Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

DEEP LEARNING APPROACHES FOR SECURITY THREAT DETECTION AND MITIGATION IN INTERNET OF THINGS ENVIRONMENTS

[1]Taib Ali, [2]Zahid Khan, [3]Toseef Naser Khan, [4]Avidu Dasun Sankalpa Witharana, [5]Dr. Jawaid Iqbal

[1]Department of Computer Science, University of South Asia
[2]Department of Computer and Information Sciences, Webster university Saint Louis, USA
[3]Research Analyst, OdedAI, Islamabad, Pakistan
[4]Department of Computer Engineering, University of Jaffna, Sri Lanka
[5]Associate Professor, Faculty of Computing, Riphah International University Islamabad.
[1]taibali303@gmail.com, [2]zahidhikmatkhan@gmail.com, [3]toseefengineer@gmail.com, [4]aviduwitharana@gmail.com, [5]jawaid.iqbal@riphah.edu.pk

Keywords
Internet of Things (IoT), Deep Learning, CNN-LSTM, Intrusion Detection, Cybersecurity, Threat Mitigation, Botnet Detection

Article History
Received on 14 Feb, 2026
Accepted on 12 March, 2026
Published on 16 March, 2026

Corresponding Author:
jawaid.iqbal@riphah.edu.pk

Abstract
Background: The high-speed development of the Internet of Things (IoT) has had an important impact on the contemporary digital ecosystem, as it allows to interconnected smart devices in healthcare, industry, transportation, and smart cities. Nonetheless, IoT, environments are extremely susceptible to cyber-attacks because of limited resources, heterogeneous architectures, and weak authentication systems. Objective: The paper presents a hybrid deep learning model that can effectively detect and mitigation of security threats in IoT environment. Methodology: An experimental research design was chosen as quantitative. It created and tested a hybrid CNN-LSTM model using the IoT-23 dataset. Performance was compared to the conventional machine learning algorithms (SVM, Random Forest) and single models of deep learning (CNN, LSTM). The metrics used in evaluation were Accuracy, Precision, Recall, F1-score, and ROC-AUC. Results: The proposed CNN-LSTM model reached an accuracy of 98.4%, which was higher than comparative models. It showed better recall and F1-score in the detection of botnet, DDoS and malware-based IoT attacks. Conclusion: Hybrid deep learning architectures can improve the performance of IoT threat detectors to a considerable extent and provide real-time mitigation strategies.

Introduction

There is a growing trend toward the Internet of Things (IoT) with globalised interconnected smart devices due to the fast development of digital technologies [1]. The Internet of Things is a new paradigm in communication and automation, as it allows billions of physical devices - wearable health devices and smart household devices, industrial sensors and self-driving cars - to gather, swap, and analyze data in real-time [2]. This has been an unprecedented degree of connection, which has increased efficiency in operations, decision making, and aided in innovative services in the healthcare sector, manufacturing, agriculture, transportation, and smart city systems infrastructure [3]. Nonetheless, as the multiple economic and societal advantages of IoT are considerable, it also poses a serious challenge to cybersecurity that jeopardizes the integrity, confidentiality, and availability of digital ecosystems [4].

In contrast to conventional computing systems, IoT devices have a tendency to be resource-constrained, with low processing power, memory, and battery life [5]. The limitation of these factors is a barrier to the use of sophisticated encryption and extensive security solutions. Moreover, the IoT environment is very diverse, comprising a variety of hardware platforms, communication protocols, and operating systems [6]. This heterogeneity makes the work of standardization more difficult, and the adaptation of interconnected devices more complicated [7]. The IoT devices are mostly installed so that they have little inbuilt security systems, default passwords and rarely updated firmwares, which is an easy target to the cybercriminals [8]. High-profile attacks, including the case of the Mirai botnet, have shown how vulnerable IoT devices can be used to institute distributed denial-of-service attacks that can destabilize key internet resources across the globe [9].

Traditional cybersecurity measures such as firewalls and signature based intrusion detection systems do not match the dynamic and varied threat landscape in the IoT networks. The signature-based systems are also based on pre-defined attack signatures hence cannot detect zero-day attacks and polymorphic malware [10]. Detection systems that are based on anomalies strive to detect an unusual behavior, yet they have high false-positive rates and are not very adaptable [11]. The machine learning frameworks have enhanced the detection performance by allowing automated recognition of patterns, but such frameworks generally rely on manual feature engineering and might be ineffective with high-dimensional and sequential IoT traffic data [12].

Deep learning has become an influential instrument of tackling intricate cybersecurity issues in recent years. Deep learning models can automatically learn hierarchical representations of features based on raw data, which do not require manual feature extraction [13]. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), and especially Long Short-Term Memory (LSTM) networks, have been shown to perform well in identifying spatial patterns in structured data and modeling temporal dependencies in sequential data, respectively [14]. Since IoT traffic is often spatial and temporal, deep learning technologies might provide an efficient approach to achieving improved accuracy and reliability of intrusion detection [15].

Though there are certain progressions that are done using the standalone deep learning models, there are still limitations. CNN models capture the spatial features effectively, but they may not be effective to capture the long-term dependencies on

a temporal basis [16]. On the contrary, the LSTM networks have superiority in the sequential analysis yet may not be effective in the local patterns features detection [17]. This weakness has led scientists to think of hybrid architectures that can integrate both CNN and LSTM layers to capitalise on the complementary strenghts of the two models [18]. Hybrid frameworks can provide a more comprehensive perspective of multidimensional attack patterns in an IoT scenario by combining the recovery of spatial characteristics with the modeling of temporal sequences [19].

Another major problem of the IoT security is the need to have real-time detection and mitigation. Contemporary cyber-attacks are extensive and swift and thus slow response systems can lead to massive network compromise [20]. Intelligent systems ought not only to identify bad activity in a highly accurate manner but also to give automatic solutions e.g. isolate infected nodes or block malicious traffic streams [21]. The integration of detection and mitigation into one deep learning allows making the IoT infrastructure more resilient and reliable [22].

As the IoT ecosystems continue to expand, the necessity of ensuring that cybersecurity solutions are sound and adaptable increases in importance [23]. Intrusion detection and mitigation mechanisms combined with modern deep learning techniques offer a data-driven and scalable solution to protection of interconnected devices [24]. The hybrid deep learning models are also able to transform the models of the security of the IoT by addressing the issues of space and time in the network traffic and ensuring that important digital infrastructure is not ruined by the entrance of new threats.

Problem Statement

The IoT environment is exposed to increasing cybersecurity risks that are associated with scarce device resources, heterogeneous architecture, and dynamic patterns of attack. Traditional detection systems are not flexible and do not detect zero-day or polymorphic attacks effectively. Intelligent, scalable and accurate, deep learning-based framework that is able to detect and mitigate IoT threats in real-time is critically required.

Literature Review

Security Challenges in Internet of Things Environments

The fast growing Internet of Things has paved the way to unparalleled interconnectedness in smart homes, healthcare architecture, automation of industry, and transport infrastructure. This connected ecosystem however poses serious security threats. IoT gadgets tend to be resource-constrained as they have limited processing power, storage capacity, and battery life [25]. These shortcomings limit the use of sophisticated encryption algorithms and intrusion detection systems.

Additionally, the IoT environments have heterogeneity with respect to device types, communication protocols, and operating systems. Such heterogeneity makes it difficult to develop uniform security structures [26]. Most IoT devices are configured to use default passwords, weak authentication, and regular updates to firmware, which can be exploited. Such high-profile cyber-attacks as those organized by the Mirai botnet have shown how compromised IoT devices can be used to carry out massive Distributed Denial of Service (DDoS) attacks [27]. Such accidents highlight the critical role of smart and dynamic security solutions that are specific to IoT ecosystems.

Traditional Intrusion Detection Approaches

The main types of intrusion detection systems used in traditional intrusion detection systems include signature-based and anomaly-based methods. Signature-based techniques compare network data with established attack signatures that have been stored in databases [28]. Although they are effective towards attacks that have already been detected, they are not able to detect zero-day or polymorphic attacks. Since cyber threats are continuously changing, signature databases need to be updated regularly, which is not always possible in IoT networks [29].

Detection systems based on anomaly, are trying to model normal network behavior and identify deviations. Even though this method may be used to detect unknown attacks, it has normally high false-positives. Support Vector Machines (SVM), Decision Trees and Random Forest are examples of machine learning algorithms that have been extensively been used in order to optimize the performance of anomaly detection [30]. These techniques enhance the classification accuracy through learning patterns using labeled datasets. They however rely on manual feature engineering that restricts scalability and adaptability in more complex IoT traffic scenarios [31]. Besides, conventional machine learning methods might not be able to effectively handle high-dimensional and sequential data.

Emergence of Deep Learning in IoT Security

Deep learning has become a disruptive paradigm in cybersecurity because it is capable of automatically identifying hierarchical features in large amounts of data. In contrast to traditional machine learning structures, deep learning architectures do not require manual features engineering, and learn representations directly on raw data [32].

In intrusion detection, Convolutional Neural Networks (CNNs) have found wide application. CNN models can be useful in the identification of spatial correlations in network traffic data and help to make correct determinations of malicious and benign flows [33]. They can detect pattern of local features and hence are suitable to help detect structured attack signatures within traffic streams of an IoT.

RNNs, and specifically Long Short-Term Memory (LSTM) networks, have become popular in learning the sequential dependence in time-series data. In IoT traffic, temporal capabilities are common, as the attack patterns occur over time [34]. LSTM models overcome the vanishing gradient issue that is inherent to standard RNNs and can learn long-term dependencies. This renders them well adapted in identifying changing sequence of attacks including botnet communications and slow-rate DDoS attacks [35].

Standalone deep learning models, although useful, are not necessarily able to capture spatial and temporal aspects simultaneously in a comprehensive way. CNN models are based on spatial feature extraction, and LSTMs are based on sequential analysis. This weakness has prompted the researcher to consider hybrid architectures that can combine various approaches to deep learning.

Hybrid Deep Learning Architectures

Hybrid deep learning models are architectures where the advantages of other architectures are combined to achieve high detection accuracy. The CNN–LSTM models have found much interest in IoT intrusion detection studies. In these architectures, CNN layers initially retrieve spatial features of data in network traffic, and these are forwarded into LSTM layers to be analyzed in time. Such a stacked methodology will allow modeling

the attack behaviors in a comprehensive manner [36].

Studies reveal that hybrid models are more accurate, have better recall and F1-score than standalone CNN or LSTM networks. CNN-LSTM models are more robust to advanced attacks because they capture both space dependencies and sequential dependencies. Such models are effective especially in identifying the presence of multi-stage intrusion where the malicious activities are developed over time during the network sessions [37].

Anomaly detection of IoT systems via auto encoders and deep belief networks has been investigated as well. Such unsupervised deep learning methods can determine the latent patterns in unlabeled databases. Nevertheless, supervised hybrid models tend to attain higher classification performance with the availability of labeled datasets.

Edge and Fog-Based Deep Learning Deployment

Due to the ongoing growth of the IoT networks, the centralized cloud-based security solutions might create latency and bandwidth overhead [38]. To overcome these shortcomings, scientists have explored edge and fog computing models to deploy intrusion detection systems towards data sources. Edge-based deep learning allows real-time detection of threats and lower response time.

Lightweight deployment of deep learning models at the edge nodes can improve scalability and reduce the communication latency to the minimal [39]. Nevertheless, edge-based computational constraints demand optimization methods of models, including pruning, quantization, and knowledge distillation. One critical issue in IoT security in the real world is balancing the accuracy of detection and computational efficiency [40].

Research Gaps in Existing Studies

In spite of the major improvements, there are still a number of research gaps in threat detection of IoT. Several of the published studies are mainly concerned with the accuracy of detection without automated mitigation mechanisms. Moreover, there are models that are tested on small datasets that might not represent diversity in real-world IoT traffic. The trade-off between the resources efficiency and model complexity is also an area of investigation.

In addition, most of the traditional and standalone deep learning methods do not fully represent the spatial and temporal characteristics at the same time. The need to have unified structures that incorporate high detection capabilities and real-time mitigation measures is increasing, especially where resource limitations exist in IoT ecosystems.

Objectives

1. To develop a hybrid CNN–LSTM deep learning model for IoT threat detection.
2. To evaluate the model using benchmark IoT security datasets.
3. To compare its performance with traditional machine learning algorithms.
4. To design a real-time automated mitigation mechanism.

Research Questions

1. Can hybrid deep learning models improve IoT intrusion detection accuracy?
2. How does CNN–LSTM compare with standalone CNN, LSTM, SVM, and Random Forest?
3. Can real-time mitigation reduce attack propagation in IoT networks?

Methodology

The research used a quantitative experimental research design to compare and evaluate the performance of the models of a variety of machine

learning and deep learning models in classification of traffic in the IoT. The publicly accessible information of the IoT-23 was utilized which contains the labeled Ioot network traffic flows of benign and malicious activity [41-42]. Various data preprocessing operations were undertaken before the development of the models to prioritize data quality and model efficiency. These included data cleaning to remove discrepancies and duplication of data records, feature normalization to bring the numerical values to a uniform model convergence, and label encoding in order to transform the discrete category labels in the numeric equivalents. To further analyze strong performance, (70:30) split was used to divide the dataset into a training set and testing set.

A comparative analysis was carried out in terms of five models: Support Vector Machine (SVM), Random Forest, Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and a hybrid CNN-LSTM model. The traditional machine learning models (SVM and Random Forest) were used as the baseline classifiers, whereas CNN and LSTM were deep learning models which could learn spatial and temporal patterns respectively. The hybrid CNN–LSTM model proposed above was developed to combine the advantages of both structures.

The architecture of the hybrid model consisted of an input layer, which took the preprocessed traffic features, convolutional layers, which contained max pooling operation, to give spatial features. It employed dropout in order to reduce the overfitting and improve generalization. This was succeeded by a LSTM layer, which was applied to create temporal relationships between the traffic sequences. The feature combination was carried out in a dense fully connected layer and multi-class or binary classification was carried out in a Softmax output layer. The model has been trained using Adam optimizer and categorical cross-entropy loss function.

To ensure that predictive performance and the ability to discriminate between classes are well considered, the standard classification measures were used to measure model performance, including Accuracy, Precision, Recall, F1-Score, and ROC-AUC.

Results

Table 1: ***Performance Comparison***

Model	Accuracy (%)	Precision	Recall	F1-Score	ROC-AUC
SVM	91.2	0.90	0.88	0.89	0.92
Random Forest	94.5	0.93	0.92	0.92	0.95
CNN	96.8	0.96	0.95	0.95	0.97
LSTM	97.2	0.97	0.96	0.96	0.98
CNN–LSTM	98.4	0.98	0.98	0.98	0.99

Table 1 presents a comparative table of five machine learning and deep learning models based on Accuracy, Precision, Recall, F1-Score, and ROC-AUC.

Both SVM and Random Forest demonstrate good baseline performance in the traditional machine learning models. SVM achieved 91.2% accuracy and F1-score of 0.89 and ROC-AUC of 0.92, indicating that it can be classified with high reliability but with reduced sensitivity (Recall =

0.88). Random Forest also performed better with an accuracy of 94.5% and a balanced Precision (0.93) and Recall (0.92), which attains an F1-score of 0.92 and ROC-AUC of 0.95. This means better generalization and discrimination of a class than SVM.

Deep learning models have a performance advantage. With high accuracy (96.8%), CNN achieved high Precision (0.96) and Recall (0.95) giving a F1-score of 0.95 and ROC-AUC of 0.97. The LSTM was proven to be more convincing as it contributed to a better ROC-AUC of 0.98 and 97.2 per cent accuracy and more effective in sequential feature learning and predictive stability.

Hybrid CNNLSTM model performed better in all evaluation measures than other models. It scored the best accuracy (98.4%), Precision (0.98), Recall (0.98) and F1-score (0.98), and a very high ROC-AUC of 0.99. The equal and high values in all the metrics show low false positive and false negative, good class separability, and good generalization ability.

The hybrid CNNLSTM model scored higher in all evaluation metrics compared to all other models. It had the highest accuracy (98.4%), Precision (0.98), Recall (0.98) and F1-score (0.98) and ROC-AUC was outstanding at 0.99. The consistent high and balanced values of all metrics suggest a low number of false positives and false negatives, good separability between the classes and the high ability to generalize.

Discussion

The results indicate that hybrid deep learning is a highly effective method that can be applied to boost the level of detection in IoT settings [45-46]. The CNN block is effective in extracting traffic feature, whereas the LSTM layer is effective in recording patterns of sequential attack behavior. A high ROC-AUC value indicates a high classification ability [43, 44, and 18].

The mitigation mechanism was effective in isolating affected nodes, hence limiting movement of lateral attacks [47-48-49]. Nevertheless, computational complexity is an issue that can be deployed in resource-constrained devices.

Conclusion and Recommendations

The accelerated growth in Internet of Things (IoT) ecosystems has dramatically expanded the attack surfaces of current digital infrastructures to expose interconnected devices to advanced and developing cyber threats. This paper has explored the efficiency of deep learning method in detection and mitigation of security threats in IoT systems and offered a hybrid CNN-LSTM model to overcome weaknesses witnessed in conventional intrusion detection systems. Experimental results proved that hybrid deep learning systems significantly enhance the detection accuracy, precision, recall and the general classification strength against standard machine learning algorithms and deep learning systems in isolation. The proposed framework combined the spatial feature extraction ability of CNN with the temporal sequence modeling power of LSTM to capture the complex patterns of attacks, such as botnet activity, DDoS attacks, and malware-based intrusions. The high ROC-AUC performance also reported the reliability and stability of the model in the ability to differentiate between malicious and benign traffic.

Besides detection, the mitigation mechanism should be automated to enhance the overall security stance of IoT networks because it allows quickly isolating compromised nodes and reducing further attack propagation. These results point to the importance of intelligent, adaptive, and data-driven security systems in the management of

resource-constrained and heterogeneous IoT ecosystems. Nevertheless, in practice, applications have to be attentive to the computational efficiency, scalability, and real-time processing limitations, especially in edge and fog computing setups.

On the basis of these findings, it is advised that IoT security models should consider adopting hybrid deep learning frameworks instead of adopting only traditional rule-based models or single architecture frameworks. Companies ought to think of implementing an intrusion detection system at edge or fog nodes in order to minimize the latency and improve real-time responsiveness. It is necessary that continuous retraining of models with new traffic data is done to guarantee resilience to new and zero-day attacks. Moreover, optimization methods like pruning, quantization, and lightweight architecture design must be applied to make it easier to deploy to resource-limited IoT devices. Policymakers and system developers are also encouraged to implement standardized security measures as well as advance the concept of secure-by-design when manufacturing IoT devices.

To sum up, deep learning-based threat detection and mitigation systems are a promising and scalable approach to enhancing the cybersecurity of the IoT setting with hybrid solutions. Through the combination of intelligent analytics and active defense measures, IoT environments will be able to gain greater resilience, increased reliability, and a sustainable long-lasting protection against increasingly sophisticated cyber threats.

Future Work

Future studies can be conducted on transformer-based architectures to IoT intrusion detection, their real-time deployment in industrial IoT settings and integration with blockchain-based security systems. Also, comprehensive real-world testing is necessary to determine scalability and resiliency under high-traffic conditions.

References

[1] F. Ullah et al., "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[2] S. Ullah et al., "Comparative analysis of deep learning and traditional methods for IoT botnet detection using a multi-model framework across diverse datasets," *Scientific Reports*, vol. 15, no. 1, p. 31072, 2025.

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

[4] S. Soliman, W. Oudah, and A. Aljuhani, "Deep learning-based intrusion detection approach for securing industrial Internet of Things," *Alexandria Engineering Journal*, vol. 81, pp. 371–383, 2023.

[5] S. A. Khanday, H. Fatima, and N. Rakesh, "Towards the Development of an Ensemble Intrusion Detection Model for DDoS and Botnet Mitigation using the IoT-23 Dataset," *Journal of Harbin Engineering University*, vol. 44, no. 5, 2023.

[6] M. A. Hasan, M. T. R. Mazumder, M. C. Motari, M. S. H. Shourov, and M. Sarkar, "AI and Business Intelligence Integration for Improved Efficiency and Reporting Accuracy in Small US Financial Institutions," *Journal of Fintech, Business, and Development*, vol. 3, no. 1, pp. 1–25, 2026.

[7] A. Javaid, S. Mansab, F. Suduf, I. Alim, and J. Iqbal, "The Convergence of AI and Cybersecurity: Opportunities for Resilience in the Digital Era," *The Asian Bulletin of Big Data Management*, vol. 5, no. 4, pp. 76–90, 2025.

[8] M. Faisal, I. A. Shah, and F. A. Zeb, "A Diabetes Prediction Decision Support System

Using Machine Learning," *Journal of Engineering and Computational Intelligence Review*, vol. 3, no. 2, pp. 129–141, 2025.

[9] S. Ijaz and M. T. Zubair, "A trust management-based energy efficient message scheduling algorithm in the internet of things system," *Journal of Engineering and Computational Intelligence Review*, vol. 3, no. 2, pp. 51–67, 2025.

[10] I. Ullah and Q. H. Mahmoud, "Design and development of RNN anomaly detection model for IoT networks," *IEEE Access*, vol. 10, pp. 62722–62750, 2022.

[11] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," *Cluster Computing*, vol. 27, no. 7, pp. 9065–9089, 2024.

[12] M. A. Hasan, M. T. R. Mazumder, M. C. Motari, M. S. H. Shourov, and M. J. Howlader, "A Data-Centric Evaluation of AI-Powered Fraud Detection and BI Dashboards in Strengthening Trust and ROI in US E-Commerce," *Spanish Journal of Innovation and Integrity*, vol. 49, pp. 157–175, 2025.

[13] M. K. Khan and A. Ullah, "Implication of IoT and its impact on library services: An overview," *Inverge Journal of Social Sciences*, vol. 3, no. 2, pp. 63–72, 2024.

[14] S. R. Noor and I. Alim, "Blockchain-Integrated ERP Platforms for Ensuring Security in US Financial Supply Chains," *Journal of Business Insight and Innovation*, vol. 2, no. 2, pp. 107–119, 2023.

[15] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, 2020.

[16] Z. Lv, L. Qiao, J. Li, and H. Song, "Deep-learning-enabled security issues in the internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9531–9538, 2020.

[17] M. Z. Afshar and M. H. Shah, "Resilience through adaptation: Examining the interplay between adaptive capacity and organizational resilience in public sector organizations," *ACADEMIA International Journal for Social Sciences*, vol. 4, no. 2, pp. 1770–1789, 2025.

[18] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things," *Sensors*, vol. 19, no. 9, p. 1977, 2019.

[19] B. A. NG and S. Selvakumar, "Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment," *Future Generation Computer Systems*, vol. 113, pp. 255–265, 2020.

[20] F. M. Alrowais, S. Althahabi, S. S. Alotaibi, A. Mohamed, M. A. Hamza, and R. Marzouk, "Automated Machine Learning Enabled Cybersecurity Threat Detection in Internet of Things Environment," *Comput. Syst. Sci. Eng.*, vol. 45, no. 1, pp. 687–700, 2023.

[21] M. Z. Afshar and M. H. Shah, "Examining the role of change management in enhancing organizational resilience in public sector entities," *Center for Management Science Research*, vol. 3, no. 3, pp. 931–942, 2025.

[22] K. A. Da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[23] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile*

Networks and Applications, vol. 28, no. 1, pp. 296–312, 2023.

[24] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms," *IEEE Access*, vol. 9, pp. 161546–161554, 2021.

[25] S. Jain, S. Dutta, M. F. M. Alvi, A. Abbasi, and V. Arul, "Implementation of IoT-Enabled Smart Devices for Real-Time Health Monitoring in Nursing Practice," in *2025 International Conference on Frontier Technologies and Solutions (ICFTS)*, Mar. 2025, pp. 1–7.

[26] O. A. Wahab, "Intrusion detection in the iot under data and concept drifts: Online deep learning approach," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 19706–19716, 2022.

[27] A. Samy, H. Yu, and H. Zhang, "Fog-based attack detection framework for internet of things using deep learning," *IEEE Access*, vol. 8, pp. 74571–74585, 2020.

[28] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021.

[29] V. Hnamte, A. A. Najar, H. Nhung-Nguyen, J. Hussain, and M. N. Sugali, "DDoS attack detection and mitigation using deep neural network in SDN environment," *Computers & Security*, vol. 138, p. 103661, 2024.

[30] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in internet of medical things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020.

[31] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, "A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, p. 8981988, 2023.

[32] S. Zaman et al., "Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey," *IEEE Access*, vol. 9, pp. 94668–94690, 2021.

[33] E. Gyamfi and A. Jurcut, "Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, no. 10, p. 3744, 2022.

[34] H. Alkahtani and T. H. Aldhyani, "Intrusion detection system to advance Internet of Things infrastructure-based deep learning algorithms," *Complexity*, vol. 2021, no. 1, p. 5579851, 2021.

[35] A. Sharma and H. Babbar, "Understanding IoT-23 dataset: A benchmark for IoT security analysis," in *2024 4th International Conference on Intelligent Technologies (CONIT)*, Jun. 2024, pp. 1–5.

[36] Y. Alotaibi and M. Ilyas, "Ensemble-learning framework for intrusion detection to enhance internet of things' devices security," *Sensors*, vol. 23, no. 12, p. 5568, 2023.

[37] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges: A. Thakkar, R. Lohiya," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, 2021.

[38] M. A. Mostafa, "Enhanced IoT Anomaly Detection Using Combined Machine and Deep Learning Techniques on the IoT-23 Dataset," *Advances in Basic and Applied Sciences*, vol. 7, no. 1, pp. 11–17, 2025.

[39] F. Restuccia, S. D'oro, and T. Melodia,

"Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[40] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, "Machine learning for the detection and identification of Internet of Things devices: A survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 298–320, 2021.

[41] Stratosphere Laboratory, "Aposemat IoT-23: A labeled dataset with malicious and benign IoT network traffic," Stratosphere Laboratory, May 5, 2021. [Online]. Available: https://www.stratosphereips.org/blog/2020/1/22/aposemat-iot-23-a-labeled-dataset-with

[42] H. Ghani, S. Salekzamankhani, and B. Virdee, "Statistical and multivariate analysis of the IoT-23 dataset: a comprehensive approach to network traffic pattern discovery," *Journal of Cybersecurity and Privacy*, vol. 5, no. 4, p. 112, 2025.

[43] T. Islam, J. Abdullah, M. M. H. Munna, N. A. A. H. Nahid, M. I. H. Tusar, and M. D. Sarder, "Multi-objective optimization for transportation mode selection: A case study in logistics," *The Asian Journal of Shipping and Logistics*, 2026, early access. doi: 10.1016/j.ajsl.2026.01.002.

[44] N. A. A. H. Nahid, T. Islam, H. A. Rube, and M. I. H. Tusar, "Circular Economy Models for Urban Logistics: The Role of Bio-Based Packaging in Sustainable Transportation Networks," in *Proceedings of the IISE Annual Conference*, 2025, pp. 1–6.

[45] A. Rahman, S. Sultana, and R. J. Lima, "Strategic Framework for Enterprise Cybersecurity Management: Integrating Intelligent Anomaly Detection for Proactive Threat Mitigation," *Journal of Computer Science and Technology Studies*, vol. 8, no. 4, pp. 58–70, 2026.

[46] A. Rahman, S. Sultana, U. Twaha, and M. Rowshon, "AI-Enhanced Web Application Firewalls for Protecting United States Critical Infrastructure Against Zero-Day Exploits," *Scientia. Technology, Science and Society*, vol. 3, no. 2, pp. 11–32, 2026.

[47] A. Ahmed, S. Rahman, M. Islam, F. Chowdhury, and I. A. Badhan, "Challenges and opportunities in implementing machine learning for healthcare supply chain optimization: A data-driven examination," *International Journal of Business and Management Sciences*, vol. 3, no. 7, pp. 6–31, 2023.

[48] I. A. Badhan, M. N. Hasnain, and M. H. Rahman, "Enhancing Operational Efficiency: A Comprehensive Analysis of Machine Learning Integration in Industrial Automation," *Journal of Business Insight and Innovation*, vol. 1, no. 2, pp. 61–77, 2022.

[49] M. Farhat, A. Javaid, T. N. Khan, and N. Arif, "The Convergence of Artificial Intelligence, Deep Learning, and Internet of Things Technologies: Concepts and Applications," *Spectrum of Engineering Sciences*, vol. 4, no. 2, pp. 778–790, 2026.