Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH
AND DEVELOPMENT

| RESEARCH ARTICLE

AI-Based Intrusion Detection & Prevention Models for Smart Home IoT Systems: A Literature Review

Jayveersinh Vansiya[1] ✉ **Asha Chandi**[2] **and Prof. Rashid A Khan Ph.D**[3]
[12]*Dept. of Computer and Information Science & Cybersecurity*
[3]*Assistant Professor, Department of Computer and Information Science & Cybersecurity; Advising Professor in Charge of Research*
Corresponding Author: Jayveersinh Vansiya, **E-mail**: jayveer804@gmail.com

| ABSTRACT

As smart home IoT devices are being increasingly adopted, a lot of cybersecurity concerns have arisen and hence, more need for advanced security measures. This study presents an AI based Intrusion Detection and Prevention Systems (IDPS) for smart home environments. AI driven IDPS utilizes ML and DL techniques to increase threat detection accuracy, and reducing false positives through adaptive security mechanisms. The results show that hybrid detection models that integrate the signature and the anomaly detection algorithms establish a robust countermeasure to known and unknown cyber threats. But true to the work's objectives, there are also key challenges that must be addressed for deployment in the real world, such as computational overhead, privacy considerations and adversarial attacks. Future work can be oriented toward developing lightweight AI models, integrating explainable AI (XAI), or looking into techniques that can be used for keeping the data private, for example, using techniques from federated learning. Moreover, such threat intelligence sharing frameworks on blockchain can further strengthen security in the connected smart home ecosystems. Future results from these advancements will lead to more resilient and efficient cybersecurity systems for smart home IoT systems.

| KEYWORDS

Smart home security, AI-based IDPS, anomaly detection, deep learning, cybersecurity.

| ARTICLE INFORMATION

ACCEPTED: 14 April 2025 **PUBLISHED:** 24 May 2025 **DOI:** 10.32996/jcsts.2025.7.3.110

1. Introduction

The rapid rise in smart home Internet of Things (IoT) systems has revolutionized modern living, looked through the lenses of convenience, automation, and energy efficiency. These systems integrate multiple connected devices, including smart thermostats, security cameras, voice assistants, and home automation controllers that usually communicate over wireless networks. Nevertheless, as IoT devices become more interconnected, serious cybersecurity concerns have arisen. Smart home environments become more vulnerable to a plethora of security threats, including unauthorized access, other forms of cyber-attacks (malware or ransomware), and data breaches. Common security mechanisms, including firewalls and signature-based detection systems, cannot address the complexity of the system being formed by dynamic IoT networks and are resource-constrained (Alsulami, 2024). The growing complexity of IoT environments is termed a force for adaptive security frameworks to identify anomalies, predict attack patterns, and actively respond to real-time emerging threats (Ampatzi, 2024).

1.1 Background

Smart home IoT systems comprise interconnected devices, enabling automation of home functions such as lighting, heating, security, and entertainment. In such systems, information is shared between devices through communication protocols such as Wi-Fi, Zigbee, Z-Wave, and Bluetooth. While the smart home IoT technology enhances the convenience of users, they transmit information wirelessly and use cloud services, thereby exposing them to security vulnerabilities subject to exploitation by cyber attackers (Awotunde & Misra, 2022). One of the main security challenges for a smart home IoT network is unpermitted access. Attackers take advantage of weak authentication mechanisms, outdated firmware, and misconfigured network settings for uncontrolled control over smart home appliances. IoT devices also tend to collect, process, and transmit sensitive data; hence, these devices are also attractive targets for leakage and stealing of user data. Conventional security solutions such as intrusion detection systems (IDSs) and firewalls have limitations in detection in sophisticated attacks in IoT environments due to high device heterogeneity, resource constraints, and dynamic network behavior (Bajahzar, 2024).

1.2 Problem Statement

Despite advancements in AI-driven security, smart home IoT systems remain vulnerable to evolving cyber threats due to the increasing complexity of networks, limited device resources, and the dynamic nature of IoT environments. Most AI-based intrusion detection models focus on known attack patterns and struggle with zero-day threats, largely due to insufficient training data and weak generalization capabilities (Chiba et al., 2022). Challenges such as high false positive rates, computational overhead, and the need for constant model updates further complicate their real-world integration. Additionally, differences in standard datasets and evaluation methods hinder fair performance comparisons, while existing research often isolates individual AI techniques without offering a comprehensive view of their relative strengths, challenges, and practical applicability (e Saher, 2023). To address these gaps, this review explores current AI-focused intrusion detection and prevention models, highlights key directions, and identifies areas for future research to enhance smart home IoT security.

1.3 Significance of the Study

With the increasing penetration of smart home IoT devices into households, the automation, convenience, and efficiency of modern homes have been transformed. Nevertheless, the rise in the number of interconnected devices has also elevated the security risks associated with unauthorized access, cyberattacks, and data breaches. Unlike traditional security mechanisms, new-age AI-based intrusion detection and prevention models consisting of intelligent, adaptable, and automated threat detection present innovative opportunities in strengthening smart home networks against threats. The significance of the study dwells in the idea that the authors will turn to AI as a means of boosting IoT security, addressing the vulnerabilities the latter endures, and promoting the development of advanced security frameworks. Another substantial contribution will be realizing cyber awareness (Jayalaxmi et al., 2022). Based on the literature on AI-enabled security models analyzed in this review, the investigation provides much-needed knowledge on how artificial intelligence can be deployed effectively to protect smart home IoT networks and educate stakeholders, that is, researchers, developers, and consumers on the change in the landscape of cybersecurity and how AI-based solutions can help mitigate emerging threats. In addition, it will serve as a base for future research by thus identifying existing gaps, limitations, and challenges in AI-based intrusion detection and prevention. Building on this work, researchers may develop more sophisticated, efficient, and scalable AI-driven security mechanisms for smart home environments. The review will give industry professionals practical guidance through a synthesis of findings from the literature, enabling them to guide the protection and adoption of these intrusion detection and prevention mechanisms by obtaining insights and lessons to be each adopted by the smart home ecosystem. On a further note, the study addresses the need early enough to standardize AI-driven security frameworks: The proper methodologies on how to evaluate and deploy AI-based intrusion detections and established prevention models enhance the reliability, scalability, and overall practicality in the real world.

1.4 Contribution to Current Literature

This review makes an original contribution by systematically examining AI-based intrusion detection and prevention mechanisms for smart home IoT systems, addressing the lack of comprehensive studies integrating diverse findings (Kaliappan et al., 2024). Unlike research focused on isolated AI techniques, this study presents a holistic analysis of common approaches, their strengths, limitations, and real-world applicability (Kumari et al., 2022). It highlights challenges like high false positive rates, limited computational resources, and difficulties in detecting zero-day attacks, offering insights into improving model generalization, optimizing resources, and enhancing threat detection (Mallidi & Ramisetty, 2025). The review concludes with practical recommendations, serving as a foundation for future advancements in smart home IoT security.

1.5 Aim and Objectives

Aim: To examine the evolution and common approaches of AI-based intrusion detection and prevention models for smart home IoT systems.

Objectives:

1. To explore the development of AI-based intrusion detection models for smart home IoT security.
2. To analyze the common approaches used in AI-driven intrusion prevention techniques.
3. To identify the challenges and limitations of AI-based security mechanisms in smart home IoT environments.
4. To provide recommendations for improving AI-based intrusion detection and prevention models for enhanced security.

1.6 Research questions

1. What are the most common cyber threats targeting smart home IoT devices, and how effectively can AI-based IDPS deal with them?
2. How can AI-based IDPS be improved to detect new and unknown threats in smart homes?
3. How can AI-based IDPS be made resistant to advanced hacking techniques targeting smart home devices?
4. What security and privacy issues might come up when using AI in smart home systems, and how can these be solved?

1.7 Methodology Approach

This literature review follows a systematic approach to collecting, analyzing, and synthesizing relevant research articles related to AI-based intrusion detection and prevention in smart home IoT systems. The methodology involves the following steps:

- **Data Collection:** Peer-reviewed journal articles, conference proceedings, and academic papers are sourced from reputable databases. Keywords such as "AI-based intrusion detection," "IoT security," "smart home cybersecurity," and "machine learning for intrusion prevention" are used for searching relevant literature.

- **Inclusion and Exclusion Criteria:** Studies published within the last five years (to ensure relevance) and those focusing on AI-driven security solutions for smart home IoT environments are included. Research focusing solely on industrial IoT security or non-AI-based intrusion detection methods is excluded.

- **Analysis and Synthesis:** The selected studies are analyzed based on their methodologies, AI techniques used, effectiveness, limitations, and applicability in smart home IoT networks. The findings are categorized to identify common themes, trends, and research gaps.

- **Presentation of Findings:** The synthesized information is structured to provide a coherent overview of AI-based intrusion detection and prevention models, their evolution, and their impact on smart home security.

2. Literature Review

With growing urbanization and lifestyle shifts, more homeowners are adopting IoT smart home devices for convenience and automation. However, these devices, reliant on wireless connections and internet protocols, face rising cyber risks as attackers exploit security gaps, while traditional IT defenses like firewalls prove inadequate (Markevych & Dawson, 2023). AI has become essential for smart home IoT security, offering adaptive, real-time intrusion detection and prevention through machine learning and deep learning models. These systems improve threat detection, predict attacks, and reduce reliance on manual monitoring within frameworks like Zero Trust Architecture (Moustafa, 2021). This review explores AI's role, challenges, and opportunities in enhancing smart home IoT security.

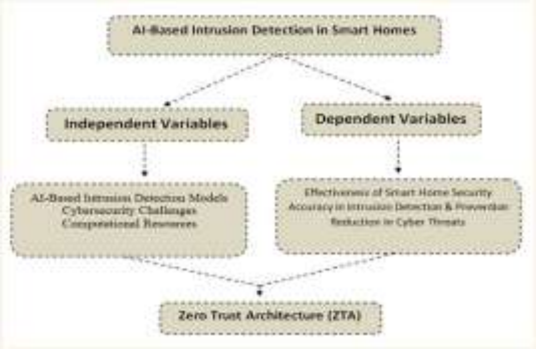
AI-Based Intrusion Detection in Smart Homes
Independent Variables
Dependent Variables
AI-Based Intrusion Detection Models
Cybersecurity Challenges
Computational Resources
Effectiveness of Smart Home Security
Accuracy in Intrusion Detection & Prevention
Reduction in Cyber Threats
Zero Trust Architecture (ZTA)

Figure 1: Conceptual Framework

The intellectually empowered AI-complemented mechanism accomplishes this by using large sets of data to understand multifaceted tactics of network attacks, which results in preponderance of threat mitigation directives (Muneer et al., 2024).

2.1 Common Approaches to AI-Based Intrusion Detection and Prevention

AI-based intrusion detection and prevention is crucial for securing smart home IoT networks, as traditional systems struggle against advanced threats (Otoum, 2022).

- **Signature-based detection:** Signature-based detection compares network traffic to known attack patterns (Rajapaksha et al., 2023). AI improves this by automating signature updates and recognizing disguised threats, though maintaining updated databases is resource-heavy for IoT environments (Rockey, 2022).

- **Anomaly-based detection:** Anomaly-based detection uses machine learning (ML) and deep learning (DL) to spot deviations from normal network behavior, effectively detecting unknown and zero-day threats (Sabit, 2025a). However, it faces issues like high false positives and computational demands (Sabit, 2025b).

- **Hybrid detection models:** Hybrid detection models combine signature-based and anomaly-based techniques, offering better accuracy and broader threat coverage for smart home systems (Schmitt, 2023).

Advanced methods like federated learning and blockchain improve security in decentralized IoT setups by protecting data privacy and ensuring tamper-proof records (Shah et al., 2023). Despite their benefits, AI-driven systems face challenges with scalability, energy efficiency, and seamless integration in resource-constrained smart home devices (Sheeja, 2023). These AI-based solutions represent a scalable, adaptive, and reliable defense against evolving cyber threats in increasingly interconnected smart home ecosystems (Scott et al., 2022).

2.2 Challenges and Limitations of AI-Based Security in Smart Home IoT Systems

Despite the imperious face of adoption and the overall variance of any threat, there are a handful of limitations that continue to negate the wide implantation and efficiency of these AI-powered security systems in the smart home. The highly interconnected and complicated nature of the IoT ecosystem, which involves a wide diversification in device capabilities, too few computational resources, and the actual evolution of cyber threats, creates numerous security challenges that must be solved properly. These major problems are characterized by high false positive rates, insufficient computing/IT force, poor data availableness with its quality issues, zero-day detection difficulties, and the complexities of putting together different security systems.

- **High False Positive Rates:** AI systems often misclassify normal activities as threats, causing frequent false alarms (Shrivastwa et al., 2022). This lowers user trust and burdens admins with verifying alerts (Sowmya & Anita, 2023).

- **Computational Resource Constraints:** IoT devices have limited processing power and memory for complex AI models. This restricts advanced security measures in resource-constrained smart devices (Sung et al., 2023).

- **Data Availability & Quality Issues:** Lack of open, labeled, and diverse IoT datasets weakens AI model training (Alsulami, 2024). Device diversity and inconsistent data patterns complicate intrusion detection (Moustafa, 2021).

- **Zero-Day Intrusion Detection Challenges:** AI struggles to detect unknown, novel zero-day attacks relying on unseen patterns (Markevych & Dawson, 2023). Techniques like transfer learning and adversarial training offer help but remain limited (Rockey, 2022).

2.3 Integration with Existing Security Infrastructure in Smart Home

To address challenges of the compatibility, interoperability and scalability, AI based intrusion detection and prevention systems have to integrate with existing security measures, including firewalls, access control and encryption (Shah et al., 2023). Proprietary protocols and security architectures are many of the smart home devices, which makes AI security solutions difficult to work universally. Besides, issues like network congestion, false positives, and limited resource on IoT devices limit the deployment of AI (Sung et al., 2023). Good AI solutions must tightly interconnect with existing security infrastructures, mitigate scalability issues and the scarcity of high quality datasets and overcome the rise of new threats (Shrivastwa et al., 2022).

3. Methodology

3.1 Research Design

In this research, a Systematic Literature Review (SLR) with Prisma approach is used to investigate the AI driven intrusion detection and prevention in the smart home IoT networks. Both in terms of selecting the peer reviewed literature, and taking a structured, transparent review process, the PRISMA methodology is used. It reviews key models for AI detection such as signature based, anomaly based and hybrid approaches, including challenges like high false positive rates and high computational complexity as well as zero day detection. The results are drawn together into a single document to make the research reliable and reproducible.

3.2 Planning Phase

3.2.1 Research Questions

- How has AI-based intrusion detection models evolved for smart home IoT?
- What are the common approaches in AI-based intrusion prevention for smart homes?

3.2.2 Objectives

1. To explore the development of AI-based intrusion detection models for smart home IoT security.
2. To analyze the common approaches used in AI-driven intrusion prevention techniques.
3. To identify the challenges and limitations of AI-based security mechanisms in smart home IoT environments.
4. To provide recommendations for improving AI-based intrusion detection and prevention models for enhanced security.

3.3 Conducting Phase

3.3.1 Selection of Keywords

- Artificial Intelligence
- Machine Learning
- Intrusion Detection
- Intrusion Prevention
- Cybersecurity
- IoT Security
- Smart Home
- IoT
- Anomaly Detection
- Hybrid Detection

3.3.2 Formulation of Search String

"("Artificial Intelligence" OR "Machine Learning") AND ("Intrusion Detection" OR "Intrusion Prevention") AND ("Cybersecurity" OR "IoT Security") AND ("Smart Home" OR "IoT") AND ("Anomaly Detection" OR "Hybrid Detection")

3.3.2.1 Selection of Databases

One of the most important stages in the process of conducting a literature review is the selection of the databases. To perform this research, Google Scholar, IEEE Xplore, and ACM Digital Library sources will be used as main libraries to get academic papers on the intrusion detection methods and preventive measures towards smart home IoT environments. Google Scholar is not just a search engine but is a repository of refereed articles; these papers include journal articles, conference proceedings, and papers on technical subjects. One of the journal's advantages is its capability to provide a variety of research papers. Journals are great sources of research output and the availability of various papers in one place is a great resource in identifying diverse research contributions. IEEE Xplore database is a leader in the field of engineering and technology. It offers state-of-the-art research on the subject of cybersecurity, AI, and IoT security among others. FSI, which is AIT, is particularly useful in getting cutting-edge and highly technical security solutions which have high prediction rates. ACM Digital Library is a notable additional source, which is concerned with CS and cybersecurity literature, hence, members are equipped with essential resources, which enable access to high-quality articles on AI as applied to security mechanisms.

Table I: Search on Database

Database	ST 1 and ST 2	Search String	Result
Google Scholar	ST 1	("Artificial Intelligence" OR "Machine Learning") AND ("Intrusion Detection" OR "Intrusion Prevention") AND ("Cybersecurity" OR "IoT Security") AND ("Smart Home" OR "IoT") AND ("Anomaly Detection" OR "Hybrid Detection")	16600
ACM Digital Library	ST 1	("Artificial Intelligence" OR "Machine Learning") AND ("Intrusion Detection" OR "Intrusion Prevention") AND ("Cybersecurity" OR "IoT Security") AND ("Smart Home" OR "IoT") AND ("Anomaly Detection" OR "Hybrid Detection")	580
IEEE Xplore	ST 1	("Artificial Intelligence" OR "Machine Learning") AND ("Intrusion Detection" OR "Intrusion Prevention") AND ("Cybersecurity" OR "IoT Security") AND ("Smart Home" OR "IoT") AND ("Anomaly Detection" OR "Hybrid Detection")	315
Google Scholar	ST 2	("Cyber Threats" OR "Hacking Techniques" OR "Adversarial Attacks") AND ("Privacy Issues" OR "Security Challenges" OR "Mitigation Strategies") AND ("Smart Home Security" OR "IoT Security" OR "Home Automation Security" OR "Connected Devices Security")	6400
ACM Digital Library	ST 2	("Cyber Threats" OR "Hacking Techniques" OR "Adversarial Attacks") AND ("Privacy Issues" OR "Security Challenges" OR "Mitigation Strategies") AND ("Smart Home Security" OR "IoT Security" OR "Home Automation Security" OR "Connected Devices Security")	138
IEEE Xplore	ST 2	("Cyber Threats" OR "Hacking Techniques" OR "Adversarial Attacks") AND ("Privacy Issues" OR "Security Challenges" OR "Mitigation Strategies") AND ("Smart Home Security" OR "IoT Security" OR "Home Automation Security" OR "Connected Devices Security")	55

3.3.3 Inclusion and Exclusion Criteria

3.3.3.1 Inclusion Criteria:

- Studies published between 2021 and 2025 to ensure the inclusion of recent advancements.
- Open-access research articles for unrestricted access to full texts.
- Studies specifically related to AI-driven intrusion detection and prevention in smart home IoT security.
- Research that focuses on machine learning, anomaly detection, or hybrid detection models for cybersecurity in IoT environments.
- Articles published in peer-reviewed.
- Studies written in English for accessibility and comprehension.

3.3.3.2 Exclusion Criteria:

- Studies published before 2021, as they may not reflect the latest developments in AI-based IoT security.
- Articles that are not open access, restricting availability of full texts.
- Research that does not specifically focus on AI-driven intrusion detection or prevention in smart home IoT environments.
- Non-peer-reviewed articles.
- Studies published in languages other than English, due to accessibility constraints.

Table II: Search on Database after Inclusion & Exclusion

Database	ST 1 and ST 2	Search String	Result
Google Scholar	ST 1	("Artificial Intelligence" OR "Machine Learning") AND ("Intrusion Detection" OR "Intrusion Prevention") AND ("Cybersecurity" OR "IoT Security") AND ("Smart Home" OR "IoT") AND ("Anomaly Detection" OR "Hybrid Detection")	6
ACM Digital Library	ST 1	("Artificial Intelligence" OR "Machine Learning") AND ("Intrusion Detection" OR "Intrusion Prevention") AND ("Cybersecurity" OR "IoT Security") AND ("Smart Home" OR "IoT") AND ("Anomaly Detection" OR "Hybrid Detection")	44
IEEE Xplore	ST 1	("Artificial Intelligence" OR "Machine Learning") AND ("Intrusion Detection" OR "Intrusion Prevention") AND ("Cybersecurity" OR "IoT Security") AND ("Smart Home" OR "IoT") AND ("Anomaly Detection" OR "Hybrid Detection")	23
Google Scholar	ST 2	("Cyber Threats" OR "Hacking Techniques" OR "Adversarial Attacks") AND ("Privacy Issues" OR "Security Challenges" OR "Mitigation Strategies") AND ("Smart Home Security" OR "IoT Security" OR "Home Automation Security" OR "Connected Devices Security")	2
ACM Digital Library	ST 2	("Cyber Threats" OR "Hacking Techniques" OR "Adversarial Attacks") AND ("Privacy Issues" OR "Security Challenges" OR "Mitigation Strategies") AND ("Smart Home Security" OR "IoT Security" OR "Home Automation Security" OR "Connected Devices Security")	3
IEEE Xplore	ST 2	("Cyber Threats" OR "Hacking Techniques" OR "Adversarial Attacks") AND ("Privacy Issues" OR "Security Challenges" OR "Mitigation Strategies") AND ("Smart Home Security" OR "IoT Security" OR "Home Automation Security" OR "Connected Devices Security")	0

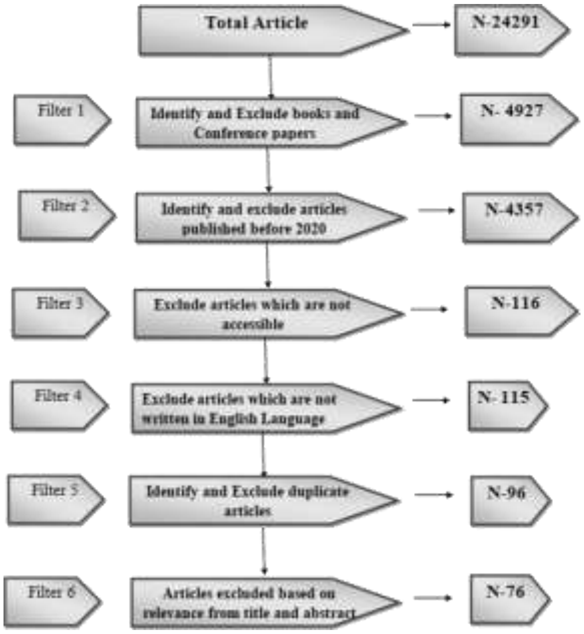
Total Article
N-24291
Filter 1
Identify and Exclude books and Conference papers
N- 4927
Filter 2
Identify and exclude articles published before 2020
N-4357
Filter 3
Exclude articles which are not accessible
N-116
Filter 4
Exclude articles which are not written in English Language
N- 115
Filter 5
Identify and Exclude duplicate articles
N-96
Filter 6
Articles excluded based on relevance from title and abstract
N-76

Figure 2: PRISMA Flowchart

3.4 Quality Assessment, Data Extraction and Synthesis

Diana et al. (2025)	
Ata Amrullah et al. (2025)	Reviews recent ML, DL, statistical, and rule-based anomaly detection methods for IoT security, addressing key attacks (MitM, replay, injection) and challenges like device heterogeneity, limited data, and privacy concerns, while highlighting research gaps and future needs.
Ejeofobiri et al. (2024)	Examines AI-powered IDS for IoT, categorizing ML techniques and assessing real-time detection effectiveness, while discussing computational constraints and feature selection. Emphasizes multi-layered security frameworks and adaptive, resource-efficient IDS solutions.
R Anandh et al. (2024)	Analyzes IoT network threats (botnets, DoS) and NIDS techniques, reviewing ML-based approaches, open-source tools, and datasets. Introduces the LTMA model for evaluating NIDS solutions and future research directions.
Srinivasan (2024)	Explores AI-driven IoT security, focusing on GANs for intrusion detection, authentication, and anomaly detection. Discusses traditional security challenges and proposes AI-based enhancements for threat prevention.
Aziz et al. (2024)	Reviews ML/DL applications in cybersecurity, analyzing over 50 studies on detecting threats like DoS, zero-day, and phishing. Compares malware detection, anomaly detection, and intrusion detection techniques, proposing a research framework.
Alsalman (2024)	Proposes FusionNet, an ensemble ML model integrating RF, KNN, SVM, and MLP for anomaly detection, achieving high accuracy. Demonstrates superiority over traditional ML models across security, healthcare, and network monitoring.
Mirza Akhi Khatun et al. (2023)	Examines Healthcare IoT security, addressing vulnerabilities in smart sensing devices, emerging threats (AI, 5G-IoT), and multilayer security protocols (Wi-Fi 6, ZigBee, LoRa). Highlights ML/DL-based authentication for resilience.
Kornaros (2022)	Reviews ML/DL-based intrusion detection in IoT, discussing anomaly detection, malware defense, and authentication. Analyzes challenges like encrypted traffic and hardware-based security, evaluating ML accelerators for IoT security.
Lundberg et al. (2022)	Investigates XAI-powered IV-IDS for in-vehicle cybersecurity, using CAN bus data and developing VisExp, a visualization-based explanation model. Demonstrates improved expert trust in AI-driven IDS.
Villegas-Ch et al. (2025)	Proposes a hybrid blockchain-AI model for IoT security, achieving high phishing detection accuracy, reduced authentication latency, and lower energy consumption. Introduces lightweight blockchain consensus and scalable deep learning-based intrusion detection.
Ozkan-Ozay et al., 2024	I-driven cybersecurity, covering ML, DL, RL applications, adversarial attacks, data issues, and ChatGPT's dual role.
Akmalbek Abdusalomov et al., 2024	IoT-based smart home security, IDS using ETC optimized with HSA, high accuracy (99.87%, 99.51%, 99.49%).
Yu et al., 2024	ML in Industry 4.0 cybersecurity, covering risk evaluation, intrusion detection, incident response, and predictive risk assessment.
Olawale & Ebadinezhad, 2024	IoHT security, AI models for threat detection, IPFS blockchain for decentralization, SVM accuracy up to 100%.
Khayat et al., 2025	AI and ML in SOC optimization, automated incident response, neural networks, AI-integrated SOC architecture with case study.
Fernando et al., 2024	Unsupervised ML for intrusion detection, I-forest on BoT-IoT dataset, high accuracy, low CPU usage (10% vs. 16%).
Christopher et al., 2021 –	Edge Computing security for IoT, EG-SMOTE and GSOM for threat detection, high F-scores across benchmark datasets.
Mohammed et al., 2024	Smart Grid cybersecurity, vulnerabilities, attack detection (rule-based, ML, AI,

	blockchain), insights for policymakers.
Kandhro et al., 2023	Proposes a deep learning-based intrusion detection framework using GANs for IoT-driven industrial control systems, achieving 95-97% accuracy.
Kim et al., 2021	Introduces Panop, an ANN-based NIDS optimized for distributed network environments, outperforming Kitsune in detecting host-oriented attacks.
Newaz et al., 2021	Surveys security and privacy threats in healthcare systems, detailing risks, attack impacts, and mitigation strategies.
Alrayes et al., 2024	Develops a Denoising Autoencoder (DAE) model for IoT intrusion detection, demonstrating high accuracy on NSL-KDD and CICIDS 2017 datasets.
D Jayalatchumy et al., 2024	Implements a multi-phase intrusion detection system using data-denoising, Crow search algorithm, and ensemble classifiers, achieving up to 99.4% accuracy.
Muniswamy & Rathi, 2024	Surveys security vulnerabilities in smart city IoT infrastructure and explores machine learning-based countermeasures.
Skopik et al., 2022	Introduces AECID, a behavior-based anomaly detection model for security breaches in cyber-physical systems using unstructured log data.
Rizvi et al., 2022	Reviews AI-driven solutions in network forensics, covering intrusion detection, traffic analysis, and IoT forensic applications.
Houkan et al., 2024	Compares MRMR and PCA for feature selection in Industrial IoT security, achieving 99.9% accuracy with Decision Trees.
Fährmann et al., 2024	Surveys anomaly detection techniques for smart environments using multivariate time series data, discussing challenges and evaluation metrics.
Almaraz-Rivera et al., 2022	Introduces LATAM-DDoS-IoT dataset, achieving >90% attack detection in real SDN-based intrusion detection.
Muhammad Maaz et al., 2024	Develops CNN-GRU and CNN-LSTM models for IoT security, achieving 99.6% accuracy on Kitsune dataset.
Alrayes et al., 2023	Proposes IRMOFNN-AD for smart city IoT, integrating IRMO and FNN for anomaly detection.
Mousa'B Mohammad Shtayat et al., 2023	Develops explainable ensemble IDS using SHAP and LIME for IIoT security.
Bakhshi et al., 2023	Evaluates AI-driven IDS on panOULU public network, integrating SDN, NFV, and Federated Learning.
Ullah & Mahmoud, 2022	Proposes hybrid deep learning models (LSTM, BiLSTM, GRU, CNN) for IoT anomaly detection.
Vadym Shkarupylo et al., 2024	Introduces ML-SP2 for predictive maintenance and ML-IDS for intrusion detection in Industry 5.0.
Salahaldeen Duraibi & Abdullah Mujawib Alashjaee, 2024	Proposes IMFOHDL-ID using LSTM-DSSAE and DTOA for IoT intrusion detection.
Mesadieu et al., 2024	Develops DRL-based anomaly detection for SCADA security, achieving 99.36% attack detection.
Koca & Avci, 2024	Proposes GCN-LSTM IDS for ICS and IoT, detecting deceptive connectivity disruptions with 99.99% accuracy.
Andreoni et al., 2024	Explores Generative AI (GANs, VAEs, LLMs) for cybersecurity in autonomous systems.
Singh Popli et al., 2025	Proposes FL-based intrusion detection for IoUT, ensuring privacy in underwater drone networks.
Ishibashi et al., 2022	Develops AI-powered NIDS dataset generation, improving reproducibility and classification model training.
Weber et al., 2023	Conducts an SLR on intrusion detection in MCPS, identifying research gaps and dataset needs.
Tsikerdekis et al., 2021	Proposes network anomaly detection using exponential random graph modeling, improving DNS exfiltration detection.
Abdinasir Hirsi Abdi et al., 2024	Analyzes SDN security using AI, MTD, and traditional approaches, identifying threats via STRIDE.
Hussain et al., 2023	Develops a GAN-based approach for APT detection in I-IoT CPS, achieving >95%

	accuracy with reduced prediction time.
Hajar Hameed Addeen et al., 2024	Proposes a CVAE-based model for detecting CPAs in WDS, achieving 98% accuracy.
Verma et al., 2023	Develops an FL-based cyberthreat detection framework for 5G IIoT, improving zero-day threat detection.
Fuentes-Garcia et al., 2021	Reviews NSM, proposes a taxonomy, and identifies key challenges in NSM deployment.
Dinesh Kumar Nishad et al., 2025	Introduces FUZZY-driven energy management using CNN, LSTM, and RL for healthcare power quality.
Cai et al., 2021	Conducts a survey on GANs in privacy and security, classifying works and outlining challenges.
Wang et al., 2024	Proposes an AED method for IoMT NID, achieving high accuracy with minimal abnormal data.
Jerez et al., 2022	Introduces the Gaussian Equivalence Criterion for benchmarking anomaly detection methods.
Bouazzati et al., 2025	Develops an HIDS for IoT using HPCs, detecting attacks with low FPGA resource overhead.
Apruzzese et al., 2022	Analyzes ML's role in cybersecurity, bridging the gap between research and practice.
Banik et al., 2023	Develops a reinforcement learning and Bayesian optimization approach for CPS attack-defense strategies.
Nguyen et al., 2024	Proposes a two-stage federated learning framework with DNNs to enhance NIDS accuracy and adaptability.
Tannishtha Devgun et al., 2025	Introduces Proof-of-INtelligence (PIN) for AI-centric consensus in blockchain-based federated learning.
Apruzzese et al., 2021	Analyzes adversarial attacks on ML-based cybersecurity defenses, refining threat models for IDS resilience.
Torre et al., 2024	Proposes a privacy-preserving FL-based IDS using 1D CNN, achieving 97.31% accuracy in IoT security.
Cordero et al., 2021	Develops ID2T to enhance reproducibility in network intrusion detection by injecting synthetic attacks into background traffic.
Sikder et al., 2019	Introduces Aegis+, a context-aware security framework for detecting malicious behavior in Smart Home Systems.
Albasir et al., 2022	Proposes a CNN-based power anomaly detection method using time–frequency images, improving malware detection accuracy.
Madani et al., 2022	Combines device fingerprinting and RMTD to defend against MAC-layer spoofing attacks in IoT networks.
Mohan Baruwal Chhetri et al., 2024	Develops the A2C Framework to reduce SOC alert fatigue through AI-driven adaptive decision-making.
Hong et al., 2023	Uses sHDP-HMM to detect attack events in cyber-physical systems based on time-series logs.
Han et al., 2024	Proposes FIOT, a lightweight federated learning model for IoT botnet detection in smart cities.
Nitz et al., 2024	Introduces a reference architecture for privacy-preserving collaboration in cybersecurity incident response.
Mundt & Baier, 2022	Develops a MITRE ATT&CK-based system for automated data exfiltration mitigation in network security.
Chernikova & Oprea, 2022	Introduces FENCE, a gradient-based adversarial attack framework for testing DNN resilience in cybersecurity.
Everson & Cheng, 2024	Reviews network attack surface mapping tools, highlighting advancements and future research directions.
Mirzaaxmedov D.M. 2024	This study reviews IoT security challenges and highlights AI-driven solutions for threat detection and prevention. However, it lacks experimental validation of AI-based security mechanisms.
Malik, M. S. (2024)	A survey on IoT malware threats, attack vectors, and mitigation strategies, emphasizing AI-based defenses. It does not address the practical challenges of

	implementing security measures.
Selvaraj & Uddin (2024)	An empirical study analyzing vulnerabilities in C/C++ IoT code snippets shared on Stack Exchange, identifying 29 CWE types. The study highlights security risks but lacks preventive solutions.
Wang et al. (2023)	Introduces FL4IoT, a federated learning system for privacy-preserving IoT device identification, achieving ~99% accuracy. However, scalability and real-world performance remain unaddressed.
Huang et al. (2021)	Conducts a survey on blockchain applications, theoretical models, and essential mechanisms, identifying open research issues. The study lacks a practical evaluation of blockchain frameworks.

4. Result and Finding

This literature review highlights the increasing reliance on AI-driven Intrusion Detection and Prevention Systems (IDPS) to counter cyber threats in IoT-enabled smart homes. The findings suggest that AI techniques growing use of AI based intrusion detection and prevention system (IDPS) to secure the cyber threats in IoT smart homes is highlighted against the unauthorized manipulation, data breach or the targeted attacks on vulnerable devices. Various AI techniques applied such as machine learning (ML), deep learning (DL), and reinforcement learning (RL) to enhance threat detection accuracy, and with reduced time and labor cost. On the other hand, the review demonstrated anomaly based models to be more effective in detecting either unknown or novel attacks, while they found signature based models to be more effective in detecting known threats. Coalescing anomaly and signature based methods, hybrid approaches are emerging as promising ways of providing more adaptive and robust protection for smart home IoT systems. While there is tremendous headway, there are still some challenges especially around scalability, real time operation and effortless upgrades of AI models to the current IoT systems. Additionally, there is significant privacy issues around collection of data and potential attacks on AI models that are barriers for using IDPSs based on AI entirely. This work suggests an urgent need for continued work on research and development aimed at addressing security and privacy concerns related to smart homes fully reliant on AI-driven systems so that the systems can provide trustworthy, cost-effective and secure defence against evolving cyber threats.

4.1 Answer to RQs

Smart home IoT devices face growing cyber threats like malware, botnets, DDoS attacks, unauthorized access, and data exfiltration, which jeopardize functionality and privacy. AI-based Intrusion Detection and Prevention Systems (IDPS) using machine learning (ML) and deep learning (DL) are more effective in detecting these threats, leveraging anomaly detection, continuous learning, and deep learning models like CNNs, LSTMs, and BiLSTMs. Hybrid AI, GANs, and blockchain integration further enhance detection and forensic analysis. Techniques like federated learning, reinforcement learning, and explainable AI improve adaptability and accuracy, while blockchain and federated learning address privacy concerns. AI-driven botnet detection and multi-layered frameworks, including NIDS and HIDS, help resist advanced hacking methods. Despite challenges such as adversarial attacks and data privacy, integrating federated learning, XAI, blockchain, and hardware-based protections ensures robust, efficient, and secure IDPS for smart homes.

5. Discussion

The analysis highlights key insights into the functionality of AI-based Intrusion Detection and Prevention Systems (IDPS) for securing smart home IoT systems. AI enhances threat detection by leveraging machine learning (ML) and deep learning (DL) models that identify abnormal patterns, outperforming traditional rule-based systems by reducing false positives and adapting to evolving threats. These systems process large datasets, using historical data to predict and prevent future attacks. Deep learning models like CNNs and RNNs are particularly effective in identifying harmful activities and time-dependent patterns. Real-world deployment benefits from edge computing and federated learning, with hybrid models combining signature-based and anomaly detection to address both known and unknown threats. However, challenges remain, such as limited diversity in training datasets, adversarial attacks, privacy concerns due to large data volumes, and resource constraints in smart home devices. Techniques like homomorphic encryption and differential privacy are explored to secure model training. Moreover, explainability is crucial, as deep learning models often lack transparency; methods like SHAP and LIME can enhance trust in AI security decisions. Adversarial robustness is also a concern, with strategies like adversarial training needed to improve resilience. Legal compliance with frameworks such as GDPR and CCPA remains a challenge in cross-border data flows. Despite these limitations, AI-based IDPS offers transformative potential for smart home cybersecurity, with future research focusing on lightweight, interpretable, privacy-preserving, and resilient AI models to better protect the smart home ecosystem.

6. Conclusion

Finally, the study demonstrates the effectiveness of machine learning and deep learning on using such AI tool—a Detection and Prevention System (IDPS)—to improve the safe use of smart home IoT devices by detecting cyber threats in "real time." Compared to traditional rule based system, these AI models are stronger and have ability to avoid false alarms and set up adaptive security solutions to handle if any. AI based IDPS can integrate IDPS signature based as well as anomaly detection techniques to effectively identify both known and new bure threats and thus help it to be more resilient towards evolving cybre attacks. While all these challenges are overcome, challenges pertinent to the broad adoption of such technologies still arise: computational efficiency and data privacy in the case of resource constrained many IoT devices. The issue are addressed through proposed optimization strategies of edge computing, and federated learning for real time threat detection without compromising device performance. Moreover, adversarial attacks on AI models are seen as a very important problem, which requires continuous retraining and robust defense mechanisms. While there are indeed challenges, AI-powered IDPS provides a lot of benefit to smart home security: no need for human intervention and increased user safety. In the future, it is important to build lightweight AI attack models and decentralized security networks and regulatory frameworks to improve the efficiency and credibility of all the AI-secure solutions. If there are applications other than smart homes, both the findings and deduction of this study are still applicable to IoT ecosystems and will shape the future of the cybersecurity as AI dominates the digital cradle.

7. Future Directions

With the new breed of cyber threats evolving matter of seconds, there is an urgent necessity for continuous improvements in AI based Intrusion Detection and Prevention Systems (IDPS) in smart home IoT security. Anomaly detection and adaptive response is enhanced by emerging AI techniques such as transformer models, GANs, and reinforcement learning. It connects both lightweight AI models and data privacy by maintaining them in federated learning. To improve model transparency, technology of explainable AI (XAI) is invented, and adversarial training is used to enhance resilience against evasion attacks. Blockchain makes the system tamper proof via tamper proof logging and decentralized security. Development of AI based IDPS should be guided by real world deployments, even privacy regulations (such as GDPR and CCPA) and ethical standards, and future exploration of increased accuracy, decreased complexity and usability in smart home environments.

References

[1] Abdinasir H A, Lukman A, Adeb S, A, M. A., Rasheed, H., Ahmed, S., & Tahir, A. (2024). Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI and MTD Approaches to Security Solutions. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3393548

[2] Akmalbek A, Dusmurod K, Rashid N, Ilkhom R, & Cho, Y. I. (2024). Optimizing Smart Home Intrusion Detection with Harmony-Enhanced Extra Trees. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3422999

[3] Albasir, A., Naik, K., & Manzano, R. (2022). Towards Improving the Security of IoT and CPS Devices: An AI Approach. Digital Threats: Research and Practice. https://doi.org/10.1145/3497862

[4] Almaraz-Rivera, J. G., Perez-Diaz, J. A., Cantoral-Ceballos, J. A., Botero, J. F., & Trejo, L. A. (2022). Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset. IEEE Access, 10, 106909–106920. https://doi.org/10.1109/access.2022.3211513

[5] Alrayes, F. S., Wafa M, Aljameel, S. S., Mashael M, Rizwanullah, M., & Salama, A. S. (2023). Improved Radial Movement Optimization With Fuzzy Neural Network Enabled Anomaly Detection for IoT Assisted Smart Cities. IEEE Access, 11, 143060–143068. https://doi.org/10.1109/access.2023.3342698

[6] Alrayes, F. S., Zakariah, M., Amin, S. U., Khan, Z. I., & Helal, M. (2024). Intrusion Detection in IoT Systems Using Denoising Autoencoder. IEEE Access, 12, 122401–122425. https://doi.org/10.1109/access.2024.3451726

[7] Alsalman, D. (2024). A Comparative Study of Anomaly Detection Techniques for IoT Security using AMoT (Adaptive Machine Learning for IoT Threats). IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3359033

[8] Alsulami, M. H. (2024). An AI-Driven Model to Enhance Sustainability for the Detection of Cyber Threats in IoT Environments. *Sensors*, *24*(22), 7179.

[9] Ampatzi, C. (2024). *How AI can Improve Intrusion Detection and Prevention System*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1893895

[10] Andreoni, M., Willian T L, Lawton, G., & Thakkar, S. (2024). Enhancing Autonomous System Security and Resilience With Generative AI: A Comprehensive Survey. IEEE Access, 12, 109470–109493. https://doi.org/10.1109/access.2024.3439363

[11] Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., & Colajanni, M. (2021). Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems. Digital Threats: Research and Practice. https://doi.org/10.1145/3469659

[12] Apruzzese, G., Laskov, P., de Oca, E. M., Mallouli, W., Rapa, L. B., Grammatopoulos, A. V., & Franco, F. D. (2022). The Role of Machine Learning in Cybersecurity. Digital Threats: Research and Practice, 4(1). https://doi.org/10.1145/3545574

[13] Ata A, Dicka Y K, & Abidin, M. M. (2025). Trends and Challenges in Anomaly Intrusion Detection at the Edge for IoT: A Review. *Intellithings Journal,* 1(1), 11–20. https://e-jurnal.unisda.ac.id/index.php/intellithings/article/view/8968

[14] Awotunde, J. B., & Misra, S. (2022). Feature Extraction and Artificial Intelligence-Based Intrusion Detection Model for a Secure Internet of Things Networks. In S. Misra & C. Arumugam (Eds.), *Illumination of Artificial Intelligence in Cybersecurity and Forensics* (Vol. 109, pp. 21–44). Springer International Publishing. https://doi.org/10.1007/978-3-030-93453-8_2

[15] Aziz, M. T., Mahmud, T., Datta, N., Sharif, M. M., & Andersson, K. (2024, December 12). A State-of-the-Art Review of Machine Learning in Cybersecurity Data Science. https://doi.org/10.1007/978-981-97-5791-6_57

[16] Bajahzar, A. (2024). The Importance of AI-Enabled Internet of everything Services for Smart Home Management. *International Journal on Smart Sensing and Intelligent Systems*, *17*(1), 20240026. https://doi.org/10.2478/ijssis-2024-0026

[17] Bakhshi, A., Saeid S, Peltonen, E., & Panos K. (2023). Autonomous Federated Learning for Distributed Intrusion Detection Systems in Public Networks. IEEE Access, 11, 121325–121339. https://doi.org/10.1109/access.2023.3327922

[18] Banik, S., Ramachandran, T., Bhattacharya, A., & Bopardikar, S. D. (2023). Automated Adversary-in-the-Loop Cyber-Physical Defense Planning. ACM Transactions on Cyber-Physical Systems, 7(3), 1–25. https://doi.org/10.1145/3596222

[19] Bouazzati, M. E., Tanguy, P., Gogniat, G., & Tessier, R. (2025). Diwall: A Lightweight Host Intrusion Detection System Against Jamming and Packet Injection Attacks. ACM Transactions on Embedded Computing Systems. https://doi.org/10.1145/3711833

[20] Cai, Z., Xiong, Z., Xu, H., Wang, P., Li, W., & Pan, Y. (2021). Generative Adversarial Networks. ACM Computing Surveys, 54(6), 1–38. https://doi.org/10.1145/3459992

[21] Chernikova, A., & Oprea, A. (2022). FENCE: Feasible Evasion Attacks on Neural Networks in Constrained Environments. ACM Transactions on Privacy and Security, 25(4), 1–34. https://doi.org/10.1145/3544746

[22] Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., & Kinta, R. (2022). A deep study of novel intrusion detection systems and intrusion prevention systems for Internet of Things networks. *Procedia Computer Science*, *210*, 94–103.

[23] Christopher, V., Tharmasanthiran A, Kayathiri M, Rashmika N, Daswin D S, Nanayakkara, V., & Damminda A. (2021). Minority Resampling Boosted Unsupervised Learning With Hyperdimensional Computing for Threat Detection at the Edge of Internet of Things. IEEE Access, 9, 126646–126657. https://doi.org/10.1109/access.2021.3111053

[24] Cordero, C. G., Vasilomanolakis, E., Wainakh, A., Mühlhäuser, M., & Nadjm-Tehrani, S. (2021). On Generating Network Traffic Datasets with Synthetic Attacks for Intrusion Detection. ACM Transactions on Privacy and Security, 24(2), 1–39. https://doi.org/10.1145/3424155

[25] Djayalatchumy, R, R., Balakrishnan, A., Safran, M., & Sultan A. (2024). Improved Crow Search-based Feature Selection and Ensemble Learning for IoT Intrusion Detection. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3372859

[26] Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. Computers, 14(3), 87. https://doi.org/10.3390/computers14030087

[27] Dinesh K Ni, Khalid, S., & Singh, R. (2025). Power Quality Assessment and Optimization in FUZZY-Driven Healthcare Devices. IEEE Access, 1–1. https://doi.org/10.1109/access.2025.3526001

[28] ESaher, N. (2023). Smart Homes and AI Based Models in Future. *International Journal of Innovations in Science Technology*, *5*, 143–159.

[29] Ejeofobiri, C. K., Victor-Igun, O. O., & Okoye, C. (2024). AI-Driven Secure Intrusion Detection for Internet of Things (IOT) Networks. Asian *Journal of Mathematics and Computer Researc*h, 31(4), 40–55. https://doi.org/10.56557/ajomcor/2024/v31i48971

[30] Everson, D., & Cheng, L. (2024). A Survey on Network Attack Surface Mapping. Digital Threats. https://doi.org/10.1145/3640019

[31] Fährmann, D., Martín, L., Sánchez, L., & Damer, N. (2024). Anomaly Detection in Smart Environments: A Comprehensive Survey. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3395051

[32] Fernando, G.-P., Almenares M F & Calderón-Benavides L (2024). Evaluation of the performance of unsupervised learning algorithms for intrusion detection in unbalanced data environments. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3516615

[33] Fuentes-Garcia, M., Camacho, J., & Macia-Fernandez, G. (2021). Present and Future of Network Security Monitoring. IEEE Access, 9, 1–1. https://doi.org/10.1109/access.2021.3067106

[34] Hajar H A Xiao, Y., & Li, T. (2024). A CVAE-based Anomaly Detection Algorithm for Cyber Physical Attacks for Water Distribution Systems. IEEE Access, 12, 48321–48334. https://doi.org/10.1109/access.2024.3384295

[35] Han, C., Li, T., Chen, Q., Wu, Y., & Qin, J. (2024). Distributed and Collaborative Lightweight Edge Federated Learning for IoT Zombie Devices Detection. ACM Transactions on Sensor Networks. https://doi.org/10.1145/3691634

[36] Hong, A. E., Malinovsky, P. P., & Damodaran, S. K. (2023). Towards Attack Detection in Multimodal Cyber-Physical Systems with Sticky HDP-HMM based Time Series Analysis. Digital Threats. https://doi.org/10.1145/3604434

[37] Houkan, A., Sahoo, A. K., Sarada P Gochhayat, S, P. K., Liu, H., Khalid, S. G., & Jain, P. (2024). Enhancing Security in Industrial IoT Networks: Machine Learning Solutions for Feature Selection and Reduction. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3481459

[38] Huang, H., Kong, W., Zhou, S., Zheng, Z., & Guo, S. (2021). A Survey of State-of-the-Art on Blockchains. *ACM Computing Surveys*, *54*(2), 1–42. https://doi.org/10.1145/3441692

[39] Hussain, S., Maaz B A Asif, M., Akram, W., Mahmood, K., Ashok K D & Shetty, S. (2023). APT Adversarial Defence Mechanism for Industrial IoT Enabled Cyber-Physical System. IEEE Access, 11, 74000–74020. https://doi.org/10.1109/access.2023.3291599

[40] Ishibashi, R., Miyamoto, K., Han, C., Ban, T., Takahashi, T., & Takeuchi, J. (2022). Generating Labeled Training Datasets Towards Unified Network Intrusion Detection Systems. IEEE Access, 10, 53972–53986. https://doi.org/10.1109/access.2022.3176098

[41] Jayalaxmi, P. L. S., Saha, R., Kumar, G., Conti, M., & Kim, T.-H. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. *IEEe Access*, *10*, 121173–121192.

[42] Jerez, C. I., Zhang, J., & Silva, M. R. (2022). On Equivalence of Anomaly Detection Algorithms. ACM Transactions on Knowledge Discovery from Data, 17(2), 1–26. https://doi.org/10.1145/3536428

[43] Kaliappan, C. P., Palaniappan, K., Ananthavadivel, D., & Subramanian, U. (2024). Advancing IoT security: A comprehensive AI-based trust framework for intrusion detection. *Peer-to-Peer Networking and Applications*, *17*(5), 2737–2757. https://doi.org/10.1007/s12083-024-01684-0

[44] Kandhro, I. A., Alanazi, S. M., Ali, F., Kehar, A., Fatima, K., Uddin, M., & Karuppayah, S. (2023). Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures. IEEE Access, 11, 9136–9148. https://doi.org/10.1109/access.2023.3238664

[45] Khayat, M., Barka, E., Serhani, M. A., Farag Sallabi, Shuaib, K., & Khater, H. M. (2025). Empowering Security Operation Center with Artificial Intelligence and Machine Learning – A Systematic Literature Review. IEEE Access, 1–1. https://doi.org/10.1109/access.2025.3532951

[46] Kim, H., Ahn, S., Ha, W. R., Kang, H., Kim, D. S., Kim, H. K., & Paek, Y. (2021). Panop: Mimicry-Resistant ANN-Based Distributed NIDS for IoT Networks. IEEE Access, 9, 111853–111864. https://doi.org/10.1109/ACCESS.2021.3103015

[47] Koca, M., & Avci, I. (2024). A Novel Hybrid Model Detection of Security Vulnerabilities in Industrial Control Systems and IoT Using GCN+LSTM. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3466391

[48] Kornaros, G. (2022). Hardware-assisted Machine Learning in Resource-constrained IoT Environments for Security: Review and Future Prospective. IEEE Access, 1–1. https://doi.org/10.1109/access.2022.3179047

[49] Kumari, A., Patel, R. K., Sukharamwala, U. C., Tanwar, S., Raboaca, M. S., Saad, A., & Tolba, A. (2022). AI-empowered attack detection and prevention scheme for smart grid system. *Mathematics*, *10*(16), 2852.

[50] Lundberg, H., Mowla, N. I., Sarder F A, Thar, K., Mahmood, A., Gidlund, M., & Raza, S. (2022). Experimental Analysis of Trustworthy In-Vehicle Intrusion Detection System Using eXplainable Artificial Intelligence (XAI). 10, 102831–102841. https://doi.org/10.1109/access.2022.3208573

[51] Madani, P., Vlajic, N., & Maljevic, I. (2022). Randomized Moving Target Approach for MAC-Layer Spoofing Detection and Prevention in IoT Systems. Digital Threats: Research and Practice. https://doi.org/10.1145/3477403

[52] Malik, M. S. (2024). IoT malware: A comprehensive survey of threats, vulnerabilities, and mitigation strategies. *International Journal for Electronic Crime Investigation, 8*(1). https://ijeci.lgu.edu.pk//article//187

[53] Mallidi, S. K. R., & Ramisetty, R. R. (2025). Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: A systematic literature review. *Discover Internet of Things*, *5*(1), 8. https://doi.org/10.1007/s43926-025-00099-4

[54] Markevych, M., & Dawson, M. (2023). A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI). *International Conference KNOWLEDGE-BASED ORGANIZATION*, *29*(3), 30–37. https://doi.org/10.2478/kbo-2023-0072

[55] Mesadieu, F., Torre, D., & Anitha C (2024). Leveraging Deep Reinforcement Learning Technique for Intrusion Detection in SCADA Infrastructure. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3390722

[56] Mirza A K, Sanober F M, Eising, C., & Lubna L D. (2023). Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. IEEE Access, 11, 145869–145896. https://doi.org/10.1109/access.2023.3346320

[57] Mirzaaxmedov D.M. (2024). CYBERSECURITY RISK ANALYSIS IN THE IOT: A SYSTEMATIC REVIEW. *Экономика и социум*, *7 (122)*. https://cyberleninka.ru/article/n/cybersecurity-risk-analysis-in-the-iot-a-systematic-review

[58] Mohammed, S. H., Abdulmajeed A, Mandeep J S, Jiménez, G., Jaber, A. S., Yaseein S H, Al-Najjar, M. M., & Dhiya A. (2024). Evaluation Feature Selection with Using Machine Learning for Cyber-Attack Detection in Smart Grid: Review. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3370911

[59] Mohan B C Tariq, S., Singh, R., Fateneh J, P, C., & Surya N (2024). Towards Human-AI Teaming to Mitigate Alert Fatigue in Security Operations Centres. ACM Transactions on Internet Technology, 24(3). https://doi.org/10.1145/3670009

[60] Mousa'B M S, Mohammad K H, Sulaiman, R., Islam, S., & Atta. (2023). An Explainable Ensemble Deep Learning Approach for Intrusion Detection in Industrial Internet of Things. IEEE Access, 11, 115047–115061. https://doi.org/10.1109/access.2023.3323573

[61] Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustainable Cities and Society*, *72*, 102994.

[62] Muhammad M, Ahmed, G., Al-Shamayleh, A. S., Adnan A, Siddiqui, S., & Abdulla H A. (2024). Empowering IoT Resilience: Hybrid Deep Learning Techniques for Enhanced Security. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3482005

[63] Mundt, M., & Baier, H. (2022). Threat-based Simulation of Data Exfiltration Towards Mitigating Multiple Ransomware Extortions. Digital Threats: Research and Practice. https://doi.org/10.1145/3568993

[64] Muneer, S., Farooq, U., Athar, A., Ahsan Raza, M., Ghazal, T. M., & Sakib, S. (2024). A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis. *Journal of Engineering*, *2024*(1), 3909173. https://doi.org/10.1155/2024/3909173

[65] Muniswamy, A., & Rathi, R. (2024). A Detailed Review on Enhancing the Security in Internet of Things-Based Smart City Environment Using Machine Learning Algorithms. IEEE Access, 12, 120389–120413. https://doi.org/10.1109/access.2024.3450180

[66] Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A Survey on Security and Privacy Issues in Modern Healthcare Systems. ACM Transactions on Computing for Healthcare, 2(3), 1–44. https://doi.org/10.1145/3453176

[67] Nguyen, Q. H., Hore, S., Shah, A., Le, T., & Bastian, N. D. (2024). FedNIDS: A Federated Learning Framework for Packet-based Network Intrusion Detection System. Digital Threats: Research and Practice. https://doi.org/10.1145/3696012

[68] Nitz, L., Gurabi, M. A., Cermak, M., Zadnik, M., Karpuk, D., Drichel, A., Schäfer, S., Holmes, B., & Mandal, A. (2024). On Collaboration and Automation in the Context of Threat Detection and Response with Privacy-Preserving Features. Digital Threats: Research and Practice. https://doi.org/10.1145/3707651

[69] Olawale, O. P., & Ebadinezhad, S. (2024). Cybersecurity Anomaly Detection: AI and Ethereum Blockchain for a Secure and Tamperproof IoHT Data Management. IEEE Access, 12, 131605–131620. https://doi.org/10.1109/access.2024.3460428

[70] Otoum, Y. (2022). *AI-Based Intrusion Detection Systems to Secure Internet of Things (IoT)* [PhD Thesis, Université d'Ottawa/University of Ottawa]. https://ruor.uottawa.ca/server/api/core/bitstreams/442830b0-132e-4085-b213-c21e12340eac/content

[71] Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access, 12, 12229–12256. https://doi.org/10.1109/access.2024.3355547

[72] RAnandh, R, T., Sagunthala R&d, Vishakha S, & Gopinath, N. (2024). Modelling a Novel Linear Transformed Attention Mechanism for Intrusion Detection Using Learning Approach. First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT). https://doi.org/10.1109/IC2SDT62152.2024.10696639

[73] Rajapaksha, S., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., Madzudzo, G., & Cheah, M. (2023). AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey. *ACM Computing Surveys*, *55*(11), 1–40. https://doi.org/10.1145/3570954

[74] Rizvi, S., Scanlon, M., Mcgibney, J., & Sheppard, J. (2022). Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions. IEEE Access, 10, 110362–110384. https://doi.org/10.1109/access.2022.3214506

[75] Rockey, H. (2022). *AI-Driven Cybersecurity in IoT: Detecting and Preventing Attacks on Smart Devices*. https://www.researchgate.net/profile/Hani-Rockey/publication/388525189_AI-Driven_Cybersecurity_in_IoT_Detecting_and_Preventing_Attacks_on_Smart_Devices/links/679bba388311ce680c4468bd/AI-Driven-Cybersecurity-in-IoT-Detecting-and-Preventing-Attacks-on-Smart-Devices.pdf

[76] Sabit, H. (2025a). *AI-Based Smart Security System Using IoT for Smart Home Applications*. https://www.preprints.org/frontend/manuscript/e8a635e9df5d7f65693b228adecd1e19/download_pub

[77] Sabit, H. (2025b). Artifical Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications. *Electronics*, *14*(3), 608.

[78] Salahaldeen D, & Abdullah M A (2024). Enhancing Cyberattack Detection Using Dimensionality Reduction With Hybrid Deep Learning on Internet of Things Environment. IEEE Access, 12, 84752–84762. https://doi.org/10.1109/access.2024.3411612

[79] Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, *36*, 100520. https://doi.org/10.1016/j.jii.2023.100520

[80] Scott, E., Panda, S., Loukas, G., & Panaousis, E. (2022). Optimising user security recommendations for AI-powered smart-homes. *2022 IEEE Conference on Dependable and Secure Computing (DSC)*, 1–8. https://ieeexplore.ieee.org/abstract/document/9888829/

[81] Selvaraj, M., & Uddin, G. (2024). A Large-Scale Study of IoT Security Weaknesses and Vulnerabilites in the Wild. *ACM Transactions on Software Engineering and Methodology*. https://doi.org/10.1145/3691628

[82] Shah, K., Jadav, N. K., Tanwar, S., Singh, A., Pleșcan, C., Alqahtani, F., & Tolba, A. (2023). AI and blockchain-assisted secure data-exchange framework for smart home systems. *Mathematics*, *11*(19), 4062.

[83] Sheeja, S. (2023). Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review. *Engineering and Applied Science Research*, *50*(6), 633–645.

[84] Shrivastwa, R.-R., Bouakka, Z., Perianin, T., Dislaire, F., Gaudron, T., Souissi, Y., Karray, K., & Guilley, S. (2022). An Embedded AI-Based Smart Intrusion Detection System for Edge-to-Cloud Systems. In A. Nitaj & K. Zkik (Eds.), *Cryptography, Codes and Cyber Security* (Vol. 1747, pp. 20–39). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-23201-5_2

[85] Sikder, A. K., Babun, L., Aksu, H., & Uluagac, A. S. (2019). Aegis. Proceedings of the 35th Annual Computer Security Applications Conference. https://doi.org/10.1145/3359789.3359840

[86] Singh Popli, M., Singh, R. P., Kaur Popli, N., & Mamun, M. (2025). A Federated Learning Framework for Enhanced Data Security and Cyber Intrusion Detection in Distributed Network of Underwater Drones. IEEE Access, 13, 12634–12646. https://doi.org/10.1109/access.2025.3530499

[87] Skopik, F., Wurzenberger, M., Höld, G., Landauer, M., & Kuhn, W. (2022). Behavior-Based Anomaly Detection in Log Data of Physical Access Control Systems. IEEE Transactions on Dependable and Secure Computing, 1–18. https://doi.org/10.1109/TDSC.2022.3197265

[88] Sowmya, T., & Anita, E. M. (2023). A comprehensive review of AI based intrusion detection system. *Measurement: Sensors*, *28*, 100827.

[89] Srinivasan, N. (2024). Artificial Intelligence in IoT Security: Review of Advancements, Challenges, and Future Directions. International Journal of Innovative Technology and Exploring Engineering, 13(7), 14–20. https://doi.org/10.35940/ijitee.g9911.13070624

[90] Sung, T.-W., Lee, C.-Y., Gaber, T., & Nassar, H. (2023). Innovative artificial intelligence-based Internet of Things for smart cities and smart homes. *Wireless Communications and Mobile Computing*, *2023*. https://salford-repository.worktribe.com/output/1654575

[91] Tannishtha D, Saha, R., Kumar, G., & Conti, M. (2025). PIN: Application-level Consensus for Blockchain-based Artificial Intelligence Frameworks. ACM Transactions on Intelligent Systems and Technology, 3. https://doi.org/10.1145/3721845

[92] Torre, D., Anitha C, Jo, J., Vyas, G., & Sabrsula, B. (2024). Towards Enhancing Privacy-Preservation of a Federated Learning CNN Intrusion Detection System in IoT: Method and Empirical Study. ACM Transactions on Software Engineering and Methodology. https://doi.org/10.1145/3695998

[93] Tsikerdekis, M., Waldron, S., & Emanuelson, A. (2021). Network Anomaly Detection Using Exponential Random Graph Models and Autoregressive Moving Average. IEEE Access, 9, 134530–134542. https://doi.org/10.1109/access.2021.3116575

[94] Ullah, I., & Mahmoud, Q. H. (2022). Design and Development of RNN Anomaly Detection Model for IoT Networks. IEEE Access, 10, 62722–62750. https://doi.org/10.1109/access.2022.3176317

[95] Vadym S, Jamil, M, Andrii O, Volodymyr A, & Safarudin G H. (2024). Exploring the potential network vulnerabilities in the smart manufacturing process of Industry 5.0 via the use of machine learning methods. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3474861

[96] Verma, P., Nitesh B, Breslin, J. G., O'Shea, D., Ankit V, & Gupta, D. (2023). Zero-Day Guardian: A Dual Model Enabled Federated Learning Framework for Handling Zero-Day Attacks in 5G Enabled IIoT. IEEE Transactions on Consumer Electronics, 1–1. https://doi.org/10.1109/tce.2023.3335385

[97] Villegas-Ch, W., Govea, J., Rommel G, & Mera-Navarrete, A. (2025). Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection. IEEE Access, 1–1. https://doi.org/10.1109/access.2025.3532800

[98] Wang, H., Eklund, D., Oprea, A., & Raza, S. (2023). FL4IoT: IoT Device Fingerprinting and Identification using Federated Learning. *ACM Transactions on the Internet of Things*, *4*(3), 1–24. https://doi.org/10.1145/3603257

[99] Wang, X., Qi, L., Wei, X., Zhu, W., Jiang, H., & Guan, Z. (2024). AED: A Novel Approach for Intrusion Detection without Abnormal Samples in Big Data Environment. Journal of Data and Information Quality. https://doi.org/10.1145/3695879

[100]Weber, S. B., Stein, S., Pilgermann, M., & Schrader, T. (2023). Attack Detection for Medical Cyber-Physical Systems–A Systematic Literature Review. IEEE Access, 11, 41796–41815. https://doi.org/10.1109/access.2023.3270225

[101]Yu, J., Shvetsov, A. V., & Saeed H A. (2024). Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3482987