zordur. Bu nedenle yalnızca cihaz güvenliğini sağlamak yeterli değildir, sesli verilerin korunmasına yönelik çok katmanlı savunma mekanizmalarının geliştirilmesi büyük önem arz etmektedir. Bu kapsamda kullanıcı farkındalığının artırılması, cihaz mikrofonlarının erişim izinlerinin dikkatle yönetilmesi, akustik veri şifreleme protokollerinin uygulanması ve güvenlik yazılımlarının bu yeni tehdit vektörlerine uyumlu şekilde güncellenmesi gereklidir. Ayrıca savunma stratejilerinin yalnızca yazılım ve donanım düzeyinde değil, aynı zamanda hukuk, etik ve sosyal farkındalık çerçevesinde de ele alınması; bu alanda disiplinler arası iş birliğini teşvik ederek daha sürdürülebilir bir siber güvenlik ekosistemi oluşturulmasına katkı sağlayacaktır.

4. SESLE İLGİLİ VERİ İHLALLERİNİN İNCELENMESİ VE HUKUKİ SÜREÇ

Günümüzde ses verilerinin dijital ortamlarda işlenmesi, depolanması ve iletilmesi, beraberinde önemli güvenlik ve gizlilik sorunlarını getirmektedir. Özellikle sesli asistanlar, akıllı cihazlar ve iletişim uygulamaları üzerinden toplanan ses verileri bireylerin kimlik bilgileri, özel hayatı ve mahrem alanları hakkında ciddi ipuçları taşıyabilmektedir. Bu nedenle ses yoluyla gerçekleşen veri ihlalleri sadece teknik bir sorun değil aynı zamanda kişisel verilerin korunması ve bireysel hakların ihlali bağlamında ciddi bir hukuki mesele haline gelmiştir. Bu bölümde, ses temelli veri ihlallerinin hukuki boyutu çok yönlü biçimde ele alınacaktır. Türkiye'de kişisel verilerin korunmasına ilişkin yasal düzenlemeler, yargı kararları ve ilgili kurumların görüşleri incelenecek; Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) başta olmak üzere çeşitli uluslararası düzenlemeler kapsamında ses verisinin niteliği ve işlenmesine dair yaklaşımlar değerlendirilecektir. Bu bağlamda ses verilerinin kişisel veri olarak kabul edilip edilmediği, veri sorumlusunun yükümlülükleri, ses kayıtlarının hukuka aykırı elde edilmesinin sonuçları ve bu durumun cezai ve idari yaptırımları ayrıntılı olarak tartışılacaktır. Böylece sesle ilgili veri ihlallerinin hem teknik arka planı hem de hukuki süreci bütüncül bir yaklaşımla analiz edilerek konunun çok disiplinli doğasına uygun bir değerlendirme ortaya konulacaktır.

4.1. Avrupa Birliği Mevzuatı (GDPR)

Ses verilerinin hukuki boyutta kişisel veri olarak değerlendirilmesi, özellikle son yıllarda teknolojinin gelişmesiyle birlikte daha belirgin hale gelmiştir. Bu alandaki ilk kapsamlı düzenlemeler, Avrupa Birliği tarafından yayımlanan Genel Veri Koruma Tüzüğü (İngilizce olarak General Data Protection Regulation, kısaltması GDPR) ile somutlaşmıştır. 2018 yılında yürürlüğe giren GDPR, ses verilerini "kimliği belirli veya belirlenebilir bir kişiye ilişkin her türlü bilgi" tanımına dahil ederek bu tür verilerin işlenmesi, saklanması ve paylaşılması süreçlerinde veri sahibinin açık rızasını zorunlu kılmıştır (Beyaz.Net, 2024). Ayrıca ses verileri biyometrik veri kategorisinde de değerlendirilmekte ve bu kapsamda daha sıkı koruma önlemleri gerektirmektedir. GDPR hem Avrupa Birliği içinde hem de veri işleme faaliyetlerinin AB vatandaşlarını kapsaması halinde üçüncü ülkelerdeki kurum ve kuruluşlara da yükümlülükler getirmektedir. Bu çerçevede sesli komut sistemleri, çağrı

merkezleri ve sesli asistan uygulamaları, kişisel veri işleyen platformlar olarak özel düzenlemelere tabi tutulmaktadır.

Avrupa Birliği'nin 2016/679 sayılı Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin korunmasını temel bir insan hakkı olarak kabul etmekte ve bu kapsamda ses verilerini de açık biçimde kişisel veri olarak değerlendirmektedir. Tüzüğün 1. maddesinde kişisel verilerin işlenmesi bakımından bireylerin korunmasının Avrupa Birliği Temel Haklar Şartı'nın 8. maddesi ile Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın 16. maddesi uyarınca güvence altına alındığı belirtilmektedir. Gerekçe bölümünde ise teknolojik gelişmelerin ve küreselleşmenin bireylerin kişisel verileri üzerinde daha önce benzeri görülmemiş düzeyde riskler yarattığı ifade edilmektedir (GDPR Recital 6). Bu bağlamda sesli asistanlar, akıllı cihazlar ve ultrasonik komut sistemleri gibi ses temelli teknolojilerin kullanıcı farkındalığı olmaksızın kişisel verilerin toplanmasına olanak tanıması, GDPR kapsamında ciddi bir ihlal potansiyeli doğurmaktadır. Tüzüğün 30. maddesinde yer alan "çevrimiçi tanımlayıcılar" (örneğin IP adresleri, cihaz tanımlayıcıları, sesli izler vb.) kişisel veriler kategorisinde değerlendirilmiş, böylece bireyin kimliğini doğrudan veya dolaylı şekilde ortaya çıkarabilecek her türlü veri işleme faaliyeti açık rıza ya da hukuki dayanak olmadıkça hukuka aykırı sayılmıştır. Ayrıca, 49. madde uyarınca veri işleme, yalnızca "ağ ve bilgi sistemlerinin güvenliğinin sağlanması" gibi meşru amaçlarla ve sınırlı biçimde gerçekleştirilebilmektedir. Bu düzenlemeler özellikle ses sinyalleri yoluyla gerçekleştirilen izinsiz veri toplama, izleme ya da manipülasyon faaliyetlerinin GDPR kapsamında ağır ihlaller olarak değerlendirilebileceğini göstermektedir. Buna göre ses verilerinin hukuka aykırı biçimde elde edilmesi, işlenmesi veya paylaşılması, GDPR açısından hem bireylerin mahremiyetine ciddi bir tehdit oluşturmakta hem de ciddi idari yaptırımlara (para cezaları, veri işleme yasağı vb.) yol açabilmektedir.

Türkiye'de ise kişisel verilerin korunmasına ilişkin temel mevzuat, 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur (KVKK). Kanun kapsamında ses kayıtları, kimliği belirli veya belirlenebilir kişiye ilişkin olması halinde kişisel veri olarak kabul edilmekte ve buna göre işlenmesi gerekmektedir. Ses verilerinin kişilik haklarına doğrudan temas etmesi nedeniyle işlenme süreçlerinde açık rıza aranmaktadır ve amaçla sınırlı kullanım gibi ilkeler devreye girmektedir (KVKK, 2016).

4.2. Türkiye'de Mevzuat (KVKK ve İlgili Kanunlar)

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), bireylerin özel hayatının gizliliğini ve kişisel verilerinin korunmasını esas alarak dijital teknolojilerle ortaya çıkan yeni tehdit türlerine karşı hukuki bir çerçeve sunmaktadır. Bu çerçevede yapay zekâ destekli deepfake teknolojilerinin kişisel verilerin işlenmesinde doğurabileceği riskler, özellikle ses verilerinin izinsiz kullanımı gibi yeni siber saldırı türlerini doğrudan ilgilendirmektedir. KVKK'nin 5. ve 6. maddelerinde kişisel verilerin işlenme şartları açık bir şekilde düzenlenmiş, özel nitelikli kişisel veriler için daha katı koşullar getirilmiştir. İlgili belgede belirtildiği üzere ses, yüz görüntüsü ve benzeri biyometrik veriler özel nitelikli kişisel veri olarak kabul edilmekte ve bu verilerin işlenebilmesi için açık rıza alınması zorunlu tutulmaktadır. Deepfake teknolojisi kullanılarak üretilen ses verileri, bireyin kimliğini taklit etmeye olanak sağladığından hem sahte içerik üretimi hem de kimlik hırsızlığı açısından ciddi riskler taşımaktadır. Kanuna göre bu tür teknolojilerin kullanımıyla kişilerin rızası olmadan oluşturulan içerikler, KVKK'nin 12. maddesi gereği veri sorumlularının veri güvenliğini sağlama yükümlülüğünü de ihlal etmektedir. Bununla birlikte deepfake yoluyla işlenen verilerin bireylerin itibarını zedeleyici ve manipüle edici şekilde kullanılmasının Anayasa'nın 20. maddesi kapsamında güvence altına alınan özel hayatın gizliliği ilkesini de ihlal edebileceği vurgulanmıştır. KVKK bağlamında ses temelli deepfake saldırıları yalnızca kişisel verilerin izinsiz işlenmesi açısından değil, aynı zamanda bireyin hak ve özgürlüklerinin ihlali bakımından da ciddi hukuki sonuçlar doğurmakta; bu nedenle kişisel verilerin işlenmesinde şeffaflık, veri minimizasyonu, açık rıza ve güvenlik gibi ilkelerin titizlikle gözetilmesi gerektiği belirtilmektedir.

Kişisel Verileri Koruma Kurumu'nun kararları da bu alana yönelik çeşitli örnekler ortaya koymaktadır. Örneğin 24/08/2023 tarihli ve 2023/1461 sayılı Kurul kararında, bir eğitim kurumu tarafından yapılan sürekli görüntü ve ses kaydının açık rıza olmadan gerçekleştirilmesinin hukuka aykırı olduğu ve ölçülülük ilkesine aykırı biçimde gerçekleştirildiği belirtilmiştir. Benzer şekilde 07/09/2023 tarihli ve 2023/1548 sayılı Kurul kararında, bir kişinin bilgisi ve rızası dışında ses kaydının alınması ve bu kaydın yargı sürecine delil olarak sunulmasının kişisel veri işleme hükümlerine aykırılık oluşturduğu ifade edilmiştir. Bu kararlar, ses verilerinin hem özel yaşamın gizliliği açısından hem de kanuni delil olarak kullanım açısından da belirli sınırlar dahilinde değerlendirilmesi gerektiğini göstermektedir.

İstanbul Barosu'nun 2023 yılında yayımladığı "Yapay Zekâ ve Hukuk: Deepfake Üzerine Bir Değerlendirme" başlıklı çalışmasında, deepfake teknolojisinin çok yönlü hukuki etkileri kapsamlı bir şekilde analiz edilmiştir. Çalışmada ses ve görüntü manipülasyonu yoluyla üretilen deepfake içeriklerin yalnızca bireylerin özel yaşamlarını tehdit etmekle kalmadığı, aynı zamanda Türk Ceza Hukuku, Borçlar Hukuku, Fikri Mülkiyet Hukuku ve Tüketici Hukuku gibi pek çok alanda ciddi hukuki belirsizlikler ve boşluklar doğurduğu vurgulanmaktadır. Özellikle bu teknolojinin kişilik hakları bağlamında doğurduğu ihlaller, Türk Medeni Kanunu'nun 24. ve Türk Borçlar Kanunu'nun 58. maddeleri kapsamında değerlendirilmekte; rıza dışı oluşturulan ve yayılan içeriklerin maddi ve manevi tazminat taleplerine konu olabileceği ifade edilmektedir. Ayrıca çalışmada 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un içeriklerin yayından kaldırılması ve erişimin engellenmesine ilişkin hükümlerine atıfla, dijital ortamlarda yayımlanan deepfake içeriklere karşı başvurulabilecek hukuki yollar ayrıntılandırılmıştır. Ceza hukuku boyutunda ise Türk Ceza Kanunu'nun tehdit (m.106), şantaj (m.107), hakaret (m.125), özel hayatın gizliliği (m.134), kişisel verilerin hukuka aykırı kaydı ve yayılması (m.135-136), dolandırıcılık (m.157-158) ve müstehcenlik (m.226) gibi hükümlerine dikkat çekilmiş; deepfake teknolojisinin bu suçların işlenmesinde bir araç olarak kullanıldığında cezai sorumluluğun doğacağı açıklanmıştır. Çalışma, özellikle sentetik içeriklerin delil olarak kullanılabileceği ceza muhakemesi süreçlerinde sahteliğin ayırt edilememesinin maddi gerçeğe ulaşmayı engelleyebileceğini ve bu bağlamda yargı sistemine ciddi zararlar verebileceğini belirtmektedir. Bu çerçevede çalışma, Türkiye'de mevcut yasal düzenlemelerin teknolojik gelişmeler karşısında yetersiz kaldığını ve deepfake özelinde mevzuatın güncellenmesinin zorunluluk haline geldiğini savunmaktadır. Bu durum bireylerin dijital ortamlarda korunabilmesi, yargı süreçlerinin sağlıklı işleyebilmesi ve kamu düzeninin korunabilmesi açısından büyük önem arz etmektedir.

Babayiğit'in 2021 yılında yayınlanan "Deepfake'in Ceza Hukuku Bakımından Değerlendirilmesi ve De Lege Ferenda Öneriler" başlıklı çalışmasında, yapay zekâ destekli sahte içerik üretimi olan deepfake teknolojisinin Türk ceza hukuku açısından doğurabileceği sorumluluk halleri kapsamlı biçimde ele alınmıştır. Deepfake içeriklerin yalnızca görüntü değil, aynı zamanda ses verilerini de manipüle edebildiği ve bu durumun bireylerin maddi ve manevi varlıklarını tehdit eden yeni türden siber saldırı yöntemlerine zemin hazırladığı vurgulanmaktadır. Özellikle kişilerin seslerinin izinsiz biçimde değiştirilerek başka

içeriklerde kullanılmasının hem özel hayatın gizliliği hem de kişisel verilerin korunması açısından ciddi bir tehlike oluşturduğu ifade edilmektedir. Bu kapsamda Anayasa'nın 17. ve 20. maddeleri çerçevesinde bireylerin maddi ve manevi bütünlükleri ile özel hayatlarının gizliliği temel haklar olarak korunmakta olup bu tür dijital sahteciliklerin anayasal güvence altındaki hakları ihlal edebileceği belirtilmiştir. Ayrıca Türk Ceza Kanunu'nda yer alan 134. madde (özel hayatın gizliliğini ihlal), 135. madde (kişisel verilerin kaydedilmesi), 136. madde (verilerin hukuka aykırı olarak verilmesi veya yayılması) gibi hükümler ile bu tür saldırılara yönelik hukuki koruma alanlarının tanımlandığı ancak teknolojinin hızlı ilerlemesi karşısında mevcut mevzuatın yetersiz kalabileceği değerlendirilmiştir. Babayiğit bu nedenle "de lege ferenda" (gelecekte yapılması gereken hukuk düzenlemeleri) perspektifiyle deepfake gibi teknolojiler karşısında Türk ceza mevzuatının daha açık, teknik temellere dayalı ve dijital delil değerlendirmesini içerecek şekilde güncellenmesi gerektiğini vurgulamaktadır. Bu yaklaşım ses temelli sahteciliğin (örneğin ses klonlama veya sahte sesli komutlar) doğrudan mağdur yaratma potansiyeline sahip olduğu günümüzde, sesli verilerin korunmasına ilişkin özel ve güncel yasal düzenlemelerin yapılması gerekliliğini ortaya koymaktadır (Babayiğit, 2021).

Özetle hem uluslararası hem de ulusal hukukta ses verileri giderek daha hassas ve korunması gereken veriler kategorisinde değerlendirilmektedir. Teknolojik gelişmelere paralel olarak ses kayıtlarının toplanması, analiz edilmesi ve işlenmesi daha yaygın ve etkili hale gelirken veri koruma kurumları da bu alanı özel olarak düzenlemeye başlamıştır. Sesli verilerin işlenmesinde açık rıza, şeffaflık, ölçülülük ve amaca bağlılık ilkeleri temel belirleyiciler arasında yer almaktadır. Özellikle otomatik karar verme süreçlerinde kullanılan ses verilerinin ayrımcılığa yol açabilecek yapay zekâ sistemlerinde değerlendirilmesi gibi ileri düzey tehditler de göz önünde bulundurulmalı ve bu alanlara yönelik mevzuat güncellemeleri sürdürülmelidir.

4.3. Hukuki Sorumluluklar ve Uygulamalar

Günümüzde hızla artan siber saldırılar karşısında bireylerin temel hak ve özgürlüklerinin korunması amacıyla ulusal ve uluslararası düzeyde çeşitli hukuki düzenlemeler geliştirilmiştir. Bu düzenlemeler, siber suçların önlenmesi ve mağduriyetin azaltılması bakımından önemli bir güvence işlevi görmektedir. Türkiye'de de siber saldırılara karşı içtihatlar, özellikle son yıllarda gelişen dijital tehditler göz önünde bulundurularak

güncellenmiş; sesli asistanlar, akıllı cihazlar ve diğer ses temelli sistemlerin yaygınlaşmasıyla ses tabanlı saldırılar gibi yeni suç türlerinin hukuki olarak ele alınması gündeme gelmeye başlamıştır.

Siber suçlara ilişkin tanımlar ve yaptırımlar, genel olarak ceza hukuku normları çerçevesinde şekillenmiştir. Türk Ceza Hukuku'nda suç ve ceza kavramları genel hatlarıyla tanımlanmakla birlikte yeni dijital tehditler, özellikle sesli veya ultrasonik temelli saldırılar, mevcut mevzuatta açık şekilde tanımlanmamıştır. Türk hukuk doktrininde genel suç tanımı, toplum düzenini ve birlikte yaşamı korumak için önemli olan hukuki değerleri ihlal eden belirli insan davranışları olarak yapılmaktadır. Türk Ceza Hukuku'nda "kanunsuz suç ve ceza olmaz" ilkesi geçerlidir, yani bir fiilin suç olarak değerlendirilebilmesi için açık bir yasa hükmü bulunması gerekir (Karanfiloğlu, 2024). Bu ilke, 5237 sayılı Türk Ceza Kanunu'nda ve Anayasa'da açıkça ifade edilmiştir: "Hiç kimse, kanunda suç olarak tanımlanmayan bir fiilden dolayı cezalandırılamaz; güvenlik tedbirine tabi tutulamaz" (Erbaş, 2015). Dolayısıyla, özellikle ses dalgaları veya ultrasonik sinyaller aracılığıyla yapılan saldırıların mevcut ceza hukuku kapsamında nasıl değerlendirileceği hususunda hukuki belirsizlikler bulunmaktadır.

Siber saldırıların temel amaçları arasında hedef sistemleri bozmak, hassas verileri ele geçirmek, verileri manipüle etmek, yasa dışı şekilde maddi kazanç sağlamak veya kişisel verileri kötüye kullanmak yer almaktadır. Türkiye'de bu kapsamda en temel düzenlemeler, 5237 sayılı Türk Ceza Kanunu'nun çeşitli maddelerinde yer almaktadır. Örneğin, 243. madde "Bilişim Sistemine Hukuka Aykırı Olarak Girme" başlığı altında, izinsiz bir şekilde bir bilişim sisteminin tamamına ya da bir kısmına giren kişilere bir yıla kadar hapis cezası öngörmektedir. 244. madde ise "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme" başlığı altında, bir bilişim sisteminin işleyişini bozan ya da bu sistemdeki verileri silen, değiştiren kişilere altı aydan üç yıla kadar hapis cezası getirmektedir. 245. madde "Banka veya Kredi Kartlarının Kötüye Kullanılması" başlığı altında ise finansal sistemlere yönelik dijital saldırılar için özel yaptırımlar düzenlemektedir (Erbaş, 2015).

Ancak bu düzenlemeler, daha çok klasik siber suçlara yöneliktir; örneğin kullanıcı farkında olmadan cihazların manipüle edilmesine yol açabilecek akustik ya da ultrasonik dalgalarla gerçekleştirilen yeni nesil saldırı teknikleri mevzuatta açıkça tanımlanmamıştır. Bu nedenle söz konusu saldırıların hukuki nitelendirilmesi konusunda uygulamada ciddi belirsizlikler

söz konusudur. Sesli asistanlara ya da sabit disk sürücülerine yönelik bu tür saldırıların artışı, mevcut yasaların yeni saldırı biçimlerine göre güncellenmesi ihtiyacını doğurmaktadır. Örneğin ultrasonik sinyallerle sistemlere gizli komut gönderilmesi veya veri manipülasyonu yapılması, "bilişim sistemine izinsiz erişim" kapsamında değerlendirilebilir; ancak bu yorum, bilişim sistemi kavramının mevcut yasal çerçevede nasıl yorumlandığına da bağlıdır.

Uluslararası düzeyde ise devletler arası iş birliğini güçlendirmeye yönelik birçok düzenleme ve sözleşme mevcuttur. Bunlar arasında en önemlisi, 2001 yılında Avrupa Konseyi tarafından kabul edilen ve siber suçlarla mücadeleyi hedefleyen Budapeşte Sözleşmesi'dir. Bu sözleşme, taraf devletler arasında siber suçlarla mücadelede ortak standartlar ve yakın iş birliği ilkesi çerçevesinde sınır ötesi koordinasyonu amaçlamaktadır (Council of Europe, 2024). Türkiye de bu sözleşmeyi imzalamış ve siber suçlarla mücadelede uluslararası yükümlülük altına girmiştir. Ancak bu hükümlerin Türk iç hukukuna yansıması, halen hukuk çevrelerinde tartışma konusudur.

Ses tabanlı saldırılara ilişkin bir diğer önemli yasal düzenleme, 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur. Bu kanun kişisel verilerin işlenmesini, saklanmasını ve güvenliğini düzenleyerek ihlaller durumunda ciddi yaptırımlar öngörmektedir. Kişisel verilerin korunması, siber saldırıların en sık hedef aldığı alanlardan biri olduğundan bu tür yasal düzenlemelerin varlığı büyük önem taşımaktadır. Ancak KVKK'de de ses verilerine dayalı müdahalelere ilişkin açık bir düzenleme yer almamaktadır. Özellikle ses tabanlı saldırılar yoluyla kişisel veri ihlalinin önlenmesine yönelik açık normların eksikliği, mevcut düzenlemelerdeki önemli hukuki boşluklara işaret etmektedir.

Günümüzde ses verilerinin yalnızca iletişim aracı olarak kullanılmadığı, aynı zamanda yasal süreçlerde önemli bir delil unsuru haline geldiği kaçınılmaz bir gerçektir. Bu kapsamda sesli verilerin dijital dünyadaki rolü, suçların aydınlatılmasında oldukça etkili bir araç haline gelmesiyle büyük oranda artmıştır. Söz konusu verilerle ve ses tabanlı saldırılarla ilgili olarak mevcut yasal düzenlemelerdeki boşluklar, bu tür saldırıların önlenmesi ve suçların tespiti açısından önemli bir eksiklik yaratmaktadır. Ayrıca yargı kararlarında ses verilerinin suçun çözülmesine olan katkısı, bu alanda yapılacak yasal düzenlemelerin gerekliliğini bir kez daha vurgulamaktadır.

Yargıtay 8. Ceza Dairesi'nin 2020/1419 E., 2022/122 K. sayılı kararında, sanığın sahte kredi kartı üretimi ve bu kartlarla menfaat temin etmesi suçlarına ilişkin mahkumiyeti onanırken delil olarak ses kayıtlarının değerlendirilmesi dikkat çekici bir unsur olarak öne çıkmıştır. Kararda sanığın banka çağrı merkezi ile yaptığı görüşmelere ait ses kayıtları ile sanığa ait olduğu tespit edilen diğer ses örnekleri karşılaştırılmış ve hem kriminal hem teknik bilirkişilerce yapılan analizler neticesinde bu ses örneklerinin sanığa ait olduğu yüksek derecede muhtemel şekilde belirlenmiştir. Ankara Kriminal Polis Laboratuvarı'nın uzmanlık raporu ve Radyo TV ve Foto Film Şube Müdürlüğü teknik bilirkişi raporu doğrultusunda konuşma aksanı, kelime telaffuzu, frekans özellikleri ve fonetik vurgular gibi akustik parametrelerdeki benzerlikler, ses tanıma yazılımı ile de desteklenmiş ve bu kapsamda ses verilerinin, failin kimliğinin belirlenmesinde önemli bir delil olduğu vurgulanmıştır. Bu karar, sesli iletişim verilerinin yalnızca dijital veri olarak değil aynı zamanda kişiyi tanımlayıcı bir delil niteliği taşıdığını açık biçimde ortaya koymaktadır. Özellikle ses tabanlı kimlik doğrulama ve delil niteliğinde ses incelemesinin, ses tabanlı siber saldırılarla mücadelede de hukuki anlamda yargı organlarınca dikkate alındığını göstermektedir. Bu duruma göre sesin ceza yargılamasında maddi gerçeğe ulaşma açısından ne denli güçlü bir araç haline geldiği anlaşılmaktadır. Tez kapsamında ele alınan ses temelli saldırıların ve özellikle Ses kayıtlarının teknik analiz yoluyla sanığın kimliğinin tespitine ve suçun sübutuna katkı sunduğu bu kararda, sesin hem bir iletişim aracı hem de yüksek delil değeri taşıyan bir unsur olduğu hali yargı kararına açıkça yansımıştır.

Yargıtay 11. Hukuk Dairesinin 2023/1184 E., 2024/4757 K. sayılı kararında, davacının banka hesabından haberi ve rızası dışında para transferi yapılmasına ilişkin açtığı alacak davasında, olayın sesli iletişim temelli dolandırıcılık yöntemi olan "voice phishing" (sesli kimlik avı) kapsamında gerçekleştiği açıkça ortaya konmuştur. Kararda davacının, kendisini banka görevlisi gibi tanıtan dolandırıcılar tarafından telefonla arandığı ve bu arama sırasında verilen yönlendirmelere inanarak banka işlemlerini gerçekleştirdiği, bu işlemler arasında döviz hesabının kapatılması, kredili mevduat hesabı açılması ve para transferleri bulunduğu tespit edilmiştir. Mahkemece yapılan değerlendirmelerde, işlemlerin bizzat davacının mobil bankacılık şifresi ile kendi cihazı üzerinden yapıldığı, dolayısıyla bankanın bilgi güvenliği açısından üzerine düşen teknik yükümlülükleri yerine getirdiği ancak davacının sesli yönlendirmelere aldanarak bu işlemleri gerçekleştirdiği vurgulanmıştır. Bu yönüyle karar, sesli iletişim yoluyla yapılan siber dolandırıcılık türlerinin ve özellikle ses tabanlı sosyal mühendislik saldırılarının oldukça etkili olabildiğini göstermekte ve bu saldırıların hukuki

sorumluluğun belirlenmesindeki rolünü ortaya koymaktadır. Bu tez kapsamında ele alınan "voice phishing" yani vishing saldırılarının somut bir yargı kararında bu kadar açık bir şekilde tanımlanması ve dolandırıcılığın sesli iletişim aracılığıyla gerçekleştirilmiş olması, bu saldırı türünün hem teknik hem de hukuki boyutlarının ciddiyetini ortaya koymaktadır. Ayrıca karar, sesin dijital bir kimlik unsuru olarak kötüye kullanımına ilişkin gerçek bir örnek teşkil etmekte ve sesin yalnızca kimlik doğrulamada değil, aynı zamanda bireylerin manipülasyonu ve maddi zarara uğratılmasında da etkili bir araç haline geldiğini göstermektedir. Bu çerçevede ses tabanlı dolandırıcılıkların artışı karşısında gerek teknik güvenlik önlemlerinin gerekse yasal düzenlemelerin daha güncel hale getirilmesinin zorunluluğu bu karar ışığında bir kez daha doğrulanmaktadır.

Yargıtay 10. Ceza Dairesinin 2022/1757 E., 2024/16786 K. sayılı kararında, uyuşturucu madde ticareti suçundan sanık hakkında verilen hükme yönelik temyiz başvurusu ele alınmıştır. Kararın sesle ilgili kısmı, suçun unsurlarının ve delil durumunun değerlendirildiği bölümde yer almıştır. Sanık müdafinin temyiz sebepleri arasında suçun unsurlarının oluşmadığı, mahkûmiyete yeterli delil bulunmadığı, güven alımına ilişkin tutanakların çelişkili olduğu ve ses kaydının sanığa ait olmadığı gibi iddialar bulunmuştur. Bu noktada ses kaydına ilişkin yapılan bilirkişi raporunda, kaydın sanığa ait olup olmadığı tartışılmakla birlikte dosyada yer alan fiziki takip tutanakları, teşhis tutanağı, ele geçen madde, güven alımı sonucu tutulan rapor ve gizli soruşturmacı tanık beyanları bir arada değerlendirilerek sanık müdafinin temyiz sebepleri yerinde görülmemiştir. Özellikle ses kaydına ilişkin yapılan incelemede, kayıttaki konuşmacının sanıkla aynı kişi olup olmadığına dair şüpheler olsa da dosya kapsamı ve mevcut deliller göz önüne alındığında hükümde hukuka aykırılık bulunmamıştır. Bu durumda Yargıtay, ses kaydının doğruluğu ve güvenilirliği konusunda ortaya çıkan şüphelere rağmen mevcut delillerin değerlendirilmesiyle sanığın suçlu olduğuna karar verilmiştir.

Yargıtay 12. Ceza Dairesinin 2012/32135 E., 2013/16483 K. sayılı kararında mahkeme, hakaret suçundan sanığı beraat ettirmiş ancak kişisel konuşmaların izinsiz kayda alınması suçundan sanığı mahkûm etmiştir. Sanık, katılanın avukatına hakaret ettiğini iddia edilen telefon konuşması için savunması yaparken hakaretin söz konusu olmadığını belirtmiştir. Mahkeme, yapılan yargılamada sanığın suçunu kanıtlayan yeterli delil olmadığına karar vererek beraat kararı vermiştir. Katılanın sanığa yönelik şüpheli ve soyut iddiaları reddedilmiştir. Sanığın katılanın bilgisi ve rızası olmadan telefon görüşmesini kaydedip bu

kaydı boşanma davasının tarafına vermesi nedeniyle kişisel konuşmaların izinsiz kayda alınması suçu işlendiği kabul edilmiştir. Ancak bu suçun kesin kanıtlarla desteklenmediği gerekçesiyle mahkeme, kaydedilen konuşmanın sanık tarafından yapıldığına dair yeterli ve kesin delil olmadığını belirtmiştir. Mahkeme, sanığın ses kaydını kaydetme ve dağıtma eyleminin hukuka aykırı olduğuna karar vererek sanık hakkında mahkûmiyet hükmü vermiştir. Ancak sanığın suçunu ispatlayan kanıtların yetersizliği nedeniyle şüpheden yararlanarak sanığa beraat kararı verilmiştir. Bu karar, sesli iletişimin ve kayıtlarının hukuki açıdan önemli bir delil unsuru olarak kabul edildiğini ancak aynı zamanda bu tür verilerin izinsiz kaydedilmesinin de suç teşkil edebileceğini ortaya koymaktadır. Ayrıca karar, delil yetersizliği nedeniyle beraat kararı verilmesi konusunda ses verilerinin hukuki anlamda hangi yollarla elde edildiğinin önemli olduğunu ve ne kadar dikkatle değerlendirilmesi gerektiğini de göstermektedir.

Yargıtay'ın bu gibi farklı kararlarında sesli iletişim ve ses kayıtlarının hukuki niteliği çeşitli açılardan ele alınmıştır. Bu bağlamda ses tabanlı saldırılarla ilgili hukuki süreçlerin ve delil değerlerinin doğru biçimde değerlendirilmesi büyük önem taşımaktadır. Zira ses kaydının yasal olmayan şekilde elde edilmesi, suçun açığa çıkmasını sağlasa da hukuka uygun bir delil sunulmadığında mahkemece değerlendirilmeyebilir.

Sonuç olarak ses verilerine yönelik siber saldırılar ve bu yolla gerçekleşen kişisel veri ihlalleri hem teknik bir güvenlik sorunu hem de karmaşık bir hukuki değerlendirme sürecini gerektiren ciddi bir dijital tehdit kategorisi haline gelmiştir. Özellikle voice spoofing, deepfake ses manipülasyonları, ultrasonik komut saldırıları ve akustik dinleme saldırıları gibi yeni nesil saldırı teknikleri, bireylerin biyometrik verileri arasında yer alan ses örüntülerini hedef alarak hem kimlik doğrulama sistemlerini aşmakta hem de kişisel mahremiyetin ihlaline yol açmaktadır. Bu tür saldırıların hem 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) hem de Türk Ceza Kanunu (TCK) kapsamında doğrudan ve açık biçimde düzenlenmemiş olması, mağdur haklarının korunması konusunda ve faillerin cezai sorumluluğunun belirlenmesinde uygulama açısından ciddi boşluklara neden olmaktadır.

Mevcut durumda KVKK madde 6 kapsamında "özel nitelikli kişisel veri" sayılan biyometrik veriler (örneğin ses örnekleri), ancak sınırlı durumlarda ve açık rıza ile işlenebilmektedir. Ses verilerinin kötü niyetli kimselerce izinsiz olarak toplanması, analiz edilmesi ve manipüle

edilmesi hukuken açıkça tanımlanmamış bir fiil olarak sıklıkla yorum farklılıklarına yol açmaktadır. Bu kapsamda sesin biyometrik bir kimlik doğrulama aracı olarak kullanılmasına rağmen sesli sistemleri hedef alan siber saldırıların açık bir suç tipi olarak TCK'de yer almaması, verilerin hukuka aykırı olarak ele geçirilmesi (TCK m. 136) ya da bilişim sistemine girme (TCK m. 243) gibi genel hükümlere başvurulmasına neden olmaktadır. Bu durum, sesli veri ihlallerine karşı özel norm ihtiyacını daha da görünür kılmaktadır.

Yargı içtihatları da bu boşluğu dolaylı biçimde ortaya koymaktadır. Özellikle Yargıtay 8. Ceza Dairesi'nin 2020/1419 E., 2022/122 K. ve Yargıtay 12. Ceza Dairesi'nin 2012/32135 E., 2013/16483 K. sayılı kararları, ses kayıtlarının delil niteliği ve kişisel verilerin ihlali bağlamında hukuki yorumların geniş bir yelpazeye yayıldığını göstermektedir. Bu kararlar, ses verisinin hem bir kimlik tespit aracı hem de bir iletişim aracı olarak kullanıldığı durumlarda delil değeri taşıyıp taşımadığına ilişkin ölçütlerin net olmadığını gözler önüne sermektedir. Örneğin adli süreçlerde sesin teknik analizle failin kimliğini ortaya koyan bir araç olarak kullanılması mümkün görülürken aynı sesin izinsiz olarak kayda alınması halinde temel hakların ihlali gündeme gelmektedir.

Buna karşın Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR), ses verilerini açık biçimde kişisel veri ve biyometrik veri olarak sınıflandırmakta ve bu verilerin işlenmesine yönelik açık, spesifik ve teknik koşullar öngörmektedir. Özellikle sesli dijital sistemlerle etkileşime giren bireylerin verilerinin hangi yollarla işlendiğine, saklandığına ve analiz edildiğine dair bilgi edinme hakları net biçimde tanımlanmıştır. Türkiye'nin de 2016 yılında yürürlüğe giren 6698 sayılı KVKK ile benzer bir uyum sürecine girmiş olmasına rağmen ses verisi gibi özel teknolojilere özgü tehditlere karşı düzenlemelerin detay seviyesi hala yetersizdir.

Sonuç itibariyle ses tabanlı ve diğer gelişmiş siber saldırı türlerine karşı etkin hukuki düzenlemeler, ulusal normlarla ve uluslararası hukuk ilkeleri çerçevesinde çok taraflı iş birlikleri yoluyla geliştirilebilecektir. Türkiye'nin uluslararası standartlara uyumlu olarak başta Budapeşte Siber Suçlar Sözleşmesi ve üyesi olduğu Avrupa Konseyi'nin kişisel veri koruma çerçevesi olmak üzere çok sayıda metni iç hukukuna entegre etmesi gereklidir. Buna göre TCK ve KVKK başta olmak üzere ilgili tüm mevzuatta ses tabanlı saldırı tekniklerinin açık biçimde tanımlandığı ve cezai sorumluluğun belirlendiği hükümlere yer verilmesi gerekmektedir. Ayrıca teknik bilirkişilik, dijital delil zinciri yönetimi, ses biyometrisi analizi

gibi uzmanlık gerektiren alanlara ilişkin adli alanlarda kapasitenin artırılması, hukuki caydırıcılık açısından tamamlayıcı bir unsur olacaktır. Hızla gelişen ve dönüşen dijital saldırı teknikleri karşısında bireylerin ve kurumların etkin biçimde bu saldırılara karşı korunabilmesi, mevzuatın teknolojiyle eş zamanlı olarak güncellenmesi sayesinde mümkün olabilecektir.

5. ARAŞTIRMA YÖNTEMİ

Bu çalışmada, ses kullanılarak gerçekleştirilen siber saldırı türlerini sistematik bir şekilde incelemek ve bu saldırıların yol açtığı veri ihlallerini kapsamlı olarak analiz edebilmek amacıyla sistematik derleme yöntemi kullanılmıştır. Sistematik derleme yöntemi, belirli bir araştırma sorusu çerçevesinde mevcut literatürde yer alan çalışmaların kapsamlı, şeffaf ve objektif kriterler doğrultusunda seçilmesi, analiz edilmesi ve sentezlenmesi esasına dayanmaktadır (Moher ve diğerleri, 2009). Sistematik derleme, önceden tanımlanmış bir araştırma sorusuna odaklanarak ilgili literatürün ön yargılardan arındırılmış ve tekrarlanabilir bir biçimde taranması, seçilmesi, değerlendirilmesi ve sentezlenmesini amaçlayan yapılandırılmış bir yöntemdir (Gough ve diğerleri 2017: 7, 13). Sistematik derlemeler, kapsamlı bir veri tabanı taraması yapılarak belirli dahil etme ve hariç tutma kriterlerine göre çalışma seçimi yapılması, seçilen çalışmaların metodolojik kalitesinin değerlendirilmesi ve sonuçların şeffaf şekilde raporlanması ilkelerine dayanır (Petticrew ve Roberts, 2006: 1, 26). Bu yönüyle sistematik derlemeler, karar vericiler ve araştırmacılar için mevcut bilgi birikiminin güvenilir bir özetini sunar. Ayrıca bu yaklaşım, literatürde mevcut olan bilgilerin organize edilmesini ve alandaki bilgi boşluklarının belirlenmesini de sağlamaktadır.

Sistematik derlemeler, özellikle yeni ortaya çıkan tehdit türlerinin ve hızlı teknolojik gelişmelerin etkisinin analiz edilmesinde önemli bir yöntem olarak görülmektedir (Higgins ve Green, 2011: 1, 12). Ses teknolojileri son yıllardaki hızlıca evrimleşmiş ve bu alanda gerçekleştirilen siber saldırılar çeşitlenmiştir. Bu nedenle bu çalışmada, mevcut literatürde yer alan konuyla ilgili çalışmaların yapılandırılmış bir yöntemle incelemesi ve ortak eğilimlerin ortaya koyulması amacıyla bu araştırma yöntemi tercih edilmiştir.

Çalışmada izlenen süreç, PRISMA 2020 yönergeleri (Page ve diğerleri, 2021) dikkate alınarak yapılandırılmıştır. Literatür taraması sırasında belirli anahtar kelimeler ve belirli veri tabanları kullanılarak kapsamlı bir tarama gerçekleştirilmiştir. Taranan çalışmaların seçim süreci, şeffaflık ve tekrarlanabilirlik ilkelerine bağlı kalınarak içerik değerlendirmesi de yapılarak yürütülmüştür. Böylelikle çalışmanın metodolojik güvenilirliği artırılmıştır.

Veri toplama aşamasında yalnızca açık erişimli akademik yayınlar ve hakemli makaleler dikkate alınmış. Ayrıca, çalışmalara dahil edilecek literatürün yayımlandığı tarih aralığı

olarak 2013-2024 yılları belirlenmiş ve bu tarih aralığındaki teknolojik gelişmelere odaklanılmıştır. Bu tarihsel sınırlama, ses teknolojilerinin özellikle yapay zekâ destekli uygulamalarla daha yoğun kullanıldığı dönemi kapsaması nedeniyle tercih edilmiştir.

Elde edilen veriler, nitel veri analizi teknikleri kullanılarak tematik kategorilere ayrılmış ve sesle gerçekleştirilen saldırı türleri, kullanılan teknikler, hedef sistemler ve saldırıların hukuki sonuçları gibi ana temalar altında sınıflandırılmıştır. Meta-sentez, nitel araştırmalarda elde edilen bulguların yorumlayıcı ve bütünleştirici bir yaklaşımla analiz edilmesini amaçlayan sistematik ancak esnek bir yöntemdir. Bu yöntem, farklı nitel çalışmaların sonuçlarını karşılaştırarak yeni anlamlar üretir ve ortak temalar etrafında kavramsal bir bütünlük oluşturur (Noblit ve Hare, 1988). Meta-sentez, özellikle bireylerin deneyimlerini anlamaya yönelik çalışmalarda kullanılır ve nicel meta-analizden farklı olarak verileri sayısal olarak değil tematik ve yorumsal olarak işler (Sandelowski ve Barroso, 2007: 1, 311). Böylece bir konuya ilişkin nitel veriler arasında derinlemesine bir bağlantı kurularak, teorik yapıların geliştirilmesine katkı sağlanır. Bu çalışmada meta-sentez yöntemi kullanılarak yapılan analiz süreci, çalışmanın bulgularının daha derinlemesine yorumlanmasına ve mevcut literatürdeki eğilimlerin belirginleştirilmesine olanak sağlamıştır (Noblit ve Hare, 1988).

Bu yöntemsel yaklaşım sayesinde ses kullanılarak yapılan siber saldırılar konusunda disiplinler arası bir perspektif sunulmuş hem teknik hem de hukuki ve etik boyutlar dengeli bir şekilde ele alınmıştır. Çalışmanın sonuçlarının ses teknolojileri alanındaki güvenlik önlemlerinin geliştirilmesi ve gelecekteki araştırmalara yön vermesi bakımından katkı sağlayacağı öngörülmektedir. Çizelge 5.1'de bu çalışmada izlenen aşamaları gösteren işlem basamaklarına yer verilmiştir:

Çizelge 5.1. Ses kullanılarak yapılan siber saldırıların sistematik derleme ve meta sentez yöntemiyle incelenmesi sürecinde izlenen aşamaları gösteren işlem basamakları

1- Araştırma Sorularının Belirlenmesi

Çalışmanın temel amacı doğrultusunda, ses kullanılarak yapılan siber saldırıların türleri, etkileri ve veri ihlalleri üzerindeki sonuçlarını araştırmaya yönelik ana araştırma sorusu ve alt araştırma soruları belirlenmiştir.

2- Literatür Taramasının Yapılması

"Voice", "sound", "audio" ve "cyber attacks" gibi anahtar kelimeler ve bunların farklı kombinasyonları kullanılarak Scopus, ScienceDirect, IEEE Xplore ve Web of Science veri tabanlarında kapsamlı bir literatür taraması gerçekleştirilmiştir. Ayrıca TRDizin ve YÖK Tez Merkezi gibi ulusal kaynaklardan da tarama yapılmış, ancak yeterli sonuç elde edilememiştir. Yapılan taramalar sonucunda toplam 102 akademik çalışmaya ulaşılmıştır.

3- Dahil Etme ve Hariç Tutma Kriterlerinin Belirlenmesi

Çalışmaya dahil edilecek çalışmalar için belirli kriterler oluşturulmuştur. Buna göre, 2013-2024 yılları arasında yayımlanmış, açık erişimli ve tam metnine ulaşılabilen, ses kullanılarak yapılan siber saldırıları doğrudan ele alan, yöntem ve bulguları açıkça belirtilmiş akademik yayınlar çalışmaya dahil edilmiştir. Ses teknolojileri dışındaki genel siber güvenlik çalışmaları, teknik donanım geliştirme odaklı mühendislik çalışmaları ve tam metnine ulaşılamayan yayınlar kapsam dışı bırakılmıştır.

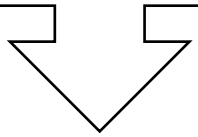
4- Dahil Etme ve Hariç Tutma Kriterlerinin Uygulanması

Elde edilen 102 çalışmadan yinelenen kayıtlar çıkarıldıktan sonra başlık ve özet incelemesi yapılmıştır. Bu aşamada konu dışı kalan veya metodolojik olarak yetersiz bulunan çalışmalar elenmiştir. Tam metin incelenmesi sonrasında dahil edilme kriterlerini karşılamayan 43 çalışma kapsam dışı bırakılmış ve toplamda 59 çalışma sistematik derlemeye dahil edilmiştir.

Çizelge 5.1. (devamı)

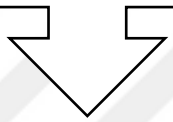
5- Dahil Edilen Çalışmaların Organize Edilmesi

Sistematik derlemeye dahil edilen çalışmalar, incelenen saldırı türlerine, kullanılan yöntemlere ve hedef sistemlere göre gruplandırılmıştır. Bu sınıflandırmada sesli kimlik avı saldırıları, sesli komut manipülasyonu, deepfake ses saldırıları, ultrasonik saldırılar ve steganografik ses saldırıları gibi temalar esas alınmıştır.



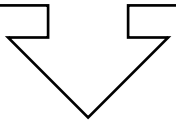
6- Verilerin Toplanması

Dahil edilen çalışmaların yöntem, bulgu ve sonuç bölümlerinden elde edilen veriler, araştırmanın amaçlarına uygun başlıklar altında sistematik bir şekilde toplanmıştır. Toplanan veriler hem nitel içerik analizi için hem de tematik sınıflandırma için kullanılmıştır.



7- Verilerin Analizi

Toplanan veriler üzerinde içerik analizi yöntemi uygulanarak ses temelli saldırıların türleri, teknik özellikleri, hedefleri ve yarattığı güvenlik açıkları ortaya konulmuştur. Elde edilen bulgular tematik kodlamalar yardımıyla sınıflandırılmış ve literatürdeki eğilimler belirlenmiştir.



8- Bulguların Değerlendirilmesi ve Yorumlanması

Son aşamada, analiz edilen veriler karşılaştırmalı olarak değerlendirilmiş, ses kullanılarak yapılan siber saldırıların günümüzdeki ve gelecekteki etkileri tartışılmış, elde edilen bulgular doğrultusunda sonuçlar ve öneriler geliştirilmiştir.

5.1. Veri Toplama Süreci ve Seçim Kriterleri

Bu çalışmada veri toplama süreci, belirlenen araştırma sorularına en uygun literatürün sistematik olarak seçilmesi amacıyla yapılandırılmıştır. Literatür taraması sürecinde ulusal ve uluslararası akademik veri tabanları taranmış, belirli anahtar kelimeler ve kombinasyonları kullanılarak ilgili çalışmalar tespit edilmiştir.

Başlangıçta TRDizin ve YÖK Ulusal Tez Merkezi veri tabanlarında "ses" + "siber saldırı" anahtar kelimeleriyle yapılan taramalarda kapsamlı ve yeterli sayıda akademik çalışmaya ulaşılamamıştır. Bu durum üzerine literatür taraması genişletilerek uluslararası veri tabanlarında tarama yapılmıştır. Scopus, ScienceDirect, IEEE Xplore ve Web of Science veri tabanlarında 2013-2024 yılları arasını kapsayan bir arama gerçekleştirilmiştir. Bu aramalarda “voice” + “cyber attacks”, “audio” + “cyber attacks” ve “sound” + “cyber attacks” kelime grupları aratılmış; daha sonra kapsam oldukça geniş olduğundan bu kapsamı saldırı yöntemleri ile sınırlı olacak şekilde daraltmak amacıyla “voice” + “cyber attacks” + “method”, “audio” + “cyber attacks” + “method” ve “sound” + “cyber attacks” + “method” gibi anahtar kelime kombinasyonları kullanılmıştır. Ayrıca sadece başlık, özet ve yazar anahtar kelimeleri alanlarında arama yapılması koşulu getirilmiştir. Bu yöntem, sistematik derlemelerde önerilen hedefe odaklı literatür bulma stratejilerine uygundur (Gough ve diğerleri, 2017: 7, 13).

Toplamda 102 akademik çalışmaya ulaşılmıştır. İlk aşamada yinelenen kayıtlar (duplicate records) tespit edilerek 19 tanesi çıkarılmış, ardından başlık ve özet incelemesi yapılmıştır. Konu dışı kalan, çalışma kapsamına girmeyen veya metodolojik açıdan yetersiz bulunan 15 çalışma da bir sonraki aşamada elenmiştir. Başlık ve özet incelemesi sonrasında uygun görülen çalışmaların tam metinleri incelenmiş; tam metne ulaşılamayan veya içerik olarak belirlenen kapsama uymayan 9 çalışma değerlendirme dışı bırakılmıştır.

Çalışmaya dahil edilecek yayınları belirlerken şu dahil etme kriterleri uygulanmıştır:

- 2013-2024 yılları arasında yayımlanmış olması,
- İngilizce veya Türkçe dillerinde yazılmış olması,
- Açık erişimli veya kurumsal erişimle tam metnine ulaşılabilen olması,
- Ses kullanılarak yapılan siber saldırıları doğrudan konu edinmesi,

- Yöntem, bulgu ve sonuç bölümleri açıkça sunulmuş olması.

Hariç tutma kriterleri ise şunlardır:

- Sesle ilgili olmayan genel siber güvenlik çalışmaları,
- Yalnızca teknik donanım geliştirme odaklı mühendislik çalışmaları (örneğin sadece mikrofon tasarımı üzerine olanlar),
- Tam metnine ulaşılamayan yayınlar.

Sonuç olarak tüm tarama ve değerlendirme aşamaları sonrasında 59 akademik çalışma sistematik derlemeye dahil edilmiştir. Literatür seçim süreci PRISMA yönergeleri doğrultusunda da yapılandırılmıştır.

Bu aşamada çalışmalarda ele alınan ses tabanlı saldırı türleri, kullanılan saldırı yöntemleri, hedef sistemler ve hukuki sonuçlar temalarına göre kategorilendirme yapılmıştır. Böylece elde edilen verilerin tematik analizi daha sistematik bir şekilde gerçekleştirilmiştir (Thomas ve Harden, 2008).

5.2. Literatür Bulguları ve Analizler

Yapılan sistematik derleme sonucunda seçilen 59 akademik çalışma, ses kullanılarak yapılan siber saldırı türleri, kullanılan yöntemler, hedef sistemler ve saldırıların hukuki boyutları açısından detaylı olarak analiz edilmiştir. Literatür analizi, nitel veri analizi teknikleri kullanılarak gerçekleştirilmiş ve elde edilen bulgular tematik kategoriler altında sınıflandırılmıştır.

Çalışmaların incelenmesi sonucunda ses kullanılarak yapılan siber saldırıların genellikle şu başlıca kategoriler altında toplandığı görülmüştür:

- Sesli kimlik avı (vishing) ve sosyal mühendislik tabanlı saldırılar: Telefon dolandırıcılığı, sahte kimlik oluşturma ve ses manipülasyonu gibi yöntemler aracılığıyla kişisel bilgilerin ele geçirilmesi (Naqvi ve diğerleri, 2023).
- Sesli komut manipülasyonu: Akıllı asistanlara yönelik sahte sesli komut gönderimi ile cihazların yetkisiz kontrol edilmesi (Yan ve diğerleri, 2020).

- Deepfake tabanlı ses taklidi: Yapay zekâ ve makine öğrenimi teknikleri kullanılarak sahte ses örnekleri oluşturulması ve kimlik doğrulama sistemlerinin kandırılması (Firc ve diğerleri, 2023).
- Ultrasonik ses dalgalarıyla yapılan saldırılar: İnsan kulağının algılayamayacağı frekanstaki ses dalgaları ile cihazların kontrol edilmesi (Zhang ve diğerleri, 2017).
- Steganografi ve kriptografi ile ses dosyaları üzerinden yapılan bilgi gizleme: Ses dosyaları içine gizli veri yerleştirilerek veri sızdırılması (Phipps ve diğerleri, 2022).

Bu tematik ayrım çerçevesinde her bir saldırı türü kullanılan teknik özellikler, hedef alınan sistemler ve potansiyel zararları açısından analiz edilmiştir. Bulgular, ses teknolojilerinin gelişmesiyle birlikte ses tabanlı saldırıların çeşitlendiğini ve hala gelişmekte olduğunu göstermektedir. Özellikle yapay zekâ ve derin öğrenme tabanlı yöntemlerin saldırıların etkinliğini artırdığı görülmektedir (Desetty ve diğerleri, 2020). Bununla birlikte saldırı türlerinin tespit edilme düzeyleri ve müdahaleyi gerektiren öncelik sıraları birbirinden oldukça farklıdır. Örneğin deepfake tabanlı ses saldırıları genellikle sosyal ve kamusal alanda etki yaratma potansiyeline sahipken ultrasonik saldırılar doğrudan donanıma zarar vererek sistemin fiziksel işleyişini tehdit eder. Literatür bulgularına göre bu tür saldırıların erken aşamada tespitinin zor olması, savunma mekanizmalarının hem yazılım hem de donanım düzeyinde yeniden yapılandırılmasını zorunlu kılmaktadır.

Aynı zamanda ses tabanlı saldırı türlerinin arkasında yer alan kimselerin profilleri de değişkenlik göstermektedir. Vishing gibi dolandırıcılık temelli saldırılar çoğunlukla bireysel veya küçük çaplı suç odaklı kişiler tarafından gerçekleştirilirken, ultrasonik veya deepfake tabanlı saldırılar teknik bilgi ve yeterlilik kapasitesi yüksek, organize yapıların çok çeşitli amaçlarla yürüttüğü saldırılardır. Bu çeşitlilik tehditlerin analizinde yalnızca saldırı tipine değil, saldırgan profiline göre de değerlendirme yapılmasını gerektirmektedir.

Ayrıca yapılan analizlerde, ses kullanılarak gerçekleştirilen saldırıların çoğunlukla aşağıdaki hedefleri amaçladığı belirlenmiştir:

- Kimlik doğrulama sistemlerini aşmak,
- Kritik veri ve finansal bilgilere erişim sağlamak,
- Akıllı cihazlar ve IoT sistemleri üzerinde yetkisiz kontrol kurmak,
- Kamuoyunda yanlış bilgilendirme veya itibar zedelemesi yaratmak.

Literatür taramasında, ses tabanlı saldırıların özellikle biyometrik kimlik doğrulama sistemleri (örneğin ses tanıma sistemleri) açısından ciddi güvenlik açıkları oluşturduğu vurgulanmıştır (Zhou ve diğerleri, 2022).

Tematik analiz sonucunda ayrıca sesle yapılan siber saldırıların hukuki ve etik boyutlarının literatürde sınırlı ölçüde ele alındığı, özellikle Türkiye bağlamında kapsamlı çalışmaların eksik olduğu tespit edilmiştir. Bu durum, bu çalışmanın önemini bir kez daha ortaya koymakta ve herkes tarafından anlaşılabilecek bir dille oluşturulduğundan gelecekte yapılacak çeşitli alanlardaki çalışmalara ilişkin bir temel teşkil edebileceğini göstermektedir.

Bu çerçevede, yapılan sistematik derleme ve meta-sentez sonucunda elde edilen bulgular, ses kullanılarak yapılan siber saldırıların yalnızca hukuki veya etik değil, aynı zamanda teknik boyutlarını da kapsamlı biçimde ortaya koymaktadır. İncelenen çalışmalarda saldırı türlerinin gerçekleştirilme biçimleri, kullanılan teknolojik yöntemler, güvenlik açıklarının niteliği, saldırıların hedeflediği sistemler ve literatürde önerilen çözüm yolları detaylı olarak değerlendirilmiştir. Aşağıda bu unsurlar temelinde elde edilen bulgular bütüncül bir yaklaşımla sunulmuştur:

Literatür incelendiğinde ses kullanılarak yapılan siber saldırıların gerçekleştirilme yöntemlerinin doğrudan sesli komut ile manipülasyon, ultrasonik ses dalgalarıyla sesli komutları iletme, deepfake teknolojileri ile ses sentezi, sesli kimlik avı ile kişisel veri elde etme ve ses dosyaları içine gömülü veri gizleme gibi teknik temellere dayandığı görülmektedir. Saldırıların uygulanmasında sıklıkla kullanılan yöntemler arasında yapay zekâ tabanlı ses sistemleri, yüksek frekanslı akustik dalga yollayıcılar (örneğin piezoelektrik dönüştürücüler), yazılım tabanlı olan sahte ses komutu üreticileri ve steganografi yazılımları öne çıkmaktadır (Firc ve diğerleri, 2023; Zhang ve diğerleri, 2017). Ayrıca ses sinyallerinin sadece bir iletim aracı olmadığı ve aynı zamanda saldırıların tespiti için de bir analiz nesnesi haline geldiği çalışmalara rastlanmaktadır. Nataraj ve diğerleri (2021) kötü amaçlı yazılım tespiti için ses, görüntü ve statik özellikleri bir arada kullanan bir model geliştirmişlerdir. Bu model ile yazılım dosyalarını ses sinyalleri olarak temsil ederek sınıflandırma başarısını artırmayı başarmışlardır. Bu model sayesinde ses tabanlı saldırılar doğrudan zararlı yazılım taşıyıcısı haline getirilebilirken aynı zamanda yeni analiz araçlarına yönelik yenilikçi bir yaklaşım sağlanmıştır.

Analiz edilen çalışmalarda saldırıların çoğunlukla ses ile çalışan sistemlerde bulunan doğrulama eksiklikleri, cihazlar arası kimlik kontrolünün zayıf olması, MEMS mikrofonların dış müdahaleye açık yapısı ve şifrelenmemiş ses iletimi gibi güvenlik açıklarından yararlanılarak gerçekleştirildiği belirlenmiştir. Özellikle sesli komut sistemlerinde erişim kontrol mekanizmalarının yetersizliği, saldırıların başarılı olarak gerçekleştirilme oranını arttıran temel faktörlerdendir (Yan ve diğerleri, 2020). En sık hedef alınan sistemler arasında sesli asistanlar, akıllı ev sistemleri, akıllı telefonlar ve biyometrik ses doğrulama sistemleri yer almaktadır. Ayrıca sesli komut sistemleri False Data Injection (FDI) gibi karmaşık saldırı türlerine karşı da savunmasız olabilir (Aluko ve diğerleri, 2022). Bu nedenle ses tabanlı sistemlerdeki veri akışlarının davranışsal modeller ile izlenmesi ve mikro ağlarda kullanılan durum tahmin yöntemlerinin geliştirilmesi, olası saldırıların erken tespiti açısından oldukça önemli bir nokta olarak görülmektedir. Aluko ve diğerlerinin (2022) çalışmasında değinilen bu yöndeki tespit sistemleri, özellikle gerçek zamanlı ses manipülasyonlarına karşı etkin savunma mekanizmaları sunmaktadır.

İncelenen literatürde ses kullanılarak yapılan siber saldırılara karşı önerilen başlıca önlemler çok faktörlü kimlik doğrulama sistemlerinin kullanılması, sesli komut sistemlerine yönelik erişimlerin kontrol edilmesi için çeşitli kontrol protokollerinin geliştirilmesi, sahte olarak üretilen ya da taklit edilen seslerin tespiti için yapay zekâ destekli analiz algoritmalarının kullanılması ve özellikle deepfake içeriğin tespitine yönelik adli bilişim araçlarının yaygınlaştırılmasıdır (Zhou ve diğerleri, 2022). Ayrıca ultrasonik ses dalgalarıyla gerçekleştirilen saldırılara karşı da fiziksel koruma önlemleri (örneğin akustik izolasyon, mikrofon kalkanları), sinyalleri şifreleme ve sensör füzyonu gibi önemlerin uygulanması önerilmektedir.

Buna ek olarak son yıllarda sesli iletişim içeriklerinin otomatik olarak analiz edilmesine yönelik geliştirilen sistemlerin de siber saldırılara karşı yeni savunma olanakları sunduğu görülmektedir. Monshizadeh ve diğerleri (2018) tarafından önerilen Lawful Interception as a Service (LiaaS) platformu sesli ve görüntülü iletişimlerin otomatik analizini, içeriklerdeki önemli bilgilerin çıkarılmasını ve bu bilgilerin kullanılabilir hale getirilmesini mümkün kılmaktadır. Bu yapı, büyük veri ortamlarında yasal olan dinleme süreçlerinin daha hızlı ve etkili bir şekilde yürütülmesini sağlamakta ve aynı zamanda sesli iletişimin muhtemel tehditlerinin erken tespiti açısından önemli bir gelişme sunmaktadır. Bu sistemin makine

öğrenmesiyle desteklenmesi, sahte ve sentetik ses üretimi gibi modern saldırı yöntemlerinin daha güvenilir biçimde saptanmasına da katkı sağlamaktadır.

Karşılaşılan bulgular ses tabanlı saldırıların kişisel veri sızdırma, sistem kontrollerini ele geçirme, finansal kayıplara yol açma ve hatta önemli altyapıların işleyişini bozma gibi sonuçlara yol açabildiğini göstermektedir. Özellikle sesli komutlar üzerinden bankacılık uygulamaları veya akıllı ev sistemlerinin kontrol edilmesi durumlarında ciddi maddi zararlar ortaya çıkmaktadır. Ayrıca deepfake ile gerçekleştirilen saldırıların bireylerin ve kurumların kişisel, kurumsal, siyasi, sosyal itibarlarına ve güvenilirliğine zarar verdiği çeşitli vakalarda görülmüştür (Desetty ve diğerleri, 2020). Bu tür saldırıların tespiti için Campi ve diğerleri (2021), ses sinyallerini analiz etmeye yönelik olarak Empirical Mode Decomposition (EMD) ve Mel-Frequency Cepstral Coefficients (MFCC) yöntemlerini birleştiren yeni bir model geliştirmiştir. Söz konusu yaklaşım, geleneksel olan doğrusal ve durağan ses işleme yöntemlerinin ötesine geçerek sahte ses örneklerini daha yüksek doğruluk oranıyla tespit edebilmekte ve deepfake tabanlı saldırılara karşı sesli biyometrik sistemlerin güvenliğine katkıda bulunmaktadır.

Ayrıca IoT sistemlerinin sadece akıllı evlerde değil; sağlık hizmetleri, endüstriyel kontrol sistemleri ve tarımsal makine sistemleri gibi çok çeşitli alanlarda kullanıldığı dikkate alındığında bu sistemlerin ses tabanlı saldırılara etkisinin daha geniş bir yelpazeye yayıldığı görülmektedir. Clinton ve Hoque (2024) tarafından geliştirilen MU-IoT veri seti, IoT ağlarının güvenlik analizleri için önemli bir kaynak olarak öne çıkmaktadır. Bu veri seti özellikle IoT sistemlerinde kullanılan uygulama katmanı protokollerine odaklanarak ağ trafiğinin detaylı bir şekilde kaydedilmesini sağlar. Teknik olarak MU-IoT veri seti, yaygın IoT uygulama protokollerinin kullanıldığı trafik örneklerini barındırmaktadır. Bu protokoller, veri iletiminde kolaylık ve düşük gecikme oranı sağlamak amacıyla tasarlanmıştır, IoT cihazlarının enerji ve bant genişliği kısıtlamaları nedeniyle tercih edilirler. Söz konusu veri setinde, protokol seviyesinde paket yakalama teknikleri kullanılarak paketlerin başlık bilgileri, içerikleri ve zaman damgaları gibi detaylar ayrıntılı biçimde kaydedilmektedir. Bu şekilde gerçek zamanlı saldırı tespiti, anormal durum tespiti ve trafik analizi gibi uygulamalar yapılmaktadır. Böylelikle çeşitli güvenlik analizleri yapılarak IoT ağlarının açıkları tespit edilmekte ve farklı savunma mekanizmaları geliştirmek için faydalanılacak teknik çalışmaların temeli oluşmaktadır.

Özellikle literatürde ses tabanlı saldırılar ve bunlara karşı alınabilecek savunma yöntemleri üzerine yapılan araştırmalar, bu alandaki güvenlik yaklaşımlarının çeşitliliğine ve etkinliğine ışık tutmaktadır. İncelenen çalışmalarda saldırı türlerinin gerçekleştirilme biçimleri, kullanılan teknolojik yöntemler, güvenlik açıklarının niteliği, saldırıların hedeflediği sistemler ve literatürde önerilen çözüm yolları detaylı olarak değerlendirilmiştir. Çizelge 5.2'de literatürdeki bulguları özetleyen ve ses tabanlı saldırılar ile bunlara karşı geliştirilen savunma teknikleri karşılaştırılmıştır:

Çizelge 5.2. Literatürde yer alan ses tabanlı saldırılar ve savunma yöntemleri

Saldırı Türü	**Hedef Sistem**	**Kullanılan Yöntem**	**Önerilen Savunma Yaklaşımları**
Vishing (Sesli Kimlik Avı)	Bankacılık sistemleri, bireysel kullanıcılar	Sosyal mühendislik, telefonla dolandırıcılık	Farkındalık eğitimleri, kimlik doğrulama sorularının çeşitlendirilmesi, çağrı analiz sistemleri (Naqvi ve diğerleri, 2023)
Sesli Komut Manipülasyonu	Akıllı asistanlar, akıllı ev sistemleri	Sahte komut ile cihaz kontrolü, ses klonlama	Çok faktörlü kimlik doğrulama, erişim kontrol protokolleri, ses doğrulama sistemleri (Yan ve diğerleri, 2020)
Sesli Deepfake Tabanlı Saldırılar	Biyometrik ses tanıma sistemleri, çağrı merkezleri	Sentetik ses üretimi, yapay zekâ tabanlı ses klonlama	MFCC ve EMD tabanlı analiz, yapay zekâ destekli sınıflandırıcılar, sahte ses tespit sistemleri (Campi ve diğerleri, 2021)
Ultrasonik Ses Dalgalarıyla Yapılan Saldırılar	MEMS mikrofon kullanan cihazlar, akıllı telefonlar	İnsan kulağının algılayamadığı frekansta komut iletimi (DolphinAttack, SurfingAttack vb.)	Mikrofon filtreleme, akustik izolasyon, mikrofon kalkanları, sensör füzyonu (Zhang ve diğerleri, 2017; Roy ve diğerleri, 2018)
Steganografi ile Veri Gizleme	Ses dosyası paylaşımı yapılan sistemler	Ses dosyalarına veri gömme, şifreleme yoluyla gizli iletişim	Steganaliz araçları, ses sinyali analiz sistemleri, içerik filtreleme (Phipps ve diğerleri, 2022)
FDI (False Data Injection) Saldırıları	IoT cihazları, sesle çalışan mikro ağlar	Komutlar üzerinden tehlikeli veriler aktarma	Durum tahmin algoritmaları, davranışsal modelleme, gerçek zamanlı anomali tespiti (Aluko ve diğerleri, 2022)
Sesle İletilen Kötü Amaçlı Yazılım	Güvenlik yazılımları, ses sinyali üzerinden iletişim	İkili dosyaların ses formatına çevrilerek analiz edilmesi	Statik analiz ve ses sinyali sınıflandırması, çoklu özellik füzyonu (Nataraj ve diğerleri, 2021)

Literatürde yer alan sınırlı sayıdaki çalışmada sesle yapılan siber saldırıların yalnızca teknik değil, aynı zamanda hukuki boyutları da analiz edilmiştir. Özellikle biyometrik verilerin hukuken "özel nitelikli kişisel veri" olarak değerlendirilmesi gerektiği vurgulanmakta, bu tür saldırıların veri ihlali kapsamına girdiği ve cezai sorumluluk doğurabileceği

belirtilmektedir. Ayrıca ses teknolojilerinin gündelik yaşamla giderek daha fazla bütünleşmesi, bu saldırıların bireysel mahremiyet üzerindeki potansiyel etkisini artırmakta ve kamusal boyutta farkındalık yaratılması ihtiyacını gündeme getirmektedir.

Ayrıca ulaşılan çalışmalarda, ses kullanılarak gerçekleştirilen siber saldırıların bölgesel dağılım açısından farklı eğilimler gösterdiği dikkat çekmektedir. Gelişmiş dijital altyapıya ve yaygın yapay zekâ teknolojisine sahip ülkelerde bu tür saldırıların daha fazla raporlandığı ve teknik açıdan daha gelişmiş biçimlerde gerçekleştirildiği görülmektedir. 2025 IBM X-Force Threat Intelligence raporuna göre Asya-Pasifik bölgesi, 2024 yılında en yüksek siber saldırı oranlarına ulaşmış ve toplam saldırıların %34'ü bu bölgede gerçekleşmiştir. Özellikle Çin, Güney Kore ve Endonezya gibi ülkeler bölgedeki siber saldırıların merkezinde yer almakta olup saldırıların büyük çoğunluğu özellikle endüstriyel alandaki kontrol sistemlerini ve kamu altyapılarını hedef almıştır (IBM, 2025). Bu durum bölgenin küresel tedarik zincirlerindeki önemli rolü ve bölgedeki teknolojik gelişmelerin artış hızıyla ilişkilendirilebilir. Ayrıca saldırganların yapay zekâ teknolojilerini kullanarak kimlik avı ve sahte web siteleri aracılığıyla gerçekleştirdikleri saldırılar da bölgede kayda değer bir artış göstermiştir. Bu tür eğilimler, bölgenin siber güvenlik altyapısındaki sorunları ve saldırganların yeni teknolojilere yönelik olarak geliştirdikleri saldırı tekniklerini ortaya koymakta olup yerel önlemlerin güçlendirilmesini ve uluslararası iş birliği yapılmasını zorunlu kılmaktadır.

Sesli kimlik avı yani vishing saldırıları ise özellikle Amerika Birleşik Devletleri ve Hindistan gibi ülkelerde yaygın olarak raporlanmıştır. Bu saldırılar genellikle finansal erişim veya kişisel bilgilerin ele geçirilmesi amacıyla gerçekleştirilmekte olup ABD'de daha çok banka ve finans uygulamaları hedeflenirken Hindistan'da sosyal medya hesapları ve iletişim bilgilerinin hedeflendiği görülmektedir. Çin ve Güney Kore kaynaklı çalışmalarda özellikle ultrasonik saldırılar ve yapay zekâ destekli ses manipülasyonları gibi ileri düzey tekniklerin ön planda olduğu görülmektedir (Zhang ve diğerleri, 2017; Bilika ve diğerleri, 2023). Avrupa merkezli akademik yayınlarda ise daha çok ses teknolojilerinin etik ve hukuki yönlerine odaklanıldığı tespit edilmiştir.

Türkiye'de ise ses kullanılarak yapılan siber saldırılarla ilgili literatür henüz sınırlı düzeydedir. Mevcut çalışmalarda ağırlıklı olarak vishing ve deepfake gibi saldırı türleri tanımsal düzeyde ele alınmış ancak diğer saldırı türlerine ve ses teknolojilerine ilişkin

çalışmalar ile analizlerin büyük ölçüde eksik kaldığı görülmüştür. Ayrıca Türkiye kaynaklı çalışmalarda örnek olay (vaka) analizi ve karşılaştırmalı araştırmalara yeterince yer verilmediği de dikkat çekmektedir. Türkiye özelinde ses tabanlı siber saldırıların henüz ele alınmamış olması yalnızca akademik araştırma eksikliği ile açıklanamaz. Kurumların örnek olay paylaşımı, saldırı raporlaması ve teknik strateji geliştirme konularında sistematik bir altyapıdan yoksun oluşu da görülmüştür. Bu durum Türkiye'de ses kullanılarak yapılan siber saldırıların yalnızca teknik değil, aynı zamanda kurumsal ve toplumsal düzeyde ele alınması gerektiğini ve bu alanda disiplinler arası yeni çalışmalara duyulan ihtiyacı açıkça ortaya koymaktadır.

Bu bölümde ses kullanılarak yapılan siber saldırıların sistematik bir derleme ve meta sentez yöntemiyle incelenmesi süreci ayrıntılı şekilde açıklanmıştır. Araştırma yöntemi sürecinde ulaşılan bulgular, çalışmanın temel amaçları doğrultusunda değerlendirilerek sistematik bir bütünlük sağlanmıştır. Bundan sonraki bölümde çalışmanın sonuçları ile önerilere yer verilecektir.

6. SONUÇ VE ÖNERİLER

Bu tez çalışmasında ses kullanılarak yapılan siber saldırıların türleri, yöntemleri, hedef sistemler üzerindeki etkileri ve bu saldırıların yol açtığı veri ihlalleri sistematik bir biçimde ele alınmıştır. Literatür taraması çerçevesinde gerçekleştirilen incelemeler sonucunda ses teknolojilerinin yaygınlaşmasıyla birlikte ses tabanlı sistemlerin çeşitli saldırı tekniklerine açık hale geldiği tespit edilmiştir. Sesle çalışan sistemlerin özellikle kimlik doğrulama, komut kontrolü ve bilgi aktarımı alanlarında kullanılmaya başlanması saldırganlar için yeni fırsatlar yaratmış ve bu sistemleri hedef alan saldırı türlerinin hem sayısal hem de teknik açıdan çeşitlenmesine neden olmuştur.

Çalışmada ses kullanılarak gerçekleştirilen siber saldırı türleri sesli kimlik avı (vishing), sesli komut manipülasyonu, deepfake teknolojileriyle yapılan ses taklitleri, ultrasonik ses dalgaları kullanılarak yapılan saldırılar ve steganografik yöntemlerle gerçekleştirilen saldırılar olmak üzere kapsamlı bir biçimde sınıflandırılmıştır. Analizler göstermektedir ki bu saldırı türleri bireylerin kimlik bilgilerinin çalınması, finansal dolandırıcılık yapılması, kurumsal sistemlere izinsiz erişim sağlanması, önemli kurumsal altyapıların manipüle edilmesi ve kamuoyunun yanıltılması gibi geniş bir tehdit yelpazesi oluşturmaktadır.

Elde edilen bulgular sesle yapılan siber saldırıların kişisel verilerin gizliliğini ciddi şekilde tehdit ettiğini, bireylerin ve kurumların maddi ve manevi zarar görme riskini artırdığını ortaya koymuştur. Özellikle sesli komut sistemlerinde meydana gelen güvenlik açıkları, hassas kişisel ve kurumsal verilerin ifşası, sistem kontrollerinin kötü niyetli kişilerce ele geçirilmesi ve veri bütünlüğünün bozulması gibi tehditler geri dönülemez sonuçlara yol açabilmektedir. Bu durum, ses teknolojilerinin güvenlik açısından da güncel olarak yeniden değerlendirilmesi gerekliliğini ortaya koymaktadır.

Çalışmanın literatür taraması aşamasında, Türkiye'de sesle yapılan siber saldırılar konusunda yapılan akademik çalışmaların sınırlı olduğu görülmüş; mevcut çalışmaların çoğunlukla teknik düzeyde kaldığı ve hukuki, etik veya toplumsal boyutların yeterince ele alınmadığı tespit edilmiştir. Uluslararası literatürde de sadece teknik saldırı yöntemleri üzerinde yoğunlaşıldığı, ancak saldırıların hukuki sonuçları ve bireysel haklar üzerindeki etkilerine ilişkin bütüncül analizlerin eksik olduğu gözlemlenmiştir. Bu durum bu tez

çalışmasının hem ulusal hem de uluslararası literatürde önemli bir boşluğu doldurmasına katkı sağlayabileceğini göstermektedir.

Yapılan analizler sonucunda mevcut güvenlik önlemlerinin günümüzün gelişen saldırı yöntemlerine karşı yetersiz kaldığı, özellikle yapay zekâ destekli ses manipülasyonlarının mevcut savunma mekanizmalarını aşabildiği de belirlenmiştir. Bu kapsamda gelecekte sesli sistemlere yönelik güvenlik stratejilerinin yeni tehdit modellerine dayanarak geliştirilmesi gerektiği anlaşılmaktadır.

Çalışma kapsamında elde edilen sonuçlar doğrultusunda aşağıdaki öneriler geliştirilmiştir:

- Sesle çalışan sistemlerde çok faktörlü kimlik doğrulama (MFA) mekanizmalarının standart hale getirilmesi, özellikle sesli komut sistemlerinde ikincil kimlik doğrulayıcıların kullanılması,
- Sesli komut sistemlerinde güçlü şifreleme ve komut doğrulama protokollerinin geliştirilmesi, böylece yetkisiz erişimlerin önüne geçilmesi,
- Deepfake algılama ve sahte ses tespiti teknolojilerinin geliştirilmesine yönelik araştırma ve geliştirme çalışmalarına öncelik verilmesi,
- Sesli verilerin işlenmesi ve korunmasına ilişkin ulusal ve uluslararası mevzuatın (özellikle biyometrik veriler bağlamında) güncellenmesi ve güçlendirilmesi,
- Kullanıcıların sesle yapılan siber saldırıların riskleri hakkında bilinçlendirilmesi amacıyla kamuya açık eğitim ve bilgilendirme kampanyalarının artırılması,
- Akustik yan kanal saldırılarına karşı fiziksel güvenlik önlemlerinin (örneğin akustik yalıtım, özel mikrofon kalkanları vb.) yaygınlaştırılması,
- Gelecek araştırmalara yönelik olarak, yapay zekâ destekli savunma sistemlerinin geliştirilmesi, deepfake kaynaklı sahte ses örneklerine karşı daha dirençli ses tanıma teknolojilerinin tasarlanması ve ses verilerinin mahremiyetini zedelemeden, güvenli ve etik biçimde işlenmesini sağlayacak yeni tekniklerin araştırılması önerilmektedir.
- Ayrıca ses verilerinin korunmasına ilişkin hukuki düzenlemelerin teknolojik gelişmelere paralel olarak dinamik biçimde güncellenmesi gerektiği değerlendirilmektedir.

Sonuç olarak ses teknolojileri, sundukları kolaylıklar ve işlevsellikler kadar önemli güvenlik tehditlerini de beraberinde getirmektedir. Sesli asistanlar, sesle kontrol edilen cihazlar ve

biyometrik kimlik doğrulama sistemleri gibi uygulamalar hayatı kolaylaştırırken aynı zamanda kötü niyetli kimseler için yeni saldırı teknikler, oluşturmaktadır. Bireyler, kurumlar ve kamu organları tarafından bu tehditlerin ciddiyetle ele alınması, sesli sistemlere yönelik kapsamlı risk analizlerinin yapılması ve gerekli önleyici tedbirlerin etkin bir şekilde geliştirilmesi günümüzde kaçınılmaz bir gereklilik haline gelmiştir. Bu kapsamda sesli sistemlere yönelik güvenlik standartlarının oluşturulması, yapay zekâ destekli saldırılara karşı dirençli savunma mekanizmalarının geliştirilmesi ve ses tabanlı biyometrik verilerin işlenmesinde etik ilkelere uyumun sağlanması büyük bir öncelik olmalıdır.

Bu tez çalışması, ses tabanlı sistemleri bilişim temelli bir güvenlik konusu olarak ele alırken aynı zamanda toplumsal etkileri ve hukuki sonuçlarıyla birlikte çok boyutlu bir şekilde ele almıştır. Bu yönüyle araştırma bilişim sistemleri, hukuk ve medya sektörü gibi farklı disiplinlerin kesişiminde yer alan sorunları görünür kılmakta ve disiplinler arası güvenlik anlayışına katkı sağlamaktadır.

Ses teknolojilerinin günlük yaşama nüfuz etmesi dijital güvenlik anlayışlarını yeniden şekillendirmiştir. Gelişen saldırı teknikleri, klasik güvenlik yaklaşımlarının ötesine geçilmesini zorunlu kılmakta, dinamik ve sürdürülebilir güvenlik stratejilerine duyulan ihtiyacı açıkça ortaya koymaktadır. Günümüzde siber güvenlik, yalnızca teknolojik savunma önlemleriyle sınırlandırılamayacak kadar çok boyutlu bir meseleye dönüşmüştür. Bu çalışma ses tabanlı sistemlere yönelik potansiyel tehditleri ve dijital sistemlerin karmaşık güvenlik gereksinimlerini ortaya koyarak bireysel mahremiyetin korunması, hukuki düzenlemelerin güncellenmesi ve farkındalık temelli toplumsal stratejilerin geliştirilmesi gerektiğini göstermiştir. Ses teknolojilerinin gelişimi eleştirel düşünme, teknik öngörü ve insan odaklı tasarım ilkeleri ile şekillendirildiğinde güvenli bir dijital gelecek mümkün olacaktır. Bu kapsamda ses teknolojilerine yönelik güvenlik, mahremiyet ve etik yaklaşımların gelecekte daha da önem kazanacağı öngörülmektedir.

KAYNAKLAR

Afchar, D., Nozick, V., Yamagishi, J., and Echizen, I. (2018, December). Mesonet: a compact facial video forgery detection network. *In 2018 IEEE international workshop on information forensics and security (WIFS),* 1-7.

Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., and Li, H. (2019). Protecting world leaders against deep fakes. *In CVPR Workshops,* 1, 38.

Ahmed, C. M., Mathur, A. P. (2017). Hardware identification via sensor fingerprinting in a cyber physical system. *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C),* 517-524.

Alabdali, N., Alzahrani, S. (2021). An overview of steganography through history. *Int J Sci Eng Sci, Kingd Saudi Arab,* 41-44.

Alchekov, S. S., Al-Absi, M. A., Al-Absi, A. A., and Lee, H. J. (2023). Inaudible attack on AI speakers. *Electronics,* 12(8), 1928.

Altamash, M., Singh, S. N. (2022). *Reconnaissance of credentials through phishing attacks & it's detection using machine learning.* Paper presented at the 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), Faridabad, India.

Aluko, A. O., Carpanen, R. P., Dorrell, D. G., and Ojo, E. E. (2022). Real-time cyber attack detection scheme for standalone microgrids. *IEEE Internet of Things Journal,* 9(21), 21481–21492.

Amezaga, N., Hajek, J. (2022). Availability of voice deepfake technology and its impact for good and evil. *In Proceedings of the SIGITE 2022,* 23–28.

Anıkaydın, İ. (2022). Deepfake uygulamalarının hukuki boyutu. *Düzce Üniversitesi Sosyal Bilimler Dergisi,* 12(2), 736-747.

Ansari, A., Nazir, M. (2022). Risk assessment of security vulnerabilities in smart home using CAPEC and defensive goals. *Advances in Data and Information Science,* 318, 705–722.

Antonio, H., Prasad, P. W. C., and Alsadoon, A. (2019). Implementation of cryptography in steganography for enhanced security. *Multimedia Tools and Applications,* 78(23), 32721-32734.

Antzoulis, I., Chowdhury, M. M., and Latiff, S. (2022). IoT security for smart home: Issues and solutions. *2022 IEEE International Conference on Electro Information Technology (eIT),* 1-7.

Apthorpe, N., Varghese, S., and Feamster, N. (2019). Evaluating the Contextual Integrity of Privacy Regulation: Parents'{IoT} Toy Privacy Norms Versus {COPPA}. *In 28th USENIX security symposium (USENIX security 19),* 123-140.

Arda, D. (2011). *Kodlama Teorisinin Kriptografik Açıdan İncelenmesi,* Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne, 28-36.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Management and Scientific Innovation,* 1(1), 24–28.

Asonov, D., Agrawal, R. (2004). Keyboard acoustic emanations. *Proceedings of the IEEE Symposium on Security and Privacy,* 2004, 3–11.

Babayiğit, B. (2021). Deepfake'in ceza hukuku bakımından değerlendirilmesi ve De Lege Ferenda öneriler. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi,* 25(4), 655-703.

Bateman, J. (2020). Deepfakes and synthetic media in the financial system: Assessing threat scenarios. *Cybersecurity and the Financial System,* 7, 1-52.

Bederson, B. B. and Shneiderman, B. (2003). *The craft of information visualization: Readings and reflections.* (First Edition). United States: Morgan Kaufmann Publishers Inc, 1-432.

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance,* 28, 24–31.

Bhardwaj, A., Goundar, S. (2020). Keyloggers: Silent cyber security weapons. *Network Security,* 2020(10), 14–19.

Bieniasz, J., Sapiecha, P., Smolarczyk, M., and Szczypiorski, K. (2016). Towards model-based anomaly detection in network communication protocols. *2016 2nd International Conference on Frontiers of Signal Processing (ICFSP),* 126–130.

Bilgin, M. (2013). Steganografi. *XV. Akademik Bilişim Konferansı Bildirileri,* 125-128.

Bilika, D., Michopoulou, N., Alepis, E., and Patsakis, C. (2024). Hello me, meet the real me: Voice synthesis attacks on voice assistants. *Computers & Security,* 137, 103617.

Birer, G. C. (2022). Kriptoloji. *Bilim ve Teknik,* Eylül 2022, 17-31.

Bishop, J., Keating, P. (2012). Perception of pitch location within a speaker's range: Fundamental frequency, voice quality, and speaker sex. *The Journal of the Acoustical Society of America,* 132(2), 1100–1112.

Bolton, C., Rampazzi, S., Li, C., Kwong, A., Xu, W., and Fu, K. (2018). Blue note: How intentional acoustic interference damages availability and integrity in hard disk drives and operating systems. *In 2018 IEEE Symposium on Security and Privacy (SP),* 1048-1062.

Boyd, J., Fahim, M., and Olukoya, O. (2023). Voice spoofing detection for multiclass attack classification using deep learning. *Machine Learning with Applications,* 14, 100503.

Brabin, D. D. R., & Bojjagani, S. (2023). A secure mechanism for prevention of vishing attack in banking system. *2023 International Conference on Networking and Communications (ICNWC),* 1–5.

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., and Nicholson, J. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior,* 145, 107770.

Campi, M., Peters, G. W., Azzaoui, N., and Matsui, T. (2021). Machine learning mitigants for speech based cyber risk. *IEEE Access,* 9, 136831-136860.

Carlini, N., Mishra, P., Vaidya, T., Zhang, Y., Sherr, M., Shields, C., and Zhou, W. (2016). Hidden voice commands. *In 25th USENIX security symposium (USENIX security 16),* 513-530.

Carlini, N., Wagner, D. A. (2018). Audio adversarial examples: Targeted attacks on speech-to-text. *2018 IEEE Security and Privacy Workshops (SPW),* 1–7.

Chavan, G. T., Agrawal, S., Sakhare, N. N., Mondal, D., Vigenesh, M., and G, V. (2023). Investigating the effectiveness of birthday attack strategies in cryptography network security. *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON),* 1–6.

Chebrolu, C. S., Lung, C.-H., and Ajila, S. A. (2022). Dynamic packet filtering using machine learning. *2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI),* 206–211.

Chen, M., Lin, J., Liu, W., Feng, W., and Wu, K. (2022). Behavicker: Eavesdropping computer-usage activities through acoustic side channel. *Wireless Communications and Mobile Computing,* 2022, 1-18.

Chen, Y., Li, W., Cheng, X., and Hu, P. (2024). A survey of acoustic eavesdropping attacks: Principle, methods, and progress. *High-Confidence Computing,* 4(4), 100241.

Cheng, W., Prodan, E., and Prodan, C. (2020). Experimental demonstration of dynamic topological pumping across incommensurate bilayered acoustic metamaterials. *Physical Review Letters,* 125(22), 224301.

Chesney, B., Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif. L. Rev.,* 107, 1753.

Clinton, U. B., Hoque, N. (2024). MU-IoT: A new IoT intrusion dataset for network and application layer attacks analysis. *IEEE Access,* 12, 166068–166092.

Connor, S. (2000). *Dumbstruck: A Cultural History of Ventriloquism*. (First Edition). Oxford: Oxford Academic, 1-449.

Conti, M., Duroyon, M., Orazi, G., and Tsudik, G. (2024). Acoustic side-channel attacks on a compu computer mouse. *In Lecture Notes in Computer Science*, 13933, 45–60.

Dagnas, R., Bkakria, A., and Yaich, R. (2023). *Robustness assessment of biometric authenticators.* Paper presented at the 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Exeter, United Kingdom.

Dang, H., Liu, F., Stehouwer, J., Liu, X., and Jain, A. K. (2020). On the detection of digital face manipulation. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition,* 5781–5790.

Değirmenli, E. (2023). Titreşim ve ses yayınım analizleri kullanılarak telli çalgılardaki tınısal niteliklerin incelenmesi: Ud örneği. *İdil,* 104, 525–534.

Deng, J., Chen, Y., Zhong, Y., Miao, Q., Gong, X., University, W.X., and University, W. (2023). Catch you and i can: Revealing source voiceprint against voice conversion. *2nd USENIX Security Symposium (USENIX Security 23),* 5163-5180.

Desetty, A., Gupta, A., Dutt, V., and Pulyala, S. (2020). Phishing attacks: Evolving techniques, emerging trends, and countermeasure strategies. *International Journal For Innovative Engineering and Management Research,* 9, 985–991.

Dhakal, R., Kandel, L. N. (2023). A survey of physical layer-aided UAV security. *2023 Integrated Communication, Navigation and Surveillance Conference (ICNS),* 1–8.

Diffie, W., Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory,* 22(6), 644–654.

Drenten, J., Psarras, E. (2023). Digital ventriloquism and celebrity access: Cameo and the emergence of paid puppeteering on digital platforms. *New Media & Society,* 25(12), 3350–3369.

Dülger, M. V. (2016). Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu bağlamında kişisel verilerin ceza normlarıyla korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi,* 3(2), 101-168.

Elitaş, T. (2022). Dijital manipülasyon 'deepfake' teknolojisi ve olmayanın inandırıcılığı. *Hatay Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 19(49), 113-128.

Erbaş, R. (2015). Organized crime-related legislation in the Turkish criminal law. *Ceza Hukuku ve Kriminoloji Dergisi,* 3(1), 275-311.

Erol-Kantarci, M., Mouftah, H. T. (2013). Smart grid forensic science: Applications, challenges, and open issues. *IEEE Communications Magazine,* 51(1), 68-74.

Firc, A., Malinka, K., and Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon,* 9(4), e15090.

Gadde, S., Amutharaj, J., and Usha, S. (2023). A security model to protect the isolation of medical data in the cloud using hybrid cryptography. *Journal of Information Security and Applications,* 73(C), 103412.

Gamage, P., Dissanayake, D., Kumarasinghe, N., and Ganegoda, G. (2023). Acoustic signature analysis for distinguishing human vs. synthetic voices in vishing attacks. *Proceedings of the 2023 IEEE International Conference on Information Technology and Renewable Energy (ICITR),* 1–6.

Gong, T., Ramos, A. G. C., Bhattacharya, S., Mathur, A., and Kawsar, F. (2019). Audidos: Real-time denial-of-service adversarial attacks on deep audio models. *In 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA),* 978-985).

Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., and Bengio, Y. (2014). Generative adversarial nets. *Advances in neural information processing systems,* 27.

Gough, D., Thomas, J., and Oliver, S. (2017). *An introduction to systematic reviews.* (First Edition). London: Sage Publishing, 7-13.

Gupta, A., Ali, A., Pandey, A. K., Gupta, A. K., and Tripathi, A. (2022). Metamorphic cryptography using AES and LSB method. *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM),* 1-8.

Guri, M. (2020). CD-LEAK: Leaking secrets from audioless air-gapped computers using covert acoustic signals from CD/DVD drives. *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC),* 808–816.

Guri, M., Kedma, G., Kachlon, A., and Elovici, Y. (2014). AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. *Proceedings of the 9th IEEE International Conference on Malicious and Unwanted Software (MALCON 2014),* 1-20.

Gutiérrez, N., Rodríguez, E., Mus, S., Otero, B., and Canal, R. (2020, July). *Privacy preserving deep learning framework in fog computing.* Paper presented at the Machine Learning, Optimization, and Data Science: 6th International Conference, LOD 2020, Siena, Italy.

Hamza, A., Javed, A. R. R., Iqbal, F., Kryvinska, N., Almadhor, A. S., and Jalil, Z. (2022). Deepfake audio detection via MFCC features using machine learning. *IEEE Access,* 10, 134018–134028.

Hariharan, U., Dhanakoti, V., Rajkumar, K., and Jeyavel, J. (2022*). Safeguarding e-healthcare documents utilizing an infrastructure for advanced keyless signature infrastructure blockchain within the cloud.* Paper presented at the 2022 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India.

Harrou, F., Bouyeddou, B., Sun, Y., and Kadri, B. (2018). A method to detect DOS and DDOS attacks based on generalized likelihood ratio test. *2018 International Conference on Applied Smart Systems (ICASS),* 1-6.

Hartmann, K., Steup, C. (2020). Hacking the AI - the next generation of hijacked systems. *2020 12th International Conference on Cyber Conflict (CyCon),* 327-349.

Hatipoğlu, C., & Tunacan, T. (2021). Türkiye'de siber saldırı ve tespit yöntemleri: Bir literatür taraması. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi,* 8(1), 430-445.

Hayashi, V. T., Ruggiero, W. V. (2022). Hands-free authentication for virtual assistants with trusted IoT device and machine learning. *Sensors,* 22(4), 1325.

Heartfield, R., Loukas, G., Bezemskij, A., and Panaousis, E. (2021). Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning. *IEEE Transactions on Information Forensics and Security,* 16, 1720-1735.

Hershey, P. C., Silio, C. B. (2011). Monitoring and management approach for cyber security events over complex systems. *2011 IEEE International Systems Conference,* 38-45.

Higgins, J. P. T., Green, S. (2011). *Cochrane Handbook for Systematic Reviews of Interventions.* (First Edition). London: The Cochrane Collaboration, 1-12.

Hijji, M., Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE Access,* 9, 7152–7169.

Hoy, M. B. (2018). Alexa, Siri, Cortana, and more: an introduction to voice assistants. *Medical reference services quarterly,* 37(1), 81-88.

Huang, D., Tian, Z., Su, S., and Jiang, Y. (2020). A defense scheme of voice control system against DolphinAttack. *Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies,* 136–142.

Huang, Y., Juefei-Xu, F., Guo, Q., Liu, Y., and Pu, G. (2022). FakeLocator: Robust localization of GAN-based face manipulations. *IEEE Transactions on Information Forensics and Security,* 17, 2657–2672.

Hussain, S., Neekhara, P., Dubnov, S., McAuley, J., and Koushanfar, F. (2021). WaveGuard: Understanding and mitigating audio adversarial examples. *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21),* 1–10.

İnternet: ABD Federal İletişim Komisyonu. (2024). Caller ID Spoofing. URL: https://www.fcc.gov/consumers/guides/spoofing, Son Erişim Tarihi: 07.03.2025.

İnternet: ABD Genel Hizmetler İdaresi. (2023). Identity theft. URL: https://www.usa.gov/identity-theft, Son Erişim Tarihi: 08.03.2025.

İnternet: ABD Kent Eyalet Üniversitesi. (2018). Vishing. URL: https://www.kent.edu/secureit/vishing, Son Erişim Tarihi: 08.03.2025.

İnternet: ABD Ticaret Bakanlığı Ulusal Standartlar ve Teknoloji Enstitüsü. (2014). Guidelines for Media Sanitization. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, Son Erişim Tarihi: 14.03.2025.

İnternet: Akıncı, A. N. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü'nün getirdiği yenilikler ve Türk hukuku bakımından değerlendirilmesi. URL: https://sbb.gov.tr/wp-content/uploads/2018/11/AvrupaBirli%C4%9FiGenelVeriKorumaT%C3%BCz%C3%BC%C4%9F%C3%BCn%C3%BCnGetirdi%C4%9FiYeniliklerveT%C3%BCrkHukukuBak%C4%B1m%C4%B1ndan-De%C4%9Ferlendirilmesi.pdf, Son Erişim Tarihi: 07.03.2025.

İnternet: Aksakallı, G. (2017). Vishing Saldırılarına Karşı Alınabilecek Önlemler. URL: https://www.guvenliweb.org.tr/galeri-detay/vishing-saldirilarina-karsi-alinabilecek-onlemler, Son Erişim Tarihi: 07.03.2025.

İnternet: American Psychological Association - Amerikan Psikoloji Birliği. (2014). What is phishing and how to spot a potential phishing attack. URL: https://www.apa.org/about/division/digest/leader-resources/phishing.pdf, Son Erişim Tarihi: 10.01.2025.

İnternet: AT&T Cybersecurity. (2017). How secure is voice recognition technology?. URL: https://www.business.att.com/learn/tech-advice/how-secure-is-voice-recognition-technology.html, Son Erişim Tarihi: 08.03.2025.

İnternet: Atac, M. (2023). SQL Injection Nedir, Nasıl Yapılır? SQL Injection Saldırıları Nasıl Önlenir?. URL: https://www.istanbulbttelekom.com.tr/post/sql-injection-nedir-nasil-yapilir-sql-injection-saldirilari-nasil-onlenir, Son Erişim Tarihi: 10.01.2025.

İnternet: Avustralya Bilgi Komisyonu Ofisi. (2023). Identity fraud. URL: https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/Identity-fraud, Son Erişim Tarihi: 08.03.2025.

İnternet: Baidu. (2021). Steganalysis. URL: https://baike.baidu.com/item/%E9%9A%90%E5%86%99%E5%88%86%E6%9E%90, Son Erişim Tarihi: 24.03.2025.

İnternet: Beyaz.Net. (2024). GDPR Nedir?. URL: https://www.beyaz.net/tr/guvenlik/makaleler/gdpr_nedir.html, Son Erişim Tarihi: 03.04.2025.

İnternet: BilgiGüvende. (2018). Siber saldırganlar, ses sinyalleri ile sabit diskleri çökertebilir. URL: https://bilgiguvende.com/sonik-ultrasonik-sinyaller-sabit-disk/, Son Erişim Tarihi: 16.03.2025.

İnternet: BleepingComputer. (2023). Inaudible ultrasound attack can stealthily control your phone, smart speaker. URL: https://www.bleepingcomputer.com/news/security/inaudible-ultrasound-attack-can-stealthily-control-your-phone-smart-speaker/, Son Erişim Tarihi: 12.03.2025.

İnternet: BotTalk. (2023). Everything You Need to Know About Deepfake Voice. URL: https://bottalk.io/learn-with-bottalk/everything-about-deepfake-voice/, Son Erişim Tarihi: 09.03.2025.

İnternet: Chen, G. (2023). Uncovering the unheard: Researchers reveal inaudible remote cyber-attacks on voice assistant devices. URL: https://www.utsa.edu/today/2023/03/story/chen-nuit-research.html, Son Erişim Tarihi: 12.03.2025.

İnternet: CNNTürk. (2018). Sabit diskler ses dalgası saldırı yöntemi ile zarar görüyorlar. URL: https://www.cnnturk.com/teknoloji/sabit-diskler-ses-dalgasi-saldiri-yontemi-ile-zarar-goruyorlar-825934, Son Erişim Tarihi: 16.03.2025.

İnternet: Council of Europe. (2024). Convention on Cybercrime (Budapest Convention). URL: https://rm.coe.int/prems-105223-gbr-2023-convention-cybercrimininalite-a5-web-4-/1680ae7118, Son Erişim Tarihi: 08.04.2025.

İnternet: Dickson, B. (2020). What are deepfakes?. URL: https://bdtechtalks.com/2020/09/04/what-is-deepfake/, Son Erişim Tarihi: 08.03.2025.

İnternet: Dülger, M. V. (2019). Kişisel Verileri Koruma Kurulunun 3 Nisan 2019 tarihli karar özetlerine ilişkin değerlendirme. URL: https://ssrn.com/abstract=3792303, Son Erişim Tarihi: 07.03.2025.

İnternet: Forbes. (2019). A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. URL: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/, Son Erişim Tarihi: 07.03.2025.

İnternet: Fremont Federal Credit Union - Fremont Federal Kredi Birliği. (2015). What is Vishing?. URL: https://www.fremontfcu.com/files/fremont/1/file/ID%20Theft%20Articles/What%20is%20Vishing.pdf, Son Erişim Tarihi: 07.03.2025.

İnternet: Garfinkel, S. (2022). Differential Privacy and the 2020 US Census. URL: https://mit-serc.pubpub.org/pub/differential-privacy-2020-us-census/release/2, Son Erişim Tarihi: 09.03.2025.

İnternet: GDPR Recital 6. URL: https://gdpr-info.eu/recitals/no-6/, Son Erişim Tarihi: 06.04.2025.

İnternet: Guri, M., Solewicz, Y., Daidakulov, A., and Elovici, Y. (2017). Diskfiltration: Data exfiltration from speakerless air-gapped computers via covert hard drive noise. URL: https://arxiv.org/pdf/1608.03431, Son Erişim Tarihi: 21.03.2025.

İnternet: Gündüz, O. ve Yücel, Ö. A. (2023). Kişisel Verilerin Korunmasının Önemi. URL: https://gunduzyucel.com/kisisel-verilerin-korunmasinin-onemi/, Son Erişim Tarihi: 06.03.2025.

İnternet: Hofing, J., Deshpande, R., Vijay, N. K., Qi, Z., and Zhou, Y. Hidden commands audio attacks on Alexa and Siri. URL: https://www.academia.edu/download/61697683/Alexa20200106-102854-lboqj8.pdf, Son Erişim Tarihi: 05.11.2023.

İnternet: IBM - International Business Machines. (1997). IBM 1997 Annual Report. URL: https://www.ibm.com/annualreport/assets/past-reports/1997-ibm-annual-report.pdf, Son Erişim Tarihi: 09.03.2025.

İnternet: IBM - International Business Machines. (2020). IBM 2020 Annual Report. URL: https://www.ibm.com/investor/att/pdf/IBM_Annual_Report_2020.pdf, Son Erişim Tarihi: 09.03.2025.

İnternet: IBM - International Business Machines. (2025). 2025 IBM X-Force Threat Intelligence Index. URL: https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index, Son Erişim Tarihi: 26.04.2025.

İnternet: İnternet Protokolü Video Marketi – IPVM. (2018). Sonic Attacks Can Interrupt HDD Recording. URL: https://ipvm.com/discussions/sonic-attacks-can-interrupt-hdd-recording, Son Erişim Tarihi: 18.03.2025.

İnternet: İstanbul Barosu. (2023). Yapay Zekâ ve Hukuk: Deepfake Üzerine Bir Değerlendirme. URL: https://www.istanbulbarosu.org.tr/files/komisyonlar/yzcg/yzcg_deepfake.pdf, Son Erişim Tarihi: 06.04.2025.

İnternet: Karakaya, N. (2024). Kişisel Veri Suçları. URL: https://karakaya.av.tr/makale-detay.php?blog_id=37, Son Erişim Tarihi: 06.03.2025.

İnternet: Karakuş, C. (2024). Ses Dalgaları. URL: https://ckk.com.tr/bilimsel/ses.pdf, Son Erişim Tarihi: 05.03.2025.

İnternet: Karanfiloğlu, K. (2024). Cybercrime and Cybersecurity Law in Turkey. URL: https://www.karanfiloglu.av.tr/en/cybercrime-and-cybersecurity-law-in-turkey/, Son Erişim Tarihi: 07.04.2025.

İnternet: Kaya, M. (2010). Sniffing ve korunma yolları. URL: https://www.mustafakaya.com.tr/sniffing-ve-korunma-yollari-%E2%80%A6.html, Son Erişim Tarihi: 12.09.2024.

İnternet: KeepNet. (2025). What is Vishing: Definition, Detection and Protection. URL: https://keepnetlabs.com/blog/what-is-vishing, Son Erişim Tarihi: 08.03.2025.

İnternet: Kişisel Verileri Koruma Kurumu. (2025). Örneklerle kişisel verilerin korunmasına ilişkin rehber. URL: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/b654ee4e-e329-49a6-9722-03561daac1aa.pdf, Son Erişim Tarihi: 06.03.2025.

İnternet: Kişisel Verilerin Korunması Kanunu – KVKK. (2016). Kişisel Verilerin Korunması Kanunu. URL: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5, Son Erişim Tarihi: 06.04.2025.

İnternet: Kurita, K., Michel, P., and Neubig, G. (2020). Weight poisoning attacks on pre-trained models. URL: https://arxiv.org/pdf/2305.15518, Son Erişim Tarihi: 10.03.2025.

İnternet: Li, Y., Chang, M. C., and Lyu, S. (2018). In ictu oculi: Exposing ai generated fake face videos by detecting eye blinking. URL: https://arxiv.org/abs/1806.02877, Son Erişim Tarihi: 09.03.2025.

İnternet: Lindemulder, G., Kosinski, M. (2024). ¿Qué es un ataque de intermediario (MITM)?. URL: https://www.ibm.com/es-es/think/topics/man-in-the-middle, Son Erişim Tarihi: 21.04.2025.

İnternet: McKee, F., Noever, D. (2023). NUANCE: near ultrasound attack on networked communication environments. URL: https://arxiv.org/pdf/2305.10358, Son Erişim Tarihi: 12.03.2025.

İnternet: Mutombo, M., Nkongolo, M. W., and Tokmak, M. (2025). Cryptojacking detection using local interpretable model-agnostic explanations. *Turk J Elec Eng & Comp Sci,* Web: https://eprint.iacr.org/2025/050.pdf adresinden 5 Mart 2025'te alınmıştır.

İnternet: Record Nations. (2024). History of Hard Drives and Backup Systems. URL: https://www.recordnations.com/articles/external-hard-drive/, Son Erişim Tarihi: 14.03.2025.

İnternet: Salas-Nino, M., Ritter, G., Hamdan, D., Wang, T., and Hou, T. (2023). The Evolution of Keylogger Technologies: A Survey from Historical Origins to Emerging Opportunities. URL: https://arxiv.org/pdf/2312.10445, Son Erişim Tarihi: 30.03.2025.

İnternet: Serene-Risc Smart Cybersecurity Network. (2017). DolphinAttack: Inaudible Voice Commands. URL: https://www.serene-risc.ca/fr/digest/can-virtual-assistants-be-controlled-by-voices-that-you-cant-hear, Son Erişim Tarihi: 11.03.2025.

İnternet: SkyNews. (2024). Scarlett Johansson speaks out about clash with OpenAI. URL: https://news.sky.com/story/scarlett-johnasson-speaks-out-about-clash-with-openai-13158491, Son Erişim Tarihi: 08.03.2025.

İnternet: Stallings, W. (2017). Cryptography and Network Security 5/e. URL: https://www.cise.ufl.edu/~nemo/crypto/slides/ch14_key_mgt_nemo.ppt, Son Erişim Tarihi: 06.03.2025.

İnternet: T.C. Millî Eğitim Bakanlığı. (2007). Disk Sürücüleri. URL: https://megep.meb.gov.tr/mte_program_modul/moduller_pdf/Disk%20S%C3%BCr%C3%BCc%C3%BCleri.pdf, Son Erişim Tarihi: 14.03.2025.

İnternet: Taşdöğen, C., (2019). Sosyal medya nedir?. URL: https://www.iienstitu.com/blog/sosyalmedya-nedir, Son Erişim Tarihi: 02.06.2024.

İnternet: Teknocityblog. (2016). Disk Sürücüleri. URL: https://teknocityblog.wordpress.com/2016/11/29/disk-suruculeri/, Son Erişim Tarihi: 14.03.2025.

İnternet: The Hacker News. (2018). Attackers Can Use Sonic and Ultrasonic Signals to Crash Hard Drives. URL: https://thehackernews.com/2018/05/hard-drive-failure-hack.html, Son Erişim Tarihi: 18.03.2025.

İnternet: Threat Hunter Team. (2024). Ransomware: Attacks Once More Nearing Peak Levels. URL: https://www.security.com/threat-intelligence/ransomware-attacks-rebound, Son Erişim Tarihi: 04.03.2025.

İnternet: Threatpost. (2018). Sonic Tone Attacks Damage Hard Disk Drives, Crashes OS. URL: https://threatpost.com/sonic-tone-attacks-damage-hard-disk-drives-crashes-os/132343/, Son Erişim Tarihi: 17.03.2025.

İnternet: Türkiye Bankalar Birliği. (2015). Bankacılıkta Dolandırıcılık Eylemleri Tespit ve Önleme Yöntemleri. URL: https://www1.tbb.org.tr/gec/KTPV14.pdf, Son Erişim Tarihi: 07.03.2025.

İnternet: URL: Ortega, A. (2017). Turning hard disk drives into accidental microphones. URL: https://www.youtube.com/watch?v=ntw32kYDryM, Son Erişim Tarihi: 21.03.2025.

İnternet: Veri Koruma Komisyonu. (2019). Data protection in the EU. URL: https://commission.europa.eu/law/law-topic/data-protection_en, Son Erişim Tarihi: 07.03.2025.

İnternet: Webrazzi. (2019). Hackerlar, pencerenize lazer ışığı yansıtarak evinizdeki sanal asistanınıza erişebiliyorlar. URL: https://webrazzi.com/2019/11/06/hacker-sanal-asistan-lazer-isigi/?utm_source=chatgpt.com, Son Erişim Tarihi: 11.03.2025.

İnternet: West, D. M. (2019). Digital threats to campaign 2020: Fake nudes, doctored images, and widespread disinformation. URL: https://www.brookings.edu/articles/digital-threats-to-campaign-2020-fake-nudes-doctored-images-and-widespread-disinformation/, Son Erişim Tarihi: 09.03.2025.

İnternet: Yakura, H., & Sakuma, J. (2018). Robust audio adversarial example for a physical attack. URL: https://arxiv.org/pdf/1810.11793, Son Erişim Tarihi: 10.03.2025.

İnternet: Yan, Q., Liu, K., Zhou, Q., Guo, H., and Zhang, N. (2020). SurfingAttack: Interactive hidden attack on voice assistants using ultrasonic guided waves. URL: https://www.ndss-symposium.org/wp-content/uploads/2020/02/24068.pdf, Son Erişim Tarihi: 30.05.2023.

İnternet: Yargıtay 10. Ceza Dairesi, 2022/1757 E. ve 2024/16786 K. sayılı kararı. URL: https://karararama.yargitay.gov.tr/, Son Erişim Tarihi: 08.03.2025.

İnternet: Yargıtay 11. Hukuk Dairesi, 2023/1184 E. ve 2024/4757 K. sayılı kararı. URL: https://karararama.yargitay.gov.tr/, Son Erişim Tarihi: 08.03.2025.

İnternet: Yargıtay 12. Ceza Dairesi, 2012/32135 E. ve 2013/16483 K. sayılı kararı. URL: https://karararama.yargitay.gov.tr/, Son Erişim Tarihi: 08.03.2025.

İnternet: Yargıtay 12. Ceza Dairesi. 2018/8295 E., 2019/6858 K. sayılı ve 29.05.2019 tarihli kararı. URL: https://karararama.yargitay.gov.tr/, Son Erişim Tarihi: 06.03.2025.

İnternet: Yargıtay 12.Ceza Dairesi, 2018/8144 E., 2019/8317 K. sayılı ve 10.07.2019 tarihli kararı. URL: https://karararama.yargitay.gov.tr/, Son Erişim Tarihi: 06.03.2025.

İnternet: Yargıtay 8. Ceza Dairesi, 2020/1419 E. ve 2022/122 K. sayılı kararı. URL: https://karararama.yargitay.gov.tr/, Son Erişim Tarihi: 08.03.2025.

İnternet: Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., and Qian, F. (2018). Understanding and mitigating the security risks of voice-controlled third-party skills on amazon alexa and google home. URL: https://arxiv.org/pdf/1805.01525, Son Erişim Tarihi: 11.03.2025.

Jain, N. (2024). Detecting deepfakes: exploring machine learning models for audio, video, and image analysis. *International Journal of Intelligent Systems and Applications in Engineering,* 12(4), 481.

Jin, X., Wang, J., Liu, L., and Lin, Y. (2023). Uncertainty-aware denoising network for artifact removal in EEG signals. *IEEE Transactions on Neural Systems and Rehabilitation Engineering,* 31, 4470–4480.

Johnson, N., Jajodia, S., and Memon, N. (2001). Information hiding: Steganography and watermarking—Attacks and countermeasures. *Journal of Electronic Imaging,* 10(4), 825.

Kahn, D. (1996). The history of steganography. *In Proceedings of the First International Workshop on Information Hiding,* 1–5.

Kalluri, R., LeBleu, V.S. (2020) The biology, function, and biomedical applications of exosomes. *Science,* 367, eaau6977.

Kalmar, G. (2019). *Smart speaker: Suspicious event detection with reverse mode speakers.* Paper presented at the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary.

Kao, D. Y. (2020). Comprehending Taiwan ATM heist: From cyber-attack phases to investigation processes. *2020 22nd International Conference on Advanced Communication Technology (ICACT),* 1232–1241.

Karabat, Ç. (2010). Steganografi ve sayısal damgalama: geçmişten günümüze bilgi gizleme teknikleri. *Bilim ve Teknik,* Şubat 2010, 82-85.

Karim, N. A., Kanaker, H., Abdulraheem, W. K., Ghaith, M. A., Alhroob, E., and Alalie, A. M. F. (2024). Choosing the right MFA method for online systems: A comparative analysis. *International Journal of Data and Network Science,* 8(2024), 201–212.

Kasmi, C., Esteves, J. L. (2015). IEMI threats for information security: Remote command injection on modern smartphones. *IEEE Transactions on Electromagnetic Compatibility,* 57(6), 1752-1755.

Kasprzak, W., Szynkiewicz, W., Stefańczyk, M., Dudek, W., Węgierek, M., Seredyński, D., Figat, M., and Zielinski, C. (2024). Agent-based approach to the design of a multimodal interface for cyber-security event visualisation control. *Bulletin of the Polish Academy of Sciences Technical Sciences,* 118(7), 1205.

Kayser, C. S., Back, S., and Toro-Alvarez, M. M. (2024). Identity theft: The importance of prosecuting on behalf of victims. *Laws,* 13(6), 68.

Khan, H. M. A., Inayat, U., Zia, M. F., Ali, F., Jabeen, T., and Ali, S. M. (2021). Voice over internet protocol: Vulnerabilities and assessments. *2021 International Conference on Innovative Computing (ICIC),* 1–6.

Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., and Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* 50(1), 73-80.

Khodabakhsh, A., Mohammadi, A., and Demiroglu, C. (2017). Spoofing voice verification systems with statistical speech synthesis using limited adaptation data. *Computer Speech & Language,* 42, 20–37.

Kim, D. Y. (2018). A study on voice phishing countermeasures of the police. *Journal of Digital Contents Society,* 19(1), 193-198.

Kim, H. (2020). 5G core network security issues and attack classification from network protocol perspective. *J. Internet Serv. Inf. Secur.,* 10, 1-15.

Kiraz, O. Z. (2021). Siber güvenlik bağlamında yeni tehdit algılamalarının Türkiye'nin güvenlik politikalarına etkileri. *Journal of Management Theory and Practices Research,* 2(2), 69-88.

Kishore, R. S., Bhaskari, D. L. (2023). Cyber crime detection and prevention techniques on cyber cased objects using SVM and smote. *International Journal on Recent and Innovation Trends in Computing and Communication,* 11(8), 259–270.

Korkmaz, Y., & Boyacı, A. (2018). Adli bilişim açısından ses incelemeleri. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi,* 30(1), 329-343.

Kreuk, F., Sheena, Y., Keshet, J., and Adi, Y. (2020). Phoneme boundary detection using learnable segmental features. *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* 2020, 8089–8093.

Kune, D. F., Backes, J., Clark, S. S., Kramer, D., Reynolds, M., Fu, K., and Xu, W. (2013). Ghost talk: Mitigating EMI signal injection attacks against analog sensors. *In 2013 IEEE symposium on security and privacy,* 145-159.

Kutlu, Ö., Kahraman, S. (2017). Türkiye'de kişisel verilerin korunması politikasının analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi,* 5(4), 45-62.

Kwong, A., Xu, W., and Fu, K. (2019). Hard drive of hearing: Disks that eavesdrop with a synthesized microphone. *2019 IEEE Symposium on Security and Privacy (SP),* 905–919.

Lee, B., Isenberg, P., Riche, N. H., and Carpendale, S. (2012). Beyond mouse and keyboard: Expanding design considerations for information visualization interactions. *IEEE Transactions on Visualization and Computer Graphics,* 18(12), 2689-2698.

Leonov, P. Y., Vorobyev, A. V., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A. K., and Morozov, N. V. (2021). The main social engineering techniques aimed at hacking information systems. *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT),* 471–473.

Levy, S. (2001*). Crypto: How the code rebels beat the government--saving privacy in the digital age.* (First Edition). United Kingdom: Penguin, 1-368.

Li, J., Chen, C., Pan, L., Azghadi, M.R., Ghodosi, H., and Zhang, J. (2023). Security and privacy problems in voice assistant applications: A survey. *Comput. Secur.,* 134, 103448.

Li, X., Wang, H., Dai, H.-N., Wang, Y., and Zhao, Q. (2016). An analytical study on eavesdropping attacks in wireless networks of things. *Mobile Information Systems,* 2016, 4313475.

Liu, K., Dolan-Gavitt, B., and Garg, S. (2018). Fine-pruning: Defending against backdooring attacks on deep neural networks. *In International symposium on research in attacks, intrusions, and defenses,* 273-294.

Liu, R., Peng, X., Sun, Z., Huang, Z., and Hu, H. (2022). *Research on cyberattack detection of connected automated vehicles based on support vector machine.* Paper presented at the 2022 IEEE 7th International Conference on Intelligent Transportation Engineering (ICITE), Beijing, China.

Liu, X., Li, Y., and Deng, R. H. (2021). UltraPIN: Inferring PIN entries via ultrasound. *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (ASIA CCS '21),* 944–957.

Lloyd, J. S., Ludwikowski, C. G., Malik, C., and Shen, C. (2023). Mitigating inaudible ultrasound attacks on voice assistants with acoustic metamaterials. *IEEE Access,* 11, 36464–36470.

Lopatovska, I., and Williams, H. (2018). Personification of the Amazon Alexa: BFF or a mindless companion. *In Proceedings of the 2018 Conference on Human Information Interaction & Retrieval,* 265-268.

Mache, S., Baheti, M., Mahender, C., and Professor, A. (2015). Review on text-to-speech synthesizer. *International Journal of Advanced Research in Computer and Communication Engineering,* 4(1), 54–59.

Madamopoulos, C., Tsoutsos, N. G. (2024). 3D printer audio and vibration side channel dataset for vulnerability research in additive manufacturing security. *Data in Brief,* 57, 111002.

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., and Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications,* 232, 104004.

Maras, M. H., Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The international journal of evidence & proof,* 23(3), 255-262.

Mazurczyk, W., Wendzel, S., Zander, S., Houmansadr, A., and Szczypiorski, K. (2016). *Information hiding in communication networks: fundamentals, mechanisms, applications, and countermeasures.* (First Edition). United Staes: Wiley-IEEE Press, 1-296.

McKee, F., Noever, D. (2023). Acoustic cybersecurity: Exploiting voice-activated systems. *Cryptography and Security,* 2023, 2312.00039.

McLoughlin, I. V. 2018. *Computer Systems: An Embedded Approach.* (First Edition). New York: McGraw-Hill Education, 1-512.

Mirsky, Y., Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys (CSUR),* 54(1), 1-41.

Moher, D., Liberati, A., Tetzlaff, J. And Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine,* 6(7), e1000097.

Mokhtari, A., Ghorbani, N., and Bahrak, B. (2022). Aggregated traffic anomaly detection using time series forecasting on call detail records. *Security and Communication Networks,* 2022, 1–9.

Monshizadeh, M., Khatri, V., Varfan, M., and Kantola, R. (2018). LiaaS: Lawful interception as a service. *2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM),* 1-6.

Mougy, A. E., Khalaf, A., Agaty, H. E., Mazen, M., Saleh, N., and Samir, M. (2017). Xenia: Secure and interoperable smart home system with user pattern recognition. *2017 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC),* 47–52.

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., and Porras, J. (2023). Mitigation strategies against phishing attacks: A systematic literature review. *Computers & Security,* 132, 103387.

Nassif, A. B., Shahin, I., Attili, I., Azzeh, M., and Shaalan, K. (2019). Speech recognition using deep neural networks: A systematic review. *IEEE Access,* 7, 19143–19165.

Nataraj, L., Mohammed, T. M., Nanjundaswamy, T., Chikkagoudar, S., Chandrasekaran, S., and Manjunath, B. S. (2021). OMD: Orthogonal malware detection using audio, image, and static features. *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM),* 703-708.

Nguyen, X. H., Tran, T. S., Nguyen, K. D., and Truong, D. T. (2021). Learning spatio-temporal features to detect manipulated facial videos created by the deepfake techniques. *Forensic Science International: Digital Investigation,* 36, 301108.

Noblit, G. W., Hare, R. D. (1998). Chapter 5: Meta-Ethnography: Synthesizing qualitative studies. *Counterpoints,* 44, 93–123.

Paay, J., Kjeldskov, J., Hansen, K. M., Jørgensen, T., and Overgaard, K. L. (2020). Digital ethnography of home use of digital personal assistants. *Behaviour & Information Technology,* 41(4), 740–758.

Page, M. J., McKenzie, J. E., Bossuyt, P. M. And Boutron, I., (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ,* 372, 71.

Panda, S., Liu, Y., Hancke, G. P., and Qureshi, U. M. (2020). Behavioral acoustic emanations: Attack and verification of PIN entry using keypress sounds. *Sensors,* 20(11), 3015.

Pearce, G., Platten, N. (1998). Achieving personal data protection in the European Union. *Journal of Common Market Studies,* 36(4), 529-547.

Pekerti, A. A., Sasongko, A., and Indrayanto, A. (2024). Secure end-to-end voice communication: A comprehensive review of steganography, modem-based cryptography, and chaotic cryptography techniques. *IEEE Access,* 12, 75146–75168.

Peng, J., Ling, Q. (2020). Byzantine-robust decentralized stochastic optimization. *Proceedings of the 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* 5935–5939.

Petticrew, M., Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide.* (First Edition). Oxford: Blackwell Publishing, 1-26.

Phipps, A., Ouazzane, K., and Vassilev, V. (2022). Securing voice communications using audio steganography. *International Journal of Computer Network and Information Security (IJCNIS),* 14(3), 1–18.

Praetorius, H. A. (2015). The primary cilium as sensor of fluid flow: New building blocks to the model. *American Journal of Physiology-Cell Physiology,* 308(3), 198–208.

Qurashi, J. M., Jambi, K. M., Eassa, F. E., Khemakhem, M., Alsolami, F., and Basuhail, A. A. (2023). Toward attack modeling technique addressing resilience in self-driving cars. *IEEE Access,* 11, 2652-2673.

Rai, V., Mehta, K., Jatin, J., Tiwari, D., and Chaurasia, R. (2020). Automated biometric personal identification: Techniques and applications. *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS),* 1023–1030.

Rajashekar, S. C., Tourani, R., and Gururajan, S. (2020). Secure Communications in Unmanned Aerial System Swarms. Paper presented at the Aiaa Aviation 2020 Forum, Virtual.

Ramati, I. (2024). Algorithmic ventriloquism: The contested state of voice in ai speech generators. *Social Media + Society,* 10(1), 1-10.

Ramati, I., Abeliovich, R. (2022). Use this sound: Networked ventriloquism on Yiddish TikTok. *New Media & Society,* 26(9), 5359-5378.

Ren, Z., Chen, Z., and Xu, S. (2019). Triplet based embedding distance and similarity learning for text-independent speaker verification. *In 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC),* 558-562.

Riadi, I., Imam, R., Umar, R., Busthomi, I., and Muhammad, A. W. (2021). Block-hash of blockchain framework against man-in-the-middle attacks. *Jurnal Ilmiah Teknologi Sistem Informasi,* 8(1), 10.

Rini, R. (2020). Deepfakes and the epistemic backstop. *Philosophers' Imprint,* 20(24), 1–16.

Rivest, R.L, Shamir, A. and Adleman, L. (1978) A method for obtaining digital signatures and public-key cryptosystems. *Communication ACM,* 21, 120-126.

Sandelowski, M., Barroso, J. (2007) *Handbook for synthesizing qualitative research*. (First Edition). New York: Springer Publishing Company, 1-311.

Sasaki, T., Sawada, K., Shin, S., and Hosokawa, S. (2017). Fallback and recovery control system of industrial control system for cybersecurity. *IFAC-PapersOnLine,* 50(1), 15247–15252.

Segal, Y., Hadar, O. (2019). Covert channel cyber-attack over video stream DCT payload: Copyright protection algorithm for video and audio streams. *In Lecture Notes in Computer Science,* 45–56.

Seow, J. W., Lim, M. K., Phan, R. C. W., and Liu, J. K. (2022). A comprehensive overview of deepfake: Generation, detection, datasets, and opportunities. *Neurocomputing,* 513, 351-371.

Sevindi, N. S., Ordu, M. E. (2023). AB ve Türk Hukukunda veri ihlalinin tespiti ve bildirim süresinin karşılaştırmalı değerlendirmesi. *Kişisel Verileri Koruma Dergisi,* 5(1), 12-22.

Shaaban, O. A., Yildirim, R., and Alguttar, A. A. (2023). Audio deepfake approaches. *IEEE Access,* 11, 132652–132682.

Shahrad, M., Mosenia, A., Song, L., Chiang, M., Wentzlaff, D., and Mittal, P. (2018). Acoustic denial of service attacks on hard disk drives. *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security,* 34–39.

Sharma, P., Raglin, A. (2018). Image-audio encoding for ınformation camouflage and ımproving malware pattern analysis. *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA),* 1059-1064.

Sharmila. S. P., Shukla, P. and Chaudhari. N. S. (2022). A distinguished method for network intrusion detection using random initialized Viterbi algorithm in hidden Markov model. *2022 OITS International Conference on Information Technology (OCIT),* 273–277.

Shete, N. L., Maddel, M., and Shaikh, Z. (2024). A comparative analysis of cybersecurity scams: Unveiling the evolution from past to present. *Proceedings of the 2024 IEEE 9th International Conference for Convergence in Technology (I2CT),* 1–8.

Shewale, A., Ladke, A., Raut, A., Tumdam, J., Fating, J., and Nakhate, R. (2023). Data steganography using LSB, XOR & AES algorithm. *2023 4th International Conference for Emerging Technology (INCET),* 1–6.

Shila, D. M., Srivastava K., O'Neill, P., Reddy, K., and Sritapan, V. (2016). A multi-faceted approach to user authentication for mobile devices — Using human movement, usage, and location patterns. *2016 IEEE Symposium on Technologies for Homeland Security (HST),* 1–6.

Shirey, R. (2000). *RFC2828: Internet security glossary.* (First edition). United States: RFC Editor, 13-43.

Siddiqi, M. A., Pak, W., and Siddiqi, M. A. (2022). A Study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences,* 12(12), 6042.

Siddiqui, M. A., Stokes, J. W., Seifert, C., Argyle, E., McCann, R., Neil, J., and Carroll, J. (2019). Detecting cyber attacks using anomaly detection with explanations and expert feedback. *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* 2872–2876.

Singh, S. (1999). *The code book: The science of secrecy from Ancient Egypt to quantum cryptography.* (First Edition). New York: Anchor Books, 1-23.

Skandylas, C., Khakpour, N., and Cámara, J. (2022). *Security countermeasure selection for component-based software-intensive systems.* Paper presented at the 2022 IEEE 22nd International Conference on Software Quality, Reliability and Security (QRS), Guangzhou, China.

Söğüt, E., Oyucu, S., and Erdem, O. A. (2021). Detecting different types of distributed denial of service attacks. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji,* 9(1), 12-25.

Stallings, W. (2017). *Cryptography and network security: Principles and practice.* (Seventh Edition). New York: Prentice Hall Press, 10-15.

Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D., and Fu, K. (2020). Light commands:{Laser-Based} audio injection attacks on {Voice-Controllable} systems. *In 29th USENIX Security Symposium (USENIX Security 20),* 2631-2648.

Suthar, D., Rughani, P. H. (2020). A comprehensive study of VoIP security. *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN),* 812–817.

Thomas, J., Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology,* 8(1), 45.

Tian, H., Qin, J., Huang, Y., Chen, Y., Wang, T., Liu, J., and Cai, Y. (2015). Optimal matrix embedding for voice-over-IP steganography. *Signal Processing,* 117, 33-43.

Tian, Y., Chen, Y., Tang, Y., and Fu, B. (2023). Deepfake algorithm recognition through multi-model fusion based on manifold measure. *In DADA@ IJCAI*, 76-81.

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., and Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion,* 64, 131-148.

Toma, A., Cecchinato, N., Drioli, C., Oliva, G., Ferrin, G., Sechi, G., and Foresti, G. (2022). Onboard audio and video processing for secure detection, localization, and tracking in counter-UAV applications. *Procedia Computer Science,* 205, 20–27.

Tosoni, L. (2020). *Personal data breach, Article 4(12) in The EU General Data Protection Regulation (GDPR): A Commentary.* (Online Edition). New York: Oxford Academic, 100-102.

Tripathi, R., Shukla, M.K., and Kumar, Y. (2021). Intelligent physical access control system through three-stage verification using IoT. *Innovations in Electrical and Electronic Engineering,* 756, 703-712.

Trippel, T., Weisse, O., Xu, W., Honeyman, P., and Fu, K. (2017). WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. *In 2017 IEEE European symposium on security and privacy (EuroS&P),* 3-18.

Truong, N. X., Phuong, P. K., and Tien, V. H. (2021, April). Fast and simple method for weapon target assignment in air defense command and control system. *In International Conference on Industrial Networks and Intelligent Systems,* 403-415.

Ulusal Siber Olaylara Müdahale Merkezi. (2014). *Siber güvenliğe ilişkin temel bilgiler.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu, 3-12.

Uluyol, Ç., Demirci, M. (2022). *Siber güvenlik: Lise (TÜBİTAK Deneyap Kitapları, No. 10).* (Birinci Baskı). Ankara: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, 11-17.

Ural Uslan, Y., Değirmenci, S. (2023). Avrupa Birliği Genel Veri Koruma Tüzüğü ışığında Türkiye'de Kişisel Verileri Koruma Kurumu. *Optimum Ekonomi ve Yönetim Bilimleri Dergisi,* 10(1), 23-38.

Vaccari, C., Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social media+ society,* 6(1), 2056305120903408.

Venkatareddy, D., Ahamad, S. Y. I., Girish, S. V. S., Babu, T. N., and Reddy, K. V. N. (2024). Adaptive intrusion detection in CAN-based vehicular networks using transfer learning for evolving threats. *2024 First International Conference on Innovations in Communications, Electrical and Computer Engineering (ICICEC),* 1–6.

Venkataswamy, N., Imtiaz, M. (2023). *Support vector machine for person classification using the EEG signals.* Paper presented at the 2023 International Conference on Emerging Technologies in Computer Engineering and Technology, Virtual.

Verdoliva, L. (2020). Media forensics and deepfakes: an overview. *IEEE Journal Of Selected Topics In Signal Processing,* 14(5), 910-932.

Vu, H. L., Khaw, K. K., and Chen, T. Y. (2015). A new approach for network vulnerability analysis. *The Computer Journal,* 58(4), 878–891.

Vuagnoux, M., Pasini, S. (2009). Compromising electromagnetic emanations of wired and wireless keyboards. *2019 USENIX Security Symposium,* 1–16.

Vural, M. (2019). *Kriptografi Programlamada Ses Steganorafisi,* Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ, 5-24.

Wang, L., Sun, H., and Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access,* 8, 85094-85115.

Wazid, M., Mishra. A., and Mohd. N., and Das. A. K. (2024). A Secure Deepfake Mitigation Framework. *Cyber Security and Applications.* 2. 100040.

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review,* 9(11): 40-53.

Westerlund, M. (2020). Digitalization, internationalization and scaling of online SMEs. *Technology Innovation Management Review,* 10(4), 48-57.

Wu, F., Ma, Y., and Zhang, Z. (2021). "I found a more attractive deepfaked self": The self-enhancement effect in deepfake video exposure. *Cyberpsychology, Behavior, and Social Networking,* 24(3), 173-181.

Wu, W., Tang, F., Dong, X., and Liu, C. (2015). Different identifications cause different types of voice: A role identity approach to the relations between organizational socialization and voice. *Asia Pacific Journal of Management,* 32, 251-287.

Wu, Z., Guo, J., Zhang, C., and Li, C. (2021). Steganography and steganalysis in voice over IP: A review. *Sensors,* 21(4), 1032.

Xia, Q., Chen, Q., and Xu, S. (2023). Near-ultrasound inaudible trojan (nuit): Exploiting your speaker to attack your microphone. *In 32nd USENIX Security Symposium (USENIX Security 23),* 4589-4606.

Xie, D., Chatterjee, P., Liu, Z., Roy, K., and Kossi, E. (2020). DeepFake detection on publicly available datasets using modified AlexNet. *In 2020 IEEE symposium series on computational intelligence (SSCI),* 1866-1871.

Yan, C., Ji, X., Wang, K., Jiang, Q., Jin, Z., and Xu, W. (2022). A survey on voice assistant security: Attacks and countermeasures. *ACM Computing Surveys,* 55(4), 36.

Yan, Q., Liu, K., Zhou, Q., Guo, H., and Zhang, N. (2020). SurfingAttack: Interactive hidden attack on voice assistants using ultrasonic guided waves. *Proceedings of the 2020 Network and Distributed System Security Symposium (NDSS),* 1-18.

Yan, X. Ji, K. Wang, Q. Jiang, Z. Jin, and W. Xu. (2023). A survey on voice assistant security: Attacks and countermeasures. *ACM Computing Surveys,* 55(4), 1-36.

Yang, T., Hu, Y., Li, Y., Hu, W., and Pan, Q. (2020). A standardized ICS network data processing flow with generative model in anomaly detection. *IEEE Access,* 8, 4255–4264.

Yang, W., Chen, J., Zhang, C., and Paynabar, K. (2022). Online detection of cyber-incidents in additive manufacturing systems via analyzing multimedia signals. *Quality and Reliability Engineering International,* 38(6), 1340–1356.

Yılmaz, S., Sağıroğlu, Ş. (2013). *Siber saldırı hedefleri ve Türkiye'de siber güvenlik stratejisi.* 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansında sunuldu, Ankara.

Yi, Z. L. M., Juremi, J. (2023). Dezvent — Digitalizing attendance system with 2FA and face recognition implementation. *2023 15th International Conference on Developments in eSystems Engineering (DeSE),* 125-130.

Zhang, G., Ji, X., Li, X., Qu, G., and Xu, W. (2021). EarArray: Defending against DolphinAttack via acoustic attenuation. *Proceedings of the 28th Annual Network and Distributed System Security Symposium (NDSS),* 1-14.

Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., and Xu, W. (2017). DolphinAttack: Inaudible voice commands. *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS '17),* 103–117.

Zhang, J., Ni, J., and Xie, H. (2021). DeepFake videos detection using self-supervised decoupling network. *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME),* 1–6.

Zhang, L., Jiang, L., Washington, N., Liu, A. A., Shao, J., Fourney, A., and Findlater, L. (2021). Social media through voice: Synthesized voice qualities and self-presentation. *Proceedings of the ACM on Human-Computer Interaction,* 5(CSCW1), 1-21.

Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., and Qian, F. (2019). Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. *2019 IEEE Symposium on Security and Privacy (SP),* 1381–1396.

Zhang, S., Pan, Y., Liu, Q., Yan, Z., Choo, K.-K. R., and Wang, G. (2024). Backdoor attacks and defenses targeting multi-domain AI models: A comprehensive review. *ACM Computing Surveys,* 57(4), 1–35.

Zhang, T., Ge, S.S. and Lewis, F.L. (2008), Intelligent control and its applications to hard disk drives. *Int. J. Adapt. Control Signal Process.,* 22: 323-324.

Zheng, W., Omote, K. (2021). *Robust detection model for portable execution malware.* Paper presented at the ICC 2021 - IEEE International Conference on Communications, Montreal, Canada.

Zhou, Y., Yang, J., Li, D., Saito, J., Aneja, D., and Kalogerakis, E. (2022). Audio-driven neural gesture reenactment with video motion graphs. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition,* 3418–3428.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: LALE, Bilge
Uyruğu	: T.C.
Doğum tarihi ve yeri	:
Medeni hali	:
Telefon	:
Faks	:
e-mail	:

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Adli Bilişim (tezli)	Devam ediyor
Lisans	Anadolu Üniversitesi / Siyaset Bilimi ve Kamu Yönetimi	Devam ediyor
Lisans	Hacettepe Üniversitesi / Hukuk Fakültesi	2020
Lise	Özel Balgat Uğur Anadolu Lisesi	2016
Lise	Ayrancı Anadolu Lisesi	2015

İş Deneyimi

Yıl	Yer	Görev
2021 - Halen	Ankara Barosu	Avukat
2020 - 2021	Ankara Barosu	Stajyer Avukat

Yabancı Dil

İngilizce, YDS 2023: 90 Puan.

Yayınlar

Yalçın, N., & Lale, B. (2025). Types of cyber-attacks with using voice. *JSR-A,* 61, 137–165.

Yalçın, N., & Lale, B. (2025). Vocal threats in the digital age: Analysis of voice-based cyber-attacks. *International Research Journal of Modernization in Engineering, Technology and Science,* 7(5), 2840–2849.

GAZİLİ OLMAK AYRICALIKTIR.