Macaw International Journal of Advanced Research in Computer Science and Engineering (MIJARCSE)
ISSN: 2455-4669. / Volume 12, Issue 1, June 2026
DOI: https://doi.org/10.70162/mijarcse/2026/v12/i1/v12i101

MACAW PUBLICATIONS
Scientific Research Journals

Review Paper

AI vs. AI in IoT Security: A Systematic Review of Autonomous Exploits and Defense Mechanisms

MNS. Rajeev Bhargava [1]

[1*] *Research Scholar, Trine University, Michigan, United States, Email: nmarupaka22@my.trine.edu*

**Corresponding Author(s): nmarupaka22@my.trine.edu*

Received: 10/01/2026, Revised: 18/03/2026, Accepted: 08/04/2026 Published: 13/04/2026

Abstract: Artificial intelligence (AI) empowered defense systems have evolved as a unique response to cyber security challenges occurring in the Internet of Things (IoT) as conventional security measures are ineffective against autonomous and adaptive threat manifestations. The paper studies the association between AI-driven offensive and defensive methods for protecting smart equipment within the AI vs AI concept. This includes systematic review aligned with PRISMA insights implemented with peer-reviews from databases including Scopus, Web of Science, IEEE Xplore, and ScienceDirect. The study involved generation of the ultimate sample of n=62 domain-based studies and it highlights the urgent requirement to develop a scalable, adaptive and strong AI framework with capabilities to manage emerging challenges of IoT security. Future research needs to emphasize on improving generalized models for reducing false positives and unifying lighter AI solutions for resource limited devices.

Key words: Artificial Intelligence, Internet of Things, Cybersecurity, AI-driven Intrusion Detection Systems, Deep Learning, Convolutional Neural Networks, Recurrent Neural Networks, Autoencoders, Adversarial Machine Learning, Reinforcement Learning, Generative Adversarial Networks.

1 Introduction

IoT (Internet of Things) architectures are rapidly expanding, transforming digital architecture for large-scale connectivity through several smart computing devices, systems, and essential services. Nevertheless, such change concurrently expanded the threat surface with increased exploration to new and advanced cyber threats. Conventional security models that are highly dependent on static principles or signature-based threat detection are proven obsolete due to the changing, dynamic nature of the IoT environment and digital structure, increasing threat patterns. To avoid such threats specific to IoT networks that lack proper resources, using AI (artificial intelligence) tools emerge as an architecture (Almiani et al., 2020). Offensive and defensive threat detection and security strategies are evolving and are integrated into a complicated digital landscape. These include adaptive defensive models, autonomous attack systems, etc.

Modern advancements encounter movement toward AI-driven systems such as adversarial intelligence like reinforcement learning architectures, GANs (generative adversarial networks) that are effective to generate and optimize strategies with real-time automation (Li et al., 2020). Simultaneously, intrusion detection systems powered with AI, deep learning models, and hybrid architectures are critical for anomaly detection. Despite such advancements, there are certain vulnerabilities and scalability challenges due to federated learning frameworks (Zhang et al., 2022). These new technologies and developments create security practices in IoT, making it a co-evolutionary system for IoT security with continuous adaptation of defensive and adversarial methods inside such a shared environment.

This paper targets to explore offensive and defensive strategies powered by AI, providing cybersecurity to IoT systems from threat against autonomous risk. Research questions are created to observe defense strategies that are highly prevailing and can be most effective, architecture options that can be implemented to attain higher performance, and challenges that prevail, obstructing scalability and adaptive threat prevention. Peer-reviewed research articles are utilized to make sure that all technology developments can be utilized to support changing threat patterns. Findings from this research offers understanding about IoT security constraints and provides a structured model to observe theoretical perspectives about adversarial learning and systems that co-evolve from security to threat.

2 Literature Review & Thematic Analysis

A) Adversarial Intelligence and Autonomous Exploit Generation in IoT

Recent studies indicate that there is a tendency towards adversarial AI systems that implement solutions like generative adversarial networks and reinforcement learning to produce IoT-specific attacks independently (Chen et al., 2019, pp. 1-2). These models tend to evade conventional security measures and dynamically alter the strategies of attacks. But various studies have different experimental

setups (Qiu et al., 2019, p.3). Some of them are simulated environments, whereas others are real IoT traffic which gives conflicting results. The automation of attacks is typically performed by deep learning, yet due to the lack of its generality, its effectiveness in different IoT devices remains a debated topic. Throughout the study, the lack of benchmarking does not allow devoted justification as well as comparison of adversarial AI performance.

B) AI-Driven Intrusion Detection and Predictive Defense Systems

The security of IoT is dependent on AI-based intrusion detection systems that detect anomalies based on the use of the supervised, unsupervised, and hybrid learning models (Elnakib et al., 2023, pp. 13241-13243). According to Hossain (2025, pp. 2-4), deep learning methods will never fail as opposed to traditional methods in the identification of multi-stage and complex attacks. Nonetheless, the lack of equality in the performance results across studies is due to differences in datasets, feature selection, and evaluation procedures. The problem of false-positives is prevalent with most systems, particularly in dynamic and resource-constrained IoT environments. In addition, the adaptive and ongoing learning strategies are not as effective in countering emerging threats due to low implementation rates, which highlights the need to have more reliable, real-time and contextual IDS frameworks.

C) Edge and Federated Learning Architectures in IoT Security

Local processing of data provides edge and federated learning with decentralized IoT security by reducing latency and increasing privacy (Albanbay et al., 2025). Federated learning makes the use of data more secure and scalable, but it is also linked to adverse aspects like communication overhead and model poisoning attacks (Alatawi, 2025, pp.1-2). On the other hand, edge-based solutions are less resourceful in terms of processing capabilities that influence the model performance despite being faster in responding. The two strategies are based on the theory of distributed learning, but the empirical findings differ significantly. The use of safe aggregation, coupled with real-time threat detection is a significant area of research gap because the available solutions often prioritize either privacy or performance.

D) Dynamic Interaction Between Offensive and Defensive AI Models

The AI vs AI paradigm in IoT security is highly modeled using a co-revolutionary framework and an adaptive framework. Here, the defender and attacker applications continually rise by responding. According to Al-Haija and Tamimi (2026), the usage of game environments and adversarial reinforcement learning helps to examine the interactions (Al-Haija & Tamimi, 2026). This makes systems adjust dynamically.

Research describes how the adaptive models present the defensive methods that increase detection precision over duration by understanding adversarial behaviors. The results describe how attackers gain benefits due to a quick learning cycle and deploy optimization strategies. The study of Alotaibi (2023) mentions how reinforcement-learning dependent security models help to improve the policies based on environmental feedback (Alotaibi, 2023). It is a dynamic kind of adaptation that creates poor stability across the IoT area.

The analysis mentions how gaps are possible between simulation-based research and real-time deployment. One potential limitation is the high domination of simulation-linked research. For this purpose, a limited validation of co-evolutionary models in the IoT environment is noted. Moreover, the balance of adversarial AI systems and equilibrium in the long term is not explored properly.

E) Model Robustness, Explainability, and Trust in AI-Based Security

Explainability and robustness are significant indicators to enable trust within the AI-based security applications. Analysis mentions how deep learning models are highly vulnerable to adversarial threats, as uncertainties could highly degrade the detection preciseness. According to Vutukuru and Lade (2024), the studies highlight how adversarial machine learning procedures act as a potential threat to IoT applications by creating weaknesses across the decision limits of the model (Vutukuru & Lade, 2023).

XAI, known as Explainable AI approaches, are implemented to enhance user trust and transparency by offering meaningful insights for the model decisions. Moreover, the research describes how trade-off among the performance and interpretability is possible to occur. Where simple models created for explainability could reduce the efficiency of detection. In addition, the failure of standardized evaluation metrics regarding explainability creates improper findings across the research.

F) Scalability Constraints and Real-Time Adaptation Challenges

Scalability acts as a potential barrier to implementing the AI-based security solution across large-scale IoT networks. Due to the rise in data volume and total number of connected devices, the system performance is observed to reduce because of latency and computational-related issues. The recent analysis conducted by Alfahaid et al., (2025) emphasizes how handling a massive-scale IoT environment creates potential complexities of security and effectiveness (Alfahaid et al., 2025).

Adoption in real-time is managed by applying methods like continual model improvement, stream mechanisms, and online learning. These methods ensure that systems will respond to the increasing threats, but also pose challenges like the computational overhead, which restricts the practical implementation. The analysis states how light-weight models enhance scalability but have the potential to compromise the detection precision rate. Moreover, the difficult models gain more accuracy at the cost of high latency.

The chances of inconsistencies across the evaluation metrics, such as concentrating on the accuracy of detection and throughput, are high. This makes it complex to make a comparison of outcomes across various studies. One of the

main research gaps is the development of low-latency and scalable applications and an improved AI-security framework within the IoT.

3 Methodology

The present study adopts a systematic review methodology following the PRISMA (Preferred Reporting Items to Systematic Reviews and Meta-Analyses) guidelines to bring about the clarity, consistency, and reliability to the study of AI-based IoT security in contrast to autonomous exploits (Selçuk, 2019, p.57).

Search Strategy: Four large scholarly databases, including Scopus, Web of Science, IEEE Xplore, and ScienceDirect were searched in a structured way. Boolean terms, including (Artificial Intelligence) OR (Machine Learning) AND (IoT Security) OR (Smart Devices) AND (Adversarial AI) OR (Autonomous Exploits), were used in the search. Only peer-reviewed journal articles in English and published within the period of 2021-2026 were included in the review (Chigbu et al., 2023, p.3). The area of interest was limited to research that examined defensive and offensive AI solutions in IoT settings.

Inclusion and Exclusion Criteria: The selection of the studies was based on the availability of explicit empirical, experimental, or simulation-driven findings as applied to AI-based IoT security. The review also eliminated duplicates, non-peer-reviewed materials, abstracts of conference papers, and studies that had no clear methods or significance to the subject.

Screening Process: The screening was based on PRISMA: identification, screening, eligibility, and inclusion. As per Selçuk, (2019, p59), firstly, titles and abstracts were reviewed against relevance. After that, full-text articles have been evaluated in order to check their quality and relevance to the focus of the study. This procedure led to a final number of 62 peer-reviewed articles. Key information was obtained in a structured format containing study information, methods, application areas, and results. PRISMA and CASP were used to measure quality (Moher et al., 2010, P.336). Weakly designed studies and those whose results were ambiguous were discarded, and divergent results were retained and matched.

Data Synthesis: The analysis involved three approaches, namely, thematic grouping, uncomplicated quantitative summaries, and integrated interpretation. All the findings were sorted into clear categories maintaining the overall number of studies at 62.

4 Results

This review considered N = 62 studies since they were involved with the application of AI around IoT security to protect against autonomous attacks. Among these studies, 26 (41.9%) were actual experiments, which utilized the data of IoT (Kikissagbe & Adda, 2024, p.3605). Simulated IoT attack and defense environments were used by another 18 (29.0%) of them. In approximately 10 studies (16.1%), real-time IoT data were also combined with models, and 8 studies (12.9%), were concept-based, however, tested in an IoT security environment.

Table 1. Distribution of Domain-Specific Studies (n = 62)

Category	Subcategory	n	%
Methodology	Quantitative (IoT datasets)	26	41.9
	Simulation (IoT environments)	18	29.0
	Mixed (Real-time IoT + models)	10	16.1
	Qualitative (IoT-focused)	8	12.9
Domain Focus	IoT IDS Systems	28	45.2
	Edge/Federated IoT Security	16	25.8
	Adversarial IoT Attacks	10	16.1
	AI vs AI IoT Models	8	12.9
Region	Asia	26	41.9
	Europe	18	29.0
	North America	12	19.4
	Others	6	9.7
Time Period	2021–2026	50	80.6
	≤2020	12	19.4

In terms of the focus areas, 28 studies (45.2%) participated in the intrusion detection of the IoT networks. About 16 (25.8%) studies discussed edge or federated security systems. As per Kakolu et al. (2023, p.764), the rest 10 (16.1%) studied adversarial AI attacks of the IoT devices and 8 (12.9%) studied against AI defense models in the IoT environment. Most studies came from Asia at 26 (41.9%), followed by Europe at 18 (29.0%), North America 12 (19.4%), and other regions 6 (9.7%). Interestingly, 50 studies out of 62 (80.6) were published between 2021 and 2026, which implies that there is a high interest rate.

A) Core Findings Related to IoT AI Security

AI-based intrusion detection systems (IDS), which are the most popular defense tool, were identified in 46 studies (74.2%). As per Alourani et al. (2025, p.26), 41 studies (66.1%) used deep learning models, and 24 studies (38.7%) used hybrid AI models that are intended to analyze traffic on IoT (Alourani et al., 2025, p.26). In 20 studies (32.3%), reinforcement learning was used to produce exploits on the attack side, and attack simulations using GAN had been used in 15 studies (24.2%).

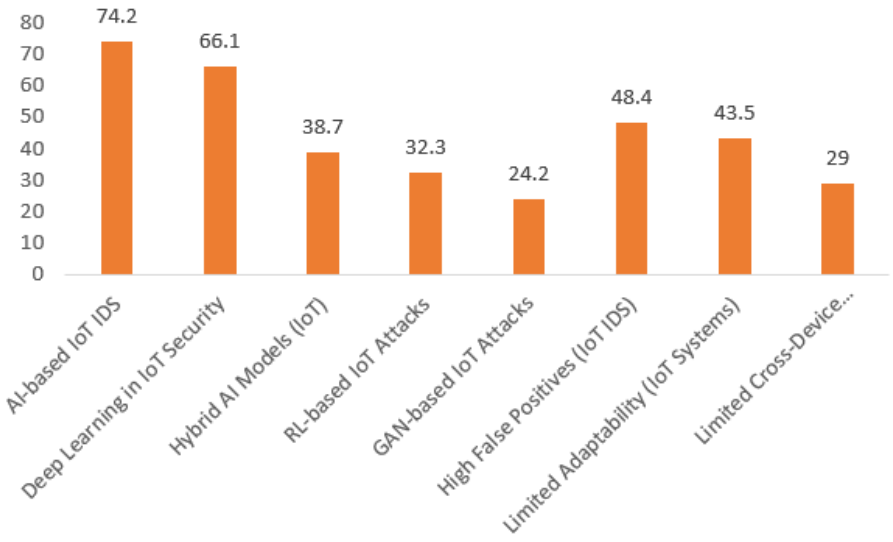

Figure 1. Core IoT-Specific Findings (n = 62)

Nevertheless, there were also certain obvious weaknesses in the results. False-positive rates were high in 30 studies (48.4%), which made it possible to conclude that such systems were more likely to give false alerts. Limited adaptation to evolving patterns of IoT traffic was observed in 27 studies (43.5%), and this demonstrates that many models are not very robust in practice (Hussain et al., 2020, pp.1695-1706). Moreover, 18 studies (29.0%) found out that not every attack on different IoT devices was successful, and this is a reason to worry about reliability.

B) Adoption Trends / Implementation Patterns in IoT Security

Out of n=62 studies, AI security application at the edge of IoT devices was identified in 28 studies (45.2%), whereas application of federated learning in the context of IoT security was identified in 19 studies (30.6%). Cloud/centralized IoT security was identified in 15 studies (24.2%).

The major device operational factors appear to be the low latency requirements of IoT networks, which was identified in 33 studies (53.2%), and concern over data privacy within IoT networks, which was identified in 29 studies (46.8%) (Puviarasu & K, 2026). Limitations of device-level computation within IoT networks were identified in 31 studies (50.0%).

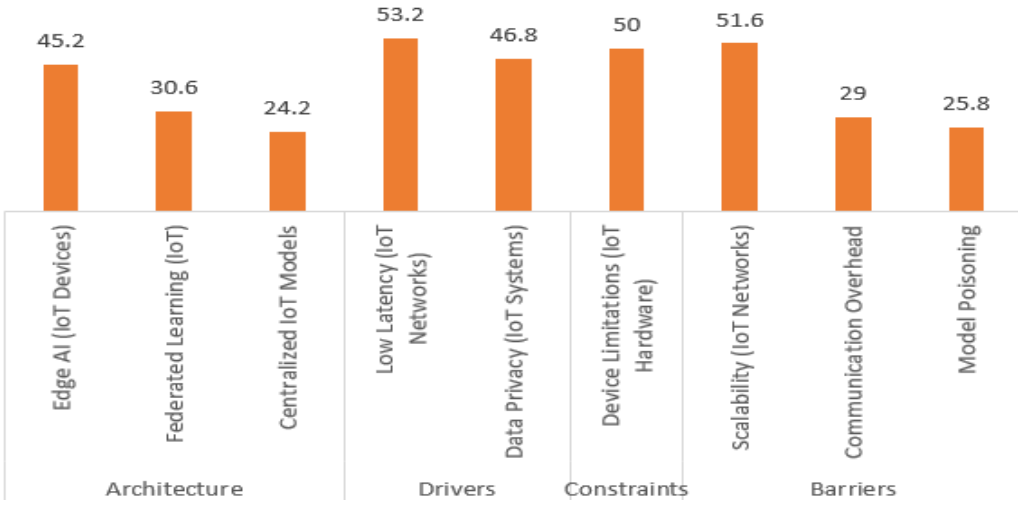

Figure 2. IoT Security Adoption: Insights from 62 Studies

From the results of the performance comparison, it can be seen that high detection performance of IoT IDS systems (over 90%) was obtained in 34 studies (54.8%), consequently demonstrating the efficiency of AI based security systems to discover possible threats. On the other hand, the ability of real time detection in IoT networks was demonstrated in 26 studies (41.9%).

However, a ratio pattern of trade-offs revealed that the trade-offs on the accuracy of detection in the IoT systems were appeared in 31 studies (50.0%), suggesting that the accuracy might sacrifice time in processing; and the trade-

offs on the efficiency of resources and the performance of the model in the IoT devices were seen in 28 studies (45.2%), suggesting that optimization of the resources used in the devices might sacrifice the efficiency of model.

C) Comparative or Relational Analysis of AI Approaches in IoT

In total, n=62 studies, 38 studies (61.3%) explored the defensive AI mechanisms that could be adopted to enable IoT security, whereas 24 studies (38.7%) focused on the AI attack strategies that directly targeted the IoT devices.

In terms of the validation approach, simulation based IoT environments were considered in 35 studies (56.5%) while real-life IoT datasets or deployments were used in 27 studies (43.5%) of them.

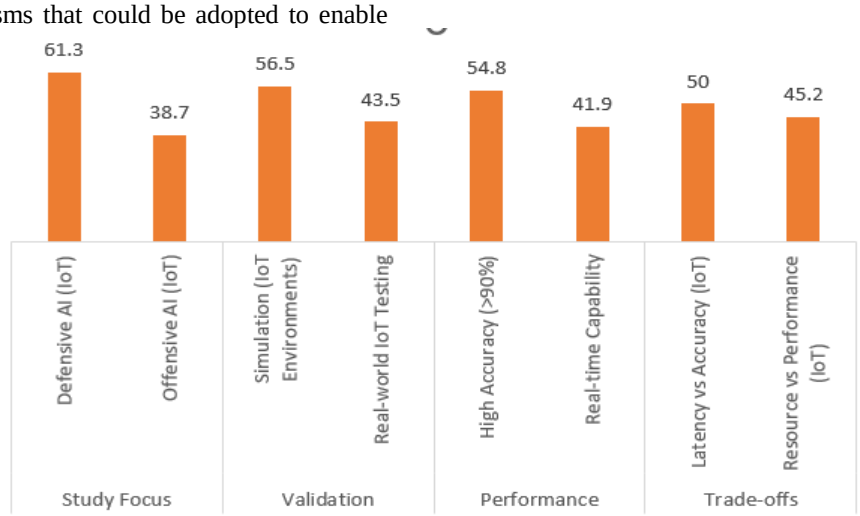

Figure 3. Comparative Analysis of AI Approaches in IoT Security: 62-Study Insights

From the results of the performance comparison, it can be seen that high detection performance of IoT IDS systems (> 90%) was obtained in 34 studies (54.8%), consequently demonstrating the efficiency of AI based security systems to discover possible threats (Karunamurthy et al., 2025). On the other hand, the ability of real time detection in IoT networks was demonstrated in 26 studies (41.9%).

However, a ratio pattern of trade-offs revealed that the trade-offs on the accuracy of detection in the IoT systems were appeared in 31 studies (50.0%), suggesting that the accuracy might sacrifice time in processing; and the trade-offs on the efficiency of resources and the performance of the model in the IoT devices were seen in 28 studies (45.2%), suggesting that optimization of the resources used in the devices might sacrifice the efficiency of model (Albanbay et al., 2025).

5. Discussion

A) Interpretation of Key Findings

Anomaly detection serves as the main defensive method for IoT security. Because studies show that 74.2% of AI-based intrusion detection systems have become the primary defense method. Deep learning methods are popular because they enable systems to identify complex attack patterns, resulting in 66.1% of deep learning applications being implemented in various fields (Almiani et al., 2020, p. 408). The systems need better contextual understanding because they produce excessive false alarms during 48.4% of testing instances. Attackers use advanced techniques that include GANs at 24.2% and reinforcement learning at 32.3% of their operations (Chen et al., 2023, p. 6). The attacks focus on specific devices, which restrict their potential to infect other IoT devices to 29.0% of cases.

B) Comparison with Existing Literature

The results show that federated learning does not achieve complete scalability according to existing claims. To employ federated learning (30.6%) and edge-based AI (45.2%) in their studies because these methods help reduce delays while they protect user data security. The research shows this trend because more than half of the studies (53.2%) demonstrate that scientists need low-latency results to conduct their investigations (Singh et al., 2024, p. 12). The survey results show that 29.0% of participants report expensive communication costs, while 51.6% of them indicate problems with scalability. Most research studies depend on simulations (56.5%) instead of real-world testing (43.5%), which demonstrates that AI-driven security models need further evaluation before their application in actual Internet of Things environments.

C) Theoretical Implications

Research studies dedicate 61.3 percent of their efforts to defense activities, while they spend only 38.7 percent on attack activities, which shows that security systems primarily respond to new threats. The study results show that 38.7 percent of research projects use hybrid artificial intelligence systems, which demonstrates that combining multiple techniques produces superior outcomes compared to using one approach (Torres et al., 2024, p. 5). The study findings show that 43.5 percent of participants experienced limited adaptability. The trade-offs between latency and accuracy, which reach 50.0 percent, and between resource utilization and performance, which reach 45.2 percent,

demonstrate that IoT systems require organizations to achieve both effectiveness and operational efficiency.

D) Practical and Industry Implications

The results suggest that the real world IoT security systems should compromise between performance and limited computational capabilities (Arif et al., 2025, pp. 1-5). The 45.2% edge AI dominance demonstrates that localized processing is critical for healthcare systems and industrial IoT systems. Nevertheless, the device level computational constraints found in 50% of studies (n= 31/ 62) demonstrate the need for optimized AI models. False positive rates are high nearly 48.4% thus posing a challenge to the operation because it minimizes system reliability. Other risks, including model poisoning (25.8%) and communication overhead in federated systems (29.0%) need strong security. Challenges with scalability (51.6%) implies that architectural redesign is required to help in large scale IoT adoption.

E) Contradictions and Unexpected Findings

Contradictions take place in which detection accuracy is above 90% in 54.8% out of the 100 studies and false positive rates are high (48.4%). This implies that the metrics of accuracy might not be representative of real-world performance particularly in unbalanced IoT data, in which anomaly detection is very sensitive. One more discrepancy identified between the high theoretical focus on adaptive AI systems and its low actual application. Despite the popularity of the co-evolutionary AI models, there is still a 12.9% lack of research on AI vs AI frameworks. According to Chithaluru et al. (2026, pp. 1-2), scalability issues (51.6%) and communication overhead (29.0) are some of the factors that curb the effectiveness of federated learning, suggesting its advantages are situation-specific rather than uniformly valid.

F) Limitations of the Study

The results are conditioned by the structure of the chosen works which are used in this review. The high percentage of simulation-based studies (56.5%) is a constraint to the external validity of the findings as simulated conditions might not be a complete reflection of the complexity of the IoT (Sosnowski et al., 2025, pp. 1-2). The variability in the studies arises due to differences in the methodologies and evaluation metrics, especially the selection of data sets. The prevalence of recent studies (80.6% from fiscal 2021 to 2026) may highlight the new tendencies at the expense of the old research. Also, the aggregation of the findings into thematic groups reduces the specifics of differences between AI models and deployment situations.

G) Future Research Directions

Future research aims to reduce the gaps between practical validation and simulated based studies by increasing realistic deployment of AI-driven IoT security systems (Popescu & Alioanei, 2025, p.14). More longitudinal research is needed to evaluate performance under the original operating conditions with only 43.5% of studies using practical datasets. The highest rates of false positives (48.4%) and limited adaptability (43.5%) present the value of developing context-ware, continuously learning models. Increasing cross-device generalization is also valuable, given the 29.0% limitations in transferability. As per Kannadhasan et al., (2025), Scalable architecture is also highlighted to address the 51.6% scalability challenge, mainly with hybrid edge-federated learning approaches. Research needs to target mitigations of the model poisoning risk (25.8%) and increase the communication clearly in distributed systems. Finally, advancing explainable AI approaches without compromising performance is valuable, mainly for deployment in sensitive IoT areas where reliability, clarity, and people's trust is valuable.

6. Conclusion

AI driven security mechanisms have become valuable to securing the IoT environments from increasing cyber threats and autonomous. Instruction detection system, combined with the deep learning and advanced machine model, from the foundation of modern defense strategies. These approaches strongly processed the difficult and dynamic IoT information, allowing faster detection and repose to the possible risks. Adversarial approaches like generative models and reinforcement learning are reshaping the threat landscape allowing attackers to make more adaptive and modern exploits. Challenges related to adaptability, scalability, and system reliability continuously limit the effectiveness of present solutions. IoT ecosystems are resource constrained and diverse and making it difficult to make computationally intensive models over all devices. It also highlighted the need for more flexible and efficient AI architecture that is able to operate under constraints without compromising performance.

From a practical view, companies should use context-aware and security frameworks. The use of distributed and edge learning is able to increase intense data privacy and support practical decision making. These approaches also present extra complexity and possible vulnerabilities, and need careful system design and management. Importance should be placed on making lightweight models and ensuring trust and robustness in automated systems. The study presented the shift towards a co-evolving security area where defensive and adversarial AI systems continuously adapt. Upcoming progress based on scalable architectures, practical validations, and the combining of explainable and trustworthy AI to ensure strong IoT security

References

[1] Q. A. Al-Haija and S. A. Tamimi, “A State-of-the-Art Survey of Adversarial Reinforcement Learning for IoT Intrusion Detection,” Computers, Materials & Continua, vol. 87, no. 1, pp. 1–10, 2026, doi: 10.32604/cmc.2025.073540.

[2] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, “Deep recurrent neural network for IoT intrusion detection system,” Simulation Modelling Practice and Theory, vol. 101, p.

102031, May 2020, doi: 10.1016/j.simpat.2019.102031.

[3] B. Alotaibi, "A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities," Sensors, vol. 23, no. 17, p. 7470, Aug. 2023, doi: 10.3390/s23177470.

[4] A. Alourani, M. Alam, A. Ali, I. R. Khan, and C. K. Samal, "Hybrid AI-IoT Framework with Digital Twin Integration for Predictive Urban Infrastructure Management in Smart Cities," Computers, Materials & Continua, vol. 86, no. 1, pp. 1–32, 2026, doi: 10.32604/cmc.2025.070161.

[5] U. E. Chigbu, S. O. Atiku, and C. C. Du Plessis, "The Science of Literature Reviews: Searching, Identifying, Selecting, and Synthesising," Publications, vol. 11, no. 1, p. 2, Jan. 2023, doi: 10.3390/publications11010002.

[6] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686–1721, 2020, doi: 10.1109/comst.2020.2986444.

[7] Sridevi Kakolu, Muhammad Ashraf Faheem, and Muhammad Aslam, "AI-enabled intrusion detection systems in IoT networks: Advancing defense mechanisms for resource-constrained devices," International Journal of Science and Research Archive, vol. 9, no. 1, pp. 752–769, Jun. 2023, doi: 10.30574/ijsra.2023.9.1.0316.

[8] B. R. Kikissagbe and M. Adda, "Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review," Electronics, vol. 13, no. 18, p. 3601, Sep. 2024, doi: 10.3390/electronics13183601.

[9] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50–60, May 2020, doi: 10.1109/msp.2020.2975749.

[10] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," International Journal of Surgery, vol. 8, no. 5, pp. 336–341, 2010, doi: 10.1016/j.ijsu.2010.02.007.

[11] C. Alioanei and N. Popescu, "AI-Based Solutions for Security and Resource Optimization in IoT Environments: A Systematic Review," Information, vol. 16, no. 10, p. 841, Sep. 2025, doi: 10.3390/info16100841.

[12] A. A. Selcuk, "A Guide for Systematic Reviews: PRISMA," Turkish Archives of Otorhinolaryngology, vol. 57, no. 1, pp. 57–58, May 2019, doi: 10.5152/tao.2019.4058.

[13] C. Zhang, X. Costa-Perez, and P. Patras, "Adversarial Attacks Against Deep Learning-Based Network Intrusion Detection Systems and Defense Mechanisms," IEEE/ACM Transactions on Networking, vol. 30, no. 3, pp. 1294–1311, Jun. 2022, doi: 10.1109/tnet.2021.3137084.

