TPM Vol. 32, No. S6, 2025
ISSN: 1972-6325
https://www.tpmap.org/

ENHANCED IOT SYSTEM SECURITY THROUGH ARTIFICIAL INTELLIGENCE

MINA ASADUZZAMAN[1], FERDOUS HOSSAIN[2,3], TAN KIM GEOK[2*], MD. ABU SAYED MAHFUZ HASAN [4]

[1]FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY, MULTIMEDIA UNIVERSITY, MELAKA, MALAYSIA.
[2]FACULTY OF ENGINEERING AND TECHNOLOGY, MULTIMEDIA UNIVERSITY, MELAKA, MALAYSIA.
[3]MES ENGINEERING, METALSA-ROANOKE, INC., VIRGINIA, UNITED STATES OF AMERICA.
[4]FACULTY OF COMPUTER SCIENCE AND ENGINEERING, DAFFODIL INTERNATIONAL UNIVERSITY DHAKA, BANGLADESH.

EMAIL: [1]asadbagerhat@gmail.com, ORCID ID: [1]0009-0006-5242-6996
EMAIL: [2]ferdous.mbstu.cse@gmail.com, ORCID ID: [2]0000-0003-0444-7320
EMAIL: [3]kgtan@mmu.edu.my, ORCID ID: [3]0000-0001-6881-4535
EMAIL: [4]mhaasaan@gmail.com, ORCID ID: [4] 0009-0000-6138-0033

Corresponding Author*: Tan Kim Geok.

ABSTRACT
The Internet of Things (IoT) transformed industries by enabling seamless device connectivity, but it also brought serious security risks like data breaches and illegal access. Traditional security measures can't keep up with the growth and evolution of IoT networks, which emphasises the need for more sophisticated solutions. By providing adaptive, real-time threat detection, anomaly identification, and automated defences against cyberattacks, integrating artificial intelligence (AI) into Internet of Things (IoT) systems has become a viable way to increase security. First, techniques like machine learning and deep learning use vast volumes of data to identify anomalous patterns and behaviours that enable prompt identification of suspicious threats. Hence, AI-based systems can be useful for improving Intrusion Detection Systems (IDS), optimizing security protocols, better protection against unauthorized access, and help minimize the risk of cyber-attacks. What is more, AI helps with predictive analytics, which enables IoT networks to predict and solve risks before they become real. With AI integration, IoT systems can even implement self-healing mechanisms to automatically recover from attacks. However, challenges such as computational power and data privacy, AI uses significantly improve IoT security offering a more flexible, undetected, and much more durable defence against impending threats. Organisations can secure and preserve the dependability and safety of their network of devices in the face of an increasingly complex cyber threat landscape by integrating AI with IoT.

KEYWORDS: Internet of Things (IoT), Artificial Intelligence (AI), Intrusion Detection Systems (IDS), Machine Learning, IoT Security, Cybersecurity, Cyber Attacks.

INTRODUCTION

The Internet of Things (IoT) is a technology that significantly expands device information, introducing smart cities, smart factories, smart homes, smart health, and many more. While this unprecedented connectivity brings great convenience and efficiency, it also makes IoT systems vulnerable to significant security threats. IoT devices are inherently different: they vary in their types, limited computing power, and the absence of homogenous security architecture. Cybercriminals take advantage of vulnerabilities through Distributed Denial of Service (DDoS), malware and botnet infiltration that can cripple critical functions and steal sensitive information. There are a lot of challenges achieving good security for IoT systems. Most IoT environments are decentralized, resource-constrained, and highly dynamic, in contrast to existing security mechanisms that are largely developed for centralised IT systems and do not reflect the relevant threats. Static rule-based approaches do not adapt quickly enough to emerging threats, putting IoT networks at risk of zero-day attacks and other advanced exploits. The enormous amount of IoT devices increases the attack surface and makes the job even more difficult and prone to breaches. To address these challenges, Artificial Intelligence (AI) has come up as a powerful technology that adds value to IoT security. Machine learning and deep learning, amongst other AI-driven methods, offer the potential for adaptive, proactive, and scalable security mechanisms [1]. These solutions have the ability to process enormous volumes of data in real time, identify odd patterns, and make highly accurate predictions about possible threats. Integrating AI can help IoT systems move from reactive security measures to pro-active, intelligent

defence systems that can better defend against modern cyber threats and provide a protected IoT landscape. In order to design a secure system, this paper describes how IoT and AI can be combined, with an emphasis on AI. Figure 1. Shows IoT Security Attack Scenarios in Different Application. This article specifically addresses the following research:

1. To analyse IoT security challenges and the inadequacies of traditional solutions.
2. To evaluate AI techniques in addressing IoT security vulnerabilities.
3. To propose architectural frameworks leveraging AI for enhanced IoT security.

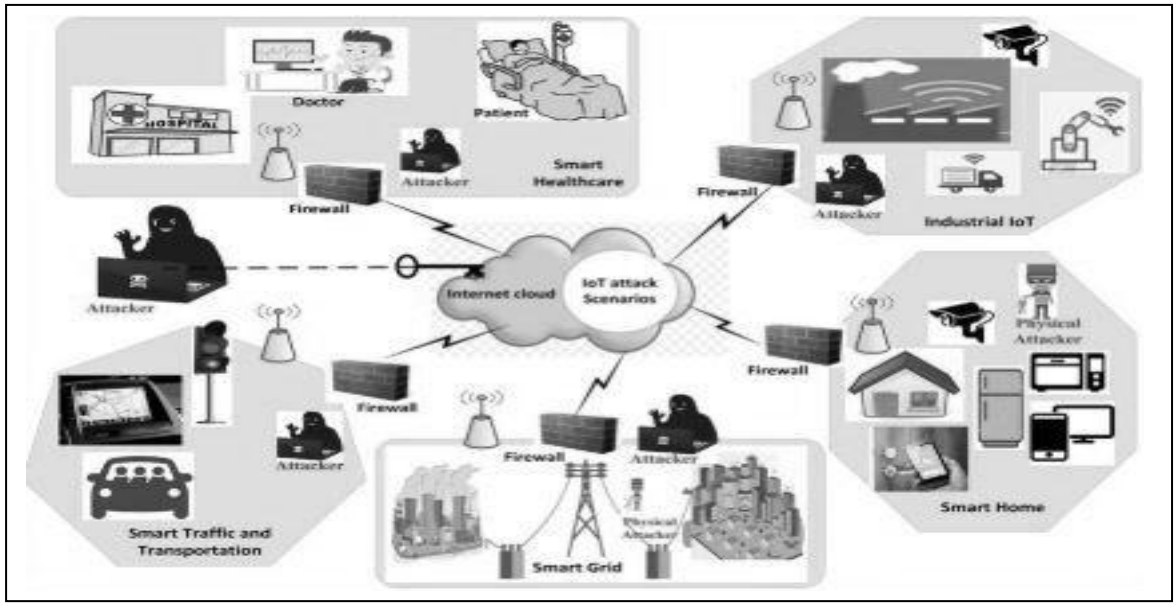

Figure 1. IoT Security Attack Scenarios in Different Application

LITERATURE REVIEW

The Internet of Things is made up of physical devices that are connected and have the ability to gather, exchange, and process data. These devices can be as simple as a smart thermostat or a wearable health monitoring device or as complex as industrial sensors and autonomous vehicles. Read about the challenges of IoT systems and their vulnerabilities. The minimal resources available on IoT devices, their dependence on wireless communication, along with the absence of standard security protocols make them susceptible to these vulnerabilities.

Deploying resource-intensive security measures is difficult because Internet of Things devices frequently have limited processing power, memory, and storage. For instance, executing advanced cryptographic algorithms or conducting even real time traffic analysis may not be practical for limited capability devices. This limitation leads to deploying minimalistic security measures, making devices easier to attack. [2]. IoT systems communicate wirelessly, which is vulnerable to interception, eavesdropping, and jamming. Unauthorised actors may use flaws in cellular networks, Wi-Fi, Bluetooth, Zigbee, and other wireless protocols to intercept private data sent by Internet of Things devices. This has serious implications on data privacy and confidentiality [3]. IoT systems' wireless communication allows for various Denial-of-Service (DoS) attacks, which can stop services from functioning and become crucial in certain applications like industrial IoT or healthcare. Another concern is the absence of global security guidelines for IoT devices. These issues are often compounded by differences between manufacturers' proprietary communication protocols and respective security mechanisms, making the various devices and systems incompatible. As a result, this lack of standardization leads to inconsistencies in the security practices across IoT networks and threatens devices to be exploited [4]. Additionally, IoT devices can be configured in a myriad of environments, from domestic use to industrial usage therefore making universal security solutions impractical. Typical IoT security risks include: Distributed Denial-of-Service (DDoS) attacks are directed at Internet of Things devices, turning them into remotely controllable bots that send malicious traffic to a target system. This can put the target system under great strain, leading to disruptions or even total service outages. Recent attacks on the Mirai botnet have shown us the damning impact of these attacks [5]. IoT devices frequently have weak authentication methods, like hardcoded or default passwords. These flaws can be used by attackers to access IoT networks without authorisation, which could result in data theft, device takeover, or additional network exploitation [6]. IoT devices frequently gather sensitive information like personal health data or location data, it can be intercepted during transmission if it is not securely encrypted. Data confidentiality can be compromised by such attacks as man-in-the-middle (MITM) or packet sniffing [7].

Through automated, scalable, and adaptable defence mechanisms, artificial intelligence (AI) and machine learning (ML) have shown a considerable ability to address IoT security issues. Traditional security systems, such as signature-based intrusion detection systems (IDS), cannot keep up with the rapidly evolving threat landscape. AI, on the other hand, is capable of processing enormous amounts of data in real time and identifying minute patterns that could indicate an attack, even if it is new or has never been seen before [8]. With AI-enabled anomaly detection systems, it is possible to monitor the behaviour of Internet of Things and networks if a certain behaviour is flagged as threatening or excessive deviations from its normal state behaviour. Using labelled datasets of both normal and attacked behaviour to train models like Support Vector Machines (SVM) and Decision Trees is an example of supervised learning techniques used in anomaly detection. [9]. In contrast, methods for unsupervised machine learning, including clustering and autoencoders are used when labelled data is limited or not existing, empowering the system to learn using unstructured data [10]. AI models can be trained to predict possible future threats by studying inflow of historical data and spotting potential threats before they occur. By analysing trends and developing patterns, these models can assist in the prediction of cyberattacks like zero-day bugs and botnet attacks [11]. Reinforcement learning (RL): RL is particularly vital in predictive security because it permits systems to learn based on prior learning, adapting and implementing response strategies based on what worked or didn't. AI can automate the response to detected threats in an IoT ecosystem as well. AI systems, utilizing reinforcement learning (RL), dynamically modify security measures based on threat severity and implications. In the event of a DDoS attack, for instance, an RL-assisted system could throttle or block connections originating from suspicious hosts without the need for human input, thus limiting the attack [12]. AI-based IoT Security The use of AI in securing Internet of Things is a broad and widening field with various studies and relevant technologies relative to each IoT challenge. Anomaly detection, intrusion detection, and predictive security are among the enhanced capabilities of machine learning (ML), deep learning (DL), and reinforcement learning (RL) technologies that have been highlighted in recent studies.

Machine Learning algorithms have been popular for identifying anomalies in IoT systems as they can classify and predict patterns in large and complex data. Support vector machines (SVMs) and random forests are two examples of algorithms that have been used to identify well-known attack patterns and detect anomalies in IoT traffic with remarkably high accuracy [13]. Moreover, clustering using k-means has been used to cluster IoT traffic and identify anomalies from the normal behaviours, including abnormal data flows and unusual behaviours of devices [14]. Example:[15] proposed a hybrid ML model using SVM and Random Forest for identifying attacks in IoT networks. By using the typical traffic patterns to train their model, they successfully identified when traffic deviated from the normal pattern, enabling them to detect potential threats before they caused serious damage. Ensemble (multiple classifiers) approach: This group of researchers [16] highlighted the advantages of applying ensemble learning methods to increase the accuracy and efficiency of anomaly detection systems. Core domains of ML that have recently been adapted to IoT security are deep learning which, as a subfield of ML, addresses more intricate and nuanced attack patterns. Pattern recognition tasks are especially well-suited for Convolutional Neural Networks (CNNs) and have achieved outstanding success in this domain and can be utilized to identify complex attack signatures and behaviours that are potentially missed by conventional methods [17]. CNNs are particularly useful in videos surveillance systems for identifying malicious activity due to the importance of visual data. Since anomaly data have a temporal nature such as the time-series data received from sensors, IoT network anomaly detection has made use of Long Short-term Memory Networks (LSTM) [18]. LSTMs are able to learn the temporal dynamics of IoT data and detect long-range dependencies in an observed behaviour manifesting to a potential threat, like a slow infiltration of an attack, or a gradual alteration of the system configuration signalling an attack occurred, [19] investigated the use of deep reinforcement learning (DRL) in Internet of Things security. By consistently gaining knowledge from the surroundings, the DRL algorithm could adapt security measures dynamically to the current state of the network, providing a more responsive and effective attack mitigation process. Reinforcement Learning (RL) has become a promising method in terms of its ability to withstand IoT risks and adjust to the changing threat landscape. Through interactions with its surroundings and feedback in the form of rewards or penalties, an agent learns to make decisions in reinforcement learning. This is especially helpful for the detection of and response of threats on evolving IoT infrastructures, where pattern of attack is not stable. [20] approached the problem of securing IoT devices and networks by training agents to autonomously detect and mitigate the network intrusions. By leveraging past experiences of interactions, the RL-based system helped to optimize security protocols, allowing adaptation to new types of cyberattacks with minimal human involvement. In a similar vein, the authors in [21] applied RL to create adaptive defence strategies against DDoS attacks and demonstrated that RL-based models are capable of effectively mitigating attacks without compromising overall network performance.

METHODOLOGY

As the number of connected devices increases, protecting the Internet of Things (IoT) has become a crucial issue. IoT systems are often targeted due to their decentralized nature, limited computational resources, and lack of standardized security measures. To counter these challenges, Artificial Intelligence (AI) provides an adaptive and scalable solution to address security concerns through intelligent detection, prediction, and mitigation techniques.

This section outlines the detailed methodology, emphasizing the integration of AI into IoT security systems. Figure 2(a) shows the block diagram of AI security framework for IoT systems and Figure 2(b) have been described detail proposed methodology as flowchart.

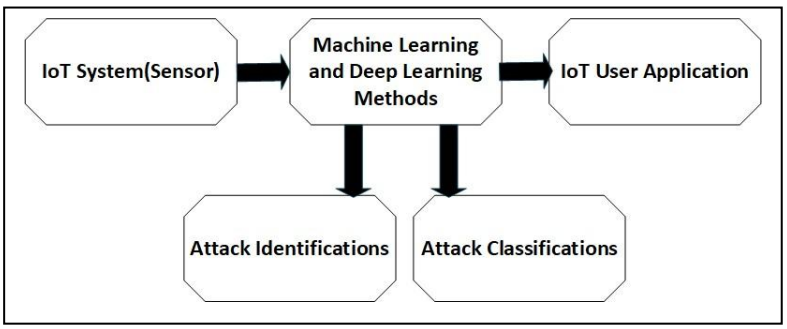

Figure 2 (a) Block diagram of AI security framework for IoT Systems

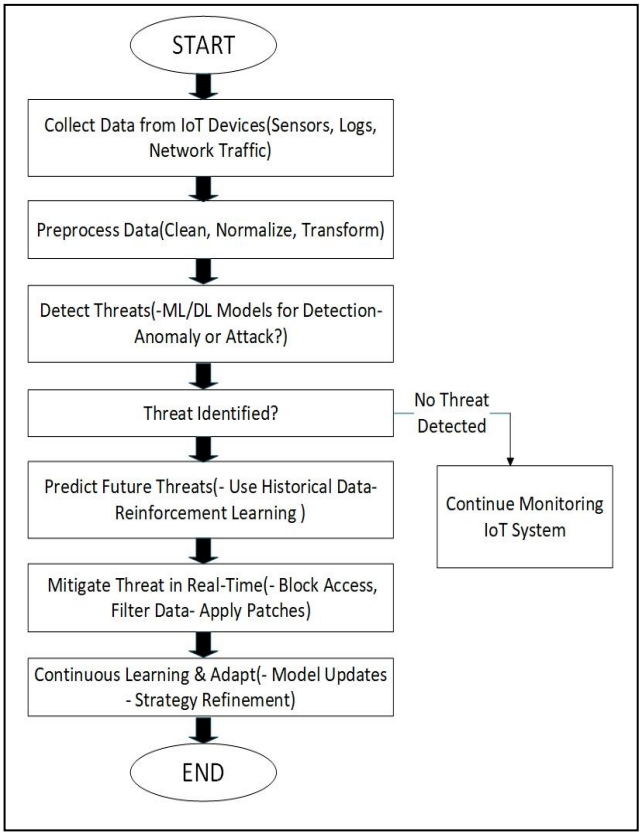

Figure 2 (b) Flow chart of Methodology of IoT System Security Through Artificial Intelligence

a) Data Collection and Preprocessing

Collect raw data from IoT systems, including device interactions, network logs, and user activity, to create a comprehensive dataset for analysis.

Data Sources- IoT sensors and actuators generate operational data. Network traffic logs capture communications between devices. Cloud platforms provide additional context about device configurations and historical behaviour. **Preprocessing-**Data preprocessing ensures the collected data is clean, consistent, and usable by AI models. **Data Cleaning-** Remove duplicate, irrelevant, or noisy data entries. **Normalization-**Scale data to standard ranges for uniform analysis. **Transformation-**Convert raw data into machine-readable formats such as time-series data or feature vectors. **Significance-** A well-pre-processed dataset lays the foundation for effective AI model training, enabling better detection and analysis of IoT system threats.

b) Threat Detection

Use AI-powered algorithms to detect anomalies or patterns associated with known malicious behaviour within IoT systems. This method uses labelled datasets and supervised learning models to find known attack patterns. Random Forests and Support Vector Machines (SVM) use classification based on different features like packet

size, frequency, and source IP address, so they excel at classifying benign and malice activities. Deep Neural Networks (DNNs), given their hierarchical structure, are well suited to identify complex features and patterns/signatures within big data, making them well placed to tackle intrusion detection and malware classification. Novel threats are identified using unsupervised learning techniques that avoid the need for labelled data since they do not require the monitoring of the system. Clustering techniques are used by anomaly detection algorithms like k-means and DBSCAN to group similar patterns together, making anomalies easier to spot. Autoencoders are a kind of neural network that learn the normal operation of a system and raise alarms when they encounter data that fall outside of expected behaviour, making them useful for detecting zero-day attacks. Deep Learning is a sophisticated kind of AI models that demonstrates superior performance in recognizing intricate and sensitive attack patterns, such as CNN and LSTMs. Convolutional Neural Networks (CNNs) are powerful tools when it comes to visual or tabular data. This makes LSTMs an ideal model for identifying time-dependent anomalies in IoT logs. It detects suspicious activity or patterns, creating alerts for further investigation or automated action.

c) Threat Prediction

Use historical data and emerging trends to predict possible future risks, so that proactive steps can be taken to strengthen IoT protection. Detect abnormal trends and predict potential vulnerabilities in real-time using historical logs. By investigating intricate relationships between traits, machine learning algorithms like gradient-boosted machines and neural networks can forecast an attack flow. Reinforcement learning models learn by interacting with the environment, allowing dynamic adaptation to evolving threats. They gain insights into the defense tactics, including updating firewalls rules or quarantining attacked endpoints, seamlessly and in real-time. These models are important for proactive threat management in dynamic IoT environments. Through predictive techniques, organizations can get ahead of attackers, where vulnerabilities are detected before they even get exploited.

d) Real-Time Response and Mitigation

By automatically responding to detected threats, potential damage can be minimized and systems can remain running. Adaptive firewall rules, dynamic rules are employed to prevent malicious access as per the threats identified. With real-time traffic filtering, harmful traffic, such as Distributed Denial of Service (DDoS) attacks, can be identified and blocked. Automated Software Patching Upon detection of vulnerabilities, automated updates and patches are pushed to affected IoT devices. Log all system activity all the time. When you detect threats, you can trigger a response. It is recommended to log response actions for both auditing and future enhancements. It automatically neutralizes threats ensuring operating IoT systems remain safe with no downtime.

e) Continuous Learning and Adaptation

Make sure the system adapts to new threats and evolving environments. Model Retraining: This process helps to feed current data to AI models in relation to the accessibility of model prediction and detection capabilities. Avoids falloff of the model over time. It allows the system to improve its decision-making strategies through feedback gathered from real-world experiences. RL agents are constantly fine-tuning the strategies they used on detecting and mitigating threats. Incorporate steps to measure the effect of response actions and feed insights back into model development. This field of active learning guarantees that the IoT safety system is adaptive, can evolve against dynamic threats, and reduce the possibilities of false positives or negatives.

Benefits of the Proposed Methodology

Proactive Security- AI-powered prediction and real-time responses ensure that threats are mitigated before causing significant harm. **Automation-** Automated detection, mitigation, and learning reduce reliance on manual interventions, improving response times and accuracy. **Adaptability-**Continuous learning mechanisms allow the system to evolve with emerging threats, maintaining high levels of security. **Scalability-** The methodology is scalable across diverse IoT environments, from smart homes to industrial IoT ecosystems.

RESULTS AND DISCUSSION

Significant improvements in the identification, forecasting, and mitigation of security threats have been made possible by the incorporation of Artificial Intelligence (AI) into IoT security. With the help of quantitative metrics, this section offers a thorough analysis of the outcomes of applying AI-driven strategies for IoT security. The discussion explores the practical implications, challenges, and potential improvements to the proposed methodology.

Metrics for Evaluation-The performance of AI models for IoT security was evaluated using the following metrics:

Accuracy- Percentage of threat classifications that are accurate (both true positives and true negatives) relative to all classifications. Precision: The percentage of actual positive detections among all of the model's positive detections. Recall (Sensitivity): The model's capacity to identify every real danger in the system. The percentage of benign activities that are mistakenly reported as threats is known as the False Positive Rate, or FPR. Response Time: The amount of time it takes the model to identify and address a threat.

Dataset: Training and testing were conducted using IoT network traffic datasets that included both benign and malicious activities (such as DDoS attacks, unauthorised access, and data breaches). Table 1 shows the sample dataset of network traffic.

Table 1. IoT Network Traffic Sample Dataset

Flow_ID	Source_IP	Destination_IP	Source_Port	Destination_Port	Protocol	Packet_Length	Flow_Duration	Packets/sec	Bytes/sec	Flag_Count	Device_Type	Time_Stamp	Label	Attack_Type
192.168.1.2-4434	192.168.1.2	172.217.164.78	4434	80	TCP	1500	5000	200	400000	2	Smart Bulb	2025-01-01 12:34	Benign	-
10.0.0.3-12345	10.0.0.3	192.168.1.10	12345	8080	UDP	600	1500	50	30000	1	Camera	2025-01-01 12:35	Malicious	DDoS
192.168.1.5-4000	192.168.1.5	192.168.1.2	4000	22	TCP	1000	8000	125	125000	3	Router	2025-01-01 12:36	Malicious	Unauthorized

AI Models Tested: Supervised Learning: Random Forest, Support Vector Machine (SVM). Autoencoders and K-Means Clustering are examples of unsupervised learning. Deep Learning: Long Short-Term Memory Networks (LSTMs), Convolutional Neural Networks (CNNs).
Environment: Simulations included diverse IoT devices such as smart home appliances, industrial IoT sensors, and edge computing nodes.
Implementation Tools: Frameworks for developing and testing models include Scikit-learn and TensorFlow.

Quantitative Results
The performance of different AI models was summarized using key evaluation metrics, as shown in the table below:

Table 2. Performance Comparison of Various AI Models

Metric	Random Forest	SVM	K-Means	Autoencoder	CNN	LSTM
Accuracy (%)	92.3	91.1	86.7	89.5	96.2	95.4
Precision (%)	91.2	89.9	84.5	88.3	94.1	93.6
Recall (%)	93.7	92.5	85.4	90.2	97.4	96.3
False Positive Rate (%)	2.3	2.8	4.6	4.1	1.5	1.8
Response Time (ms)	240	275	325	310	170	190

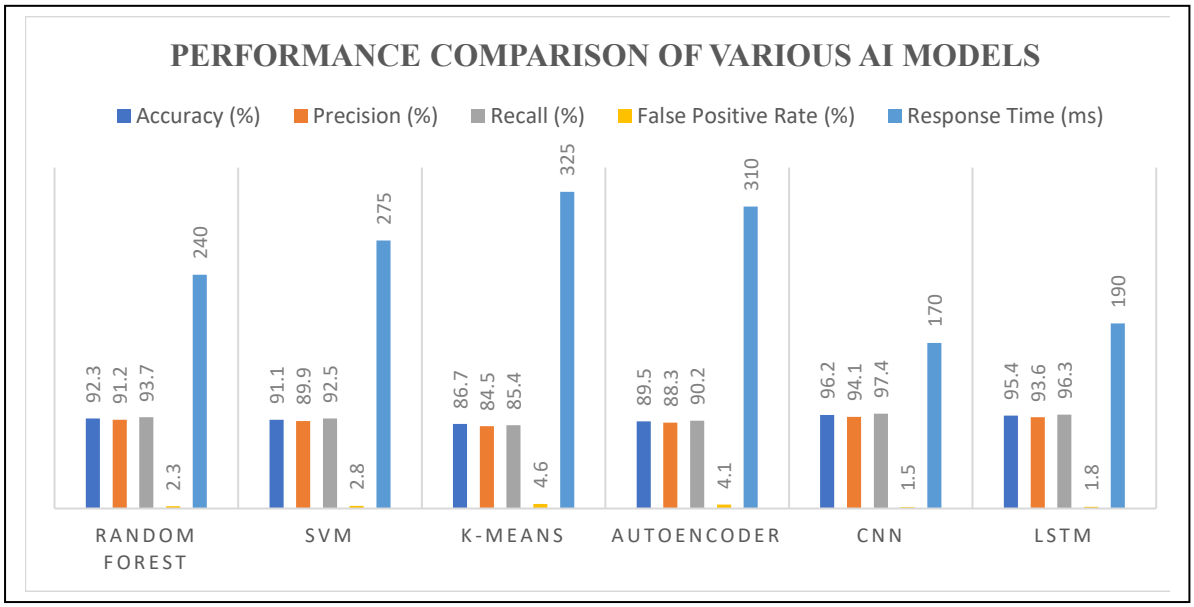

Figure 3. Performance Comparison of Various AI Models

DISCUSSION OF RESULTS

a) Performance Analysis of AI Models

Supervised Learning Models: Random Forest achieved a high accuracy of 92.3% and precision of 91.2%, indicating its effectiveness in classifying known threats. Its relatively low response time (240 ms) makes it suitable for environments requiring timely interventions. SVM **d**emonstrated slightly lower accuracy (91.1%) compared to Random Forest but excelled in high-dimensional data processing. SVM is effective for specific use cases but requires extensive computational resources for large datasets.

Unsupervised Learning Models: K-Means Clustering provided moderate accuracy (86.7%) and higher false positive rates (4.6%). It is more suitable for detecting novel anomalies but may require post-processing to minimize false alarms. Autoencoders performed better than K-Means, achieving 89.5% accuracy and relatively lower false positive rates (4.1%). They excel in anomaly detection tasks involving unlabelled data.

Deep Learning Models: CNN outperformed other models with the highest accuracy (96.2%) and precision (94.1%). CNNs are particularly effective for identifying complex attack patterns in IoT network traffic. LSTM achieved an accuracy of 95.4% and demonstrated its strength in analysing time-series data to detect sequential anomalies. The slightly higher response time (190 ms) compared to CNN is acceptable for real-time applications.

b) Implications for IoT Security

Real-Time Threat Mitigation-The low response times of CNN (170 ms) and LSTM (190 ms) models make them ideal for real-time applications. These models can detect and mitigate threats before significant damage occurs, ensuring uninterrupted IoT operations. **Adaptability to Emerging Threats-** Deep learning models, particularly LSTM, have demonstrated adaptability in identifying new and complex attack patterns by learning temporal dependencies in network traffic. **Scalability-** AI models can handle large datasets generated by IoT systems, making them scalable across diverse applications, from smart homes to industrial IoT. **Reduction in False Positives-**The low false positive rates of CNN (1.5%) and LSTM (1.8%) minimize unnecessary interventions, improving the efficiency of security operations.

c) Challenges and Limitations

Computational Overheads- For IoT devices with limited resources, deep learning models may not be practical due to their high computational requirements. Cloud-based solutions or edge computing frameworks can address this limitation by offloading computational tasks to more capable systems.

Data Dependency- The calibre and variety of training datasets determine how well AI models perform. Limited or biased datasets may lead to inaccurate predictions.

Scalability Concerns-While AI models are scalable, the deployment of these models in large-scale IoT systems may require optimized hardware and network infrastructure.

Evolving Threat Landscape-Attackers continually adapt to existing defences. The inclusion of reinforcement learning and continuous retraining of AI models can address this challenge.

CONCLUSION

Security challenges in IoT system are increasingly evolving in parallel with this growing IoT ecosystem, and the combination of Artificial Intelligence (AI) with IoT system security has reshaped our way of tackling them. In particular, IoT systems are vulnerable to cyber threats because of being wireless-driven, low processing power, and absent of security framework. This is where AI can help as it can offer proactive, precise, and scalable protection from such threats. Deep learning, supervised learning, and unsupervised learning are among the AI techniques that have shown great promise in threat detection and mitigation. Other models, such as Long Short-Term Memory Networks (LSTMs) and Convolutional Neural Networks (CNNs), are able to predict time series patterns and distinguish sophisticated attack literature with remarkable accuracy and flexibility. In addition, the ability of AI to deliver real-time threat mitigation goes a long way in bolstering system resilience and maintaining operational continuity. The deployment of AI in IoT security lungs with computational overheads, data privacy concerns, and the requirement for high-quality datasets that hamper the transformative capability of AI in IoT security. Edge computing, federated learning, and hybrid AI models are some potential approaches for addressing these challenges. From this, we can conclude that AI is a very important factor that will allow a robust and adaptive IoT security. With the ever-evolving landscape of technology, AI-powered solutions will be integral to securing IoT systems, ensuring their security, scalability, and reliability in a growingly interrelated universe.

FUTURE DIRECTIONS

A blend of deep learning, supervised, and unsupervised methods that capitalise on each method's advantages to enhance performance overall. Edge deployment of AI models supports holistic latency reduction and thereby enhances the real-time decision-making capabilities. AI models must adopt privacy-preserving mechanisms to maintain data confidentiality while training and deploying the AI models.

AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. The authors confirmed that the paper was free of plagiarism.

REFERNCES

[1].T. Mazhar et al., "Analysis of IoT security challenges and its solutions using artificial intelligence," Brain Sci, vol. 13, no. 4, p. 683, 2023.
[2].H. Bilakanti, S. Pasam, V. Palakollu, and S. Utukuru, "Anomaly detection in IoT environment using machine learning," Security and Privacy, vol. 7, no. 3, p. e366, 2024.
[3].K. Hussain, A. R. Rahmatyar, B. Riskhan, M. A. U. Sheikh, and S. R. Sindiramutty, "Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT)," in 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), 2024, pp. 1–8.
[4].N. Islam et al., "Towards Machine Learning Based Intrusion Detection in IoT Networks.," Computers, Materials & Continua, vol. 69, no. 2, 2021.
[5].Y. Al-Hadhrami and F. K. Hussain, "DDoS attacks in IoT networks: a comprehensive systematic literature review," World Wide Web, vol. 24, no. 3, pp. 971–1001, 2021.
[6].T. Mazhar et al., "Analysis of IoT security challenges and its solutions using artificial intelligence," Brain Sci, vol. 13, no. 4, p. 683, 2023.
[7].R. Singhai and R. Sushil, "An investigation of various security and privacy issues in Internet of Things," Mater Today Proc, vol. 80, pp. 3393–3397, 2023.
[8].A. A. Alahmadi et al., "DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions," Electronics (Basel), vol. 12, no. 14, p. 3103, 2023.
[9].A. Abusitta, G. H. S. de Carvalho, O. A. Wahab, T. Halabi, B. C. M. Fung, and S. Al Mamoori, "Deep learning-enabled anomaly detection for IoT systems," Internet of Things, vol. 21, p. 100656, 2023.
[10]. M. A. Belay, S. S. Blakseth, A. Rasheed, and P. Salvo Rossi, "Unsupervised anomaly detection for IoT-based multivariate time series: Existing solutions, performance analysis and future directions," Sensors, vol. 23, no. 5, p. 2844, 2023.
[11]. E. Cadet, O. S. Osundare, H. O. Ekpobimi, Z. Samira, and Y. Wondaferew, "AI-powered threat detection in surveillance systems: A real-time data processing framework," ResearchGate, October, 2024.
[12]. R. Aljohani, A. Bushnag, and A. Alessa, "AI-Based Intrusion Detection for a Secure Internet of Things (IoT)," Journal of Network and Systems Management, vol. 32, no. 3, p. 56, 2024.
[13]. V.-D. Ngo, T.-C. Vuong, T. Van Luong, and H. Tran, "Machine learning-based intrusion detection: feature selection versus feature extraction," Cluster Comput, vol. 27, no. 3, pp. 2365–2379, 2024.

[14]. O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions," Blockchain: Research and Applications, vol. 5, no. 2, p. 100178, 2024.
[15]. M. Usoh, P. Asuquo, S. Ozuomba, B. Stephen, and U. Inyang, "A hybrid machine learning model for detecting cybersecurity threats in IoT applications," International Journal of Information Technology, vol. 15, no. 6, pp. 3359–3370, 2023.
[16]. C. Hazman, S. Benkirane, A. Guezzaz, M. Azrour, and M. Abdedaime, "Building an intelligent anomaly detection model with ensemble learning for IoT-based smart cities," in Advanced Technology for Smart Environment and Energy, Springer, 2023, pp. 287–299.
[17]. A. Kumar and D. Singh, "Detection and prevention of DDoS attacks on edge computing of IoT devices through reinforcement learning," International Journal of Information Technology, vol. 16, no. 3, pp. 1365–1376, 2024.
[18]. A. Abusitta, G. H. S. de Carvalho, O. A. Wahab, T. Halabi, B. C. M. Fung, and S. Al Mamoori, "Deep learning-enabled anomaly detection for IoT systems," Internet of Things, vol. 21, p. 100656, 2023.
[19]. R. G. Goriparthi, "Reinforcement Learning in IoT: Enhancing Smart Device Autonomy through AI," computing, vol. 2, no. 01, 2024.
[20]. "IoT Security and Privacy-Challenges and Solutions3".
[21]. J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," Eng Appl Artif Intell, vol. 123, p. 106432, 2023.