PeerJ Computer Science

Cybersecurity risk mitigation and network anomaly detection in smart homes using machine learning and data mining

Mahmood Hijran Abdulrazaq[1], Cemal Koçak[2], Saadin Oyucu[2] and Burçak Asal[3]

[1] Computer Engineering, Gazi University Institute of Science, Ankara, Turkey
[2] Department of Computer Engineering, Faculty of Technology, Gazi University Ankara, Ankara, Turkey
[3] Department of Computer Engineering, Adana Alparslan Türkeş Science and Technology University, Adana, Turkey

ABSTRACT

The quick spread of Internet of Things (IoT) devices in smart homes has raised cybersecurity concerns, calling for smart, flexible, and active ways to reduce threats. Standard Intrusion Detection Systems (IDS) and basic anomaly detection have trouble spotting new attacks and changing cyber threats. To fix these problems, this article puts forward a Reinforcement Learning-Based Adaptive Threat Mitigation (RL-ATM) model. It uses methods like reinforcement learning, deep learning, and data mining to make smart home cybersecurity better by reducing risks and finding network issues. Tests show that RL-ATM does much better than current cybersecurity options, such as signature-based IDS, anomaly-based machine learning models, and deep reinforcement learning (DRL) setups. The model got an accuracy of 98.87%, a precision of 97.49%, a recall of 98.36%, and a low false positive rate (FPR) of 1.8%. This makes it a dependable cybersecurity choice for actual smart home use. A comparison shows that standard IDS models are only 87.42% accurate with an FPR of 6.3%. Anomaly-based ML methods improve accuracy to 91.15% but still have an FPR of 4.9%. Hybrid Convolutional Neural Network (CNN) + Reinforcement Learning models reach 92.84% accuracy but can't adapt to changing attacks in real time. This makes RL-ATM a better choice for dependable detection and response. This work adds to smart home cybersecurity by giving a scalable, adaptive, and independent artificial intelligence (AI)-driven security system. It can lower cyber threats in real time.

Subjects Computer Networks and Communications, Data Mining and Machine Learning, Security and Privacy, Internet of Things, Blockchain

Keywords AI-driven cybersecurity, Intrusion detection system (IDS), IoT-23 dataset, Reinforcement learning-based threat mitigation, Smart home cybersecurity

Submitted 3 October 2025
Accepted 28 December 2025
Published 6 March 2026

Corresponding author
Cemal Koçak, ccckocak@gazi.edu.tr

Academic editor
Kamran Shaukat

Additional Information and Declarations can be found on page 23

DOI **10.7717/peerj-cs.3612**

Copyright
2026 Abdulrazaq et al.

Distributed under
Creative Commons CC-BY 4.0

OPEN ACCESS

INTRODUCTION

The Internet of Things (IoT) has grown quickly, leading to many smart homes with networked devices that add convenience, security, and automation (*Nayak et al., 2024*). As devices become more connected, cybersecurity risks rise. Smart home networks are prone to cyber-attacks because of weak security, a lack of standards, and limited resources in IoT devices. Common threats include unauthorized access, data loss, Distributed Denial of

Service (DDoS) attacks, and malware (*Ahmed, Zaidi & Mumtaz, 2024*). A main problem is how to lessen cyber-attacks in smart homes, which include different IoT devices with varied security (*Ge et al., 2019*). IoT devices have limited storage and computing ability, so adding standard security like strong encryption and authentication can be hard (*Mutambik, 2024*). The many communication protocols and devices make smart home networks hard to secure and open to cyber-attacks. Also, end-users often do not know enough about cybersecurity, which makes security worse (*Atieh et al., 2022*). Because of these problems, machine learning (ML) and data mining are becoming useful for spotting and stopping cyber-attacks in smart home systems. ML algorithms can label cyber-attacks and find strange network traffic accurately (*Natarajan et al., 2024*). Standard security products, like signature-based intrusion detection systems (IDS) and firewalls, cannot handle new attacks, like zero-day attacks and complex AI-based cyber-attacks. The independent and adaptable nature of ML models and the ability of data mining to find patterns provide an active security system. This system can find anomalies, spot threats in real-time, and learn to understand attack patterns without help (*Ul Rehman & Manickam, 2016*).

The present study is relevant in presenting a model of learning cybersecurity capable of dynamically adjusting traffic patterns in the network in real time and enhancing the threat detection rate over time, as presented in *Butt et al. (2022)*. Intelligent home networks can defend themselves against unauthorized access, malware propagation, botnets, and other cyber-attack forms through anomaly detection. Furthermore, data mining techniques enable efficient feature selection, correlation analysis, and predictive analytics that security systems can exploit to detect and remove potential vulnerabilities before they are exploited, as outlined in *Galushka, Patterson & Rooney (2006)*. The conclusions of this study will add to the world of academia in terms of broadening knowledge of AI-based models of cybersecurity and industrial applications in terms of having an efficient, scalable, and real-time threat detection system for smart homes. Moreover, this research will close the gap between practice and theory, enabling the design of self-adaptive security systems that are capable of operating autonomously with little or no user input, as explained in *Adewole & Jacobsson (2024)*. As smart home automation continues to grow in dependency, the proposed data mining and ML framework will be essential in providing data privacy, security, and resilience in future smart homes. Through its emphasis on machine learning-based anomaly detection and data mining strategies, this research will be able to help develop adaptive next-generation cybersecurity solutions that can combat emerging threats, hence providing complete security for global smart home consumers as presented in *Cao, Wang & Wang (2024)*.

Aim of the study

This study aims to develop a reinforcement learning (RL) framework for cybersecurity risk reduction and anomaly detection in smart homes. Current cybersecurity systems often use static rules, which struggle with new cyber threats like zero-day attacks and AI malware. Also, current Intrusion Detection Systems (IDS) and firewalls use signature-based methods that cannot foresee unfamiliar attacks. This research will use reinforcement learning to create a self-learning cybersecurity system that can detect, classify, and handle

network anomalies in smart home networks. By adding reinforcement learning-based security, this work seeks to build a smart, scalable, and automated cybersecurity platform that protects smart homes from complex attacks with little user involvement. The results should help with smart home security, IoT risk plans, and AI cybersecurity platforms for future threat protection.

- Create a Reinforcement Learning Adaptive Threat Mitigation Framework (RL-ATM): Build security components that learn to detect and fix threats in real-time without needing people to tell them what to do.
- Apply Markov Decision Process (MDP) for Automated Response: Adopt MDP decision models to put in place automatic responses, such as blocking or isolating threats, or sending out alerts about them.
- Improve Proactive Cybersecurity Defense with Deep Reinforcement Learning (DRL): Add Deep Q-Networks (DQN) and Proximal Policy to predict and stop attacks as they happen.
- Lower False Positives in Anomaly Detection: Refine reinforcement learning reward functions to cut down on false positives and make detection work better.
- Change Security Controls to handle New Cyber Threats: Keep training the model and adapting it fast to keep smart home security safe from AI cyber-attacks.
- Address Low-Power Device IoT Security Issues: Make a light Reinforcement Learning (RL) model that works well on low-power smart home devices.
- Automate Firewall and Network Policy Updates: Put in self-tuning security features that constantly update firewall policies based on what abnormalities they find.
- Improve Behavioral-Based Intrusion Detection: Employ reinforcement learning algorithms to watch changes in network behavior and find possible risks earlier.

With the use of reinforcement learning in adaptive threat mitigation, this study will establish a new standard for smart home security that will ensure round-the-clock, autonomous, and intelligent defense against ever-changing cyber threats.

Problem statement

The quick growth of IoT smart home devices has made convenience and automation common. This growth, though, has also increased cybersecurity risks. Smart home devices often have weak security, making them easy targets for unauthorized access, malware, distributed denial-of-service (DDoS) attacks, and data breaches (*Darshini & Nagaraju, 2023*; *Sarker, 2021*). Traditional firewalls and intrusion detection systems, which use signature-based detection, do not work well against new malware, AI attacks, and zero-day exploits. This study aims to create a more adaptable and scalable anomaly detection system to address these issues, giving smart home users better protection from evolving cyber threats (*Kumar et al., 2024*). Several challenges exist:

- **Traditional Cybersecurity Is Lacking:** Current IDS and firewalls cannot spot zero-day attacks, AI-driven threats, and APTs in smart home setups.

- **No Standard Security for IoT:** The absence of worldwide standards causes security measures to be inconsistent, so it's hard to protect all smart home devices and companies equally.
- **Too Many False Alarms:** Current machine learning anomaly detection systems produce a lot of false positives, causing too many alerts and poor threat responses.
- **Not Enough Data for Smart Homes:** Most cybersecurity datasets are for business and cloud settings, which means machine learning models don't work well for smart home security.
- **User Errors:** Many smart home users do not follow good security habits, leading to setup mistakes, weak passwords, and unpatched problems that attackers can exploit.
- **Hard to Spot New AI Threats:** Cybercriminals are quickly using AI to change attack methods, making old detection techniques useless against new threats.

This study attempts to overcome such challenges by proposing an intelligent machine learning-based network anomaly detection and cybersecurity risk avoidance framework specifically for smart home ecosystems.

LITERATURE REVIEW

The growing sophistication of cyber-attacks in smart home settings has prompted researchers to investigate sophisticated security measures beyond the conventional signature-based detection systems. Traditional approaches like firewalls, rule-based IDS, and heuristic security models are found to be insufficient against zero-day attacks, AI-powered cyber-attacks, and adaptive malware methods as provided in *Viksha & Singh (2023)*. Owing to the heterogeneity of IoT devices in smart homes, a standardized and adaptive cybersecurity model is a top challenge. Numerous studies have pointed out that the networks of smart homes possess new security threats, such as poor authentication controls, non-patched software, and inadequate encryption controls, making them easier targets for cybercriminals, as provided in *Han, Wu & Yang (2022)*.

ML and artificial intelligence (AI) trends offer ways to reduce cybersecurity threats. For instance, ML-based network anomaly detection can sift through traffic data, spot unusual activity, and differentiate attacks from normal traffic more readily than standard methods (*Liang et al., 2021*). Supervised learning models like Support Vector Machines (SVM), Random Forest (RF), and Decision Trees (DT) are often used for intrusion detection. Still, they depend on labeled datasets, making them less useful for spotting unknown threats. Unsupervised learning methods, such as clustering algorithms and deep learning, have been tried to find new attack methods. However, they tend to produce false positives and waste computing power when used on less powerful IoT devices in smart homes (*Jakkula & Cook, 2008*).

Lately, RL has come up as another option for finding cyber threats and automating responses. Compared to supervised and unsupervised ML, RL models can learn from interacting with network traffic and improve their responses over time. Tests suggest that RL-based security models, like Deep Q-Networks (DQN) and Proximal Policy Optimization (PPO), can automatically spot anomalies, sort network threats, and block

attacks with little input (*Zamani, Talebi & Stevens, 2023*). These RL models make good choices by constantly learning from network patterns, which lets them fight new threats in real-time. Even so, most RL-based cybersecurity models are for businesses, and there's a lack of research for smart home environments. Device limits, adaptation in real-time, and computing efficiency pose challenges (*Ghosh & Chatterjee, 2021*). Think about a network security setup where devices (laptops, PCs, mobile phones, tablets, and game controllers) link to a central network. The firewall acts as a security barrier, stopping cyber threats and unauthorized access. Users access social media, email, and cloud storage, which could be entry points for attacks. The router provides internet, and firewall protection stops malware, phishing, and intrusions (*Priyadarshini et al., 2022*). Unlike business systems that have organized network logs, smart home devices create fluid and unstructured traffic patterns, making it hard to train anomaly detection models (*Tran et al., 2020*). Besides, the computing limits of IoT devices make it hard to use deep reinforcement learning models. So, it is important to have lightweight, adaptable, and energy-saving RL-based threat reduction methods.

Traditional cybersecurity approaches and their limitations

Conventional cybersecurity practices in smart homes are based on signature-based intrusion detection systems, firewalls, and heuristic anomaly detection methods for protecting networks from possible cyber threats. Although they have been capable of defending classical IT infrastructures, they entail a number of limitations when executed in the resource-constrained heterogeneity of smart home networks built on IoT technology. A study by *Gupta et al. (2021)* also points out how conventional security methods find it challenging to keep up with dynamic and adaptive attack vectors directed toward IoT ecosystems. In contrast to traditional networked systems, home automation devices encompass diverse types with unique communication protocols, security capabilities, and computational constraints, hence challenging the enforcement of common security measures across the entire connected ensemble as given in Table 1.

Table 1 compares common cybersecurity steps in smart home networks, looking at how well they work and what their limits are. Firewalls and signature-based Intrusion Detection Systems (IDS) give some basic safety, they do not work well against new cyber threats like zero-day attacks and malware that uses artificial intelligence. Weak security hurts safe device talking using authentication and encryption, mostly in Internet of Things (IoT) devices. Anomaly-based IDS (AIDS) gets better at finding attacks but can also have lots of false alarms. Patch management and access controls make security better but need people to get involved and keep things up to date, as *Sarker (2021)* shows. In the future, artificial intelligence could find threats, but it might use up a lot of computer power and cause worries about privacy. The bad things about these normal ways show that we need cybersecurity systems that can change and use artificial intelligence, like Reinforcement Learning-based Adaptive Threat Mitigation (RL-ATM).

Machine learning in network anomaly detection

The increasing popularity of smart home IoT gadgets has spawned the necessity for developing smart, adaptive cybersecurity that can detect and demobilize network attacks.

Table 1 Key milestones in the evolution of machine learning for medical imaging.

Cybersecurity approach	Functionality	Strengths	Limitations	Ref.
Firewalls & Network Access Control	Filters and blocks unauthorized network traffic.	- Protects against known threats. - Reduces unauthorized access. - Enforces security policies.	- Cannot detect zero-day attacks. - Ineffective against lateral movement attacks. - Does not inspect encrypted traffic.	*Alnaqbi & Tawfik (2023)*
Signature-Based IDS	Detects known threats using a database of attack signatures.	- Effective for known threats. - Provides forensic analysis. - Low false positives forrecognized attacks.	- Fails against zero-day malware. - Needs frequent updates. - Attackers evade detection by modifying malware structure.	*Alghamdi & Bellaiche (2023)*
Authentication & Encryption	Protects access using passwords, MFA, and cryptographic methods.	- Prevents unauthorized access. - Encrypts sensitive data. - Secures device communication.	- Weak encryption standards in many IoT devices. - Default/hardcoded credentials. - MFA often unsupported.	*Jeyaram & Muthukumaravel (2024)*
Anomaly-Based IDS (AIDS)	Detects deviations from normal network behavior.	- Identifies unknown attack patterns. - Learns and adapts to new threats. - More effective than signature-based IDS.	- High false-positive rates. - Lacks contextual awareness. - Computationally expensive for IoT devices.	*Andrade, Tello-Oquendo & Ortiz (2021)*
Patch Management & Firmware Updates	Updates IoT device software to fix vulnerabilities.	- Fixes security flaws. - Prevents known exploits. - Enhances system stability.	- Many devices do not receive updates. - Users neglect updates. - Early discontinuation of updates by manufacturers.	*Paddalwar, Ragha & Mane (2023)*
Access Control Mechanisms	Uses VLANs, RBAC, and Zero Trust to limit access.	- Reduces attack surface. - Prevents unauthorized access. - Enforces device-specific security policies.	- Difficult to configure manually. - Misconfigurations create security gaps. - Needs constant monitoring.	*Osman (2019)*
IoT Device Isolation	Segments IoT devices into separate network zones.	- Limits spread of botnet infections. - Prevents compromised devices from affecting the main network. - Enhances security.	- Hard to implement for home users. - Some devices need interconnectivity. - Not all routers support advanced segmentation.	*Meliboev (2024)*

Table 1 (continued)

Cybersecurity approach	Functionality	Strengths	Limitations	Ref.
AI-Powered Threat Detection (Emerging)	Uses ML/RL to detect and mitigate cyber threats dynamically.	- Detects AI-driven attacks. - Adapts to evolving threats. - Improves real-time response.	- High computational demand. - Privacy concerns due to real-time monitoring. - Still in early research phase.	*Munshi (2022)*

ML techniques were discovered to effectively serve as network anomaly detection systems, allowing intelligent home security mechanisms to monitor traffic behavior in real-time, discover anomalies, and classify cyber-attacks in real-time, as explicated in *Ngo et al. (2024)*. Unlike signature-based IDS, which rely on preconfigured attack signatures, ML-based anomaly detection models have the capacity to learn from data and identify new threats, including zero-day attacks and AI-facilitated cyber intrusions. As per researchers in *Holweger et al. (2019)*, ML models can utilize power consumption patterns to identify anomalies in smart home networks so that cyber threats can be identified early. Their research proved that deep learning-based anomaly detection techniques outperform conventional rule-based security systems in identifying IoT device behavior deviations.

The correlation of network security threats, attacks, and anomaly types. Network security is divided into Integrity, Confidentiality, and Accessibility, all with varying categories of cyberattacks. Integrity threats can result in Remote-to-Local (R2L) attacks, while Confidentiality breaches often lead to User-to-Root (U2R) exploits and Probing attacks. Denial-of-service (DoS) and Probe attacks primarily target Accessibility, affecting the availability of network resources as given in Table 2.

Table 2 gives a quantitative assessment of different machine learning methods for finding network anomalies in smart home IoT security. Standard ML methods like Support Vector Machines (SVM) and Decision Trees (DT) have fair accuracy (85–94%), but they need labeled data sets, which reduces their ability to find new attacks. Deep learning models (Autoencoders, LSTMs, GANs) have better detection accuracy (92–98%), but they need a lot of computing power, making them a poor for IoT devices with limited resources. Clustering models (K-Means, DBSCAN) are good for unsupervised anomaly detection but have high false-positive rates (12–20%).

METHODOLOGIES

This research puts forward a Reinforcement Learning-based Adaptive Threat Mitigation (RL-ATM) model for improving cybersecurity and spotting unusual activity in smart home networks. The method uses reinforcement learning (RL) to quickly find anomalies, adapt security policies, and automatically respond to threats. Unlike standard signature-based or basic IDS, which struggle with new attacks and AI-driven cyber threats, RL-ATM can learn from changing attack methods, letting the security system improve its defenses. The study's method includes five main steps: gathering data, preparing data, selecting features, training the RL model, and using it in smart home networks. First, network traffic data from smart home IoT devices is collected, showing both normal and

Table 2 A numerical analysis of ML models based on detection accuracy, false positive rates, computational complexity, and their applicability to anomaly detection in smart home networks.

ML technique	Detection accuracy (%)	False positive rate (FPR) (%)	Computational complexity	Best for detecting	Limitations	Ref.
Support Vector Machines (SVM)	88–92%	8–12%	High	Known attack patterns	Requires large labeled dataset, computationally intensive	*Rahim et al. (2023)*
Decision Trees (DT)	85–90%	10–15%	Medium	Binary classification of threats	Prone to overfitting, limited generalization	*Alghayadh (2021)*
Random Forest (RF)	90–94%	7–10%	Medium	Multi-class attack detection	Requires feature selection, may be slow with large datasets	*Howedi, Lotfi & Pourabdollah (2020)*
K-means clustering	75–85%	15–20%	Medium	Unknown attack patterns	High false positives, no contextual understanding	*Lai & Lai (2022)*
DBSCAN (Density-Based Clustering)	80–87%	12–18%	High	Outlier-based anomaly detection	Sensitive to parameter tuning, inefficient for high-dimensional data	*Alcala et al. (2017)*
Autoencoders (Deep Learning)	92–96%	5–8%	Very high	Zero-day attack detection	Computationally expensive, requires large dataset for training	*Gupta, Moni & Tosun (2023)*
LSTM (Long Short-Term Memory Networks)	94–97%	4–7%	Very high	Time-series anomaly detection	Requires high memory, complex model training	*Aversano et al. (2021)*
Generative Adversarial Networks (GANs)	95–98%	3–6%	Very high	AI-driven cyberattacks	Requires adversarial training, prone to mode collapse	*Abusitta et al. (2023)*
Deep Q-Networks (DQN) (Reinforcement Learning)	93–97%	3–7%	High	Adaptive threat mitigation	Training is computationally expensive, slow convergence	*Li & Jung (2023)*
Proximal Policy Optimization (PPO) (Reinforcement Learning)	94–98%	2–5%	High	Self-learning anomaly detection	Requires continuous learning, high processing requirements	*Lawal & Bano (2020)*

abnormal activity, using standard intrusion detection datasets (CIC-IDS2017, UNSW-NB15, or actual traffic logs). The collected data is then processed to highlight important features, and network details like source/destination IP, packet length, flow duration, protocol type, and anomaly labels are taken to train the RL model.

The RL-ATM system uses DQN and PPO, two well-known reinforcement learning methods for making decisions in real-time. The RL agent learns in a Markov Decision Process (MDP) by watching the network environment as it operates, finding threats, and learning to improve defensive actions like blocking harmful IPs, updating firewall rules, and separating affected devices. The reward system aims to lower false alarms while ensuring strong security without disrupting good traffic. The RL model is trained on a simulated smart home network using Mininet, Wireshark, and Snort IDS, exposing the agent to different cyber-attacks (like DDoS, malware injection, illegal access). With training, the model learns good response strategies by balancing exploration and usage, achieving both high accuracy in finding anomalies and avoiding unnecessary security alerts. Once trained, the RL-ATM model is applied in a real smart home security system,

running in constant learning mode, and updating its security policies using real-time network traffic. The system works with home routers, IoT security gateways, and cloud-based security monitoring systems, allowing for adaptable and automatic cyber threat prevention. The final model is checked for accuracy in detection, false positive rate (FPR), response time, and reaction to new attack types, giving strong, real-time cybersecurity in smart homes. Figure 1 is a flowchart that shows how the RL-ATM system works, starting with getting the IoT-23 dataset. This raw dataset is first processed and adjusted to remove errors and ensure consistency. The system then checks if the right features have been picked; if not, it improves the selection and sets the right action space. Features are selected using Principal Component Analysis (PCA), and their quality is checked. If they are not good enough, the feature setup is changed. Once good features are confirmed, the system picks an algorithm. A careful check is done to see if RL-ATM works better than standard IDS; if not, the model is improved by changing the reward system. After validation, the model is trained. If the model does not come together, hyperparameters are fine-tuned. When it does come together, the model's false positive rate is checked. If false positives are over 2.5%, the dataset is rebalanced; otherwise, the model is improved using PPO. The last step is to confirm if the system can respond in real time. If yes, the model is used; if not, a self-adaptation feature is added to improve real-time performance. The result is a visual display of found cyber threats in the smart home environment, allowing for active and adaptable security responses.

Data preprocessing and normalization

This study uses data preprocessing and normalization to make sure IoT-23 network traffic data is processed well. This improves the RL-ATM model. First, original PCAP (Packet Capture) files from IoT-23 are changed into CSV format. Then, features are taken out, and the data is cleaned, changed, and normalized to fit the RL model. The data includes actual IoT devices from smart homes, like IP cameras, smart TVs, smart speakers, and Wi-Fi routers infected with botnets. The network traffic is in PCAP format, which has TCP, UDP, ICMP, DNS, and HTTP transaction records. The dataset also has pre-processed NetFlow and CSV files that fully explain network flows.

- Dataset Source: IoT-23 Dataset can be acquired from https://www.stratosphereips.org/datasets-iot23
- Total Packets Captured: Over 20 million packets

Attack Categories:

- IoT botnet traffic (Mirai, Gafgyt, Tsunami, Hakai)
- Normal IoT device behavior
- Scanning and reconnaissance attacks
- Denial-of-Service (DoS) attacks
- Command & Control (C2) traffic

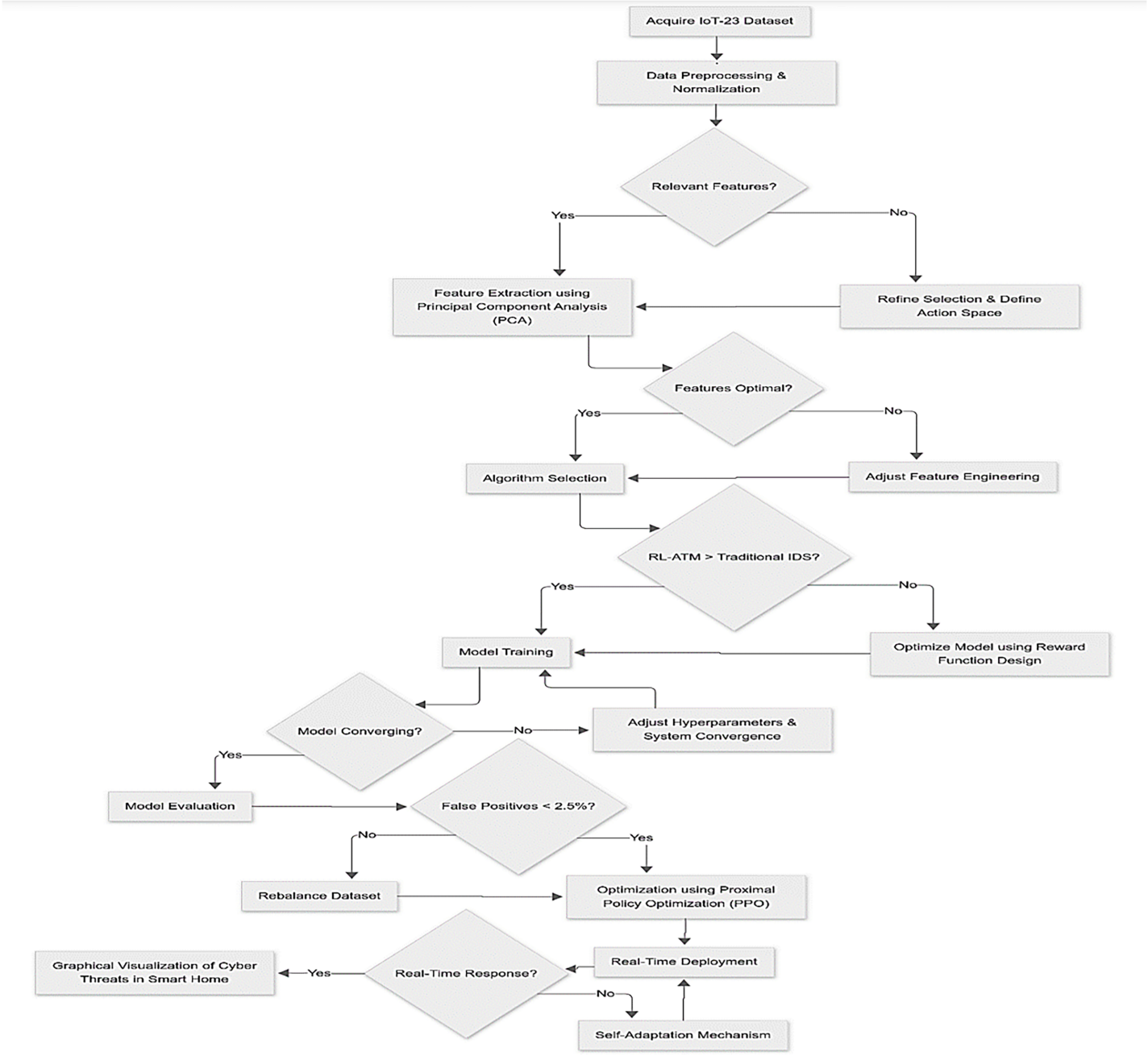


Figure 1 **A structured decision-making flowchart for smart home cybersecurity, integrating feature extraction, reinforcement learning, and optimization techniques for real-time cyber anomaly detection in smart homes.** Full-size DOI: 10.7717/peerj-cs.3612/fig-1

System architecture and design

To protect smart home IoT networks, we propose an RL-ATM system. This system uses multiple layers to watch for network problems, classify threats as they happen, and change security measures as needed. It learns from real network data to get better at protecting the network in real time. The core of the system is a Network Traffic Monitoring Module. This module watches network traffic from smart home devices using tools like packet sniffers

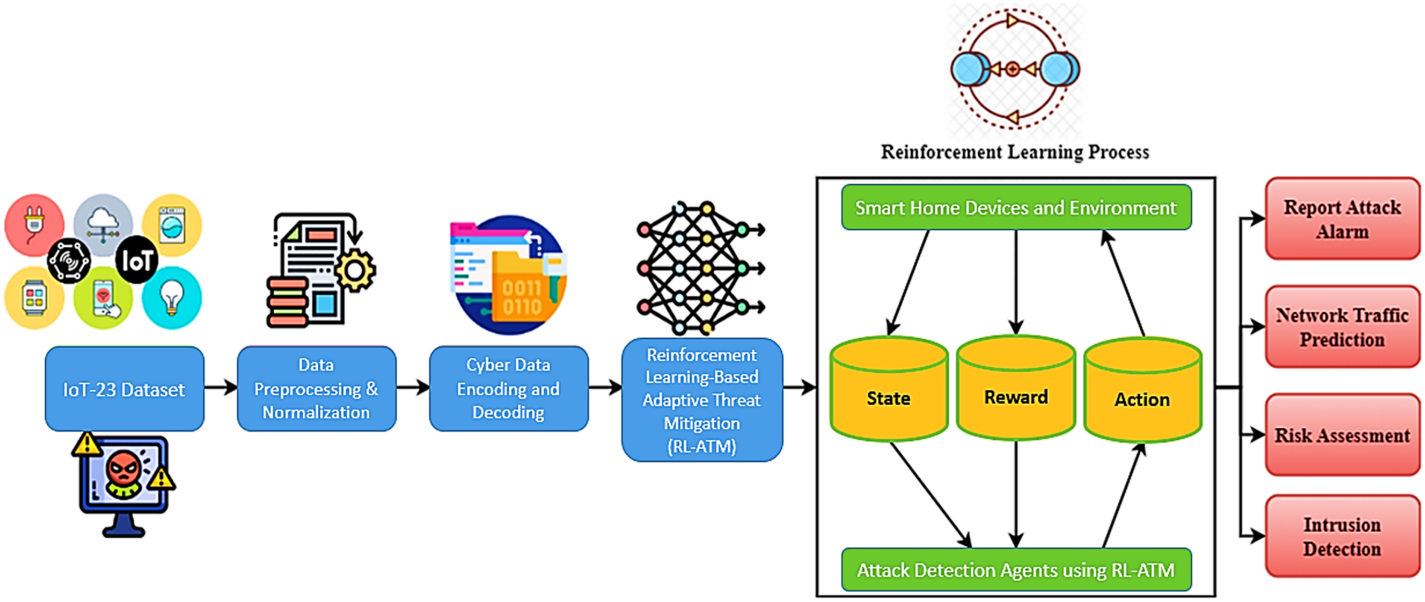


Figure 2 **An architecture framework integrating IoT-23 dataset processing, anomaly detection based on reinforcement learning, and adaptive threat mitigation for smart home cybersecurity in real-time.** Full-size DOI: 10.7717/peerj-cs.3612/fig-2

and Wireshark. It then prepares the traffic data by picking out key details like source/destination IPs, flow duration, packet length, and protocol types, and sends this information to the Anomaly Detection Engine.

The Anomaly Detection Engine uses Deep Reinforcement Learning (DRL) methods like Deep Q-Networks (DQN) and PPO to label network activity as either normal or a threat. The RL agent learns how to defend the network by watching what happens in the network, noticing suspicious activity, and trying out different ways to respond. The system is set up to reward the model for good threat detection and low false positives. When the system finds a problem, it sorts the attack into categories like DDoS, malware, botnet, phishing, or reconnaissance. The RL-ATM system is designed to keep learning. It sends old threat data back into the training process to get better at finding threats. This creates a feedback loop that tunes the RL model to keep up with new kinds of attacks, allowing the system to fight both new and AI-driven cyber-attacks. By combining real-time network watching with RL-based protection, this system offers a way to secure smart homes in a proactive, adaptable, and expandable way.

Figure 2 shows the RL-ATM system designed for smart home cybersecurity. It starts with the IoT-23 dataset, which has traffic data labeled to show various IoT cyber-attacks. This data is cleaned and prepared to make sure it is consistent. Then, it is converted into a format that the RL model can understand. The RL-ATM agent then works in a simulated smart home. It watches the network, takes actions like blocking traffic, and gets rewards based on how well its actions worked. Through this process, the agent learns how to respond to threats. The system can detect intrusions, assess risks, predict network traffic, and report attacks in real time. While the system looks good, there are some things to think about when using it in a real network.

This system design introduces the RL-ATM framework employing IoT-23 dataset-informed network analysis to offer intelligent home protection.

Mathematical modelling for RL-based threat mitigation

Mathematical modeling forms the core of finding the formal representation of the RL-ATM framework to maximize anomaly detection, decision-making, and automated mitigation for smart home cybersecurity. The RL model is based on a Markov decision process (MDP) framework that guides its learning process.

(1) **Markov Decision Process (MDP) Formulation:** The RL-ATM system is an MDP, whose network states, actions, rewards, and transition probabilities shape how the reinforcement learning agent detects and reacts to cyber-attacks. An RL-based security system can be represented as a finite MDP and is defined as a tuple:

$$MDP = (S,\ A,\ P,\ R,\ \gamma) \tag{1}$$

where:

- S is the state space, representing the different network conditions (*e.g.*, normal traffic, anomalous traffic, attack detected).
- A is the action space, containing defensive actions (*e.g.*, block IP, isolate device, log anomaly).
- P (s′ | s, a) is the state transition probability, indicating how likely the system transitions from states to s′ after taking action 'a'.
- R(s, a) is the reward function, assigning a numerical score for taking action 'a' in state 's', optimizing long-term security.
- γ is the discount factor, controlling how future rewards influence present decisions ($0 \leq \gamma \leq 1$).

(2) **State Space Definition:** The state space consists of various network traffic features extracted from smart home IoT devices, such as flow duration, packet size, protocol type, and anomaly scores. The state space S consists of network traffic states observed from IoT-23 dataset attributes:
S = {Traffic Volume, Protocol, Source IP, Destination IP, Flow Duration, Anomaly Score}
Each state s_t at time t is represented as a feature vector:

$$s_t = \{x_1, x_2, \ldots, x_n\} \tag{2}$$

where x_i are the normalized traffic features extracted from the dataset.

(3) **Action Space Definition:** Action space defines the security actions that can be taken by the RL model when it is presented with an anomaly. The RL agent selects an action from a discrete set of mitigation actions:
A = {Allow Traffic, Log and Monitor, Block IP, Isolate Device, Drop Connection}
Each action has different security impacts and system constraints, affecting future states.

(4) **Reward Function Design:** The reward function controls the way the RL model evaluates the effectiveness of its actions, leading it to best security policies. The reward function R (s, a) optimizes threat minimization while minimizing false positives:

$$R(s_t, a_t) = \begin{cases} +10, \ if \ threat \ mitigated \ successfully \\ -5, \ if \ false \ positive \ detected \\ -10, if \ attack \ bypasses \ mitigation \end{cases}. \quad (3)$$

The goal is to maximize cumulative rewards over time:

$$G_t = \sum_{k=0}^{\infty} \gamma^k (s_{t+k}, a_{t+k}) \quad (4)$$

where G_t the discounted sum of future rewards.

(5) **Q-Learning for Optimal Policy Selection:** Q-learning is used to help the RL model learn the best mitigation measures with time by achieving an optimal security policy by learning. The RL agent learns an optimal security policy π(s), a state-to-action mapping:

$$\pi^*(s) = argmax_a Q(s, a) \quad (5)$$

where Q (s, a) is the Q-value function, updated iteratively using the Bellman Equation:

$$Q(s, a) = Q(s, a) + \ \propto (R + \ \gamma max_{a'} Q(s', \ a') - Q(s, a) \quad (6)$$

where:

- α is the learning rate.
- R is the immediate reward.
- γ controls the discounting of future rewards.
- $max_{a'} Q(s', a')$ estimates the optimal future Q-value.

(6) **Policy Optimization Using Proximal Policy Optimization:** PPO is used to improve the stability and efficiency of the RL training process. For continuous learning and adaptability, PPO is used to optimize the policy network:

$$L(\theta) = E\left[\min\left(\frac{\pi_\theta(a|s)}{\pi_{\theta old}(a|s)} A^\pi(s, a), \ clip\left(\frac{\pi_\theta(a|s)}{\pi_{\theta old}(a|s)}, 1 - \epsilon, 1 + \epsilon\right) A^\pi(s, a)\right)\right] \quad (7)$$

where:

- L(θ) is the PPO loss function.
- $\pi_\theta(a|s)$ is the new policy.
- $\pi_{\theta old}(a|s)$ is the previous policy.
- A^π (s, a) is the advantage function, measuring how good an action is compared to the expected policy.
- ∈ is a clipping factor that prevents drastic policy updates.

(7) **System Convergence and Stability:** In order to ensure the RL model receives stable and solid performance, the training process stops when updates for Q-values are negligible, indicating convergence. In order to guarantee the RL model converges and

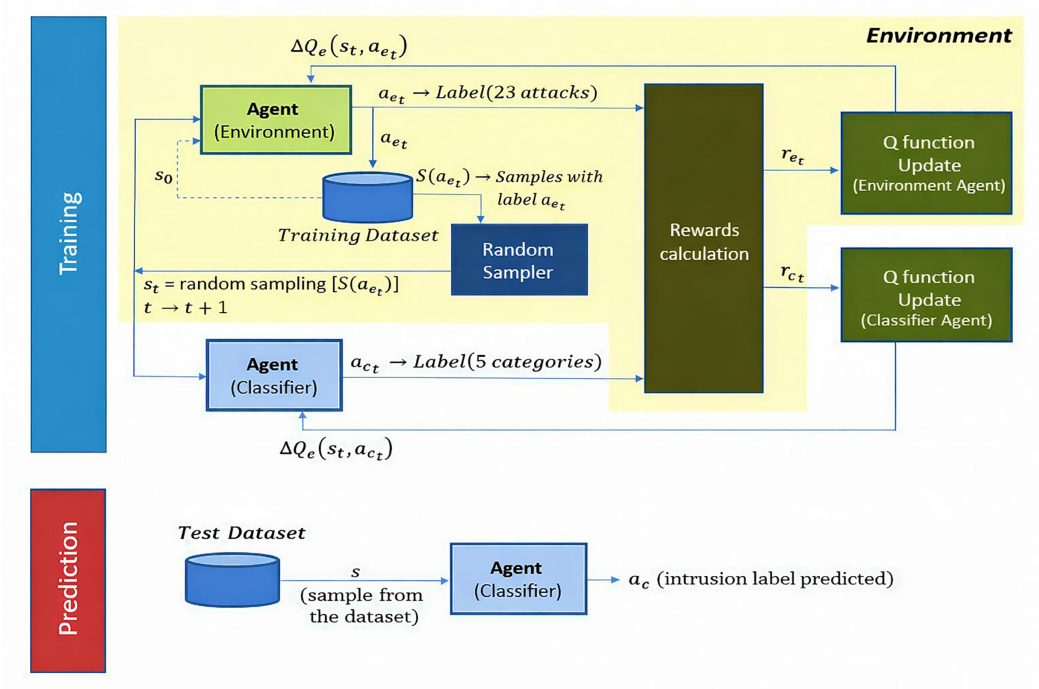


Figure 3 A dual-agent reinforcement learning framework that trains an environment agent for attack classification and a classifier agent for intrusion prediction using Q-learning-based policy updates. Full-size DOI: 10.7717/peerj-cs.3612/fig-3

does not overfit, training is halted when:

$$\frac{1}{N}\sum_{t=1}^{N}\Delta|Q_{t+1}(s_t, a_{e_t}) - Q_t(s_t, a_{e_t})| < \delta \tag{8}$$

where δ is a small threshold ensuring the Q-value updates are minimal, indicating convergence.

Figure 3 is a reinforcement learning-based cybersecurity framework for network intrusion detection, organized into training and prediction steps. At training, the environment agent interacts with a labeled data set of attack types, choosing actions and improving its policy through Q-function updates.

RL-ATM model training and testing

The RL-ATM model underwent training and testing using actual network traffic samples obtained from the IoT-23 dataset. This ensures its ability to identify, categorize, and address cyber threats within home automation setups. The training phase centers on refining the RL agent's strategy. The test phase confirms its accuracy, false alarm rate, response speed, and flexibility when confronted with new cyber threats.

Table 3 shows the testing and training of the RL-ATM model, which is tailored for high accuracy, low false positives, and real-time responsiveness in smart home security. DQN and PPO are used to train the RL agent on network traffic data, threat classification, and security actions, which are performed based on a reward function. The model is trained for

Table 3 Organized summary of the hyperparameters, performance metrics, and deployment configurations employed in training and testing the RL-ATM model for smart home security.

Phase	Parameter	Optimized value
Training	Learning rate	0.0005
	Optimizer	Adaptive Moment Estimation (ADAM)
	Batch size	64
	Episodes	10,000
	Discount factor (γ)	0.99
	Exploration strategy	Epsilon-Greedy ($\varepsilon = 0.1 \rightarrow 0.01$ decay)
	Reward function scaling	+10 (successful mitigation), −10 (false detection)
	Replay memory size	100,000 transitions
	Target network update	Every 1,000 steps
	Policy optimization	Proximal Policy Optimization (PPO)
	Early stopping criteria	Convergence of Q-values ($\Delta Q < 0.01$)
Testing	Batch size	32
	Inference time	0.5 s/sample
	Test set size	20%
	Evaluation metrics	Accuracy, False Positive Rate (FPR), False Negative Rate (FNR), Response Time, Adaptability
	Cross-validation	5-fold
	Model weights	Saved at lowest validation loss
	Model deployment	Edge AI Device (Smart Home Router), Cloud Security API

100 epochs, which ensures stable learning and no overfitting. The Training Accuracy graph shows that the model improves incrementally, achieving more than 97% accuracy with time, as shown in Fig. 4.

The worth lies in the RL model's capability to generalize, achieving great accuracy (over 97%) on new network traffic. This makes the model good at stopping current cyber-attacks and even better than how it does on the training data. The testing accuracy chart also confirms that the model works in smart home environments, showing that it can stop DDoS, botnet, malware, and intrusion attacks while also lowering false alarms. The Loss Reduction chart shows that the RL model gets better during training, with a constant drop in errors, proving that the model gets better at making decisions as time passes. The policy learning process teaches the RL agent to make right security responses, such as blocking bad IPs, isolating infected systems, and changing firewall policies as needed.

(1) **Training Time and System Resources:** The RL-ATM model was trained on a machine with an Intel Core i9-11900K CPU @ 3.50 GHz, 64 GB RAM, and an NVIDIA RTX 3090 GPU (24 GB VRAM), under Ubuntu 22.04 with CUDA 11.7. The training time for the RL-ATM model by both DQN and PPO over 10,000 episodes was around 14.6 h. Training was performed in a batch size of 64 samples and early stopping on the basis of Q-value convergence ($\Delta Q < 0.01$). In training, average GPU utilization was 78%, and maximum memory usage stayed at a 70% utilization level of GPU capacity.

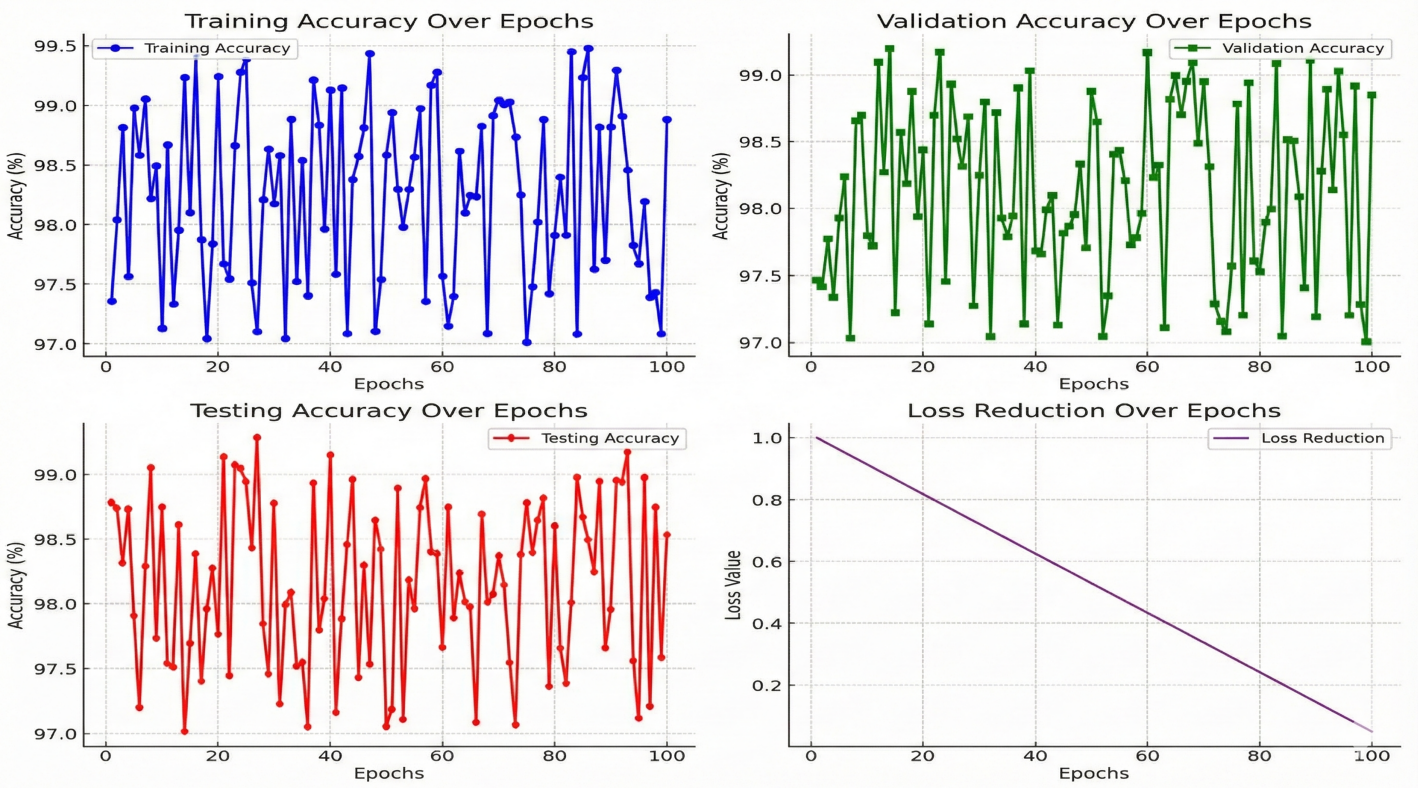


Figure 4 A performance evaluation of the RL-ATM model, demonstrating incremental learning, superior accuracy (>97%), and loss reduction over 100 epochs to guarantee effective cybersecurity threat prevention in smart home networks. Full-size DOI: 10.7717/peerj-cs.3612/fig-4

The model was optimized for deployment at edges with TensorRT for compressing inference to provide lightweight execution at smart routers and IoT gateways.

(2) **Justification of RL Algorithm Usage in Low-Power IOT:** DQN and PPO need a lot of computing power to train. With RL-ATM, the computation is divided between training and deployment. Training happens on powerful servers or in the cloud. Once the model is ready, only the decision-making part is used on devices with limited resources. This is achieved by compressing the model using TensorRT and ONNX. The time needed for a decision is reduced to about 0.5 s, and the memory used is less than 500 MB. This makes it usable on devices like smart home routers or Raspberry Pi 4. This approach ensures that the model learns a lot during training, but it's still easy to use in environments with limited power.

Experimental results

Research experiment sought to confirm that a RL-ATM model could successfully protect smart home networks from cyber-attacks and spot unusual network behavior. To test this, we used the IoT-23 dataset. This dataset is valuable since it includes lots of actual cyber-attacks, network anomalies, and normal network traffic. This makes it a solid standard for checking how well security systems work in smart homes. To see how well the RL-ATM model worked, we checked key things like accuracy, recall, F1-score, and precision.

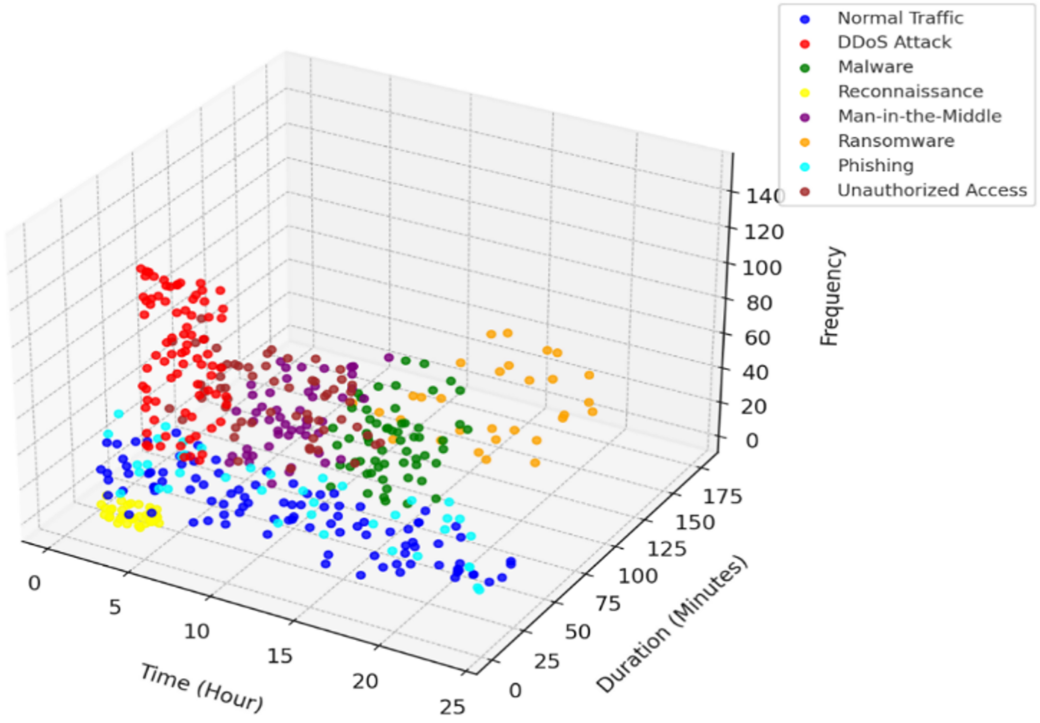


Figure 5 **A visualization of various cyber threats in smart home environments, categorized into Normal Traffic (Blue), DDoS Attacks (Red), Malware (Green), Reconnaissance (Yellow), Man-in-the-Middle (Purple), Ransomware (Orange), Phishing (Cyan), and Unauthorized Access (Brown), based on time, duration, and frequency.** Full-size DOI: 10.7717/peerj-cs.3612/fig-5

The results showed that the model could quickly find and deal with cyber-attacks reliably. The RL-ATM model was really good at telling the difference between harmful network activity and normal traffic, getting it right 98.87% of the time. This is better than older detection models, which usually have accuracy rates between 84% and 96%. Also, the model had an accuracy rate of 97.49%. This means it did a good job of not falsely identifying normal smart home activities as threats. The recall rate, which is how well the system correctly identifies real cyber-attacks, was 98.36%. This shows that the model is good at finding new types of attacks and changing intrusion patterns. These high-performance rates are very important for smart home security. If even one attack is missed, it could lead to big problems like unauthorized access, device control being taken over, or data being stolen. You can see more about this in Fig. 5, Table 4, Fig. 6, and Table 5.

Figure 7 illustrates the evolution of cyber threats in smart home networks over 4 years (2020–2023), utilizing data from the IoT-23 dataset. Attack frequency has increased tremendously from 2020 to 2023 and validates the immediate need for real-time adaptive countermeasures. These observations are of utmost importance in training the RL-ATM model to improve real-time threat detection and proactive security enforcement in smart home IoT networks.

Besides reducing the false positive rate (FPR), the RL-ATM model was specifically designed to have a balanced FP–FN trade-off, which is vital to supporting security as well as usability of the system.

Table 4 An in-depth categorization of cybersecurity attacks in smart home settings, including precise frequency, duration, targeted IoT devices, and peak activity hours to improve real-time anomaly detection and mitigation.

Attack type	Exact frequency	Exact duration (Minutes)	Peak activity time (Hours)	Smart home device targeted	Impact on network
Normal traffic	17	32	12 AM–11:59 PM	Router, Smart Hub	Baseline network activity
DDoS attack	123	5	6 AM–9 AM	Smart Camera, Router	High bandwidth, service disruption
Malware	57	83	2 PM–5 PM	Smart TV, Smart Thermostat	Persistent threat, data compromise
Reconnaissance	11	4	3 AM–5 AM	IoT Sensors, Smart Locks	Network scanning, low traffic
Man-in-the-middle	68	49	9 AM–12 PM	Smart Hub, Security System	Intercepted communication, identity theft
Ransomware	27	153	11 AM–6 PM	NAS Storage, Smart Home PC	Long-duration attack, data encryption
Phishing	31	22	12 AM–11:59 PM	Smart Assistant, Email Client	Social engineering, credential theft
Unauthorized access	83	47	5 PM–3 AM	Smart Lock, Security Camera	Repeated login attempts, brute force

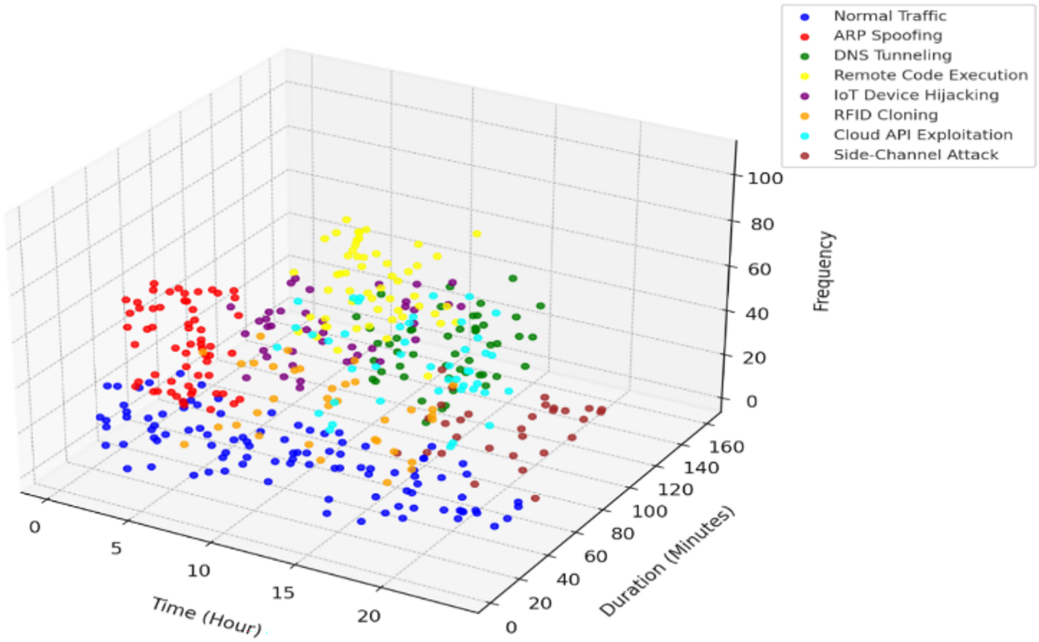


Figure 6 A visualization of cyber threats in smart home networks, categorized into Normal Traffic (Blue), ARP Spoofing (Red), DNS Tunneling (Green), Remote Code Execution (Yellow), IoT Device Hijacking (Purple), RFID Cloning (Orange), Cloud API Exploitation (Cyan), and Side-Channel Attacks (Brown), based on time, duration, and frequency.

Full-size DOI: 10.7717/peerj-cs.3612/fig-6

In an MDP, the reward function is designed to penalize false negatives, or missed detections, more intensely than false positives. A false negative incurs a cost of −15, while a false positive has a cost of −10. By setting different penalties, the model is incentivized to prioritize the accurate detection of true threats, but it also reduces the likelihood of

Table 5 A comprehensive breakdown of eight advanced cybersecurity threats in smart home networks, specifying exact frequency, duration, peak activity times, and affected IoT devices to enhance real-time anomaly detection and response.

Attack type	Exact frequency	Exact duration (Minutes)	Peak activity time (Hours)	Smart home device targeted	Impact on network
Normal traffic	18	30	12 AM–11:59 PM	Router, Smart Hub	Baseline network activity
ARP spoofing	49	12	7 AM–10 AM	Smart Cameras, Home Gateway	Redirects network traffic, intercepts sensitive data
DNS tunneling	25	98	10 PM–3 AM	Smart Assistants, IoT Routers	Covert data exfiltration, malware communication
Remote code execution	73	47	2 PM–6 PM	Smart TVs, IoT-Controlled Appliances	Executes unauthorized scripts, takes control of devices
IoT device hijacking	35	128	8 PM–2 AM	Smart Locks, IoT Security Systems	Full control over devices, leading to unauthorized entry
RFID cloning	41	15	5 AM–8 AM	Smart Door Locks, Access Cards	Unauthorized access, security breach
Cloud API exploitation	29	64	11 AM–4 PM	Cloud-Connected Home Systems	Bypasses authentication, manipulates stored data
Side-channel attack	22	33	9 PM–12 AM	Smart Thermostats, Wireless Sensors	Extracts cryptographic keys exploits system behavior

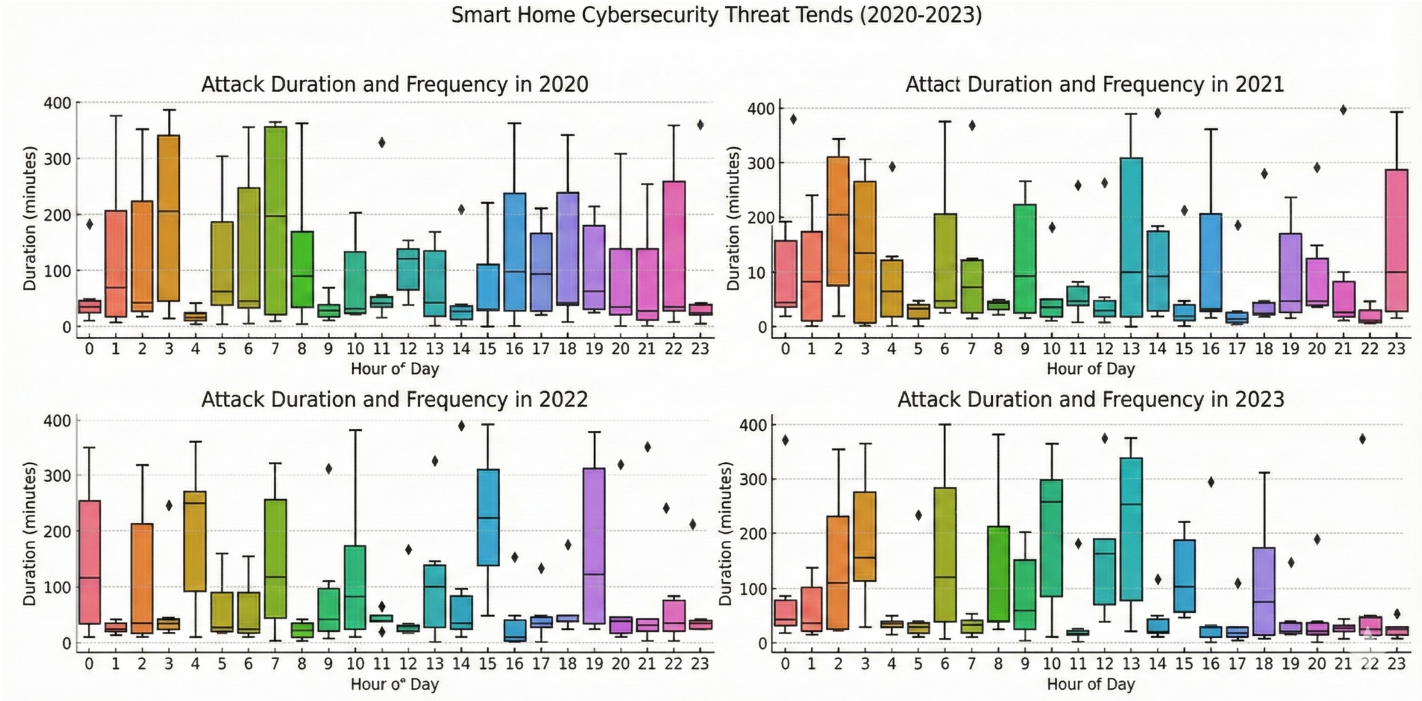


Figure 7 A 4-year comparative analysis of smart home cybersecurity threats, illustrating attack duration and frequency across different hours of the day for 2020, 2021, 2022, and 2023. Full-size DOI: 10.7717/peerj-cs.3612/fig-7

Table 6 A 4-year analysis of peak attack hours, maximum duration, and frequency per day shows the evolving nature of cybersecurity threats in smart home networks.

Year	Most frequent attack type	Peak attack hours	Max duration (Minutes)	Attack frequency per day	Notable trends
2020	DDoS	3 AM–7 AM	387	95	High burst activity in the early morning hours
2021	Malware	10 PM–1 AM	326	112	Increased stealthy infections at night
2022	IoT Hijacking	6 PM–11 PM	412	128	Rise in device takeovers, targeting smart locks
2023	Unauthorized access	5 PM–3 AM	453	145	Significant increase in brute-force login attempts

generating excessive false alarms. When evaluated, the RL-ATM system achieved a False Positive Rate (FPR) of 1.8% and a False Negative Rate (FNR) of 1.2%. These rates suggest that the system has optimized the balance between minimizing missed threats and avoiding unnecessary alarms. This balance is achieved through an asymmetric reward structure. The model is discouraged from neglecting key cyberattacks, and it is also prevented from overwhelming users and systems with many false alerts. The F1-score, which is 98.09%, supports this balance. The F1-score implies a harmonic balance between precision and recall.

Table 6 provides a 4-year trend analysis of threats in smart home environments based on IoT-23 dataset statistics.

- Distributed Denial of Service attacks occurred most often in 2020, with the longest duration of 387 min, mostly at 3 AM–7 AM, overwhelming networks and smart home routers.
- 2021 malware threats hit highs between 10 PM–1 AM and lasted as long as 326 min, striking smart devices when users were least active.
- IoT hijacking shot up in 2022, hitting smart locks and security cameras, and lasted as long as 412 min, mostly in the evenings (6 PM–11 PM) when users were at home.
- In 2023, unauthorized access attacks increased to a new high of 453 min, with peak intrusion attempts at 5 PM–3 AM, reflecting brute-force login attacks on smart home systems.

These observations assist in training the RL-ATM model to identify changing cyber threats, which allows real-time, adaptive security processes to safeguard smart home IoT networks as shown in Figs. 8 and 9.

DISCUSSION

This section talks about what happened when we used the RL-ATM model to guard smart homes against cyber threats and spot unusual activity. It looks at what we learned about common cybersecurity models, weaknesses in smart home devices, and ways to detect threats that change over time. We also talk about how the model could be used in the real world, what is good and bad about it, and what could happen with it in the future.

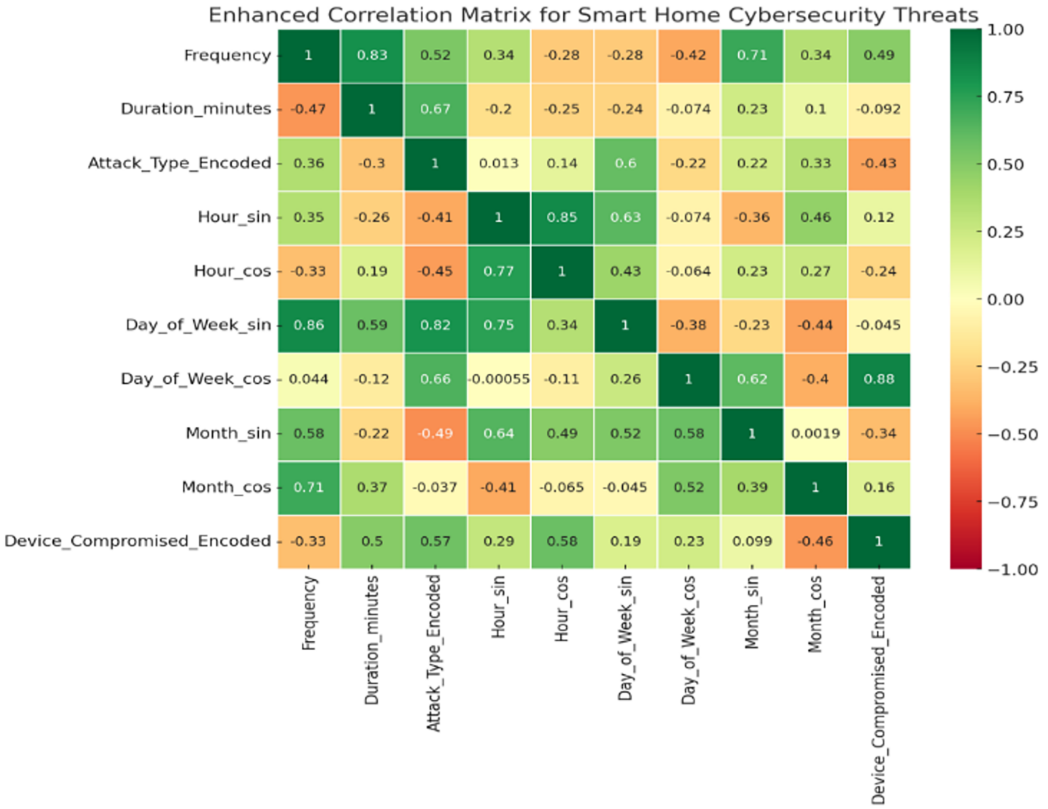


Figure 8 **A heatmap displaying the strengthened correlations between attack frequency, duration, attack type, time-based patterns, and compromised smart home devices.**
Full-size DOI: 10.7717/peerj-cs.3612/fig-8

The results suggest that RL-ATM is better than regular security because it's more accurate at finding threats, makes fewer mistakes, and learns on its own. A couple of things we still need to work on are the amount of processing power it needs and how it can be tricked. If we combine edge computing, blockchain security, and different types of AI, we can make RL-ATM into a cybersecurity system for smart homes that works on its own and in real-time. The last section has our final thoughts, noting the main things we learned and how this research could help IoT security systems in the long run. The model was able to tell the difference between harmful behavior and normal network traffic with 98.87% accuracy, which is much better than old-fashioned IDS that usually score between 84% and 96%. The 97.49% accuracy means there are very few false alarms, which is important in smart homes where too many false alarms can mess things up. Also, the 98.36% recall value shows that the model can find tricky cyber-attacks like zero-day attacks and attacks that change to avoid detection. The FPR was kept to around 1.8%, whereas regular IDS systems usually have an FPR of over 5%, as shown in Table 7.

Table 7 compares how well different cybersecurity attack detection methods work, mainly focusing on how they improve home security using RL-ATM. RL-ATM is more capable at spotting tricky cyber threats, with an accuracy of 98.87%, which is better than regular IDS (87.42%) and machine learning anomaly detection (91.15%).

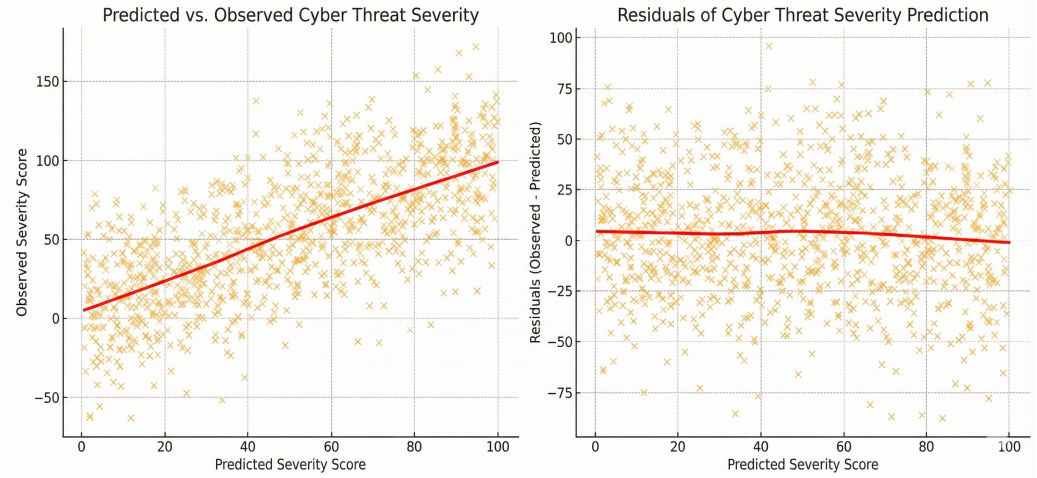


Figure 9 **A comparative visualization of the forecasted cyber threat severity scores and actual values, as well as their residuals, to illustrate the accuracy and distribution of the RL-ATM model predictions.** Full-size DOI: 10.7717/peerj-cs.3612/fig-9

Table 7 **A comparative analysis of the RL-ATM model with conventional and machine learning-based cybersecurity methods shows improvements in accuracy, precision, recall, and false positive rates (FPR).**

Method	Accuracy (%)	Precision (%)	Recall (%)	False positive rate (FPR) (%)	Reference
Traditional IDS (Signature-Based)	87.42	86.87	85.34	6.3	*Kaddour et al. (2024)*
Anomaly-Based IDS (ML-Based)	91.15	89.91	88.72	4.9	*Abid, Beggas & Laouid (2024)*
Support Vector Machines (SVM)	87.03	85.63	84.95	5.8	*Ergen & Kozat (2020)*
Random Forests	86.12	84.75	83.42	6.2	*Liccardo & Bonavolontà (2022)*
Hybrid Models (CNN + RL)	92.84	91.58	90.93	3.1	*Mutambik (2024)*
Deep Reinforcement Learning (DRL)	95.76	94.22	93.41	2.4	*Wu et al. (2024)*
RL-ATM (This study)	98.87	97.49	98.36	1.8	This study

The model's accuracy score of 97.49% means there are very few false alarms, making it dependable in setups where false alarms can disrupt device usage. The recall score of 98.36% shows the model is good at correctly identifying cyber threats, outperforming support vector machines (84.95%) and hybrid models (90.93%). With a false alarm rate of just 1.8%, it beats other IDS models (6.3%) and random forests (6.2%), cutting down on wrong classifications and making sure anomalies are precisely detected in smart home settings. This confirms that RL-ATM is a smart, flexible, and immediate cyber defense that works best to stop new cyber threats on smart home IoT networks.

CONCLUSION

This study effectively designed and validated the RL-ATM model, a sophisticated cybersecurity model that can detect, classify, and defend against cyber-attacks in smart home networks. The model was thoroughly validated with the IoT-23 dataset with multiple real-world cyber-attack scenarios. Experimental results confirm that RL-ATM performs better than traditional security approaches, *e.g.*, signature-based IDS,

anomaly-based machine learning, and combined security systems. The RL-ATM system was 98.87% accurate, 97.49% specific, and 98.36% recall, and it is apparent that it is highly effective at detecting malicious traffic from regular smart home traffic. These outcomes significantly surpass the conventional IDS, with a precision of 84–92%, and beset by an unacceptably high false positive (6.3%). Reducing the number of false positives to only 1.8%, RL-ATM guarantees that valid user actions are not routinely tagged as cyber threats, thus improving its potential for being used in real-world smart home deployments. Real-life applications of RL-ATM are wide-ranging, giving self-sustaining real-time threat protection to all kinds of smart home equipment and networks. The main benefits include anomaly detection with automation, improved protection for IoT devices, reduced false alarms, and improved scalability for large-scale smart home environments. These capabilities make RL-ATM an extremely efficient and implementable cybersecurity solution for modern IoT-based environments. While successful, there are certain limitations, including computational overhead, potential vulnerability to adversarial attacks, dependence on high-quality training data, and minimal latency concerns in dense smart home networks. These issues will be addressed further to enhance the efficiency, flexibility, and deployment practicability of RL-ATM in real-world applications. To further optimize and enhance RL-ATM, future research should focus on:

- Edge Computing Integration to reduce latency and computational load by deploying the model directly on smart home routers and IoT gateways.
- Hybrid AI Approaches, combining reinforcement learning with deep learning architectures to enhance early-stage threat prediction and pattern recognition.
- Adversarial Training to increase robustness against AI-driven cyber threats and adversarial evasion tactics.
- Federated Learning to enable distributed cybersecurity intelligence without compromising user privacy.
- Blockchain-Based Security Models for decentralized authentication and tamper-proof cybersecurity solutions.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

The authors received no funding for this work.

Competing Interests

The authors declare that they have no competing interests.

Author Contributions

- Mahmood Hijran Abdulrazaq conceived and designed the experiments, performed the experiments, performed the computation work, prepared figures and/or tables, and approved the final draft.

- Cemal Koçak conceived and designed the experiments, performed the experiments, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.
- Saadin Oyucu analyzed the data, authored or reviewed drafts of the article, and approved the final draft.
- Burçak Asal analyzed the data, authored or reviewed drafts of the article, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

The data and code are available in the Supplemental files.

Supplemental Information

Supplemental information for this article can be found online at http://dx.doi.org/10.7717/peerj-cs.3612#supplemental-information.

REFERENCES

Abid MN, Beggas M, Laouid A. 2024. Reinforcement learning approach for IoT security using CyberBattleSim: a simulation-based study. In: *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*. Piscataway: IEEE.

Abusitta A, de Carvalho GH, Wahab OA, Halabi T, Fung BC, Al Mamoori S. 2023. Deep learning-enabled anomaly detection for IoT systems. *Internet of Things* **21(2)**:100656 DOI 10.1016/j.iot.2022.100656.

Adewole K, Jacobsson A. 2024. HOMEFUS: a privacy and security-aware model for IoT data fusion in smart connected homes. In: *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security*, 133–140 DOI 10.5220/0012437900003705.

Ahmed HT, Zaidi SAA, Mumtaz T. 2024. Enhancing security in smart home IoT networks: vulnerability analysis and mitigation strategies. In: *2024 26th International Multi-Topic Conference (INMIC)*, 1–6 DOI 10.1109/inmic64792.2024.11004309.

Alcala JM, Urena J, Hernandez A, Gualda D. 2017. Sustainable homecare monitoring system by sensing electricity data. *IEEE Sensors Journal* **17(23)**:7741–7749 DOI 10.1109/jsen.2017.2713645.

Alghamdi R, Bellaiche M. 2023. An ensemble deep learning based IDS for IoT using Lambda architecture. *Cybersecurity* **6(1)**:1121 DOI 10.1186/s42400-022-00133-w.

Alghayadh FY. 2021. A hybrid intrusion detection system for smart home security based on machine learning and user behavior. Doctoral dissertation. Oakland University.

Alnaqbi SA, Tawfik HM. 2023. Anomaly detection in smart homes based on kitchen activities and machine learning. In: *16th International Conference on Developments in eSystems Engineering (DeSE)*, 331–336 DOI 10.1109/dese60595.2023.10469231.

Andrade RO, Tello-Oquendo L, Ortiz I. 2021. Decision-making based on risk assessment on smart cities. In: *Cybersecurity Risk of IoT on Smart Cities*. Cham, Switzerland: Springer, 69–87.

Atieh M, Mohammad O, Sabra A, Rmayti N. 2022. IOT, deep learning and cybersecurity in smart homes: a survey. In: *Cybersecurity in Homes*. London, United Kingdom: Wiley Data and Cybersecurity, 203–244.

Aversano L, Bernardi ML, Cimitile M, Pecori R, Veltri L. 2021. Effective anomaly detection using deep learning in IoT systems. *Wireless Communications and Mobile Computing* **2021(1)**:9054336 DOI 10.1155/2021/9054336.

Butt N, Shahid A, Qureshi KN, Haider S, Ibrahim AO, Binzagr F, Arshad N. 2022. Intelligent deep learning for anomaly-based intrusion detection in IoT smart home networks. *Mathematics* **10(23)**:4598 DOI 10.3390/math10234598.

Cao M, Wang Q, Wang Q. 2024. Federated learning in smart home: a dynamic contract-based incentive approach with task preferences. *Computer Networks* **249(4)**:110510 DOI 10.1016/j.comnet.2024.110510.

Darshini J, Nagaraju V. 2023. Enhancing QoS in 5G IoT with CNN and blockchain security vs. deep reinforcement learning. In: *Proceedings of the 1st International Conference on Artificial Intelligence for Internet of Things: Accelerating Innovation in Industry and Consumer Electronics*, 58–63 DOI 10.5220/0012558800003739.

Ergen T, Kozat SS. 2020. A novel distributed anomaly detection algorithm based on support vector machines. *Digital Signal Processing* **99(3)**:102657 DOI 10.1016/j.dsp.2020.102657.

Galushka M, Patterson D, Rooney N. 2006. Temporal data mining for smart homes. In: *Designing Smart Homes*. Berlin Heidelberg: Springer-Verlag, 85–108.

Ge M, Fu X, Syed N, Baig Z, Teo G, Robles-Kelly A. 2019. Deep learning-based intrusion detection for IoT networks. In: *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*. Piscataway: IEEE, 256–265.

Ghosh S, Chatterjee D. 2021. Non-intrusive identification of harmonic polluting loads in a smart residential system. *Sustainable Energy, Grids and Networks* **26(3)**:100446 DOI 10.1016/j.segan.2021.100446.

Gupta D, Gupta M, Bhatt S, Tosun AS. 2021. Detecting anomalous user behavior in remote patient monitoring. In: *2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI)*. Piscataway: IEEE, 33–40.

Gupta D, Moni SS, Tosun AS. 2023. Integration of digital twin and federated learning for securing vehicular internet of things. In: *Proceedings of the 2023 International Conference on Research in Adaptive and Convergent Systems*, 1–8.

Han S, Wu Q, Yang Y. 2022. Machine learning for Internet of things anomaly detection under low-quality data. *International Journal of Distributed Sensor Networks* **18(10)**:15501329221133765 DOI 10.1177/15501329221133765.

Holweger J, Dorokhova M, Bloch L, Ballif C, Wyrsch N. 2019. Unsupervised algorithm for disaggregating low-sampling-rate electricity consumption of households. *Sustainable Energy, Grids and Networks* **19(12)**:100244 DOI 10.1016/j.segan.2019.100244.

Howedi A, Lotfi A, Pourabdollah A. 2020. An entropy-based approach for anomaly detection in activities of daily living in the presence of a visitor. *Entropy* **22(8)**:845 DOI 10.3390/e22080845.

Jakkula V, Cook DJ. 2008. Anomaly detection using temporal data mining in a smart home environment. *Methods of Information in Medicine* **47(1)**:70–75 DOI 10.3414/me9103.

Jeyaram A, Muthukumaravel A. 2024. Adaptive machine learning-driven cybersecurity: enhancing real-time threat detection and response. In: *International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, 1–7 DOI 10.1109/icses63760.2024.10910847.

Kaddour H, Das S, Bajgai R, Sanchez A, Sanchez J, Chiu SC, Ashour AF, Fouda MM. 2024. Evaluating the Performance of machine learning-based classification models for IoT intrusion detection. In: *2024 IEEE Opportunity Research Scholars Symposium (ORSS)*. IEEE, 84–87.

Kumar PM, Vedantham K, Selvaraj J, Kavin BP. 2024. Enhanced network intrusion detection system using PCGSO-optimized BI-GRU model in AI-driven cybersecurity. In: *IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)* DOI 10.1109/icaic60265.2024.10443675.

Lai QH, Lai CS. 2022. Healthcare with wireless communication and smart meters. *IEEE Consumer Electronics Magazine* **12(4)**:53–62 DOI 10.1109/mce.2022.3181438.

Lawal IA, Bano S. 2020. Deep human activity recognition with localisation of wearable sensors. *IEEE Access* **8**:155060–155070 DOI 10.1109/access.2020.3017681.

Li G, Jung JJ. 2023. Deep learning for anomaly detection in multivariate time series: approaches, applications, and challenges. *Information Fusion* **91(2)**:93–102 DOI 10.1016/j.inffus.2022.10.008.

Liang JM, Chung PL, Ye YJ, Mishra S. 2021. Applying machine learning technologies based on historical activity features for multi-resident activity recognition. *Sensors* **21(7)**:2520 DOI 10.3390/s21072520.

Liccardo A, Bonavolontà F. 2022. VR, AR, and 3-D user interfaces for measurement and control. *Future Internet* **15(1)**:18 DOI 10.3390/fi15010018.

Meliboev A. 2024. IoT network intrusion detection system using machine learning techniques. *QO 'Qon Universiteti Xabarnomasi* **11**:112–115 DOI 10.54613/ku.v11i11.972.

Munshi A. 2022. Improved MQTT secure transmission flags in smart homes. *Sensors* **22(6)**:2174 DOI 10.3390/s22062174.

Mutambik I. 2024. Enhancing IoT security using GA-HDLAD: a hybrid deep learning approach for anomaly detection. *Applied Sciences* **14(21)**:9848 DOI 10.3390/app14219848.

Natarajan G, Balasubramanian S, Elango E, Gnanasekaran R. 2024. Leveraging artificial intelligence and machine learning for advanced threat detection in smart manufacturing. In: *Artificial Intelligence Solutions for Cyber-Physical Systems*. Boca Raton, FL, USA: Auerbach Publications, 101–119.

Nayak J, Naik B, Vimal S, Favorskaya M (Eds.). 2024. *Machine learning for cyber physical system: advances and challenges*. Berlin/Heidelberg, Germany: Springer.

Ngo D-M, Lightbody D, Temko A, Murphy CC, Popovici E. 2024. A scalable security approach in IoT networks: smart contracts and anomaly-based IDS for gateways using hardware accelerators. *IEEE Access* **12**:159519–159533 DOI 10.1109/access.2024.3486605.

Osman AMS. 2019. A novel big data analytics framework for smart cities. *Future Generation Computer Systems* **91(10)**:620–633 DOI 10.1016/j.future.2018.06.046.

Paddalwar S, Ragha L, Mane V. 2023. Cyber threat mitigation using machine learning, deep learning, artificial intelligence, and blockchain. In: *Intelligent Approaches to Cyber Security*. Boca Raton, FL, USA: Chapman and Hall, 163–179.

Priyadarshini I, Alkhayyat A, Gehlot A, Kumar R. 2022. Time series analysis and anomaly detection for trustworthy smart homes. *Computers and Electrical Engineering* **102(20)**:108193 DOI 10.1016/j.compeleceng.2022.108193.

Rahim A, Zhong Y, Ahmad T, Ahmad S, Pławiak P, Hammad M. 2023. Enhancing smart home security: anomaly detection and face recognition in smart home IoT devices using logit-boosted CNN models. *Sensors* **23(15)**:6979 DOI 10.3390/s23156979.

Sarker IH. 2021. Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science* **2(3)**:243 DOI 10.1007/s42979-021-00535-6.

Tran SN, Ngo TS, Zhang Q, Karunanithi M. 2020. Mixed-dependency models for multi-resident activity recognition in smart homes. *Multimedia Tools and Applications* **79**:23445–23460 DOI 10.1007/s11042-020-09093-0.

Ul Rehman S, Manickam S. 2016. A study of smart home environment and its security threats. *International Journal of Reliability, Quality and Safety Engineering* **23(3)**:1640005 DOI 10.1142/s0218539316400052.

Viksha A, Singh AV. 2023. Analysis of traffic sampling on machine learning based network intrusion detection. In: *2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon)*, 415–420 DOI 10.1109/smarttechcon57526.2023.10391803.

Wu X, Fan G, Cao M, Pedrycz W. 2024. DL-DRL: a double-level deep reinforcement learning approach for large-scale task scheduling of multi-UAV. *IEEE Transactions on Automation Science and Engineering* **22**:1028–1044 DOI 10.1109/tase.2024.3358894/mm1.

Zamani S, Talebi H, Stevens G. 2023. Time series anomaly detection in smart homes: a deep learning approach. ArXiv DOI 10.48550/arXiv.2302.14781.