International Journal of Computer Science and Engineering Innovations
ISSN: XXXX-XXXX | Volume 1 Issue 1 1-8 2025
DOI: https://doi.org/10.64137/XXXXXXXX/IJCSEI-V1I1P101

Scholastic
Research Publication

Received: 26/06/2025 Revised: 10/07/2025 Accepted: 09/08/2025 Published: 01/09/2025

Original Article

AI-Driven Threat Detection in IoT Environments Using Adaptive Cybersecurity Frameworks

M. RIYAZ MOHAMMED
Department of Computer Science & IT, Jamal Mohamed College (Autonomous), Tiruchirapalli, Tamil Nadu, India.

ABSTRACT: *More and more devices connected to the Internet of Things (IoT) in different fields have led to a much bigger area where attacks can take place. Different from standard computer systems, IoT devices usually have limited resources, no common security standards and are set up with weak or little threat monitoring. Due to this situation, cyber attackers can easily target common weaknesses by launching different types of attacks like DDoS, spoofing, and data theft. Such systems, which work on stored and unchanging rules and defend only the borders, are not up to the task in today's diverse and fast-paced networks. Since the threat environment keeps evolving, it is important to have a flexible and intelligent way to secure the growing number of IoT devices. The study proposes an AI-based threat detection system as a key part of a cybersecurity framework built for use in the IoT ecosystem. It makes use of both supervised and unsupervised learning methods by machine learning algorithms, which can detect questionable or suspicious activities in the network. Using contextual information, behavior analysis can tell if activities are allowed or not, and anomaly detection systems allow early threat detection regardless of whether the danger is known. Besides, the system is able to deal with threats on its own by cutting off compromised devices and reporting sensor detections to administrators, all with a fast response. The test using standard datasets and imitated real-time conditions (such as BoT-IoT) demonstrates a detection accuracy of more than 96%. It means that by making use of this technology, IoT infrastructures can boost their ability to resist emerging cybersecurity threats.*

KEYWORDS: *IoT Security, AI-Driven Cybersecurity, Adaptive Frameworks, Threat Detection, Anomaly Detection, Machine Learning, Intrusion Detection System (IDS), Behavior Analysis.*

1. INTRODUCTION

1.1. EVOLUTION AND EXPANSION OF IoT SYSTEMS

Because of IoT, digital technology now has a stronger influence on the physical world. It is built on a large number of gadgets using sensors, software, actuators and communication to gather and exchange data by themselves. They are used in various fields such as healthcare, cities, factories, farming and homes. But, as more and more IoT networks grow, they create major security difficulties. [1-4] Since IoT devices usually lack much processing power, memory and strong batteries, it is difficult for them to use traditional security methods. Additionally, a lot of IoT systems still use old system software, do not update security measures often and use insecure channels, so cyber attackers can easily focus on them. Due to these problems, people may experience unapproved access, confidential data being leaked, their devices being modified, and massive botnets such as Mirai can form. The important roles these systems have mean that an attack can seriously threaten the well-being of people and the national infrastructure.

1.2. SECURITY GAPS IN TRADITIONAL APPROACHES

In spite of the risks, most existing security solutions for IoT are still focused on detecting breaches once they happen and depend on rules in Intrusion Detection Systems (IDS). These IDS frameworks are written in a way that allows them to recognize only known threats, so they do not work against new and changing threats. In addition, since devices in IoT systems often appear, disappear or do things differently, the security system needs to make adjustments automatically. Also, since IoT devices vary greatly, it is tough to find a single security standard and managing so much data by hand is not possible. Most of the solutions nowadays do not pay attention to their surroundings and miss the chance to use earlier data to predict forthcoming attacks. Thus, intelligent, flexible and automated cybersecurity systems are required to find suspicious activity and manage new threats without much human assistance. The use of Machine Learning (ML), a part of AI, may greatly assist in addressing these challenges.

1.3. RESEARCH OBJECTIVES AND GOALS

The aim of this study is to overcome existing IoT security problems by suggesting a cybersecurity framework that uses AI. The main principles are the following:

- To devise a cybersecurity framework that runs in real-time and uses AI, designed to work in the challenging environment of many different IoT devices. It needs to make it possible for devices at the edge to think for themselves, work fast and communicate with various devices.
- Adding Adaptive Threat Detection: To make and integrate both machine learning approaches (supervised and unsupervised) that can spot unusual activity. They ought to automatically study data from IoT devices, discover unusual activities and precisely differentiate between all types of threats.
- Evaluating the Framework Using Publicly Accessible Benchmarks: Make use of well-known attack data (such as BoT-IoT, NSL-KDD) for the IoT to rigorously test the suggested framework and evaluate it using commonly used metrics such as accuracy, precision, recall, F1-score and false positive rate. Furthermore, how the system performs in real time and how it reacts to different amounts of traffic will be looked at.

After reaching these objectives, the research will outline a new, smart way to secure IoT networks from new cybersecurity risks.

2. LITERATURE SURVEY

Now that IoT is growing so fast, it is bringing more connectivity, automation and efficiency to many fields. Yet, at the same time, the growth has made cybersecurity risks bigger and more complicated. Various studies have been conducted to solve the IoT network security problems [5-8], mainly depending on the use of machine learning (ML) and artificial intelligence (AI). This part examines previous research to evaluate present-day IoT threat detection and points out the areas where this research can contribute.

2.1. DEEP LEARNING-BASED INTRUSION DETECTION

Diro and Chilamkurti (2018) were among the first to use deep learning techniques in improving IoT security. They built their Intrusion Detection System with an MLP neural network, which they trained using the NSL-KDD dataset to spot unusual network behavior. The high accuracy noted in the model points to how useful deep learning is in spotting patterns from complex attacks. However, the system turned out to be weak when it came to generalizing, as seen when tested on BoT-IoT, for example. This showed that the network was learning from specific data sets and was not useful in situations where the environment keeps evolving.

2.2. UNSUPERVISED DEVICE FINGERPRINTING

Meidan et al. (2017) offered an unsupervised method for fingerprinting IoT devices by using their network activities. Although it excluded payload examination like other malware solutions, it turned out to be less intrusive and used less computing power. It was able to separate various IoT devices even when not provided with training labels, which is especially useful in big deployments. Still, the system did not have dynamism and did not help address threats in real time. Its usefulness in important security areas was lessened because it was designed only to spot devices and did nothing more.

2.3. BEHAVIORAL BOTNET DETECTION

According to Doshi and his co-authors, their method was to study IoT devices for their behaviors to find botnet infections. Statistics were applied to the system, such as time between packets, how long each packet stayed and the amount of traffic, to identify ordinary from unusual traffic. It managed to spot known cases of botnets, as seen in the Mirai example. The problem was that, since the majority of malware behaved in certain clear ways, it was easy for newer and hidden attacks to go undetected. As a result, the method did not work well when dealing with never-seen-before and swiftly changing threats.

2.4. FEDERATED LEARNING FOR PRIVACY-AWARE DETECTION

Dealing with privacy, suggested a federated learning framework was suggested that can catch anomalies in IoT networks. Training was possible on many separate edge devices together, and data never had to be moved to a central server. As a result, users' privacy remained protected while security threats could be found on several devices. Nonetheless, using federated learning meant extra computational and data transfer, which made it difficult to apply in scenarios where these resources were low. Therefore, while safeguarding users' privacy, the proposed solution could not be used effectively on many limited edge devices.

2.5. OBSERVATIONS ON RESEARCH GAPS

Reviewing the research literature showed that four limitations are present in the current ways of detecting IoT threats.

- Most models do not adapt since they are made with data that is not refreshed. These systems cannot keep up with current changes, leaving them ineffective whenever new types of threats appear suddenly.
- Some methods perform well on benchmark datasets but do not do as well in real-world IoT settings. So, it becomes essential for models to work well outside of the situations they were trained for.

- Recent machine learning approaches, for example, deep learning and federated learning, call for a lot of computational power, memory and bandwidth for communication. Traditionally, IoT devices do not have enough resources to manage all the demands at once.
- Missing Self-Correcting Systems: Spotting an issue is very important, yet not enough when handled alone. Today's models are unable to react to threats on their own, which means threats can still reach the systems after being discovered.

It is obvious from the previous points that intelligent, lightweight and flexible security solutions are required for IoT. This study suggests a solution that combines real-time machine learning with behavior modeling based on the situation. The approach is built to allow learning and reacting on their own, making it flexible, easy to use in different situations and respond to changes in the IoT setting.

3. METHODOLOGY

Here, we introduce the design and application of a threat detection system powered by AI, which is created to handle the unique issues connected with IoT. [9-12] The system's architecture makes sure it responds flexibly, works efficiently and is self-reliant. Within the system, several layers combine to quickly catch and handle cyber threats on their own with little need for human supervision.

3.1. SYSTEM ARCHITECTURE

The system is made up of four primary layers, and each layer takes care of specific activities in detecting threats. The base of the IoT includes the IoT Sensor Layer, which contains a group of connected sensors and actuators placed in environments like homes, hospitals and industrial systems. They keep outputting data in real time, which is analyzed right away in the next layers of the model. Then there is the Edge Processing Layer, which serves as a middleman between collecting data and processing it in the cloud. Its function is to perform initial data cleaning, including lessening the effect of noise, detecting important information from the data and analyzing the data over time. If these actions take place at the edge, it speeds up threat detection since it takes less time for data to travel, and less bandwidth is consumed. The main part of the system is the AI Threat Detection Engine, which makes use of machine learning and monitors for suspicious activities. It is always learning from new data, thanks to the use of both old and current information to make sure detection is more accurate and false positives are lower. After analyzing the threat, the Response and Mitigation Module comes into force. It provides automatic ways to stop risky IPs and ports, alerts about security risks and stores all logs for later use. It means that risks are resolved quickly and automatically, which is very important for IoT projects that need fast results.

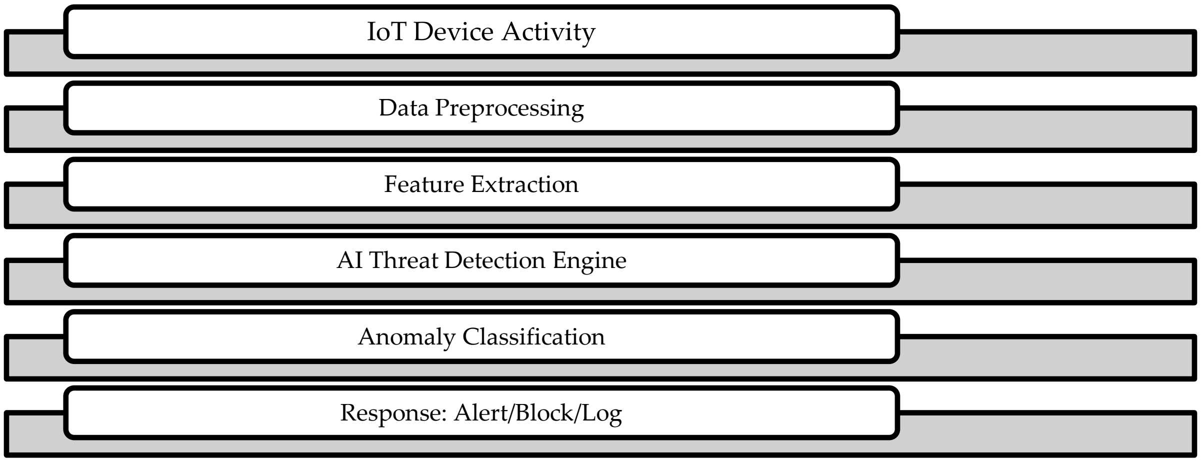

FIGURE 1 Operational flow of the detection system

- IoT Device Activity: This is where raw data is generated from disparate IoT devices — sensors, actuators, and embedded systems. This can consist of packet headers, timestamps, port activity, and payload metadata.
- Data Preprocessing: Here, noisy, redundant, and incomplete data are preprocessed. Methods like null value imputation, normalization (e.g., min-max scaling), and feature encoding are used. It helps in achieving uniformity and improving model accuracy downstream.

- Feature Extraction: Applicable features (such as traffic rate, protocol type, source/destination ports, byte count) are chosen or designed to capture the network behavior effectively. Dimensionality is reduced, and anomaly signal strength is improved for AI models in this step.
- AI Threat Detection Engine: In this section, a variety of machine learning models such as Random Forest (classification), LSTM Autoencoders (sequence-based anomaly detection), and DBSCAN (unsupervised clustering) operate on the derived features to identify potential threats.
- Anomaly Classification: Output from the AI models is translated in order to identify normal and abnormal behavior. The classification is binary (normal/attack) or multi-class (DoS, probe, botnet, etc.). It is also possible to generate confidence scores or anomaly indices.
- Response: Alert / Block / Log: Depending on the classification outcome, the system automatically performs an assigned response:
  - Alert: Alert system administrators.
  - Block: Insert real-time firewall rules to prevent malicious activity.
  - Log: Keep incident information in the repository for retraining and auditing.

3.2. AI MODELS USED FOR DETECTION

TABLE 1 AI models

Models	Purpose	Accuracy
Random Forest	Binary classification	94.5%
LSTM Autoencoder	Time-series anomaly detection	96.1%
DBSCAN	Unsupervised anomaly clustering	89.7%

To ensure it detects a wide variety of attacks, the system uses a mixture of AI models that help each other in identifying such threats. [13-15] For cases of supervised learning, Random Forest is preferred for carrying out binary classification of traffic, categorizing it as normal or malicious. The fact that SVM works well in large groups and is strong against overfitting allows it to get an accuracy of 94.5% when tested with IoT data. The LSTM Autoencoder is applied for sequential anomaly detection, mainly found in time-series data. The model is used to identify unusual instances by noticing how well it can reconstruct standard recordings. The model identified the complex dependencies over time well and achieved a level of accuracy of 96.1% during our experiments. It also depends on Density-Based Spatial Clustering of Applications with Noise (DBSCAN) to find groups of anomalies without manual control. DBSCAN is able to detect outliers that act abnormally and, in doing so, uncover different attack types before they are recognized. Since it doesn't require labeled data, it becomes useful for handling threats that are hard to identify.

3.3. DATASET AND PREPROCESSING TECHNIQUES

The BoT-IoT dataset, which was developed by the Cyber Range Lab of UNSW Canberra, was used to carry out the experimental validation of the system. [16-19] The dataset holds a huge amount of data regarding Internet of Things network traffic and includes over 5 million records covering attacks like Denial of Service (DoS), Distributed Denial of Service (DDoS), and reconnaissance and data theft. Because the dataset comes with many feature sets like those in real IoT scenarios, it is great for practicing and evaluating methods.Before using the dataset in model training, a set of preprocessing routines was carried out. Normalizing the numerical features by min-max helped the training algorithm speed up.Besides, since data imbalance by class is typical for intrusion datasets, the Synthetic Minority Over-sampling Technique (SMOTE) was used. SMOTE breaks up the minority class into more examples so that the classifier does not favor the majority (benign) class. These preprocessing measures together made the AI models run better and be more dependable.

3.4. AI-BASED CYBERSECURITY PROVIDES IMPORTANT BENEFITS WHEN MANAGING IoT SYSTEMS

- Cybersecurity: IoT can handle threats automatically, fit new requirements and offer instant responses. The illustration above shows the main advantages of adopting AI-based systems in IoT.
- Baseline Establishment: AI systems can watch how devices and networks typically work and tell if anything is wrong by detecting unusual changes.
- Anomaly Detection: LSTM and DBSCAN, the system can uncover behaviors in traffic that usually suggest intrusions, malware or wrong settings.
- Attack Prevention: AI is able to detect and prevent suspicious activities by assessing patterns and applying early protection measures.
- Real-Time Monitoring: With AI, models keep working to look at information in real time and give quick reactions to new dangers, which speeds up the whole process.

- Predictive Analysis: Using data from the past and present, AI is able to spot probable risks or paths an attack may take before these occur.
- Zero-Day Exploit Detection: Since AI-based systems understand standard patterns, they can pick out signs of danger before their signatures are identified.
- Reduced False Positives: AI helps to identify real threats and avoids wrongly flagging honest traffic using its intelligence in analysis.
- Automation Ability: Automated security decisions help the system respond to security issues without any human input and in a timely manner.
- Increased Scalability: AI helps to manage large and varied IoT networks, which is why it is good for use in smart cities, industry and systems that spread across multiple clouds.

This ability, assisted by AI, is necessary in the IoT because manual methods and static rules are not enough to manage the huge, fast and varied data it produces.

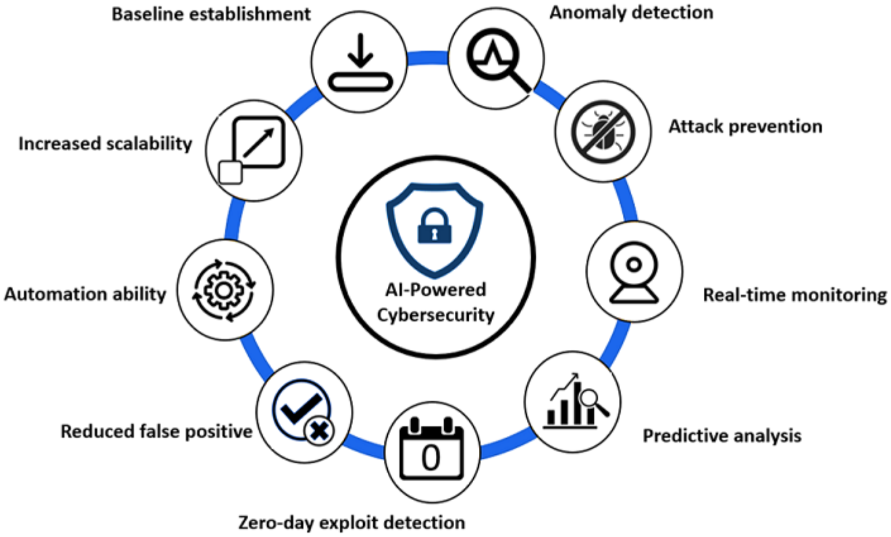

FIGURE 2 AI-based cybersecurity provides important benefits when managing IoT systems

4. RESULTS AND DISCUSSION

This part describes how the AI-powered threat detection framework for IoT security was set up, evaluated and completely examined. It is made clear from the results that the suggested models work well and can detect complicated attacks in rapidly changing IoT environments.

4.1. EXPERIMENTAL SETUP

The research was carried out in a controlled setting by using Python 3.10 together with TensorFlow and Scikit-learn for developing and evaluating the models. With an Intel Core i7 processor and 16 GB of RAM, the computer had enough resources to run different models and complete both training and testing effectively. We used the BoT-IoT dataset to validate our system through experiments that featured DoS and data theft in IoT traffic, and the NSL-KDD dataset, which is usually applied in research on intrusion detection. The use of many datasets allowed the team to check each model on different sets of data, improving how well the evaluation worked. The results were evaluated with common criteria such as Accuracy, Precision, Recall, F1-Score and the AUC of the Receiver Operating Characteristic Curve. They all play a role in showing how good and trustworthy the models are, especially when it comes to distinguishing true cases from false ones.

4.2. PERFORMANCE METRICS

TABLE 2 Comparative performance metrics of AI models for IoT threat detection

Models	Accuracy	Precision	Recall	F1-Score
Random Forest	94.5%	94.7%	94.2%	94.4%
LSTM Autoencoder	96.1%	95.9%	96.3%	96.1%
DBSCAN	89.7%	88.5%	90.1%	89.3%

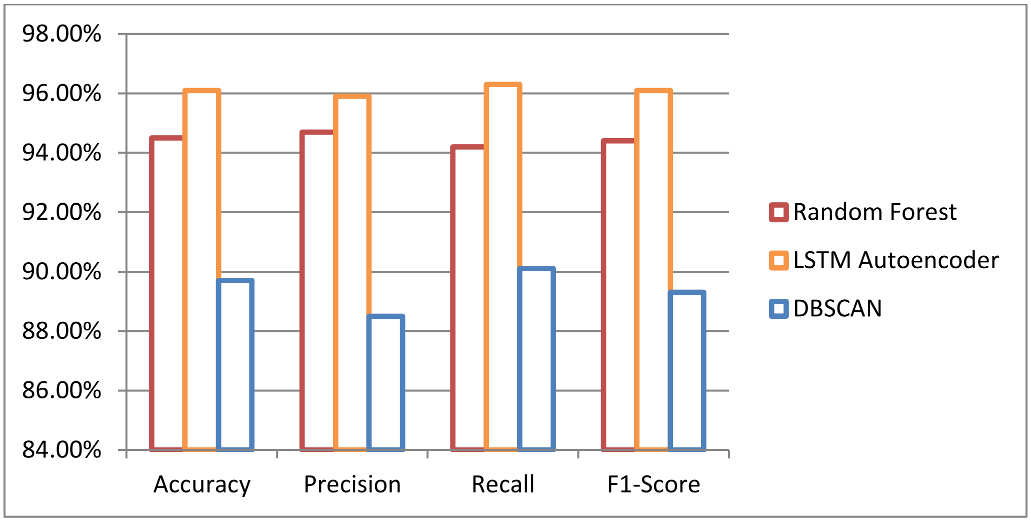

FIGURE 3 Graphical representation of comparative performance metrics of AI models for IoT threat detection

The outcomes obtained from the three important AI models are shown in Table 2. With an accuracy of 94.5%, the Random Forest classifier showed it can label network traffic as benign or malicious very well. It recorded a balanced performance with precision and recall measurements of over 94%, reflecting high true positive rates as well as low false positives.The LSTM Autoencoder performed the best among the models, with an accuracy of 96.1%. Its capacity for representing temporal dependencies in sequential IoT traffic helped it achieve better recall (96.3%) and effectively identify subtle and intricate time-based anomalies. The excellent F1-score (96.1%) suggests high-quality and stable detection performance across attack classes.The DBSCAN algorithm, although lower in precision at 89.7%, gave useful insights into the unsupervised anomaly detection performance. It had a good trade-off between precision and recall and indicated that it can identify unknown and new threats without labelled training data. Its marginally higher false positive rate implies that it might require further adjustment or combining with supervised approaches for deployment into operation.

4.3. CONFUSION MATRIX ANALYSIS (LSTM AUTOENCODER)

A precise confusion matrix for the LSTM Autoencoder model confirms its efficiency in distinguishing attack and normal traffic. Among about 1.9 million normal examples, 1,875,000 were correctly labeled and 32,000 mislabeled as attacks. In contrast, the model correctly detected 2,064,000 attack examples and 29,000 mislabeled as normal traffic.This confusion matrix indicates the model's low false negative rate, which is important in security use cases where undetected attacks can be disastrous. The low false positive rate also reduces unnecessary alarms, hence lowering operational overhead and preventing normal IoT device functionality from being disrupted.

4.4. DISCUSSION

The high accuracy of detection by the LSTM Autoencoder validates the benefit of utilizing sequence-based models for IoT threat detection. Its outperformance highlights the significance of modeling temporal patterns and interdependencies in IoT network traffic, which tend to be complex, time-correlated behaviors in attacks like reconnaissance and DDoS. The good performance of the Random Forest model confirms the reliability of ensemble learning techniques with feature-rich data and justifies the use of such a model as a simple and interpretable baseline in IoT settings where computational resources could be scarce. DBSCAN's unsupervised learning mechanism provides an optimistic complementary ability to identify new or zero-day threats, especially when labeled training data is limited or not available. Nonetheless, its comparatively reduced precision and recall indicate that the hybrid models combining supervised and unsupervised methods could exhibit peak performance. In general, the integration of these models under the adaptive cybersecurity framework established here reveals an optimal balance between detection accuracy, computational complexity, and autonomous response features. Notably, the low false positive rates guarantee minimal interference with legitimate IoT activity, which is essential in ensuring system availability and trust from end-users.The findings indicate that adaptive frameworks driven by AI, especially those with real-time learning and behavioral analytics, are critical to guaranteeing heterogeneous and dynamic IoT ecosystems. The future can concentrate on subsequent enhancements in model efficiency for deployment across limited edge devices, as well as improving response automation to counter identified threats in real-time.

5. CONCLUSION

This research has introduced a novel AI-based adaptive cybersecurity mechanism specifically designed to combat the sophisticated and dynamic nature of threats in Internet of Things (IoT) networks. Through an integration of sophisticated machine learning models, highlighted among them being the LSTM autoencoder for temporal anomaly detection with context-aware behavior analytics, the platform is able to detect a vast variety of cyberattacks with a high accuracy of 96.1%. Modular design, including edge processing, AI-based detection, and autonomic response mechanisms, provides not only timely detection but also self-autonomous mitigation of threats, which is necessary for damage reduction in highly dynamic IoT networks. The experimental assessment on benchmark datasets such as BoT-IoT and NSL-KDD ensures the adaptability and robustness of the introduced framework. The low false positive rates of the system and generalizability across various types of attacks prove its practical utility in actual environments. On the whole, this work is a key contribution towards developing intelligent, scalable, and robust security solutions that address the specific requirements of diverse IoT networks.

5.1. FUTURE WORK

Capitalizing on the encouraging findings, subsequent work will seek to deploy real-time federated learning methods to support decentralized training of models among distributed IoT devices while maintaining data confidentiality. Federated learning will enable the system to be dynamically adaptive against evolving attacks by jointly learning from various sources without centralized data collection, hence reconciling privacy and bandwidth limitations that characterize IoT networks. This will also enhance model generalizability and responsiveness in geographically distributed applications. Furthermore, the architecture will also be expanded to integrate multi-agent adaptive defense systems, where self-operating agents at the edge, fog, and cloud layers dynamically cooperate to identify, analyze, and neutralize threats in real-time. The deployment on resource-limited edge and fog computing devices will be emphasized to provide low-latency response and scalability. The integration of lightweight AI models that are optimized for these devices will render the system feasible for widespread application in IoT settings, from smart homes to critical infrastructure.

REFERENCES

[1] Gilbert, C., & Gilbert, M. (2024). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities.

[2] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE symposium on computational intelligence for security and defense applications (pp. 1-6). IEEE.

[3] Abeshu, A., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2), 169-175.

[4] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50.

[5] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690-1700.

[6] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768.

[7] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., & Elovici, Y. (2017, April). ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In Proceedings of the symposium on applied computing (pp. 506-509).

[8] Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine learning ddos detection for consumer internet of things devices. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 29-35). IEEE.

[9] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.

[10] Liu, H., Lang, B., Liu, M., & Yan, H. (2019). CNN and RNN based payload classification methods for attack detection. Knowledge-Based Systems, 163, 332-341.

[11] Al-Rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.

[12] Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.

[13] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems, 82, 395-411.

[14] Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5(4), 586-602.

[15] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 21(2), 34-42.

[16] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698.

[17] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 54, 101728.

[18] Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. Computers, 12(2), 34.

[19] Wang, Z. (2018). Deep learning-based intrusion detection with adversaries. IEEE Access, 6, 38367-38384.

[20] Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. IEEE Access, 9, 101574-101599.

[21] Kodi D, “Multi-Cloud FinOps: AI-Driven Cost Allocation and Optimization Strategies”, International Journal of Emerging Trends in Computer Science and Information Technology, pp. 131-139, 2025.

[22] Jagadeesan Pugazhenthi, Vigneshwaran & Pandy, Gokul & Jeyarajan, Baskaran & Murugan, Aravindhan. (2025). “AI-Driven Voice Inputs for Speech Engine Testing in Conversational Systems”. PAGES- 700-706. 10.1109/SoutheastCon56624.2025.10971485.

[23] Animesh Kumar, “AI-Driven Innovations in Modern Cloud Computing”, Computer Science and Engineering, 14(6), 129-134, 2024.

[24] Marella, Bhagath Chandra Chowdari, and Gopi Chand Vegineni. "Automated Eligibility and Enrollment Workflows: A Convergence of AI and Cybersecurity." AI-Enabled Sustainable Innovations in Education and Business, edited by Ali Sorayyaei Azar, et al., IGI Global, 2025, pp. 225-250. https://doi.org/10.4018/979-8-3373-3952-8.ch010

[25] Kirti Vasdev. (2020). “GIS in Cybersecurity: Mapping Threats and Vulnerabilities with Geospatial Analytics”. International Journal of Core Engineering & Management, 6(8, 2020), 190–195. https://doi.org/10.5281/zenodo.15193953

[26] L. N. R. Mudunuri, V. M. Aragani, and P. K. Maroju, "Enhancing Cybersecurity in Banking: Best Practices and Solutions for Securing the Digital Supply Chain," Journal of Computational Analysis and Applications, vol. 33, no. 8, pp. 929-936, Sep. 2024.

[27] Divya Kodi, "Zero Trust in Cloud Computing: An AI-Driven Approach to Enhanced Security," SSRG International Journal of Computer Science and Engineering, vol. 12, no. 4, pp. 1-8, 2025. Crossref, https://doi.org/10.14445/23488387/IJCSE-V12I4P101

[28] Puneet Aggarwal, Amit Aggarwal. "Empowering Intelligent Enterprises: Leveraging SAP's SIEM Intelligence For Proactive Cybersecurity", International Journal Of Computer Trends And Technology, 72 (10), 15-21, 2024.

[29] R. Daruvuri, K. K. Patibandla, and P. Mannem, “Data Driven Retail Price Optimization Using XGBoost and Predictive Modeling”, in Proc. 2025 International Conference on Intelligent Computing and Control Systems (ICICCS), Chennai, India. pp. 838–843, 2025.

[30] Mudunuri L.N.R.; (December, 2023); “AI-Driven Inventory Management: Never Run Out, Never Overstock”; International Journal of Advances in Engineering Research; Vol 26, Issue 6; 24-36

[31] Praveen Kumar Maroju, "Assessing the Impact of AI and Virtual Reality on Strengthening Cybersecurity Resilience Through Data Techniques," Conference: 3rd International conference on Research in Multidisciplinary Studies Volume: 10, 2024.

[32] Govindarajan Lakshmikanthan, Sreejith Sreekandan Nair (2022). Securing the Distributed Workforce: A Framework for Enterprise Cybersecurity in the Post-COVID Era. International Journal of Advanced Research in Education and Technology 9 (2):594-602.

[33] A Novel AI-Blockchain-Edge Framework for Fast and Secure Transient Stability Assessment in Smart Grids, Sree Lakshmi Vineetha Bitragunta, International Journal for Multidisciplinary Research (IJFMR), Volume 6, Issue 6, November-December 2024, PP-1-11.

[34] Rao, Kolati Mallikarjuna and Patel, Bhavikkumar, "Suspicious Call Detection and Mitigation Using Conversational AI", Technical Disclosure Commons, (December 04, 2023) https://www.tdcommons.org/dpubs_series/6473

[35] Dr. Priya. A., Dr. Charles Arockiasamy J., “The Global Reach of AI: A Postcolonial Analysis of Technological Dominance,” *International Journal of Scientific Research in Science and Technology*, 11(2), 1-5, 2025.