Check for updates

Original Paper

MEASUREMENT AND CONTROL

Measurement and Control
2019, Vol. 52(5-6) 338–353
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0020294019837991
journals.sagepub.com/home/mac
SAGE

Assessing risks and threats with layered approach to Internet of Things security

Murat Aydos[1], Yılmaz Vural[2] and Adem Tekerek[3]

Abstract

Internet of Things is the next-generation Internet network created by intelligent objects with software and sensors, employed in a wide range of fields such as automotive, construction, health, textile, education and transportation. With the advent of Industry 4.0, Internet of Things has been started to be used and it has led to the emergence of innovative business models. The processing and production capabilities of Internet of Things objects in hidden and critical data provide great advantages for the next generation of Internet. However, the integrated features of Internet of Things objects cause vulnerabilities in terms of security, making them the target of cyber threats. In this study, a security model which offers an integrated risk-based Internet of Things security approach for the Internet of Things vulnerabilities while providing detailed information about Internet of Things and the types of attacks targeting Internet of Things is proposed. In addition, in this study, the vulnerabilities of Internet of Things were explained by classifying attack types threatening the physical layer, network layer, data processing layer and application layer. Moreover, the risk-based security model has been proposed by examining the vulnerabilities and threats of smart objects that generate the Internet of Things. The proposed Internet of Things model is a holistic security model that separately evaluates the Internet of Things layers against vulnerabilities and threats based on the risk-level approach.

Keywords

Internet of things, information security, threats, vulnerabilities, security model

Date received: 3 January 2019; accepted: 23 February 2019

Introduction

Technological advances have been an important factor that increase the productivity and efficiency by determining the direction of industrial development and have led to significant industrial revolutions until today.[1] As of 1765, the first phase of industrialization has begun with the invention of steam engines and steam-powered machines were used in production. In the second stage of industrialization, mass production has started along with the use of production of electricity and the utilization of electricity, oil and chemicals in production processes.[2,3]

In the third stage of industrialization, electronic and computer systems have been integrated into the industry via programmable logic circuits (PLCs) to automate the production processes. In this phase, the transition from the industrial society to the information society has emerged and the automation of electronics, information and communication has been provided. In this period, technologies such as computer, microelectronics, telecommunication, fiber optics and laser in line with the sciences such as nuclear, biotreatment and biogenetics have shaped the direction of the industrial production.[4,5]

As of today, with the beginning of the fourth stage of industrialization called "Industry 4.0," new technologies such as smart robots, health, big data, Internet of Things (IoT), three-dimensional (3D) printers, cloud computing and renewable energy have appeared.[6–9] Furthermore, in addition to automation, Industry 4.0 has defined objects that work collaboratively with each other.[10] Likewise, through the sensors of objects, light, image, heat, sound, position, humidity, pressure,

[1]Department of Computer Engineering and Institute of Informatics, Hacettepe University, Ankara, Turkey
[2]Department of Computer Engineering, Hacettepe University, Ankara, Turkey
[3]Gazi University, Information Technology Department, Ankara, Turkey

Corresponding author:
Adem Tekerek, Gazi University, Information Technology Department, 06560, Ankara, Turkey.
Email: atekerek@gazi.edu.tr

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (http://www.creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).

proximity, seismic and different types of large volumes of real-world data are collected. Moreover, with the processing of the collected data, real-time communication between objects is ensured and a fast, flexible, human-independent, high-quality and more efficient production process is provided.[11]

Cyber-physical systems, the industrial application of IoT, enable the control of a physical environment with cyber infrastructures.[12] The concept of Industrial IoT, which emerged with the creation of cyber-physical systems, has enabled human-free industrial processes by providing machine-to-machine (M2M) communication.[13] Moreover, the machines that communicate in real time via sensors in IoT platforms enable the optimization of industrial production processes using resources efficiently and effectively.[14–16]

On the IoT platforms, providing cyber security is critical in human-free decision-making processes, independent of human, by means of communication between machines.[17] As a result, given the heterogeneous nature of IoT with different types of objects, its operation in distributed architecture and misuse of objects and constraints (energy, computation, etc.), it is a difficult problem to ensure a high level of security in IoT platforms.[18]

With the expansion of IoT, the quality and quantity of cyber-attacks affecting the industry is increasing day by day and the cyber-attacks are directly affecting every aspect of the industry. Significant violations by sector on IoT platforms are summarized as follows:

- *Nuclear facilities*. A total of 19 cyber-attacks were carried out between 2010 and 2014 to the National Nuclear Security Authority, the institution responsible for managing and ensuring the security of US nuclear weapon stocks.
- *Steel factories*. The German Federal Information Security Authority has issued a report of numerous cyber security violations, including the components of a steel mill's production network.
- *Energy network*. According to the report of the Congress Research Service (CRS) in June 2015, attacks on the US electricity grid system are increasing. Attackers are developing malware to infiltrate critical systems and endanger electrical networks. The attackers conducted more than 150 attacks between 2010 and 2014 to the US Department of Energy systems.
- *Health*. As a result of the attack on the hospital network of the University of California, Los Angeles in 2017, leakage was detected to computer systems containing sensitive data of 4.5 million people.
- *Infrastructure*. The Department of Homeland Security announced in 2012 that hackers infiltrate a government agency's thermostats and a production facility in New Jersey. In addition, Internet-connected industrial heating systems have been exploited using security vulnerabilities.
- *Oil wells*. According to the Reuters 2014 report, hackers have disabled a floating oil drilling rig. Another oil tower was damaged by a malware, and it took 19 days to re-launch the oil tower.

On the other hand, important challenges in ensuring the safety of IoT are given as follows:

- Increasing number and variety of intelligent objects in IoT platforms;
- Lack of security policies and procedures to manage security on IoT platforms;
- Managing security patches for critical software on IoT platforms;
- Increased diversity and number of attacks on IoT platforms.

In this study, we describe IoT-specific vulnerabilities and their features by investigating related security weaknesses and threats. Rest of this paper has been organized as follows. Section "IoT" provides detailed information about IoT. In section "Threats and vulnerabilities," threats and vulnerabilities of IoT are detailed. In section "A risk-based layered approach to IoT security assessment," a risk-based IoT security model is presented. In section "Conclusion," the conclusion of the study is given.

IoT

IoT is a large network of interconnected objects over the Internet, which has been rapidly evolving in recent years.[19] The concept of IoT was first used by Kevin Ashton in 1999. It should be mentioned that Ashton has used this concept while describing the benefits of the Internet-based information service architecture that uses radio-frequency identification (RFID) technology in the supply chain of Procter & Gamble (P&G).[20,21]

Today, the IoT is seen as a new-generation network that has advanced enough to establish the connection between the real world and the virtual world. Figure 1 visualizes the use of many IoT applications for the use of people, vehicles, houses, cities, trade and industry. As is seen, computers, smartphones, smart sockets, school services, smart grids, smart health, smart office and wearable materials are some of the IoT applications.

The common feature of IoT applications is that the data collected from intelligent objects with embedded sensors are gathered and used over the network. IoT applications are increasing day by day, expanding the usage areas and making human life easier (Figure 2). In fact, a huge amount of personalized data collected by convenient IoT applications covering smart cities,

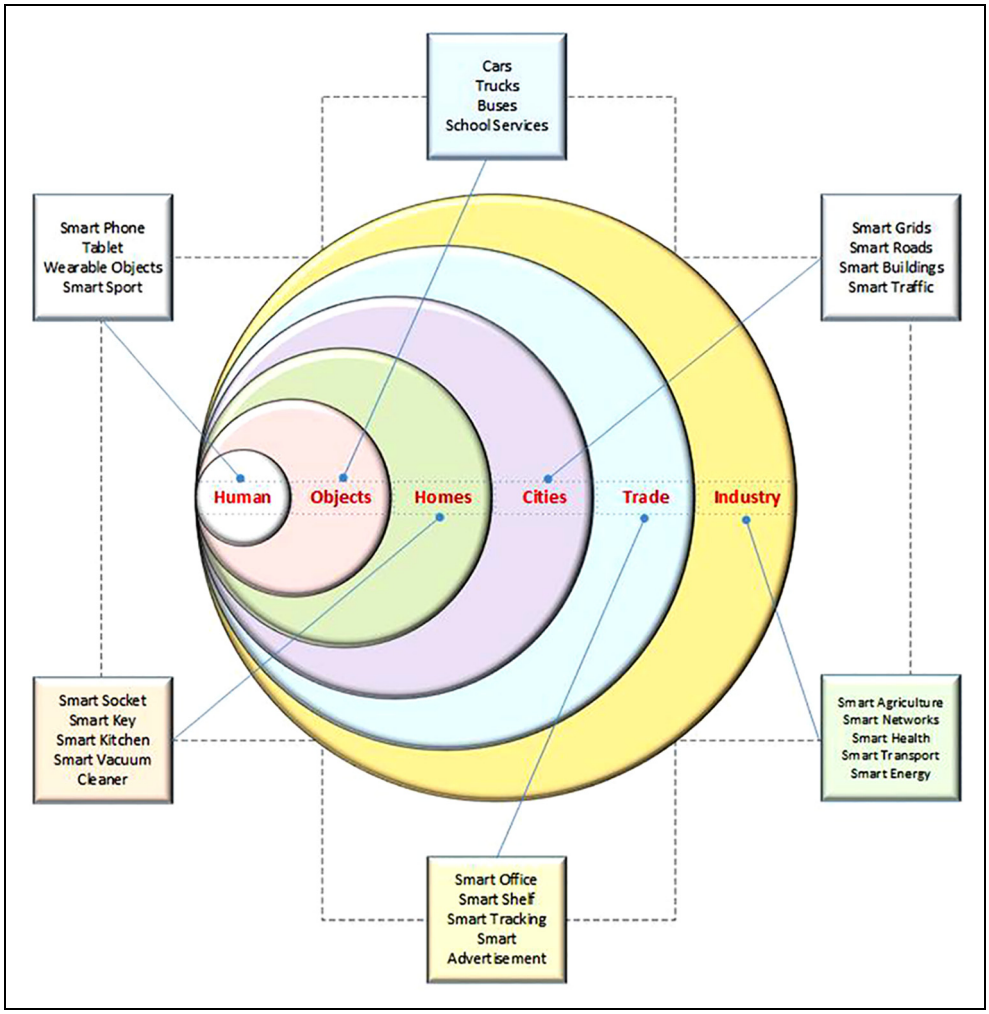


Figure 1. IoT applications.

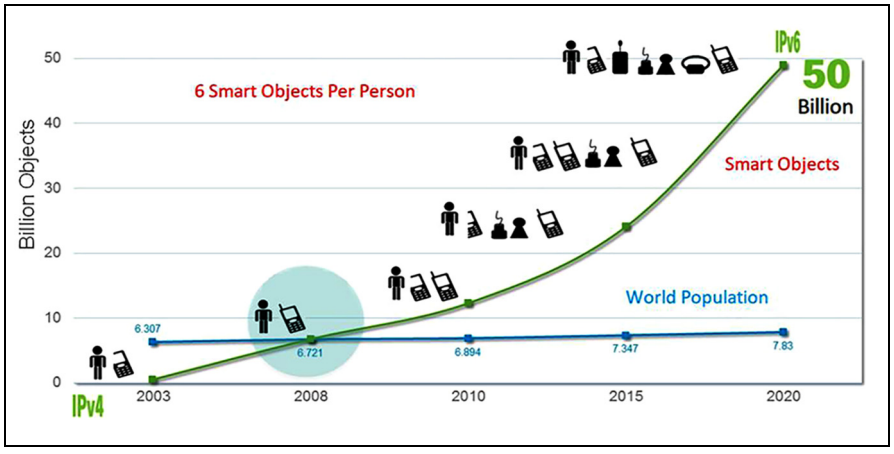


Figure 2. IoT growth chart by years.

smart environments, smart metering, security and emergency, retail sales, logistics, smart farming, smart livestock and smart health are being shared and analyzed.[22]

According to Cisco's research shown in Figure 3, approximately 50 billion devices are expected to be connected to the Internet as of 2020.[23] Considering that the United Nations' world population is estimated to be 7.7 billion[24] in 2020, it is estimated that each person on earth will have approximately six electronic devices. In addition, it is estimated that in 2020 smart devices will be brought into daily life because of their communication ability with each other and their environment. At this point, it is being forecasted that the tendency to

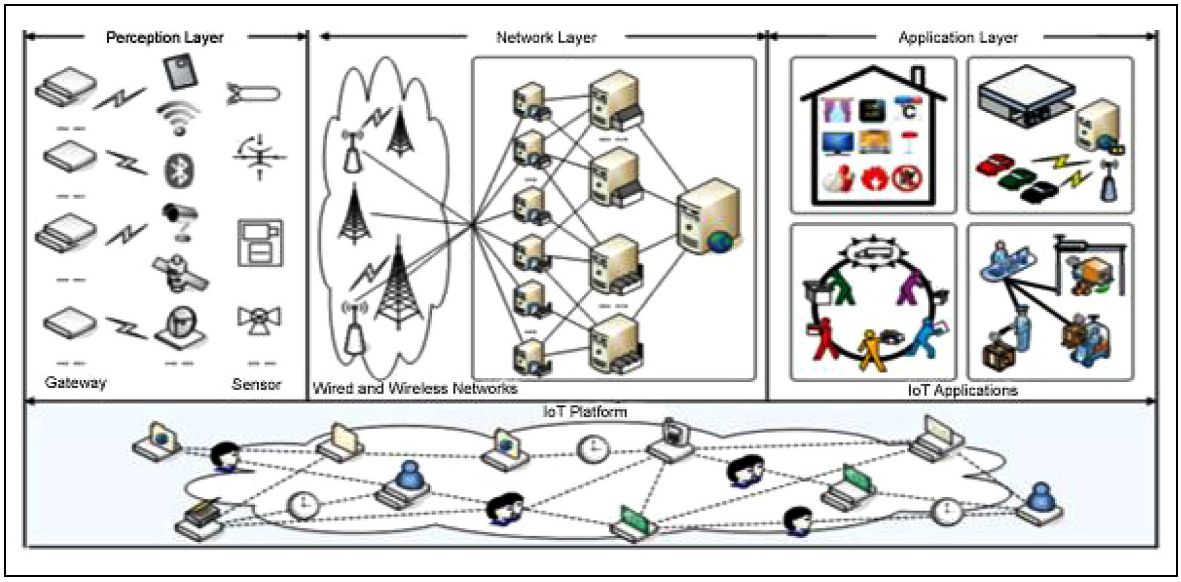


Figure 3. IoT platform.

personalize with IoT platforms will peak and the world will experience a constant change after this stage.

The personalization trend created using the collected data as a result of the widespread use of IoT platforms has an important place. Data collected through IoT applications can be shared outside of applications, for different purposes such as advertising, marketing, statistics and commercial, without the permit of users.

As a result, these incidents in IoT make it necessary to take new measures by increasing security concerns.[25] Regarding the features of IoT, such as having inherently composed of diverse types of devices, generating big data, serving M2M interaction and providing limited computational and operational power constitute challenges against solutions of the security problems.[26]

IoT includes not only collection and employment of data, but also covers inferring enabled intelligent systems that can decide and apply via large data analysis methods by utilizing human-independent M2M interaction when required.[27] Nonetheless, IoT-specific behaviors such as the increasing personalization of IoT platforms and the exclusion of M2M interaction from human control bring increasing demands on security protection.[28,29] Misuse of sensors or devices that can communicate directly with each other through M2M interaction without human intervention, the shortcomings of conventional security methods to meet IoT security requirements and the fact that IoT devices can be ubiquitously found anywhere without space limit have made the issue an NP-hard problem. The IoT platform is presented in Figure 3.

The IoT consists of three basic layers, as shown in Figure 4, including the perception layer, the network layer and the application layer.[30] On the other hand, the architecture shown in Figure 5 is a general reference model that can be applied to different application

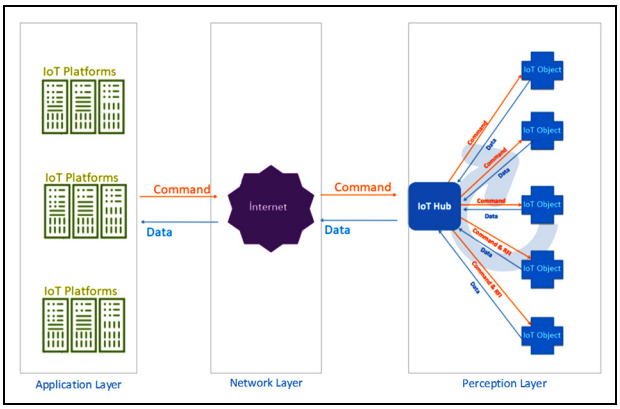


Figure 4. IoT reference model.

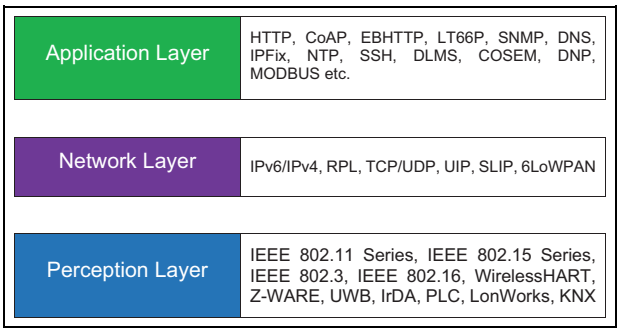


Figure 5. IoT protocols.

platforms including all components involved in data collection, sharing and processing.[31]

An overview of architecture and protocols

The architecture shown in Figure 4 is a general reference model that can be applied to different IoT

application platforms including all components involved in the process of data collection, sharing and processing.[31]

The reference model is described below in terms of the layers it is composed of which are given as follows:

Perception layer. It is the layer in which data are produced and collected through devices that can be directly communicated. This layer is examined in two object classes such as (1) IoT devices that detect in itself and (2) IoT hub nodes acting as gateways.[32] The data are acquired through the detection nodes, while the gateway nodes are used for transmitting and checking the obtained data.[18]

Network layer. It is the layer of communication between IoT objects and IoT application servers that provide wired or wireless communication. It is also used in protocols in which network security measures are taken. This layer creates the IoT gateway, processes the data coming from the detection layer and transmits them to a higher layer.[33]

Application layer. It is a presentation and service layer where the data collected by the devices are employed, understood and shared as well as their results can be observed.[34] The application layer can be configured in different ways according to the service provided.

The IoT protocols according to the layers are shown in Figure 5 and summarized in the following items:

IoT detection protocols. Regarding the used wireless communication protocols for sensors and objects in the IoT detection layer, IEEE 802.11 series, 802.15 series, HART (Highway Addressable Remote Transducer) and so on are employed.[34] While the IEEE 802.15.4 standard includes the long-range wireless personal area network (LR-WPAN), ZigBee, Wireless HART protocols based on IEEE802.15.4 are included in this layer.[35]

IoT network layer protocols. IPv6/IPv4, Transmission Control Protocol (TCP)/User Datagram Protocol (UDP), micro IP (UIP), Serial Line Interface Protocol (SLIP) and 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) protocols are used in the network layer. As the TCP is more costly compared to the UDP, mostly UDP is selected in IoT applications.[36]

Moreover, IoT application layer protocols use HTTP to provide web service to end users in application layers. However, since the IoT platform has HTTP high computational complexity, low data rate and high energy consumption, it is not preferred to use HTTP as it is. Therefore, IoT-specific web-based light protocols such as IETF (Internet Engineering Task Force), CoAP (Constrained Application Protocol), Embedded Binary HTTP (EBHTTP) and Lean Transfer Protocol (LTP) are used.[36] The CoAP is an important IoT-specific web protocol that has been developed to be used on restricted nodes and constrained networks (low power, low loss).[37] EBHTTP is a binary-formatted, field-efficient, stateless derivative of the standard HTTP/1.1 protocol.[38] Besides, EBHTTP has been primarily designed to transport small data between resource-restricted nodes. On the other hand, LTP is a lightweight web service migration protocol that enables transparent exchange of web service messages between any resource-restricted devices and server or personal computer systems.[39]

Security in IoT

Transport Layer Security (TLS) and its predecessor Secure Socket Layer (SSL) protocols are used to securely communicate by encrypting IoT data transmitted over problematic computer networks having no resource and energy shortages.[40] Meanwhile, in protocols that provide security on the transport layer, authentication is handled via symmetric key distributed by asymmetric encryption with X.509 certificates. DTLS (Datagram Transport Layer Security) protocol has been developed to provide three main principles of security, such as UDP-based integrity, authentication and privacy, to enable the TLS protocol to work more efficiently in slow and problematic networks such as IoT.[41]

The location of the DTLS protocol in the IoT architecture is shown in Figure 6. As shown in Figure 6, the DTLS protocol running between the application and the network layer is an important protocol that provides end-to-end transfer security. It should be noted that, in the absence of end-to-end protection, it will be possible to gain unauthorized access and misuse of data through an object seized by the attacker.

The ability of the DTLS protocol to operate in limited environments also prevents the performance-

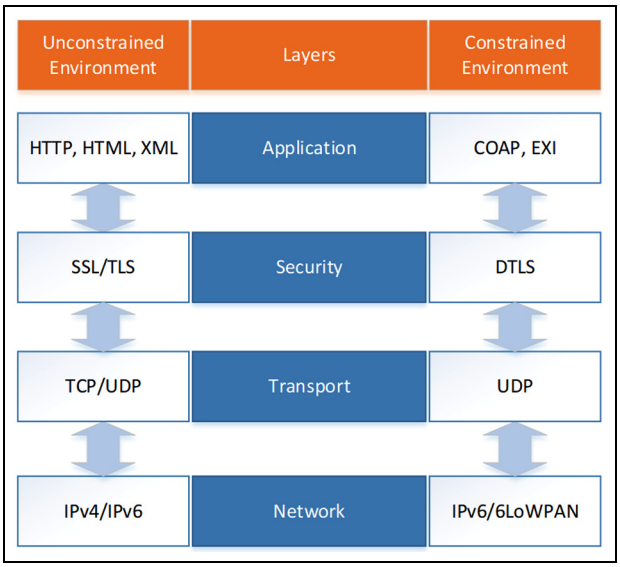


Figure 6. Position of DTLS in protocol stack.

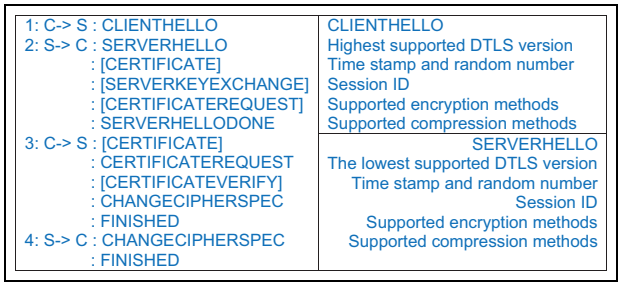


Figure 7. The process of DTLS handshaking.

related problems in IoT environments. DTLS consists of two layers: registration protocol and handshake. The data are shared with the client and server using the handshake protocol, while the data are encrypted with symmetric encryption keys with the registration protocol. The process of mutual authentication between the parties that will communicate with each other is handled via the exchange of the encryption algorithm and keys.[42] In Figure 7, the process of DTLS handshaking is presented.

The registration protocol protects application data using keys created during handshake.[43] DTLS partitions, compresses and encrypts each outgoing message in order to generate the message verification code. Similarly, for the incoming messages, it combines, decompresses and decrypts in order to verify the message.

Another important security element in ensuring IoT security is the access control. Access control mechanisms should be used to manage permissions on the use of network resources of data owners and data sharing agents on a large IoT network.

Threats and vulnerabilities

IoT data collected by connecting heterogeneous objects with different communication features in wired and wireless environments are generally processed via transferring to the cloud computing environment. Thus, in order to ensure the high level of information security in the process from the collection of IoT data to processing, it is necessary to take precautions by knowing the threats and weaknesses in IoT environments.

As is known, IoT is a large platform that involves intelligent objects, sensors, software interfaces and mobile applications. Nevertheless, communication and data processing infrastructures on IoT platforms bring security vulnerabilities and threats while accelerating business processes. Unlike traditional security approaches, new security solutions that take into account IoT constraints and architecture should be created in order to prevent any security breaches that could affect the entire IoT platform. An end-to-end security architecture should be designed and implemented in the IoT, which has a large number of attack interfaces, taking all of the IoT security requirements related to physical environments, objects, sensors and communications into account.[17,44]

Attacks on IoT platforms are classified as physical, network, data processing and application attacks and instances of IoT attacks according to the layers are given as follows:

- Physical layer attacks—jamming, denial-of-service and tampering;
- Network layer attacks—man-in-the-middle (MITM), exhaustion, collision and spoofing;
- Data processing layer attacks—malware, collision and unfairness attacks;
- Application layer attacks—Trojans, viruses, malicious code injection and social engineering–based attacks.

As shown in Figure 8, internal and external attacks threaten the layers of IoT such as physical, network, data and application. The details of the suggested layered threat approach presented in Figure 8 are described in the following subsections.

Location of attack

Attacks on IoT platforms are carried out in two different locations such as internal and external. The internal attacks made by the users or objects classified as

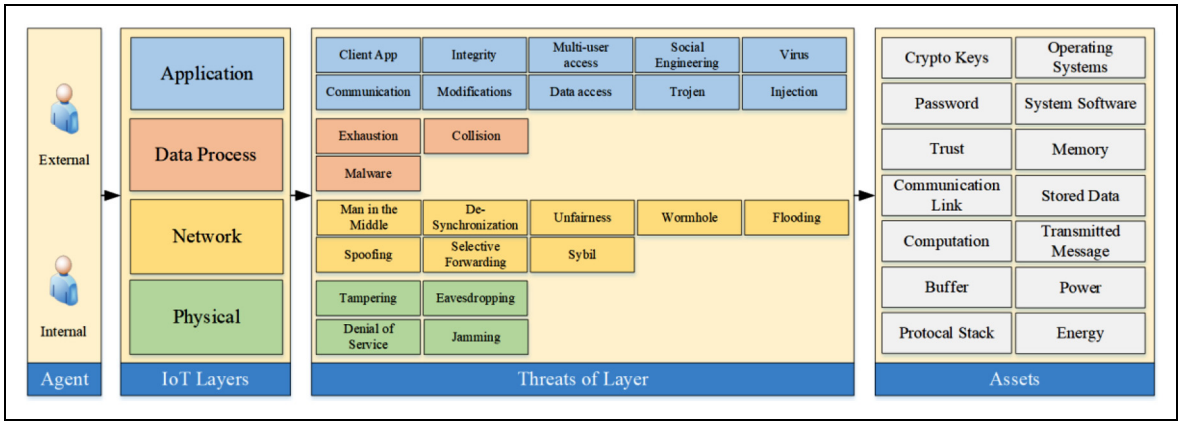


Figure 8. Threat classification according to IoT layers.

"trusted" due to having access privileges within the platform significantly affect all the layers of IoT. Similar to the internal ones, external attacks by users or objects that exist outside the platform and having no special access privileges also affect all layers of IoT platforms. Nonetheless, the impact of internal attacks on IoT may be more severe since the internal attacks are less controlled than attacks from outside the network. While external attacks can be prevented by network firewall, intrusion detection and attack prevention systems, internal attacks can reach their goal without going through any security tool or mechanism. Thus, attacks within the network are more likely to be successful.

Physical layer

The physical layer of IoT platforms is the layer where objects, sensors and actuators take place in data generation. Moreover, the physical layer of IoT is targeted by attacks such as tampering, eavesdropping, denial of service (DoS) and jamming. Besides, the most vulnerable interface of IoT platforms is the sensors since they can easily be exploited as they are the devices which collect data directly. Yet, in most of the cases, sensors are directly targeted by attacks of tampering and jamming.

Tampering. In the type of attacks which are called tampering, the hardware or software features of IoT objects are modified by the attackers via physical or cyber methods. Furthermore, with the attacks of tampering targeting the physical layer, attackers can violate fundamental security policies such as privacy, availability and integrity by providing direct access to all IoT objects.[45] Tampering targets the integrity of IoT systems.

Jamming. By definition, jamming is the type of attack in which the data integrity is damaged by interfering the network traffic during the communication of the sender and receiver objects. In jamming attacks, positioned between the sender and the receiver, the jammer transmits a high-power signal across the sensitive band range in order to disrupt the communication medium between the objects and violate fundamental security principles such as integrity and accessibility. Jamming is one of the most dangerous types of attacks used to block the IoT network and data exchange between IoT objects communicating wirelessly. This situation is visualized in Figure 9. The "hs" signal sent to the IoT objects by the source is also received by the reactive jammer. Nevertheless, the jammer disturbs traffic by emitting the "hj" signal and suppressing the receiver sensors of the IoT objects.[46,47] Jamming targets the accessibility of IoT systems.

Eavesdropping. Eavesdropping is a technique that is used to access and retrieve the communication traffic

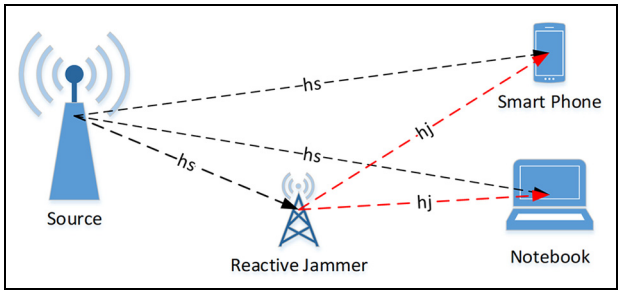


Figure 9. Jamming attack.

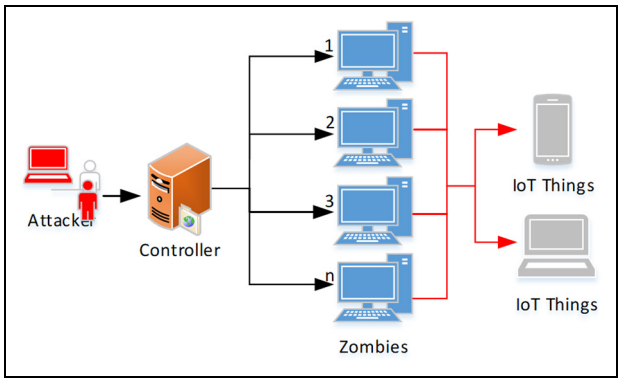


Figure 10. Denial of service attack.

between IoT objects. Encryption methods are applied in order to eliminate the threat that occurs as a result of eavesdropping. Meanwhile, IoT sensors are generally simply designed and low-energy-consuming end devices. Due to the limited functionality of the IoT sensors, security measures such as encryption are made on the hardware. It should be noted that, in eavesdropping, a passive listening attack is made when the communication packet is not changed and the sender does not get any feedback. This method has been named as "replay attack."[48,49] Eavesdropping targets the confidentiality of IoT systems.

DoS. DoS attacks are being made to disrupt the services of IoT platforms. In detail, the communication network between IoT objects is blocked resulting in being non-communicating. The use of IoT in many areas, heterogeneous structure, resource constraints and the multitude of objects in the network make it difficult to get protected from DoS attacks. The security of IoT objects' communication can be ensured by end-to-end or point-to-point encryption techniques.[50] However, IoT has a weakness against attacks that disrupt its functioning, occupy resources and consume the energy of devices. The most important type of attack affected by such weaknesses is the DoS attacks. Likewise, DoS attacks can target all of the physical, data link, network, transmission and application layers of TCP/IP. Moreover, any weakness in TCP/IP—the main Internet Protocol (IP)—also threatens IoT. As

shown in Figure 10, the attacker gets control of the target system by sending a continuous data request to the target IoT platform from different locations using the computers he has converted to "zombie."[51,52] DoS targets the accessibility of IoT systems.

Network layer

Network attacks on IoT platforms, where real-time data collection and data processing are carried out, have very serious consequences. The network layer on the IoT platform is the target of various cyber-attacks such as in information systems. Some of the IoT attacks were listed and explained below.

MITM. The MITM attack is a type of attack to capture, read and modify data between two communicating objects on the IoT platform.[53] Data packets that do not communicate between objects in the network can be captured by all objects connected to the same network. Furthermore, network objects can intervene and read the contents if desired. Thus, the goal of the MITM attacks is to change the data content by capturing and replacing the data packets on the IoT platform via sabotaging the traffic. What is worse is that IoT can have a lot of neglected, open and uncontrolled objects. These objects, for which security has been compromised in IoT networks, have the potential to be the source of MITM attack traffic. Figure 11 shows the MITM attack process.[53,54]

Note that the complete elimination of MITM attacks is very challenging and can only be reduced with a good security policy. IoT devices are manufactured for specific purposes and therefore their safety can also be provided according to certain policies. In addition, however, the number and diversity of IoT objects make it difficult to provide the IoT security. This situation causes security weaknesses in the IoT and MITM attacks start threatening IoT.[55,56]

Spoofing. Data on IoT platforms are usually encrypted through the network traffic and data packets carried via the routing protocol are transmitted by the IP address. Attackers can emulate, modify or resend IP addresses or transport protocol information (UDP, TCP ports, etc.) to poison network traffic. In order to create spoofing attacks, it is possible to generate routing nodes, extended or shortened transmission paths and false error messages.[25,52] Figure 12 shows a spoofing attack. Spoofing targets the integrity of IoT systems.

Desynchronization. The desynchronization attack is a wireless communication attack. On IoT platforms, objects mostly communicate using wireless communication. The way the attackers apply is to make the communication desynchronized via interfering with the communication parameters of the objects which

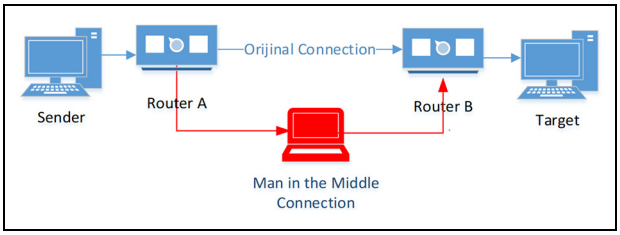


Figure 11. MITM attack.

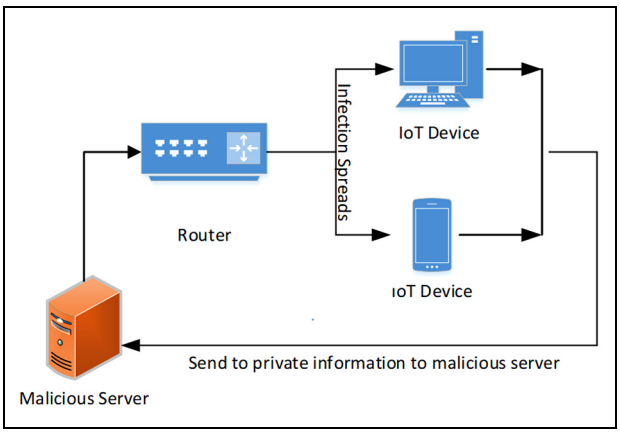


Figure 12. Flowchart of an example spoofing attack.

initially communicate synchronously. As a result, desynchronizing the traffic of the objects communicating synchronously causes network traffic not to work properly.[57,58]

Selective forwarding. The IoT consists of intelligent and multiple objects that require multiple routing for communication between objects. Moreover, in IoT networks, a node seized by an attacker can change network traffic by reducing some data packets and redirecting to different locations. Thus, the data that should reach its target may be missing or corrupted.[59]

Unfairness. Unfairness is a repeated collision attack that can also be referred to as exhaustion-based attacks. Data link layer–based attacks usually aim to disrupt the equal load sharing mechanisms of wireless sensor networks (WSNs). This method of attack may cause takedown of a service, and if the number of nodes increases, the impact of the attack gets spread.[60]

Wormhole. By definition, a wormhole is a maliciously crafted and low-latency link where the attacker can replicate messages. In a wormhole attack, the attacker sends packets at a point in the network to another point on the network through the tunnel and then sends them back to the network from there.[18]

Sybil. Sybil attacks are performed using network objects or devices with multiple IDs in order to generate multi-

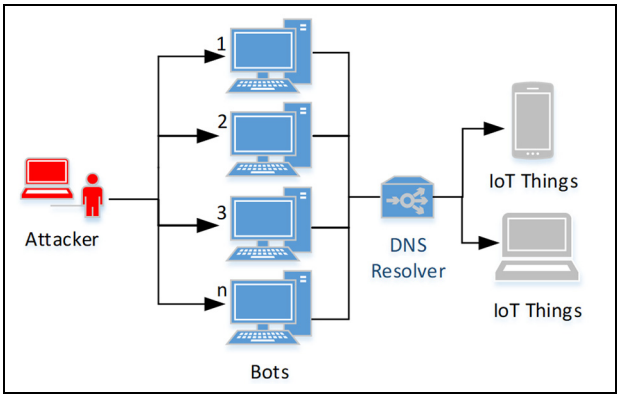


Figure 13. A schematic illustration of a flooding attack.

source and distributed network traffic. Furthermore, Sybil attacks sabotage equal resource usage of IoT platforms. Although malicious nodes are fake, they act as real nodes, producing extra and unnecessary network traffic. In this way, resource consumption of the network increases and causes the network with limited resources to be halted. Sybil attackers manipulate fake abuse pseudo-identities to compromise the effectiveness of the IoT.[61]

Flooding. Flooding attacks are one of the most common types of attacks to disable all or part of the IoT network. Flooding attacks can reduce the speed of traffic flowing between objects on the IoT platform and are capable of stopping the network via occupying the hub or node's resources. In flooding attacks, network traffic is reduced or stopped completely by occupying Domain Name System (DNS) connections of IoT objects.[62] Figure 13 shows a flooding attack. Flooding targets the accessibility of systems.

DNS flooding attacks directly affect DNS servers using high bandwidth connections of IoT devices. The volume of requests from IoT devices disrupts the services of the DNS service provider and prevents real users from accessing their DNS servers.[63]

Data processing layer

The data collected using sensors in IoT are generally processed in cloud systems and this process generates the data processing layer. Attacks on the data processing layer are performed using malware that is embedded in data from edge nodes or sensors.

Exhaustion. Exhaustion attacks aim to interrupt the data processing of the IoT infrastructure. There is no high risk for this kind of attacks since these attacks occur in a higher layer and the ecosystem of the IoT is distributed. It should also be noted that, in cloud-based systems, it is much easier to implement protective measures against the exhaustion attacks.[25]

Malware. It is the general name of malware that threatens IoT infrastructures such as viruses and Trojan horses. Malware can penetrate information systems as a plug-in of software, or it can infiltrate computers from the website. Malware is a malicious software which is injected into the data of IoT platforms in order to grant access for seized cloud or distributed systems. Furthermore, malware-based attacks are difficult to detect and prevent. Therefore, it is not enough to have a strong firewall, rather it is also necessary to take protective measures before the data processing stage.[64]

Collision. Collision is a jam-type attack since it targets the data transfer and data link layers on IoT. Even if the data traffic is not completely stopped in such attacks, it may be intended to make the network unusable.[18]

Application layer

The application layer is the layer where end users communicate with the IoT platform directly. Application layer is employed for several tasks including report generation, querying, analysis and visualization of the data, authentication and interaction with IoT. On IoT platforms, methods such as authentication and restriction of data access can be used to provide security to the application layer. A large amount of data are continuously generated in IoT environments, which also makes it difficult to store such amounts of data. Therefore, it is also difficult to secure the application layer.

Client application. The application layer is the layer where people or machines communicate directly with IoT platforms. At this point, the human–machine interface (HMI) is used for this communication. The HMI facilitates the use of IoT platforms in the application layer while also constituting weaknesses against cyber-attacks. It should be noted that the most common threats in this field are related to the vulnerabilities of web environments. Likewise, in order to access IoT system configurations, devices use the HTTP, which is also important in web application security. In fact, malicious software can infiltrate the IoT system via client-side vulnerabilities. Such attacks, instead of directly damaging the system, remain in the passive mode and cause faulty production on the outputs of the system. In order to filter out such applications in IoT, malware detection and antivirus solutions should be used. In addition, the IoT client application status, operating system status or hardware status should not depend on the state of the other parts of the IoT system. The status (e.g. active, sleep, failure) should not have any negative impact on the layers such as data processing, network or physical.[65,66]

Communication. In order to weaken the IoT platforms, it is necessary to be able to enter the configuration interface or the communication channel. Applications

allowing remote configuration of the IoT system, including the physical layer, provide remote access to systems that they normally configure.

System integrity. System integrity is an important feature of IoT systems and the disruption of the integrity on IoT platforms leads to security risks and threats. The system must continue to operate during high workload or abnormal work processes without compromising system integrity. Besides, in order to test the integrity of the IoT platform, a complex and reliable stress test should be performed.

Modifications. It is also possible to observe security weaknesses due to changes in IoT platforms, such as environmental, systemic and configuration changes. As IoT platforms grow, weaknesses due to system changes may lead to greater problems and impacts. The security vulnerabilities caused by the changes can be minimized by thorough verification of system elements, complex tests and continuous system monitoring.

Multi-user access. IoT platforms must have multi-user access and adequate security level. Furthermore, when the configurations of the IoT system partitions are changed by users, the simultaneous modification of the configuration files and the simultaneous operation of configuration changes can cause conflicts of updates. As a result, a careful process should be planned for multi-user systems.

Data access. Data access security measures should be seriously considered in the application layer. Data access security measures should be rearranged in case of system status change with the update and configuration change made on IoT platforms.

Social engineering. Social engineering, in essence, is the act of capturing and manipulating people's confidential information. The kinds of information that the attacker wants to gather vary according to purpose, and they can often apply deception methods to collect people's passwords or confidential information such as banking information. Social engineering attacks can be done via e-mail/website or by one-on-one interview with the victim.

The threat area of social engineering is expanding since the IoT environments involve social engineering tools such as industrial control systems and smart industrial objects. Thus, it can be deduced that the impacts of social engineering go beyond the cyber environment and eventually physical damages come true. Some of these impacts were listed as follows:

- Deactivation and damage to production facilities;
- Death and injury due to deterioration of signaling of transportation systems such as trains and trams;
- Damage to water treatment plants;
- Damage to nuclear power plants.

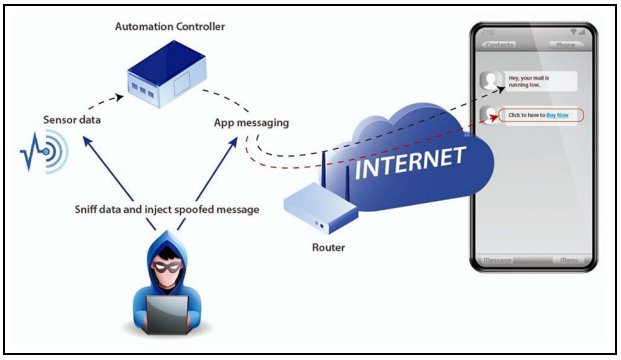


Figure 14. Flowchart of a fake message–based attack to a smart IoT system.

Cyber events in cyber environments such as computers will now be seen in physical environments such as an automobile's control panel, intelligent heating systems or medical systems. Attackers do not need to have direct access to attack physical cyber systems, rather they can access the distributed structures of the system instead of direct access and manipulate the entire industrial infrastructure. This manipulation is achieved by seizing the sensor nodes, where the objects are connected to each other via the broadband router in an unencrypted fashion. Figure 14 shows a manipulation on a smart IoT system using the deception method.

It is a well-known fact that social engineering attacks and exploitation against IoT's smart objects are observed. For instance, from December 2013 to January 2014, 100,000 e-mails per day were identified as IoT targeting cyber-attacks which aim at firms and individuals. Furthermore, in industrial environments, IoT botnets carry out cyber-attack using a network connection to all intelligent objects.[66,67]

A risk-based layered approach to IoT security assessment

On IoT platforms, it is essential to ensure high level of security in order to stay secured against various unwanted cases such as unauthorized usage, modification and disclosure of data. Moreover, security vulnerabilities occur when IoT platforms fail to provide any of the three fundamental security elements known as "privacy,""integrity" and "accessibility." In order to ensure a high level of security of IoT platforms consisting of sensors and intelligent objects, a new approach with four layers has been proposed to determine the threats and weaknesses according to the layers and to take countermeasures based on three fundamental elements of security according to the risk-based

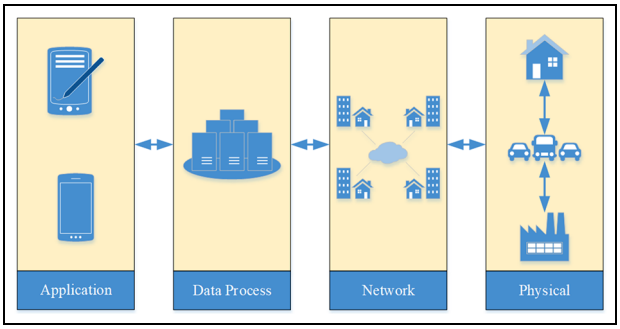


Figure 15. Layered IoT architecture.

assessments. With the layered IoT security approach, it is aimed to minimize or prevent the impact of security attacks via risk assessments.

The risk-based layered security approach is based on the following four stages:

- Securing the layers;
- Understanding and evaluating layered threats;
- Measuring the likelihood of layered threats;
- Determination of layered risk by combining the probability and impact of the layered threat.

Following the risk assessment, a high level of protection is ensured by taking security measures in accordance with its own risk level on each layer.

Securing the layers

The four-tier IoT architecture based on the risk-based layered IoT security approach is shown in Figure 15.

Physical layer, known as the sensor layer, can be summarized as the sensory organs of the IoT platforms, where the data are collected and the objects are detected. In this layer, RFID labels, barcode, Bluetooth, wireless sensors and protocols such as LTE (long-term evolution), ZigBee and NFC (near-field communication) are employed for different types of sensors. With the proposed approach, the source of information obtained as a security measure should be authenticated in this layer. Besides, each object in the physical layer has the responsibility for ensuring the IoT security. In order to authenticate IoT platforms, the public key infrastructure (PKI) is employed. Furthermore, the PKI infrastructure is assumed in such a way that it consists of tree structured nodes. The most appropriate node having no computation and energy constraint is selected as the root node in the mentioned tree structure. While the public key is stored on the root node, private keys are distributed to each node by the root node via key exchange protocol. In this configuration, if the receiving node is found on the same network, the message is transmitted from the sender to the receiving node through the child nodes. On the other hand, if the receiving node is not found on the same network, the message is transmitted to the entire network via the root node and the receiving node is searched on other networks. Meanwhile, if the receiving node is found on a different network, the message received with the root node of the respective network is transmitted to the destination node using the child nodes of the receiving node. Nodes that fail to pass authentication on the physical layer are declared to all networks as insecure nodes through the root node in the network. In this way, the nodes which are marked as insecure are prevented from transferring data between the nodes itself, to other nodes or to the network layer for the next process.

Network layer, known as the transmission layer, is the layer where data from the physical layer are processed and transmitted to a higher layer using protocols such as IP, LowPAN (Low-Power Wireless Personal Area Network), UDP and Internet Control Message Protocol (ICMP). The transmission medium can be wireless or wired according to users' needs or communication technologies. In this layer, the encryption and digestion methods must be applied in order to protect data integrity. Moreover, the encryption methods in accordance with IoT constraints are employed to eliminate the security issue on this layer. For message integrity, methods such as digestion, message authentication code (MAC) and digital signatures which are computed regarding the content of the message are used. The encryption methods used in the network layer ensure the data privacy along with converting the sent message in a way that anybody except the recipient cannot understand. Many IoT devices have limited storage, memory and processing capabilities, and they are usually expected to run at low power usage. Due to these limitations, IoT devices use fast and light encryption algorithms. Therefore, IoT systems should utilize multiple layers of defense, such as splitting devices into separate networks and using firewalls to compensate for these restrictions.

Data processing layer is the layer in which the data generated and transmitted on IoT platforms are stored, analyzed and processed. In this layer, different analytical technologies enabling utilization of the data and online databases stored in cloud computing environments are employed. The proposed approach requires countermeasures to avoid disclosure of sensitive information during processing of the data. Thus, prior to the data processing stage, privacy protection procedures are carried out on the data in order to protect data privacy. Within the scope of these transactions, the individual identifiers that directly identify the individuals are separated from the data and performance improvement is ensured due to not processing unnecessary data. With the privacy protection approaches taken in this layer, both non-essential data will be safely decomposed and compliance with the regulatory frameworks will be ensured for the protection of personal data. Encryption methods should be used to protect data in the third-party or untrusted environments where privacy

Table 1. Level of impacts and their descriptions.

Level of impact	Description
Low	IoT applications may face some minor threats that can be easily combated with
Medium	Despite the difficulties, IoT applications may face significant problems
High	IoT applications may face significant problems that cannot be overcome and have irreversible consequences

IoT: Internet of Things.

protection methods cannot be used, or in other cases where it is needed.

Application layer is the last layer of the proposed *layered security architecture*, which allows the users to present and use the processed data on IoT platforms. Likewise, various applications where IoT can be used, such as smart home, smart transportation, smart cities, smart health and smart farming, are defined in this layer. Unfortunately, the application layer of IoT platforms is the weakest link that provides the biggest attack surface for hackers. The application layer involves any application that has connection to any IoT device that may include local web applications, cloud-based applications and smartphone or tablet applications. Therefore, IoT application security should be part of the software development life cycle (SDLC) for all IoT applications, especially all design, development (coding) and testing phases. In order to minimize the weaknesses caused by the human factor during the design phase of the proposed model, which requires the most stringent protection, IoT user account management should be designed along with taking the security to forefront. Passwords of the user accounts must be digested with a one-way digestion-salting algorithm in a way that cannot be reversed in case of a violation. Specifically, two-factor authentication must be verified for applications that will process confidential data intended to be accessed from untrusted networks. In addition, a secure software update feature should be designed in order to apply digitally signed (original) updates to the application layer as much as possible. Moreover, applications on IoT platforms should be powered with secure record management to show security warnings such as security monitoring system or record management and failed login attempts.

Understanding and evaluating layered threats

In order to evaluate the impacts of possible threats on IoT platforms, the impact levels given in Table 1 have been defined.

Impact assessment is performed on nodes in IoT platforms. The questions and evaluations given in Table 2 have been used to obtain the security parameters in terms of confidentially, integrity and accessibility by taking into account the elements such as the number of threats to each node, layers affected by the threats on the node, size of the attack surface and the criticality of the node. Among the impact assessments obtained as shown in Table 2, the highest impact value indicates the measurement result of the threat level according to the suggested risk-based layered approach.

Table 2. CIA risk assessment table.

Order	Question	Evaluation
1	What is the impact of confidentiality loss in IoT data?	Low Medium High
2	What is the impact of integrity loss of IoT data?	Low Medium High
3	What is the impact of accessibility loss of IoT data?	Low Medium High

CIA: confidentiality, integrity and accessibility.

Measuring the occurrence likelihood of layered threats

In this section, it is aimed to understand the general threats to IoT security and to evaluate the likelihood of these threats. In order to facilitate this process, assessment questions regarding threats on IoT platforms have been defined. The evaluation questions are discussed in four main headings (Table 3) as follows:

(a) Measuring threats to the layers;
(b) Processes/procedures for data security in the layers;
(c) Third parties and human factors affecting the security of the layers;
(d) Criticality of the layers and the scale of the attack surface.

The probability of occurrence of each threat for layer evaluation fields is defined (Tables 4 and 5) as follows:

- Low—the lowest probability of the threat to occur.
- Medium—although it is low, there is a likelihood of the threat to occur;
- High—it is more likely to have the threat occurrence.

Upon evaluating the impact of the likelihood of layer threats, the assessment of security risks on IoT platforms is performed in accordance with Table 6.

Conclusion

IoT is the infrastructure of different intelligent objects that work with an end-to-end integration with a combination of different systems. A single security solution is not enough to ensure the security of the integrated structure of such a diverse system.

Table 3. Measuring the occurrence likelihood of layered threats.

No.	Question for the threat	Description
(a) Measurement of threats to the layers		
1	Is the processing of data on the IoT platform carried out over the Internet?	When the processing of IoT data is fully or partially over the Internet, possible threats to off-platform attackers for IoT nodes increase (denial of service, SQL injection, XSS, ransomware, man-in-the-middle, etc.).
2	Is it possible to access a node on the IoT network over the Internet?	If there exists an access to a personal data processing system on the IoT network over the Internet, the possibility of external threats increases. It also increases the possibility of misuse (accidentally or intentionally) by users (outsiders in the external world). Particular attention should be paid to remote management of the IoT platform.
3	Is there any services consumed through different networks during the process of IoT data?	The connection to external systems from IoT platforms, in addition to external threats, also poses the threat of not configuring access permissions appropriately.
4	What are the measures taken in order to protect physical security on IoT platforms?	If the physical environment on IoT platforms is not satisfactorily protected, it is more likely to have significant problems that may seriously endanger safety.
5	Have the best recommendations been taken during the stage of designing, implementing and protecting the IoT security?	Poorly designed, implemented or highly unprotected hardware and software components can pose significant risks to IoT security. For this purpose, it is necessary to apply the rules for best practices.
(b) Processes/procedures for data security activities in layers		
6	Are the roles and responsibilities related to IoT data security clearly defined?	Access control of the data cannot be managed if the roles and responsibilities are not clearly defined. This jeopardizes the unauthorized use of resources and the security of IoT platforms.
7	Is the employment of network, system and physical resources clearly defined on IoT platforms?	Security threats may arise as a result of accidental or intentional misuse of the system if the use of resources is not carried out in a certain way. A clear definition of security policies for network, system and physical resources can reduce potential risks.
8	Are data allowed to be transferred, stored or processed outside of IoT platforms?	Processing IoT data outside the platforms may offer a significant amount of flexibility. However, in addition to this flexibility, there may be additional risks such as unsafe network channels (such as open Wi-Fi networks) and the unauthorized use of this information.
9	Can data processing activities on IoT platforms be performed without creating log files?	Lack of appropriate logging and monitoring mechanisms may increase the likelihood of exploitation in processes/procedures along with resources that may result in the misuse of IoT data.
(c) Third parties and human factor that affect the data security of the layers		
10	Is there any management of employees that operate on IoT data?	In the case of more than enough people accessing IoT data, the human factor will adversely affect data security.
11	Are there any IoT data processing activities performed by third-party data handlers?	If third-party access is available to IoT data, precautions must be taken against third-party threats.
12	Is there any employee who is untrained or unaware of IoT data security?	Employees who are unaware of data security become a threat factor since they are fundamentally unaware of the security principles.
(d) Criticality of the layers and scale of the attack surface		
13	Is the surface of the layered attack large?	In order to minimize cyber-attacks against layers, additional security measures should be taken according to the size of the attack surfaces.
14	Are the security breaches to the layers in the last 2 years evaluated?	If there was a cyber-attack on IoT platforms based on layer threats, additional countermeasures should be taken into account in order to prevent similar events in the future.
15	Are the best security recommendations for layer threats being followed?	Security measures that are specific to layer threats are usually taken according to the risks of the layers and the best security practices as well.

XSS: cross-site scripting; IoT: Internet of Things.

IoT is the technology that enables production systems to enter the new process and launch industry 4.0. IoT-based intelligent production mechanisms consist of self-optimizing and organizing production systems in terms of resource availability and consumption. These systems are possible with the use of new smart services, including product optimization, based on product, production, employee and customer use.

IoT systems carry risks in terms of security and privacy. Without eliminating these risks, the IoT requirements are not adequately fulfilled. Because cyber-attacks on cyber physical systems may threaten human life by causing physical damage to the IoT. IoT has a heterogeneous structure and a holistic cyber security framework should be established to ensure the security of the IoT by isolating heterogeneous systems and defining platform boundaries. Since existing security solutions cannot respond to real-time IoT security requirements and cannot be scaled to cyber-physical systems, they are insufficient to ensure the security of IoT with a heterogeneous structure.

Table 4. Rating of probability of assessment fields.

Fields of assessments	Probability	
	Level	Score
Measuring the threats according to the layers	Low	1
	Medium	2
	High	3
Processes/procedures for data security in layers	Low	1
	Medium	2
	High	3
Third parties and human factors affecting the security of the layers	Low	1
	Medium	2
	High	3
Criticality of the layers and the scale of the attack surface	Low	1
	Medium	2
	High	3

Table 5. Evaluation of threat occurrence.

Range	Level
4–5	Low
6–8	Medium
9–12	High

Table 6. Risk assessment.

Likelihood of threat occurrence	Impact level		
	Low	Medium	High
Low			
Medium			
High			

Green color indicates low risk; yellow color indicates medium risk; red color indicates high risk.

In this study, the application fields of IoT, increasing usage rate by years, architecture and protocols and security requirements are mentioned in detail. Assets that create vulnerability are described by classifying the types of attacks that threaten the physical layer, network layer, data processing layer and application layer of IoT. The contribution of this study is to explain the layers of cyber-physical systems that make up the IoT which were evaluated separately and their vulnerabilities and threats were examined and a security model was proposed. The proposed IoT security model is a holistic security model that evaluates each layer of cyber-physical systems separately against vulnerabilities and threats, based on the risk-level approach to ensure IoT security.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

ORCID iD

Adem Tekerek https://orcid.org/0000-0002-0880-7955

References

1. Jensen MC. The modern industrial revolution, exit, and the failure of internal control systems. *J Finance* 1993; 48(3): 831–880.
2. Hazarika M, Dixit US and Davim JP. Chapter 1—history of production and industrial engineering through contributions of stalwarts. In: Davim JP (ed.) Manufacturing *engineering education*. Oxford: Chandos Publishing, 2019, pp. 1–29.
3. Lee CKM, Zhang SZ and Ng KKH. Development of an industrial internet of things suite for smart factory towards re-industrialization. *Adv Manuf* 2017; 5(4): 335–343.
4. Stock T and Seliger G. Opportunities of sustainable manufacturing in Industry 4.0. *Proced CIRP* 2016; 40: 536–541.
5. Fonseca LM. Industry 4.0 and the digital society: concepts, dimensions and envisioned benefits. *Sciendo* 2018; 12(1): 386–397.
6. Nur Altun S, Dörterler M and Alper Dogru I. Fuzzy logic based lighting system supported with IoT for renewable energy resources. In: *Proceedings of the innovations in intelligent systems and applications conference*, Adana, Turkey, 4–6 October 2018, pp. 1–4. New York: IEEE.
7. Almada-Lobo F. The Industry 4.0 revolution and the future of manufacturing execution systems (MES). *J Innov Manage* 2016; 3(4): 16–21.
8. Yao H, Cao H and Li J. Design and implementation of a portable wireless system for structural health monitoring. *Meas Control* 2016; 49(1): 23–32.
9. Kirbas I. Developing and remote controlling a multi-zone cooling plant using web services and a secure token mechanism. *Meas Control* 2015; 48(9): 278–284.
10. Kang HS, Lee JY, Choi S, et al. Smart manufacturing: past research, present findings, and future directions. *Int J Precis Eng Manuf Green Technol* 2016; 3(1): 111–128.
11. Zhang Y, Qiu M, Tsai CW, et al. Health-CPS: healthcare cyber-physical system assisted by cloud and big data. *IEEE Syst J* 2017; 11(1): 88–95.
12. Wang L, Törngren M and Onori M. Current status and advancement of cyber-physical systems in manufacturing. *J Manuf Syst* 2015; 37: 517–527.
13. Cui Z, Ye W and Choi-Grogan YS. *User equipment categories for machine-to-machine devices operating in an internet of things network*. Patent 9848279, USA, 2017.
14. Jeschke S, Brecher C, Meisen T, et al. Industrial internet of things and cyber manufacturing systems. In: Jeschke S, Brecher C, Song H, et al. (eds) *Industrial internet of things*. Cham: Springer, 2017, pp. 3–19.
15. Monostori L, Kádár B, Bauernhansl T, et al. Cyber-physical systems in manufacturing. *CIRP Ann* 2016; 65(2): 621–641.

16. Bosso N, Pasquale GD, Somà A, et al. Design and control of a sensorized trolley for the measurement of industrial craneways. *Meas Control* 2016; 49(10): 307–316.
17. Sicari S, Rizzardi A, Grieco LA, et al. Security, privacy and trust in internet of things: the road ahead. *Comput Netw* 2015; 76: 146–164.
18. Jing Q, Vasilakos AV, Wan J, et al. Security of the internet of things: perspectives and challenges. *Wirel Netw* 2014; 20(8): 2481–2501.
19. Alaba FA, Othman M, Hashem IAT, et al. Internet of things security: a survey. *J Netw Comput Appl* 2017; 88: 10–28.
20. Cui X. The internet of things. In: Moran S (ed.) *Ethical ripples of creativity and innovation*. Berlin: Springer, 2016, pp. 61–68.
21. Madakam S, Ramaswamy R and Tripathi S. Internet of things (IoT): a literature review. *J Comput Commun* 2015; 3(5): 164–173.
22. Lee I and Lee K. The Internet of things (IoT): applications, investments, and challenges for enterprises. *Bus Horizon* 2015; 58(4): 431–440.
23. Evans D. *The internet of things: how the next evolution of the internet is changing everything*. San Jose, CA: CISCO, 2011.
24. United Nations Report. World population projections to 2150. *Foreign Pol Bull* 1998; 9(2): 115–118.
25. Farooq MU, Waseem M, Khairi A, et al. A critical analysis on the security concerns of internet of things (IoT). *Int J Comput Appl* 2015; 111(7): 1–6.
26. Riahi A, Challal Y, Natalizio E, et al. A systemic approach for IoT security. In: *Proceedings of the international conference on distributed computing in sensor systems*, Cambridge, MA, 20–23 May 2013, pp. 351–355. New York: IEEE.
27. Pyo C, Kang H, Kim N, et al. IoT (M2M) technology trends and development prospects. *Inf Commun* 2013; 30: 3–10.
28. Heer T, Garcia-Morchon O, Hummen R, et al. Security challenges in the IP-based internet of things. *Wirel Pers Commun* 2011; 61(3): 527–542.
29. Weber RH. Internet of things—new security and privacy challenges. *Comput Law Secur Rev* 2010; 26(1): 23–30.
30. Zhao K and Ge L. A survey on the internet of things security. In: *Proceedings of the 9th international conference on computational intelligence and security*, Leshan, China, 14–15 December 2013, pp. 663–667. New York: IEEE.
31. Wu M, Lu T-J, Ling F-Y, et al. Research on the architecture of internet of things. In: *Proceedings of the 3rd international conference on advanced computer theory and engineering*, Chengdu, China, 20–22 August 2010, vol. 5, pp. 484–487. New York: IEEE.
32. Tsai C-W, Lai C-F and Vasilakos AV. Future internet of things: open issues and challenges. *Wirel Netw* 2014; 20(8): 2201–2217.
33. Montenegro G, Kushalnagar N, Hui J, et al. *Transmission of IPv6 packets over IEEE 802.15.4 networks*. 2007, https://datatracker.ietf.org/doc/rfc4944/
34. Raza S, Shafagh H, Hewage K, et al. Lithe: lightweight secure CoAP for the internet of things. *IEEE Sens J* 2013; 13(10): 3711–3720.
35. Zheng J and Lee MJ. A comprehensive performance study of IEEE 802.15.4. *Sens Netw Oper* 2006; 218–237, https://pdfs.semanticscholar.org/622f/702aec96d4fe2ffe426f901f542aa92657d0.pdf
36. Al-Fuqaha A, Guizani M, Mohammadi M, et al. Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Commun Surv Tut* 2015; 17(4): 2347–2376.
37. Shelby Z, Hartke K and Bormann C. *The constrained application protocol (CoAP)*. 2014, https://tools.ietf.org/html/rfc7252
38. Kovatsch M. CoAP for the web of things: from tiny resource-constrained devices to the web browser. In: *Proceedings of the conference on pervasive and ubiquitous computing adjunct publication*, Zurich, 8–12 September 2013, pp. 1495–1504. New York: ACM.
39. Glombitza N, Pfisterer D and Fischer S. LTP: an efficient web service transport protocol for resource constrained devices. In: *Proceedings of the 7th annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks*, Boston, MA, 21–25 June 2010, pp. 1–9. New York: IEEE.
40. Modadugu N and Rescorla E. *The design and implementation of datagram TLS*. New York: NDSS, 2004.
41. Kothmayr T, Schmitt C, Hu W, et al. DTLS based security and two-way authentication for the internet of things. *Ad Hoc Netw* 2013; 11(8): 2710–2723.
42. Kothmayr T, Schmitt C, Hu W, et al. A DTLS based end-to-end security architecture for the internet of things with two-way authentication. In: *Proceedings of the 37th annual conference on local computer networks—workshops*, Clearwater, FL, 22–25 October 2012, pp. 956–963. New York: IEEE.
43. Rescorla E and Modadugu N. *Datagram transport layer security version 1.2*. 2012, https://tools.ietf.org/html/rfc6347
44. Roman R, Zhou J and Lopez J. On the features and challenges of security and privacy in distributed internet of things. *Comput Netw* 2013; 57(10): 2266–2279.
45. Sándor H, Genge B and Gál Z. Security assessment of modern data aggregation platforms in the internet of things. *Int J Inform Secur Sci* 2015; 4(3): 92–103.
46. Namvar N, Saad W, Bahadori N, et al. Jamming in the internet of things: a game-theoretic perspective. In: *Proceedings of the global communications conference*, Washington, DC, 4–8 December 2016, pp. 1–6. New York: IEEE.
47. Chen Y, Li Y, Xu D, et al. DQN-based power control for IoT transmission against jamming. In: *Proceedings of the 87th vehicular technology conference*, Porto, 3–6 June 2018, pp. 1–5. New York: IEEE.
48. Hossain MM, Fotouhi M and Hasan R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In: *Proceedings of the world congress on services*, New York, 27 June–2 July 2015, pp. 21–28. New York: IEEE.
49. Mahalle PN, Anggorojati B, Prasad NR, et al. Identity authentication and capability based access control (IACAC) for the internet of things. *J Cyber Secur Mob* 2013; 1(4): 309–348.
50. Babar S, Mahalle P, Stango A, et al. Proposed security model and threat taxonomy for the internet of things (IoT). In: Meghanathan N, Boumerdassi S, Chaki N, et al. (eds) *Recent trends in network security and applications*. Berlin: Springer, 2010, pp. 420–429.

51. Zhang C and Green R. Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. In: *Proceedings of the 18th symposium on communications & networking*, Alexandria, VA, 12–15 April 2015, pp. 8–15. San Diego, CA: Society for Computer Simulation International.
52. Nawir M, Amir A, Yaakob N, et al. Internet of things (IoT): taxonomy of security attacks. In: *Proceedings of the 3rd international conference on electronic design*, Phuket, Thailand, 11–12 August 2016, pp. 321–326. New York: IEEE.
53. Farooq MU, Waseem M, Mazhar S, et al. A review on internet of things (IoT). *Int J Computr Appl* 2015; 113(1): 1–7.
54. Covington MJ and Carskadden R. Threat implications of the internet of things. In: *Proceedings of the 5th international conference on cyber conflict*, Tallinn, 4–7 June 2013, pp. 1–12. New York: IEEE.
55. Suo H, Wan J, Zou C, et al. Security in the internet of things: a review. In: *Proceedings of the international conference on computer science and electronics engineering*, Hangzhou, China, 23–25 March 2012, vol. 3, pp. 648–651. New York: IEEE.
56. Li C, Qin Z, Novak E, et al. Securing SDN infrastructure of IoT–fog networks from MitM attacks. *IEEE Internet Things J* 2017; 4(5): 1156–1164.
57. Rostampour S, Bagheri N, Hosseinzadeh M, et al. A scalable and lightweight grouping proof protocol for internet of things applications. *J Supercomput* 2018; 74(1): 71–86.
58. Virat MS, Bindu SM, Aishwarya B, et al. Security and privacy challenges in internet of things. In: *Proceedings of the 2nd international conference on trends in electronics and informatics*, Tirunelveli, India, 11–12 May 2018, pp. 454–460. New York: IEEE.
59. Raza S, Wallgren L and Voigt T. SVELTE: real-time intrusion detection in the internet of things. *Ad Hoc Netw* 2013; 11(8): 2661–2674.
60. Borgohain T, Kumar U and Sanyal S. Survey of security and privacy issues of internet of things, https://arxiv.org/ftp/arxiv/papers/1501/1501.02211.pdf
61. Zhang K, Liang X, Lu R, et al. Sybil attacks and their defenses in the internet of things. *IEEE Internet Things J* 2014; 1(5): 372–383.
62. Yaqoob I, Hashem IAT, Ahmed A, et al. Internet of things forensics: recent advances, taxonomy, requirements, and open challenges. *Future Gener Comput Syst* 2019; 92: 265–275.
63. Brun O, Yin Y, Gelenbe E, et al. Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments, https://san.ee.ic.ac.uk/publications/9articleICL.pdf
64. Zhang ZK, Cho MCY, Wang CW, et al. IoT security: ongoing challenges and research opportunities. In: *Proceedings of the 7th international conference on service-oriented computing and applications*, Matsue, Japan, 17–19 November 2014, pp. 230–234. New York: IEEE.
65. Alcaraz C, Roman R, Najera P, et al. Security of industrial sensor network-based remote substations in the context of the internet of things. *Ad Hoc Netw* 2013; 11(3): 1091–1104.
66. Varga P, Plosz S, Soos G, et al. Security threats and issues in automation IoT. In: *Proceedings of the 13th international workshop on factory communication systems*, Trondheim, 31 May–2 June 2017, pp. 1–6. New York: IEEE.
67. Ryan Heartfield R and Gan D. Social engineering in the internet of everything. *J Inform Technol Manage* 2016; 29(7): 20–29.