Jurnal Informatika dan Teknologi Interaktif
Volume 2, Number 1, April 2025

DOI : 10.63547/jiite.v2i1.64
e-ISSN : 3048-1023

Enhancing IoT Security: A review of Machine Learning-Driven Approached to Cyber Threat Detection

Misbah Ali[1], Aamir Raza[2], Malik Arslan Akram[3], Haroon Arif[4], Aamir Ali[5]
[1]Department of Computer Science and Information Technology, Virtual University, Lahore, Pakistan
[2] Department: Department of Information Technology & Management, Illinois Institute of Technology, Chicago, USA
[3]Software Engineering, Southwest University of Science and Technology, China.
[4]Department: Department of Computer Science, Illinois Institute of Technology, Chicago, USA
[5]Department of Computer Science and Information Technology, Government College University Faisalabad Sahiwal campus
Email:[1] talktomisbah@gmail.com, [2]araza7@hawk.iit.edu [3]arsslan96@mails.swust.edu.cn [4]harif@hawk.iit.edu [5]Amirali4436823@gmail.com

Article Info

Article history:
Received 28-02-2025
Revised 14-03-2025
Received 10-04-2025

Keywordsi:
Internet of Things (IoT)
Cybersecurity
Machine Learning (ML)
Deep Learning (DL)
Intrusion Detection System

ABSTRACT

The Internet of Things (IoT) is rapidly adopted and implemented across various industries. The fast growth of IoT devices poses a risk, as these devices are ideal targets to be breached and exploited. However, given the heterogeneous nature and resource limitations of IoT networks, the traditional security mechanisms often fail to provide the required security. This study investigates recent IoT security breaches and showcases vulnerabilities exploited by attackers, as well as their impact on consumer, industrial, and healthcare IoT systems. The proposed solutions through ML and DL-driven security are summarized for adaptive threat detection, anomaly-based intrusion prevention, and intelligent risk mitigation. We also analyzed different approaches based on ML and DL to identify and prevent cyber-attacks as an effective solution. These ML and DL – based research papers have been reviewed within the IEEE repository and the publications span from 2020 to 2024, ensuring current literature on IoT security. The results highlight that security models based on ML and DL techniques improve resilience against IoT by allowing real-time detection of attacks, reducing the volume of false positives, and adapting to new threats. Furthermore, this work identifies the existing barriers to the adoption of ML/DL technologies for IoT security and emphasizes the potential areas for future research that may solidify the overall security framework for IoT ecosystems.

Corresponding author:
Misbah Ali
Department of Computer Science and Information Technology, Virtual University, Lahore, Pakistan
Email: talktomisbah.ali@gmail.com

1. INTRODUCTION

The Internet of Things (IoT) is revolutionizing various sectors with improved connection and automated processes. This expansion faces critical security challenges as most of the IoT devices are resource-restricted leading to limited implementation of strong security mechanisms. Furthermore, the lack of standardized security protocols for the cooperation of various IoT devices provides the risk of vulnerabilities causing data breaches and unauthorized access. These risks can expose critical infrastructure and have devastating consequences [1].

IoT security framework is an organized approach that shields IoT devices from cyber-attacks by integrating protection protocols, threat detection mechanisms, and mitigation strategies. A general IoT framework comprises an application layer, cloud layer, edge layer, network layer, and perception layer. Each layer applies its own security protocols that ensure data confidentiality and security mechanisms against IoT devices [2].

The solution to these challenges is the emergence of smart security mechanisms using cutting-edge Artificial Intelligence (AI)-based technologies. AI-based techniques have been playing a critical role in improving the security of IoT [3]. They lead to adaptive security frameworks that can detect and respond to IoT threats in real-time. AI-powered solutions can proactively counter advanced cyber-attacks, by detecting patterns and anomalies in IoT networks, thereby preserving the integrity and resilience of IoT systems [4]. IoT devices can also adapt or learn from past threats using traditional and advanced ML algorithms by appropriately perceiving unusual activity in the future hence enhancing security with less reliance on human intervention [5], [6].

Traditional security models are not sufficient to protect IoT systems as they perform Static Rule-Based Detection relying on predefined rules and signatures to identify threats [7]. Additionally, the differences among various implementations and large-scale deployment cause the scalability issue and prevent from applying uniform security protocols, leaving many vulnerabilities unaddressed. These constraints demand specialized security solutions based on modern AI for IoT systems [8].

Machine Learning (ML) and Deep Learning (DL) have emerged as crucial techniques in improving the security of IoT networks. These techniques are highly effective for processing large volumes of data to find patterns that may be indicative of potential threats. ML and DL can be used to identify anomalies and malicious activities in real-time using sophisticated algorithms that allow quick responses to breaches [9].The application of ML and DL models can inherently enable ongoing learning with an evolving ability to cope with new data patterns, providing an improved ability to identify future automatic malicious attacks [10]. The potential benefits achieved by implementing ML DL approach for IoT security are presented in Figure 2.

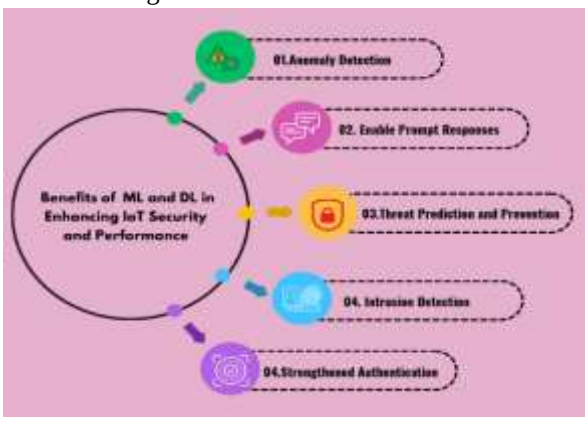

Figure 1. Advantages of ML and DL approaces for IOT security

The rest of this paper is organized as follows: recent case studies of security attacks in IoT environments are discussed in Section 2. Section III presents ML-based security solutions; then it examines the ML techniques adopted for intrusion detection in IoT networks. DL-driven approaches are described in section IV while discussing advanced models to discover cyber threats in real-time. Section V describes the challenges in terms of IoT security and future research directions. Lastly, in VI, the paper is concluded with a summary of its findings and a call for systems integrating an AI-driven security framework.

2. RECENT ATTACKS ON IOT DEVICES

IoT devices are the primary targets for cybercriminals owing to the dynamic growth of IoT technology. Over the past few years; the retail market, manufacturing, and healthcare IoT systems have been badly affected based on the crucial vulnerabilities causing data breaches, service disruptions, and physical harm. Real-world case studies provide crucial information regarding dynamic cybersecurity attacks. We can analyze the effectiveness of current security mechanisms by determining common vulnerabilities and frequent attack patterns. Below section will discuss recent attacks on IoT devices causing damage to industrial sectors, healthcare devices, and smart home devices. These case

studies were selected based on the diversity of attack techniques and their significance in the current security landscape. The potential damages of IoT-based systems are graphically presented in Figure 3.

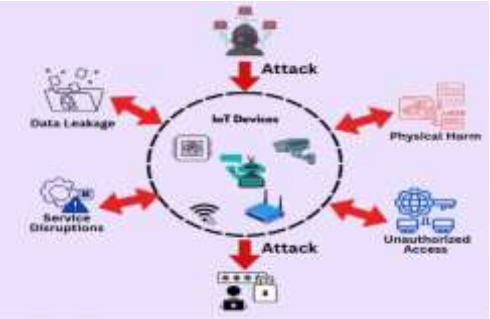

Figure 2. Potential damages to IoT systems

2.1 Incident: Security Breach in PSA-Certified IoT Chip

A critical security issue was found in an IoT security chip that was certified against the Arm Platform Security Architecture (PSA) Level 2 standard [11]. The chip was extensively embedded in smart home devices, industrial IoT systems, and authentication systems, where it used AES-128 to protect sensitive data. However, researchers discovered that the certified chip remained susceptible to a non-invasive electromagnetic (EM) side-channel attack, enabling attackers to obtain parts of the encryption key by passively observing the electromagnetic signals leaked during encryption processing. This vulnerability casts serious doubt on the ability of certification standards to protect IoT hardware against advanced physical attacks.

The intruders used an electromagnetic probe and an oscilloscope to chart emissions from the chip as it conducted encryption work. With thousands of EM traces, the attackers drove secret patterns in how the chip processed encryption keys. Statistical T-tests and correlation analysis verified a significant data leak that permitted attackers to recover almost 50% of the 16-byte AES encryption key. Until half of the key is revealed it is impossible to use brute-force techniques to recover the remaining bytes, which would greatly speed things up in terms of time and computational power required to break the encryption. The execution of this attack without direct physical tampering of the chip demonstrated the stealthy and dangerous nature of side-channel attacks in IoT security.

These findings led many security experts to call for stronger countermeasures to protect IoT devices from this kind of vulnerability. The recommendation was to upgrade to PSA Level 3 certification, which requires stronger safeguards against side-channel attacks. Instead, experts proposed hardware-level changes, like masking techniques and noise injection, to block EM signal leaks. The researchers also proposed software-level security improvements, including secure key management and advanced cryptographic techniques, to reduce the risk of similar attacks in future IoT deployments, in addition to hardware enhancements. One of the key learnings from this case study is the need to strengthen IoT security across both hardware and software layers so that critical devices can withstand an evolving threat landscape.

2.2 Incident 2: Baby Monitoring Camera Hijacking

An alarming security incident involved baby monitoring cameras (BMCs) which reported that attackers obtained unauthorized access to live video streams and interacted with children [12]. The breach was linked to several security vulnerabilities, including default login credentials, unencrypted peer-to-peer (P2P) cloud streaming, and open TCP ports (554, 5000). These vulnerabilities enabled hackers to hack the cameras remotely, watch live feeds, and change the camera's settings — a serious privacy threat to families. In some instances, hackers raided home networks by scanning for vulnerable cameras and then brute-forcing default admin credentials. Once they were inside, they exploited intercepted cloud-based communications to control the device remotely, often speaking through the camera's built-in microphone to scare or manipulate the users. Parents whose kids had been affected reported unsettling incidents where strangers addressed their children at night or shouted orders using hooked-up smart home systems.

To mitigate these threats, manufacturers introduced required password changes at the time of setup, improved encryption for data sent over the cloud, and reduced the number of unnecessary open ports. Users were also urged to

turn off remote access features when they are not needed to use strong, unique passwords and to keep firmware up to date to head off similar breaches in the future.

2.3 Incident 3: Exploiting Medical IoT Devices for Cyberattacks

Hackers attacked hospital-based IoT-enabled equipment, such as MRI machines, infusion pumps, and patient monitoring systems, by exploiting weak authentication mechanisms and default credentials left unchanged [13]. These devices were infected and became part of a botnet, enabling attackers to swamp targeted networks with huge volumes of traffic, disrupting critical healthcare services. Security experts discovered a common vulnerability on used hospital IoT networks, where hacked medical devices were being used to perform DDoS attacks.

In this incident, "MedJack," a botnet malware was found inside hospital networks, slowly infecting at-risk medical IoT devices. Unlike conventional malware, which was directed at consumer and enterprise systems that featured better monitoring to discover intruders, the MedJack was designed to go undetected, hiding inside medical equipment that didn't have such monitoring. The attackers exploited these infected devices to carry out DDoS attacks against hospital databases and medical record systems, resulting in network slowdowns and disruptions in patient care Emergency treatments were delayed in some cases, when hospitals lost access to critical patient records.

To defend against these risks, hospitals were recommended to segment their networks so that medical IoT devices could operate over isolated, secure networks that weren't intertwined with administrative or patient data systems. Also helped were intrusion detection systems (IDS) that helped detect unusual traffic patterns early on before larger disruptions could take place. The best practices to keep hospital IoT environments more secure against similar cyber included regular software updates, enforcing strong passwords, and disabling unnecessary remote access.

3. MACHINE LEARNING DRIVEN APPROACHES FOR SAFEGUARDING IOT NETWORKS

Traditional security mechanisms have proven slow to respond to the increasing complexity and volume of cyber threats. ML has become a powerful instrument for strengthening IoT security, providing adaptive, real-time capabilities for threat detection and mitigation. In the next section, we will describe different ML-based techniques that improve the security of IoT devices against complex attacks and maintain low false positives and system overhead [14], [15].

In a separate study [17], the researcher created an ML-based spam detection framework for IoT systems that utilized BGLM, Boosted Linear Model, XGBoost, GLM with Stepwise Feature Selection, and Bagged Model. Detection accuracy on the REFIT Smart Home dataset was enhanced with PCA and entropy-based filters, achieving a reduction in false positives.

Furthermore, it was also previously examined from the perspective of adversarial ML to evade traditional ML-based malware detection within an IoT setting [19]. The use of IoT devices was expanded to include the study of bypassing traditional malware detection frameworks using adversarial machine learning techniques. Benign-appearing apps were crafted as adversarial samples using Euclidean Distance and PSO, achieving 89.6% accuracy and surpassing traditional classifiers. The static feature-based models were shown to be vulnerable, and the absence of adversarial training was highlighted as a gap.

In another study, researchers recently proposed a framework driven by ML to secure IoT-based data transmission [21]. A secure framework of data transmission in IoT networks was designed combining iForest for anomaly detection, SVM for intrusion detection, and AES encryption. They achieved accuracy rates of 99.5% in anomaly detection and 98.61% in intrusion detection, outperforming traditional cryptographic techniques.

Summary

Recent research applied various ML techniques including XGBoost, RF, SVM, and iForest for IoT intrusion detection, anomaly detection, and cyber threat mitigation showing their efficiency in this study. With adaptive learning, automated threat classification, and reduced false positives, these approaches produce improved results as compared to the traditional rule-based security mechanisms. Nonetheless, challenges pose serious concerns such as adversarial attacks, limited datasets, and testing ML-based solutions in real time on resource-constrained IoT devices.

Addressing adversarial attacks is crucial to strengthen ML-based models for robust IoT security measures. Adversarial training is the most widely followed technique in which model training is performed both on cleaned data and thoughtfully designed adversarial examples which expand the flexibility against modified input data. Techniques such as defensive distillation and input preprocessing methods improve the model's response against minor changes

in input. Moreover, feature squeezing, randomization, and data sanitization methods can neutralize adversarial noise prior to data feeding into the models.

4. STRENGTHENING IT NETWORKS AGAINST CYBER THREATS USING DEEP LEARNING

Traditional ML-based security mechanisms have limitations against modern techniques being used in real-world attacks, as IoT networks have become increasing targets of cyber threats. Deep learning (DL) is an advanced approach in AI that has growing applications in many areas [23]. DL models process large amounts of network traffic data, capturing subtle attack patterns that traditional rule-based and ML methods may overlook. DL techniques, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Generative Adversarial Networks (GANs), facilitate real-time intrusion detection and allow adaptive cybersecurity measures [24]. In this section, we highlight the most common deep learning methods applied to protect IoT networks and their efficacy in identifying cyber-attacks.

In another study [26], authors proposed a solution addressing IoT security threats through an intrusion detection mechanism, observing that a real-time detection mechanism of cyber threats could be developed by identifying gateway traffic. A hybrid DL-based IDS was proposed that employed CNNs to extract spatial features along with LSTM networks to analyze temporal features. They used the CSE-CIC-IDS2018 dataset which is a comprehensive and current intrusion detection dataset with multiple attack scenarios for training and evaluating the model. The experimental results showed that the CNN-LSTM model reached 99% accuracy for binary classification and 97.11% accuracy for multiclass classification, exceeding the classification performance of prior DL-based approaches for IDS. These results demonstrated that hybrid CNN-LSTM architectures are capable of accurately detecting and classifying different types of IoT security threats while offering a promising solution for real-time IDSs.

A recent research targeted intrusion detection tasks in IoT networks, aiming the secure resource-constrained IoT nodes against diverse cyber threats [29]. They presented Deep-IDS, an LSTM-based Intrusion Detection System (IDS) for the task of real-time intrusion detection and mitigation. The model was trained using the CIC-IDS2017 dataset that included diverse attacks such as DOS, DDoS**,** Brute Force, Man-in-the-Middle (MITM), and Replay Attacks**.** The experimental results showed that Deep-IDS can accurately classify benign (normal) and malicious (attack) traffic, with an accuracy of 97.67%, a detection rate of 96.8%, and a low false alarm rate. The results emphasized that Deep-IDS is ideal for edge-server implementation, offering low-latency, high-accuracy threat detection to protect IoT networks against constantly evolving cyber threats

The aim of the study [30] was to address the intrusion detection problem in IoT networks while particularly focusing on the difficulties related to detecting real-time threats and classifying malicious network traffic. The authors suggest a hybrid deep learning model approach for an IDS, employing CNNs for spatial feature extraction and LSTM networks for temporal pattern recognition. The CICIoT2023 dataset is used to train and evaluate the model involving different types of IoT attacks including DDoS, brute force, spoofing, and web-based attacks, while the testing was performed on the CICIDS2017 dataset. The experimental results showed that 98.42% accuracy is achieved by the CNN-LSTM model with a 0.0275 low loss rate and an F1-score is 98.57% proving their system is far better than the existing techniques of intrusion detection. The results indicated that deep learning-based IDS models present a promising method for effective real-time anomaly detection, reinforcing IoT network security in the face of emerging cyber threats. DL technique used for the security of IoT is shown in graphical form in Figure 6.

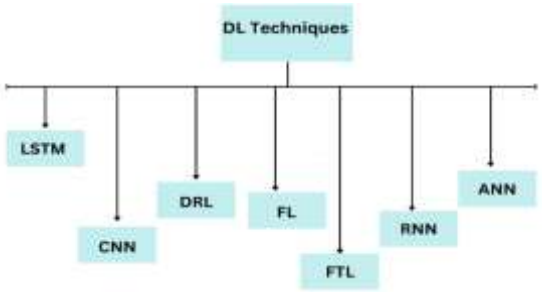

Figure 3. DL techniques applied fot IOT security

Summary

The summary of ML and DL approaches to mitigate IoT security challenges is presented in Table 1.

Table 1. Summary of ML and DL approaches to mitigate IoT security challenges

Study	Year of publication	Proposed Approach	ML Techniques Used	Dataset Used	Key Findings
[16]	2020	z-classifiers to achieve zero false positives in detecting malicious activities	Custom z-classifiers, iterative learning firewall	KDD CUP'99, Power Grid Monitoring System	Reduced false positives while maintaining a reasonable false negative rate
[17]	2020	Spamicity score development using ML-based classification for IoT spam detection	BGLM, Boosted LM, XGBoost, GLM, Bagged Model	REFIT Smart Home Dataset	Improved accuracy in identifying malicious IoT activity, reducing false positives
[22]	2021	ML techniques for DDoS detection and mitigation	SVM, ANN, KNN, Decision Trees, Random Forest	CICIDS2017, IoTPOT	Hybrid ML models (K-Means + Decision Trees) reduced false positives and improved attack detection
[25]	2021	Vulnerability identification and zero-day attack detection	LSTM-EVI – An LSTM-based penetration testing framework	Smart Airport Cybersecurity Testbed (Physical IoT + Virtual Simulation)	Achieved 99% detection accuracy, outperforming MLP, SVM, Naive Bayes, and KNN
[18]	2022	Anomaly detection and replication attack identification	XGBoost (Gradient-Boosted Decision Trees)	IoT-23 Dataset	Achieved 93.6% accuracy and 99.9% recall, proving superior to traditional models
[19]	2022	Explored adversarial ML attacks to bypass IoT malware detectors	Euclidean Distance (ED), Particle Swarm Optimization (PSO)	AndroZoo, AMD datasets	100% evasion success (PSO), 89.6% evasion success (ED), highlighting weaknesses in ML malware detection
[20]	2023	Detect malware, DDoS attacks, and intrusions in 5G networks	RF, SVM, Decision Trees	Real-World 5G Network Dataset	RF demonstrated higher accuracy and efficiency in intrusion detection
[27]	2023	Autonomous intrusion detection and cyber-physical system security	DRL for multi-agent cyber defense and intrusion detection	Network intrusion datasets, CPS logs, adversarial cybersecurity simulations	DRL models outperformed traditional security mechanisms, enabling adaptive real-time threat detection
[21]	2024	Anomaly detection, intrusion detection, and encryption for IoT security	Isolation Forest (Anomaly Detection), SVM (Intrusion Detection), AES (Encryption)	Real-World IoT Dataset	Achieved 99.5% anomaly detection accuracy, 98.6% intrusion detection accuracy, with minimal processing overhead

[26]	2024	Intrusion detection in IoT networks for real-time cyber threat analysis	Hybrid CNN-LSTM Intrusion Detection System (IDS)	CSE-CIC-IDS2018	Achieved 99% accuracy (binary classification) and 97.11% accuracy (multiclass classification), outperforming existing IDS models
[29]	2024	Cyberattack detection in IoT with limited labeled data and heterogeneous networks	FTL integrating FL and TL for collaborative deep learning-based intrusion detection	N-BaIOT, KDD, NSL-KDD, UNSW-NB15	Achieved 99% accuracy, improving by 40% over unsupervised DL approaches, proving efficiency in diverse IoT environments
[30]	2024	Real-time anomaly detection and classification of malicious IoT network traffic	Hybrid CNN-LSTM IDS for spatial and temporal pattern recognition	CICIOT2023, CICIDS2017	Achieved 98.42% accuracy, F1-score of 98.57%, and low loss rate of 0.0275, outperforming traditional IDS models

A year-wise distribution of selected studies is presented in Figure 7.

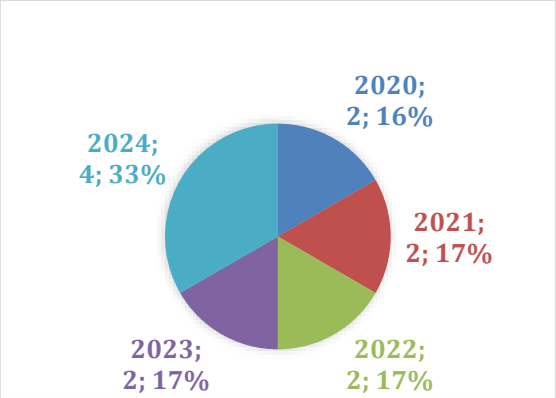

Figure 4. Year-wise distribution of selected studies

5. CHALLENGES AND FUTURE DIRECTIONS

Regardless of notable advancements of ML and DL in IoT security, there are certain challenges in applying state-of-the-art techniques. The potential short-term and long-term challenges along with future research directions are given in the following section.

5.1 Short-term challenges

IoT security issues that require immediate attention include weak passwords, unencrypted data transmission, lack of firmware updates, physical tempering, and over-permissive device pairing. Moreover, monitoring gaps, insecure APIs, and vendor backdoors pose serious concerns for IoT security models [1]. These challenges can be addressed by eliminating default credentials, applying security measures on transit data, and ensuring regular firmware updates. Furthermore, hardening insecure APIs, avoiding physical tempering, employing secure device pairing mechanisms, and eliminating vendor backdoors can tackle the most alarming short-term hazards [13].

5.2 Long term challenges

The major hurdle is limited data availability and imbalanced datasets producing overfitted models with poor generalization [31]. Moreover, ML-DL-based models often require high computational power along with significant memory; hence posing difficulties in their deployment on lightweight IoT nodes. Finally, the low generalizability of ML-DL security models leads to inconsistent results restricting the large-scale implementation in real-world applications [32].

Certain challenges are crucial in both short-term and long-term perspectives. For example, attackers can modify incoming data by manipulating the adversarial vulnerability of ML-DL models resulting in misclassified activities [33]. Additionally, IoT networks produce huge amounts of heterogeneous data which demand efficient and low-latency security mechanisms; hence scalability and real-time data processing remain major concerns.

To mitigate all these IoT security challenges, researchers should explore federated learning and edge AI to design lightweight and energy-efficient models while investigating distributed computational workloads and reduced dependency on centralized cloud computing. Moreover, adversarial defense strategies should be designed that integrate robust model training and adversarial detection mechanisms to improve model resistance against evasion attacks [34]. Furthermore, to address data scarcity, researchers need to develop more diverse datasets that represent real-world IoT security datasets and dynamic attack scenarios [35]. Additionally, there is a dire need for cooperation among academia, industry, and regulatory bodies to develop standardized security protocols preserving a streamlined integration of ML/DL-driven approaches.

A general comparison of ML and DL models for IoT security is presented in Table 2.

Table 2. General comparison of ML and DL models for IOT security

Aspect	ML Methods	DL Methods
Accuracy	Moderate to high	Generally high
Latency	Low to moderate	High
Resource Usage	Low (can run on lightweight IoT devices)	High (requires powerful hardware)
Feature Engineering	Manual and domain-specific	Automated hierarchical feature learning
Training Data Requirements	Suitable for smaller datasets	Large-scale datasets required for optimal results
Scalability	Moderate	High
Adaptability to New Threats	Requires retraining	More adaptive
Interpretability	Easier	Difficult
Robustness to Adversarial Attacks	Lower robustness depending upon model	Generally high robustness
Deployment Complexity	Simple deployment	Complex deployment
Energy Consumption	Lower energy footprint	Higher energy consumption
Suitability for Edge Computing	Highly suitable for lightweight deployments	Challenging as needs optimization for edge devices

6. CONCLUSION

The rapid expansion of IoT ecosystems has introduced new security vulnerabilities, making them attractive targets for cyber threats. Traditional security mechanisms often struggle to provide real-time threat detection and adaptive defense, necessitating the integration of Machine Learning (ML) and Deep Learning (DL) approaches. This paper examined recent IoT security breaches, highlighting real-world case studies that expose vulnerabilities in consumer, industrial, and healthcare IoT systems. To address these challenges, we surveyed ML – and DL–powered solutions and highlighted how techniques such as classification, clustering, anomaly detection, and deep reinforcement learning help improve intrusion detection and risk mitigation. The results showed that the use of ML and DL models can help enhance the security of IoT by conducting automated and real-time attack detection, reducing false positives, and adapting to constantly changing cyber threats. Nonetheless, challenges such as adversarial attacks, data sparsity, computational limits, and scalability issues still remain. In future research, we aim to build lightweight and energy-efficient ML/DL models that can be executed on resource-constrained IoT devices while avoiding performance degradation.

REFERENCES

[1] L. P. Rachakonda, M. Siddula, and V. Sathya, "A comprehensive study on IoT privacy and security challenges with a focus on spectrum sharing in Next-Generation networks (5G/6G/beyond)," *High-Confid. Comput.*, p. 100220, 2024.

[2] S. K. Sahu and K. Mazumdar, "Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance," *Front. Artif. Intell.*, vol. 7, p. 1397480, 2024.

[3] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, "AI-powered biometrics for Internet of Things security: A review and future vision," *J. Inf. Secur. Appl.*, vol. 82, p. 103748, 2024.

[4] S. Baral, S. Saha, and A. Haque, "An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs," in *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*, IEEE, 2024, pp. 469–474. Accessed: Feb. 28, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10811456/

[5] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, "Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey," *IEEE Access*, vol. 12, pp. 25469–25490, 2024, doi: 10.1109/ACCESS.2024.3365634.

[6] T. Al-Shurbaji *et al.*, "Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review," *IEEE Access*, 2025, Accessed: Feb. 28, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10829842/

[7] A. Attkan and V. Ranga, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex Intell. Syst.*, vol. 8, no. 4, pp. 3559–3591, Aug. 2022, doi: 10.1007/s40747-022-00667-z.

[8] W. Villegas-Ch, J. Govea, R. Gutierrez, and A. Mera-Navarrete, "Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection," *IEEE Access*, vol. 13, pp. 16933–16958, 2025, doi: 10.1109/ACCESS.2025.3532800.

[9] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1646–1685, 2020.

[10] V. S. Desanamukula, M. A. Priyadarshini, D. Srilatha, K. V. Rao, R. V. S. L. Kumari, and K. Vivek, "A Comprehensive Analysis of Machine Learning and Deep Learning Approaches towards IoT Security," in *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Jul. 2023, pp. 1165–1168. doi: 10.1109/ICESC57686.2023.10193209.

[11] F. Chen, D. Luo, J. Li, V. C. M. Leung, S. Li, and J. Fan, "Arm PSA-Certified IoT Chip Security: A Case Study," *Tsinghua Sci. Technol.*, vol. 28, no. 2, pp. 244–257, Apr. 2023, doi: 10.26599/TST.2021.9010094.

[13] E. Fazeldehkordi, O. Owe, and J. Noll, "Security and Privacy in IoT Systems: A Case Study of Healthcare Products," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, May 2019, pp. 1–8. doi: 10.1109/ISMICT.2019.8743971.

[14] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Netw.*, vol. 123, p. 102685, 2021.

[15] Y. Alsouda, S. Pllana, and A. Kurti, "A Machine Learning Driven IoT Solution for Noise Classification in Smart Cities," Sep. 01, 2018, *arXiv*: arXiv:1809.00238. doi: 10.48550/arXiv.1809.00238.

[17] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim, and M. Alrashoud, "An efficient spam detection technique for IoT devices using machine learning," *IEEE Trans. Ind. Inform.*, vol. 17, no. 2, pp. 903–912, 2020.

[18] M. A. Da Cruz, L. R. Abbade, P. Lorenz, S. B. Mafra, and J. J. Rodrigues, "Detecting compromised IoT devices through XGBoost," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 15392–15399, 2022.

[19] G. Renjith, P. Vinod, and S. Aji, "Evading machine-learning-based Android malware detector for IoT devices," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2745–2755, 2022.

[21] K. Subathra, G. R. Vignesh, S. T. Babu, D. Mendhe, R. kumar Yada, and R. Maranan, "Secure Data Transmission in IoT Networks: A Machine Learning-Based Approach," in *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, IEEE, 2024, pp. 1–5. Accessed: Feb. 23, 2025. [Online].

[23] M. Luqman *et al.*, "Intelligent parameter-based in-network IDS for IoT using UNSW-NB15 and BoT-IoT datasets," *J. Frankl. Inst.*, vol. 362, no. 1, p. 107440, 2025.

[24] P. M. Kumar, B. P. Kavin, A. Jagathpally, and T. Shahwar, "Transforming the cybersecurity space of healthcare IoT devices using Deep Learning," in *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, 2025, pp. 1–6. Accessed: Feb. 28, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10849305/

[26] R. Jablaoui and N. Liouane, "An effective deep CNN-LSTM based intrusion detection system for network security," in *2024 International Conference on Control, Automation and Diagnosis (ICCAD)*, Paris, France: IEEE, May 2024, pp. 1–6. doi: 10.1109/ICCAD60883.2024.10553826.

[30] A. Gueriani, H. Kheddar, and A. C. Mazari, "Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems," in *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, EL OUED, Algeria: IEEE, Apr. 2024, pp. 1–7. doi: 10.1109/PAIS62114.2024.10541178.

[31] R. Mishra and A. Mishra, "Current research on Internet of Things (IoT) security protocols: A survey," *Comput. Secur.*, p. 104310, 2025.

[32] C. Ni and S. C. Li, "Machine learning enabled industrial IoT security: Challenges, trends and solutions," *J. Ind. Inf. Integr.*, vol. 38, p. 100549, 2024.

[33] M. N. Halgamuge and D. Niyato, "Adaptive edge security framework for dynamic IoT security policies in diverse environments," *Comput. Secur.*, vol. 148, p. 104128, 2025.

[34] Z. Rehman, I. Gondal, M. Ge, H. Dong, M. Gregory, and Z. Tari, "Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception," *Comput. Secur.*, vol. 139, p. 103685, 2024.

[35] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet Things Cyber-Phys. Syst.*, vol. 4, pp. 167–185, 2024.