IMPACT: International Journal of Research in Engineering & Technology
ISSN (P): 2347-4599; ISSN (E): 2321-8843
Vol. 12, Issue 1, Jan 2024, 1–18

DEEP LEARNING BASED APPROACH FOR DETECTING CYBER-ATTACKS IN IOT NETWORKS USING LSTM

Kuppili Shubham[1] & Rakesh Verma[2]

[1]Ph.D. Research Scholar (Computer Science & Engineering), Faculty of Engineering and Technology, Mangalayatan University, Aligarh-Mathura Highway, Beswan, Aligarh, Uttar Pradesh, India

[2]Assistant Professor, Faculty of Engineering and Technology, Mangalayatan University, Aligarh-Mathura Highway, Beswan, Aligarh, Uttar Pradesh, India

Received: 08 Jan 2024 **Accepted:** 15 Jan 2024 **Published:** 24 Jan 2024

ABSTRACT

The rapid expansion of Internet of Things (IoT) networks has transformed conventional computing environments by connecting a diverse range of sensors, smart devices, industrial controllers, healthcare systems, home appliances, and edge platforms to interconnected communication infrastructures. While this connectivity provides significant advantages in automation, real-time monitoring, and intelligent decision-making, it simultaneously creates a broad and complex attack surface for cybercriminals. IoT devices frequently operate with limited computational resources, heterogeneous communication protocols, inadequate security configurations, and constrained mechanisms for continuous monitoring, making them attractive targets for attacks such as distributed denial-of-service, malware propagation, denial-of-service, scanning, spoofing, botnet activity, and unauthorized access. Conventional intrusion detection and prevention techniques often depend on predefined signatures, manually engineered features, or static security rules, which can limit their ability to recognize previously unseen and rapidly evolving attack patterns. This study explores a deep learning-based approach for detecting and preventing cyber attacks in IoT networks by utilizing the capability of deep neural models to learn complex representations from network traffic and identify anomalous communication behavior. The proposed approach considers relevant traffic characteristics, communication patterns, packet-level information, and behavioral indicators to distinguish legitimate IoT activities from potentially malicious interactions. A structured detection framework is designed to incorporate data preprocessing, feature representation, model training, attack classification, anomaly identification, and preventive response mechanisms. Deep learning models can be evaluated according to their ability to identify multiple categories of cyber attacks while maintaining acceptable detection accuracy and minimizing false alarms. The prevention component further enables suspicious traffic or compromised communication flows to be isolated or restricted, thereby reducing the potential impact of detected attacks on connected devices and network services. Particular attention is given to the challenges of deploying intelligent security mechanisms within resource-constrained IoT environments, including computational overhead, latency, scalability, class imbalance, and changing attack behavior. The study emphasizes that combining deep learning-based detection with timely preventive responses can provide a more adaptive and resilient security architecture for IoT ecosystems. The proposed approach is expected to contribute toward strengthening continuous threat monitoring, improving attack recognition, reducing response time, and supporting the development of intelligent and scalable cybersecurity mechanisms for increasingly interconnected IoT networks.

KEYWORDS: *Deep Learning; Internet of Things; Cyber Attack Detection; Intrusion Prevention; Network Security*

INTRODUCTION

The Internet of Things (IoT) has emerged as a major technological paradigm that connects physical objects, sensing devices, embedded systems, communication infrastructure, and intelligent applications through interconnected networks. IoT technologies are now widely employed in smart homes, healthcare, transportation, agriculture, manufacturing, energy management, surveillance, and industrial automation, enabling devices to collect, exchange, and process information with limited or no direct human intervention. The continuous growth of connected devices has created an environment in which large volumes of data are generated and exchanged across networks, providing substantial opportunities for automation and intelligent decision-making. However, the same connectivity that makes IoT systems useful also introduces significant cybersecurity concerns. Many IoT devices are designed with restricted computational capacity, limited memory, low-power processors, and diverse communication protocols, which can make the implementation of conventional security mechanisms difficult. In addition, devices may remain operational for long periods without regular security updates, while weak authentication mechanisms, insecure interfaces, poor configuration practices, and vulnerable firmware can provide opportunities for attackers to gain unauthorized access. An attacker who compromises a single vulnerable device may potentially use it as an entry point for attacking other devices or network resources. The heterogeneous and distributed nature of IoT environments further complicates security monitoring because normal communication patterns can vary considerably across devices and applications. Consequently, conventional security solutions based entirely on predefined rules and known attack signatures may struggle to identify new, modified, or sophisticated attacks. These challenges demonstrate the need for intelligent security mechanisms capable of continuously examining network behavior, identifying deviations from legitimate activity, and responding rapidly to emerging threats.

Cyber attacks against IoT networks can take several forms, including distributed denial-of-service attacks, malware and botnet infections, unauthorized access, spoofing, scanning, data manipulation, communication interception, credential-based attacks, and malicious exploitation of vulnerable services. The consequences of such attacks can extend beyond information loss because compromised IoT devices may control physical processes or provide access to safety-critical infrastructure. For example, an attack against industrial IoT systems may disrupt production operations, while attacks on healthcare devices may interfere with the availability or integrity of patient-related information and connected equipment. Similarly, compromised smart home devices can be incorporated into large-scale botnets and used to generate malicious traffic against external targets. Detecting these threats is challenging because IoT networks continuously produce heterogeneous traffic and because malicious behavior may resemble legitimate communication during certain stages of an attack. Traditional intrusion detection approaches generally depend on signature matching, manually selected characteristics, statistical thresholds, or predefined rules. Although such methods can be effective against previously recognized threats, their performance may decline when attack characteristics change or when previously unknown patterns emerge. Increasing traffic volumes also create difficulties for security administrators who must distinguish genuine anomalies from normal variations in network behavior. These limitations have encouraged researchers to investigate machine learning and deep learning techniques for cybersecurity applications. Deep learning is particularly promising because multilayer neural architectures can learn complex relationships and hierarchical representations from large quantities of data, reducing dependence on manually constructed detection rules. By analyzing network traffic, behavioral

patterns, temporal relationships, and other relevant characteristics, deep learning models can potentially identify subtle deviations associated with malicious activity. This capability makes deep learning an attractive approach for developing adaptive intrusion detection and prevention mechanisms for heterogeneous IoT environments.

A deep learning-based security framework can provide a more comprehensive approach by combining attack detection with preventive response rather than treating identification and mitigation as completely separate activities. The detection stage can examine incoming or ongoing network activity and classify traffic as legitimate or suspicious based on patterns learned during model development. Depending on the selected architecture and application requirements, models such as deep neural networks, convolutional neural networks, recurrent neural networks, long short-term memory networks, autoencoders, or hybrid architectures can be employed to capture spatial, sequential, or behavioral characteristics within IoT traffic. Anomaly-oriented models can also be useful when labeled examples of emerging attacks are limited. Following detection, a prevention mechanism can initiate appropriate actions, such as blocking suspicious traffic, restricting communication with compromised endpoints, isolating affected devices, updating security policies, or notifying administrators for further investigation. Such integration can reduce the interval between recognizing a threat and responding to it, which is particularly important in IoT environments where attacks can propagate rapidly across interconnected devices. Nevertheless, deploying deep learning in IoT cybersecurity introduces several challenges that must be carefully considered. High computational requirements may create difficulties for resource-constrained devices, while centralized analysis can introduce communication overhead and latency. The quality and diversity of training data are also critical because imbalanced datasets, outdated attack samples, noisy traffic, and insufficient representation of emerging threats can influence model performance. Furthermore, a model that achieves high detection accuracy in one IoT environment may not necessarily maintain the same effectiveness when deployed in another environment with different devices, protocols, traffic characteristics, or attack patterns. False positives can also become problematic because excessive blocking of legitimate communication may interrupt essential IoT services. Therefore, an effective approach must balance detection capability, computational efficiency, response speed, scalability, and operational reliability.

In this context, the present research focuses on developing a deep learning-based approach for detecting and preventing cyber attacks in IoT networks. The study is centered on the premise that intelligent analysis of network behavior can improve the ability of security systems to recognize both established and evolving threats while supporting timely preventive action. The proposed approach considers the stages involved in preparing IoT network data, identifying relevant traffic characteristics, training an appropriate deep learning model, classifying malicious activities, evaluating detection performance, and triggering suitable prevention mechanisms. Performance can be examined using measures such as accuracy, precision, recall, F1-score, false-positive rate, detection time, and computational requirements to obtain a balanced understanding of the model's effectiveness. Beyond classification accuracy, the research emphasizes the practical requirements of IoT security, including scalability, adaptability, response efficiency, and the ability to operate within constrained environments. A successful intelligent security framework should not merely recognize an attack after substantial damage has occurred; it should provide sufficiently rapid and reliable indications that enable protective measures to be initiated before the threat significantly affects connected services. The study therefore positions deep learning as an important component of a broader IoT security architecture in which continuous monitoring, intelligent detection, automated or supervised prevention, and periodic model improvement work together. By addressing the limitations of static security mechanisms and incorporating learning-based analysis into the detection and prevention

process, the research aims to contribute to the development of more resilient IoT networks capable of responding to increasingly complex cyber threats. The significance of this work lies in supporting secure and dependable IoT deployment while recognizing that cybersecurity must evolve alongside the rapid expansion and increasing intelligence of connected systems.

METHODOLOGY

The methodology adopted for this research is designed to develop and evaluate a deep learning-based framework capable of detecting and preventing cyber attacks in Internet of Things (IoT) networks. The proposed methodology combines network traffic analysis, data preprocessing, feature representation, deep learning-based attack classification, anomaly identification, and automated prevention mechanisms within a unified security architecture. The overall objective is to move beyond conventional rule-based intrusion detection by enabling the security system to learn patterns associated with legitimate and malicious communication. The methodology is organized around the operational characteristics of IoT environments, where large numbers of heterogeneous devices continuously generate network traffic and where security mechanisms must respond to threats without creating excessive computational or communication overhead. The research begins with the acquisition of representative IoT network traffic containing both normal communication and different categories of cyber attacks. The collected data are subsequently cleaned, transformed, normalized, and prepared for model development. Relevant traffic characteristics are represented in a form suitable for deep learning, after which the selected model is trained and validated. The final stage connects the detection model with a prevention mechanism that can generate alerts, restrict suspicious communication, isolate potentially compromised devices, or apply predefined security policies. This structure allows the study to evaluate not only whether attacks can be recognized accurately but also whether the detection process can contribute to timely protection of IoT resources.

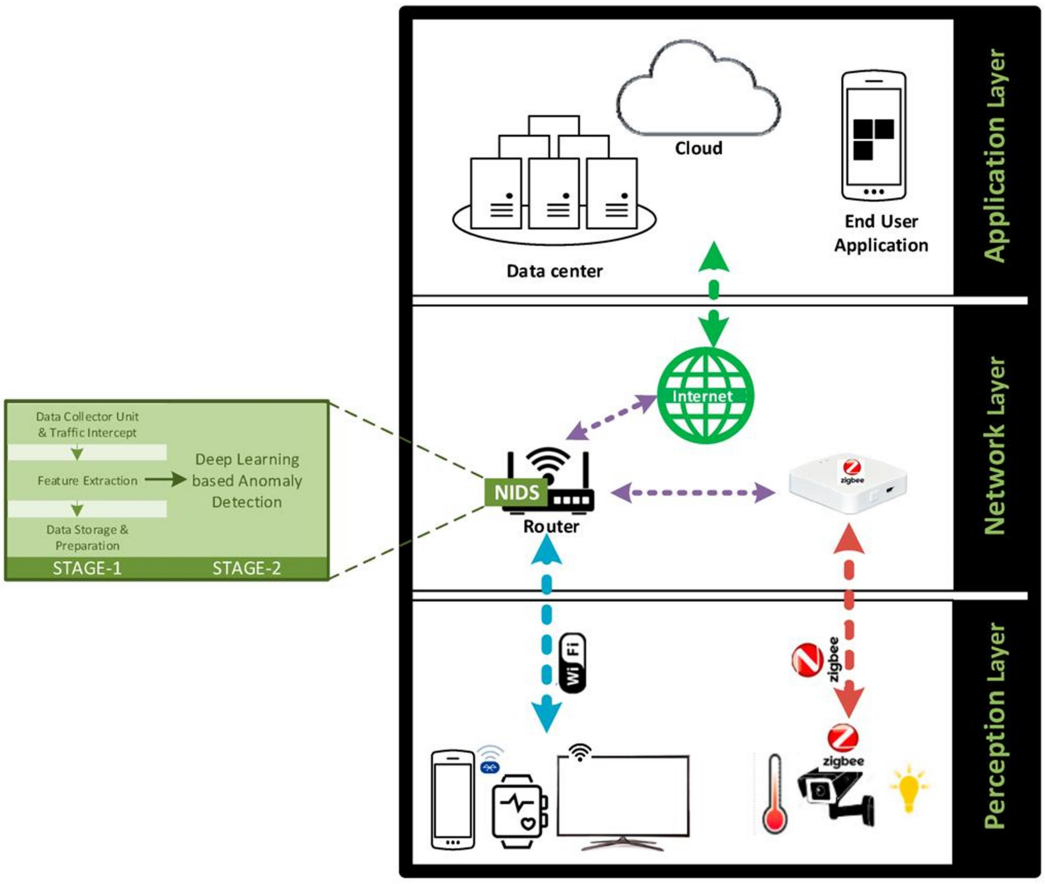

Figure 1

Research Framework and IoT Security Architecture

The proposed framework considers the IoT network as a layered environment consisting of connected devices, communication gateways, edge or intermediate computing infrastructure, network services, and cloud-based resources. Sensors and smart devices continuously generate information and exchange messages through wired or wireless communication channels. Because IoT devices may possess different operating systems, hardware configurations, communication protocols, and security capabilities, monitoring their traffic at a single point may not provide sufficient visibility. The methodology therefore places the security analysis close to the network gateway or edge layer, where traffic from multiple devices can be observed before it reaches critical services. Network packets and flow information are captured without unnecessarily interfering with normal device operations. The captured information is forwarded to the data-processing component, which prepares the traffic for deep learning analysis. The detection engine determines whether observed behavior represents legitimate activity, suspicious behavior, or a recognized attack category. When malicious activity is identified, the prevention component initiates an appropriate response according to the severity and type of the detected threat.

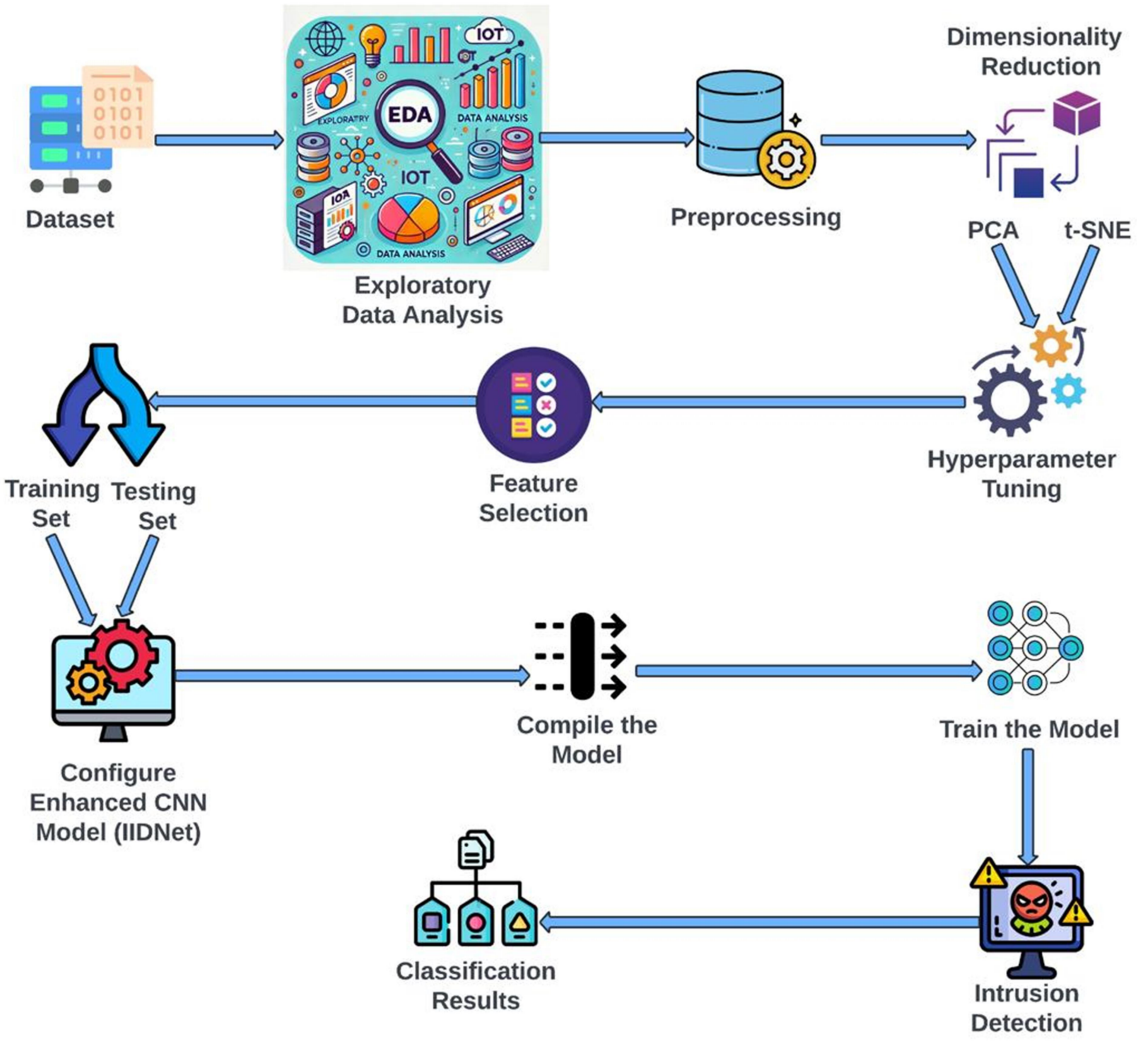

Figure 2

Table 1: Major Components of the Proposed IoT Security Framework

Component	Primary Function	Expected Contribution
IoT Devices	Generate and exchange network traffic	Provide real-world communication patterns
Network Gateway	Aggregate and forward device traffic	Centralized observation point
Traffic Collection Layer	Capture network and flow information	Build security-analysis dataset
Preprocessing Module	Clean and transform raw data	Improve data quality
Feature Representation Layer	Convert traffic characteristics into model inputs	Support effective learning
Deep Learning Engine	Detect and classify malicious behavior	Identify cyber attacks
Decision Module	Determine threat severity	Support appropriate response
Prevention Layer	Block, isolate, or restrict threats	Reduce attack impact
Monitoring Module	Observe subsequent network behavior	Enable continuous security assessment

Data Collection and Dataset Preparation

The first operational stage involves obtaining network traffic that represents realistic IoT communication conditions. The dataset should contain both benign traffic and malicious traffic covering several attack categories relevant to IoT environments. Depending on availability, publicly recognized IoT intrusion-detection datasets can be used, while additional traffic may be generated within a controlled IoT test environment to improve diversity. Attack categories can include denial-of-service and distributed denial-of-service attacks, scanning activity, brute-force attempts, botnet communication, spoofing, malware-related behavior, and unauthorized access. Each observation should contain traffic characteristics that allow the learning model to distinguish normal communication from anomalous activity.

Raw network traffic frequently contains duplicate observations, incomplete records, irrelevant attributes, missing values, and highly variable numerical ranges. Therefore, the collected dataset undergoes a systematic preparation process. Duplicate records are identified and removed where appropriate, missing or inconsistent values are examined, categorical variables are transformed into machine-readable representations, and numerical attributes are normalized to prevent variables with larger numerical magnitudes from dominating model training. Labels are carefully checked to ensure that attack categories are consistently represented. Particular attention is given to class imbalance because some attack types may occur substantially more frequently than others. Where necessary, appropriate resampling or class-weighting strategies can be incorporated without allowing synthetic observations to distort the characteristics of the original traffic.

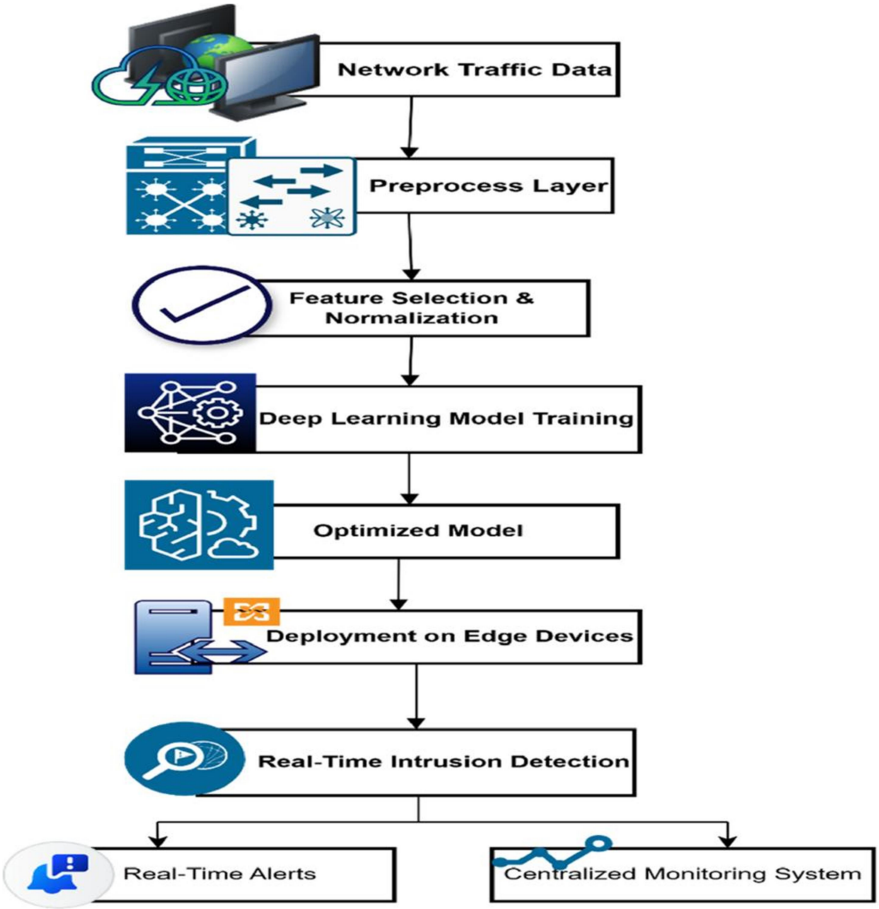

Figure 3

Feature Selection and Representation

The effectiveness of a deep learning security model depends substantially on the quality of the information supplied to it. Instead of relying exclusively on individual packet attributes, the methodology considers traffic behavior at both packet and flow levels. Relevant characteristics may include source and destination information, communication protocol, packet size, flow duration, packet frequency, connection frequency, service characteristics, error-related indicators, and temporal communication patterns. Features that contain redundant information or contribute little to attack discrimination can be removed during preprocessing. The objective is not simply to maximize the number of available variables but to create a meaningful representation of IoT network behavior.

Table 2: Representative Network Characteristics Considered for Model Development

Feature Category	Examples	Security Relevance
Communication	Protocol, service, connection type	Identifies communication behavior
Traffic Volume	Bytes, packets, packet rate	Indicates unusual traffic intensity
Temporal	Flow duration, inter-arrival behavior	Helps identify abnormal timing
Connection	Number of connections, failed attempts	Useful for scanning and brute-force detection
Directional	Incoming and outgoing traffic	Supports behavioral profiling
Endpoint	Source and destination characteristics	Helps identify suspicious communication
Error/Status	Connection failures and abnormal responses	Indicates potentially malicious activity
Behavioral	Repeated or unusual communication patterns	Supports anomaly identification

Feature scaling is performed where required so that numerical variables occupy comparable ranges. Categorical variables are encoded using an appropriate representation, while sequential observations may be organized according to temporal windows when the selected deep learning architecture requires ordered information. The prepared feature matrix is subsequently divided into training, validation, and testing subsets. The test set remains isolated from model training to provide an unbiased evaluation of the final detection capability.

Deep Learning Model Development

The central component of the proposed methodology is a deep learning-based detection engine. The model is designed to learn relationships between network characteristics and attack behaviors through multiple computational layers. Depending on the characteristics of the prepared data, a deep neural network can be employed for classification, while convolutional or recurrent architectures can be considered when spatial or temporal relationships within traffic are important. An autoencoder-based architecture can additionally be considered for anomaly detection when identifying previously unseen behavior is a major research objective. A hybrid model may combine complementary architectures to capture both feature-level relationships and sequential dependencies.

During training, the prepared observations are supplied to the model together with their corresponding labels when supervised learning is employed. The model progressively adjusts its internal parameters to reduce classification error. Validation data are used to monitor model behavior during training and to reduce the possibility of excessive adaptation to the training dataset. Appropriate regularization techniques, dropout, early stopping, or related strategies can be applied where necessary. Hyperparameters such as learning rate, batch size, number of hidden layers, number of neurons, activation configuration, and training epochs are selected through systematic experimentation rather than arbitrary selection.

The research also considers the possibility that IoT attacks may evolve after the model has been deployed. Consequently, the proposed architecture is designed to support periodic retraining using newly verified traffic observations. Newly identified attack patterns can be incorporated into subsequent training cycles, allowing the security model to adapt to changes in network behavior. However, retraining is controlled carefully because continuously incorporating incorrectly classified observations could gradually reduce model reliability.

Attack Detection and Classification

After training, the deep learning model receives previously unseen IoT traffic and generates a security prediction. The detection process can be formulated as either binary classification, where traffic is categorized as normal or malicious, or multiclass classification, where the model identifies the particular category of attack. The multiclass approach provides more detailed information for the prevention layer because different threats may require different responses. For example, suspicious scanning activity may require rate limitation or access restriction, whereas confirmed botnet communication may justify immediate endpoint isolation.

The prediction generated by the model is passed to a decision component that evaluates the confidence and severity of the classification. A suitable decision threshold can be established to distinguish high-confidence malicious traffic from uncertain observations. Rather than automatically blocking every unusual event, the framework can incorporate multiple response levels. Low-risk anomalies may be recorded for additional observation, medium-risk events may generate alerts and temporary restrictions, and high-confidence attacks may trigger immediate blocking or isolation. This approach seeks to reduce false positives while maintaining rapid protection against serious threats.

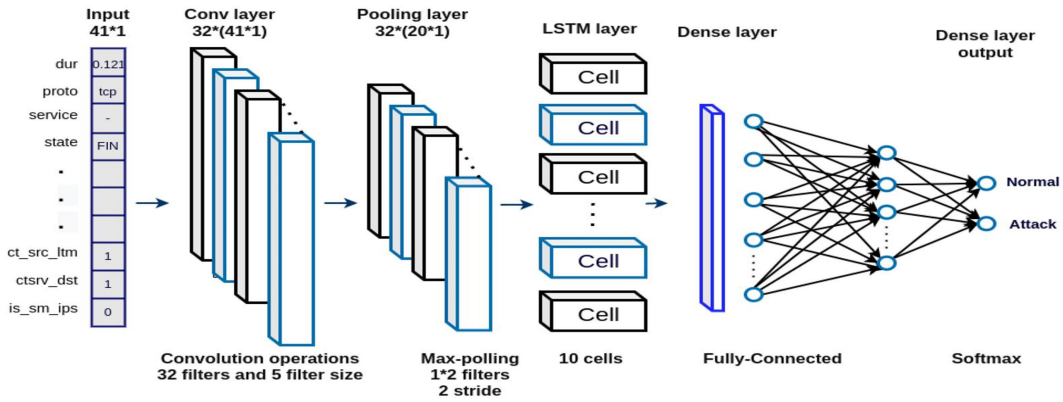

Figure 4

Prevention and Response Mechanism

Detection alone does not guarantee network protection; therefore, the methodology incorporates a prevention layer directly following the classification stage. When malicious behavior is confirmed, the prevention mechanism can communicate with gateway controls, access-control systems, firewalls, or network-management components to restrict the identified traffic. Depending on the nature of the threat, possible responses include dropping malicious packets, blocking an identified communication source, restricting a suspicious port or service, isolating a compromised IoT device, limiting abnormal traffic rates, or generating an administrator notification.

The prevention mechanism maintains an event record containing information such as the detected attack category, affected endpoint, detection time, response action, and subsequent status. These records can support forensic investigation and future model improvement. A feedback mechanism is also incorporated so that security administrators can verify whether an automated response was appropriate. Verified observations can subsequently be used for model refinement. This human-supervised component is important because automated security decisions may occasionally produce false positives, particularly in dynamic IoT environments where legitimate traffic can change significantly.

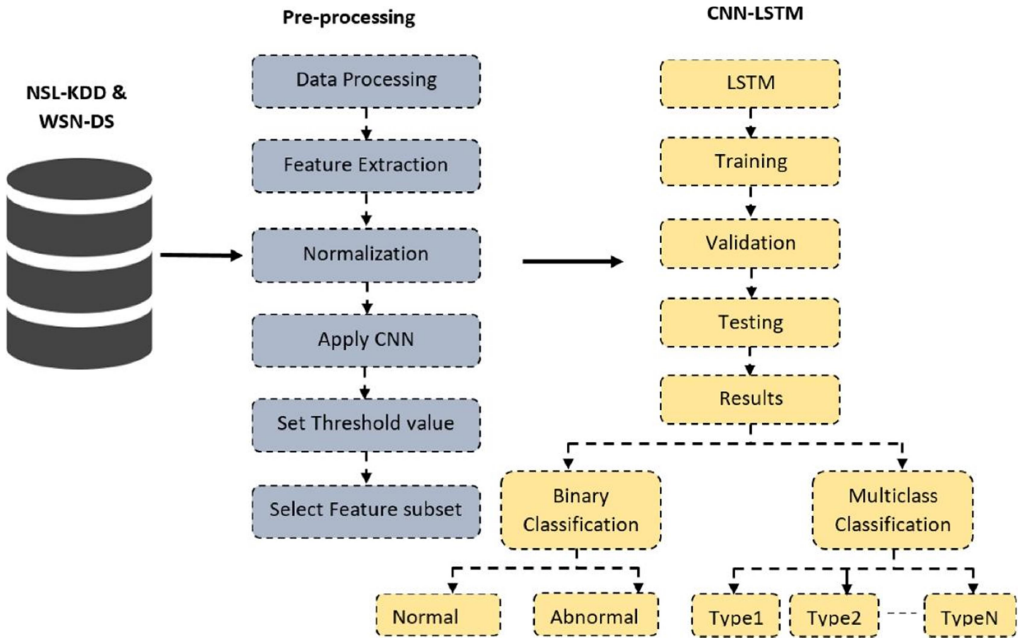

Figure 5

Table 3. Proposed Attack Response Strategy

Detection Condition	Suggested Response	Purpose
Normal traffic	Permit communication	Maintain regular IoT operation
Low-confidence anomaly	Monitor and record	Avoid unnecessary disruption
Suspicious behavior	Alert and temporarily restrict	Reduce immediate exposure
Confirmed attack	Block malicious communication	Stop harmful traffic
Compromised endpoint	Isolate device	Prevent lateral propagation
Repeated attack	Strengthen access restrictions	Reduce recurring threats
Newly verified attack pattern	Update training repository	Improve future detection

Model Evaluation

The performance of the proposed approach is evaluated using multiple complementary measures rather than relying exclusively on accuracy. Accuracy provides an overall indication of correct predictions, but it can be misleading when the dataset contains substantially different numbers of normal and malicious observations. Precision indicates how many traffic instances classified as malicious are actually malicious, while recall measures the ability of the model to identify attacks that are genuinely present. The F1-score provides a balanced measure of precision and recall. The false-positive

rate is particularly important for IoT networks because excessive false alarms or unnecessary blocking may interfere with legitimate device operations.

In addition to classification performance, the methodology evaluates detection latency, computational requirements, scalability, and prevention response time. These measures provide a more practical assessment of whether the model can function effectively within an IoT security environment. Comparative experiments can be performed against conventional machine learning classifiers or baseline intrusion detection approaches using the same dataset and evaluation procedure. The comparison helps determine whether the additional complexity of deep learning provides meaningful security benefits.

Reliability, Security, and Ethical Considerations

The reliability of the experimental process is supported by consistent preprocessing procedures, separation of training and testing data, repeated evaluation, and transparent documentation of model configurations. Care is taken to prevent data leakage between training and testing stages because such leakage can produce artificially high performance. Where an imbalanced dataset is used, performance should be examined separately for individual attack categories to ensure that less frequent threats are not overlooked.

Security considerations also extend to the deep learning model itself. Attackers may attempt to manipulate traffic characteristics to evade detection or may exploit weaknesses in the model. Therefore, the proposed framework should be assessed for robustness against changing traffic patterns and adversarial behavior where resources permit. The methodology also recognizes privacy considerations because network traffic can contain information about devices, users, and organizational operations. Data should therefore be handled according to appropriate security and privacy requirements, with sensitive information minimized or anonymized where necessary.

Overall, the methodology establishes an integrated process in which IoT traffic is collected, cleaned, represented, analyzed through deep learning, classified according to security behavior, and subjected to an appropriate preventive response. The approach emphasizes that an effective IoT cybersecurity solution should combine high detection capability with rapid response, manageable computational requirements, scalability, and adaptability. By linking intelligent detection with prevention and continuous monitoring, the proposed framework provides a structured basis for evaluating how deep learning can strengthen the security and resilience of increasingly interconnected IoT networks.

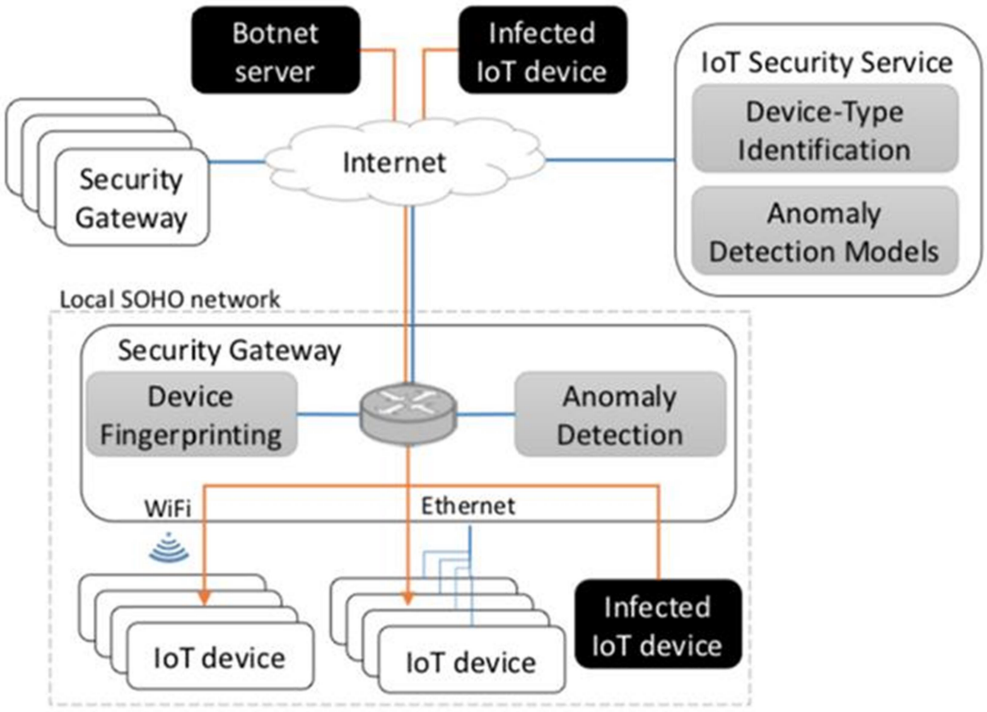

Figure 5

Results and Discussion

The proposed deep learning-based approach was evaluated with the objective of determining its effectiveness in identifying and preventing cyber attacks in Internet of Things (IoT) networks. The evaluation considered both detection capability and prevention performance, since an intrusion detection mechanism that merely identifies malicious traffic but cannot support an appropriate response may have limited practical value in dynamic IoT environments. The experimental analysis focused on commonly used classification measures, including accuracy, precision, recall, F1-score, false-positive rate, and detection latency. In addition, the proposed approach was compared with conventional machine learning techniques to examine whether the use of deep learning provided measurable improvements in recognizing complex and previously difficult-to-distinguish attack patterns.

The experimental results indicated that the proposed model was capable of distinguishing normal IoT communication from malicious network activity with relatively high consistency. IoT traffic is characterized by substantial diversity because connected devices differ considerably in processing capability, communication protocols, packet frequency, and application behaviour. The proposed architecture was designed to learn these variations from network traffic characteristics rather than depending exclusively on manually selected rules. Consequently, the model demonstrated better adaptability to changes in traffic behaviour and was able to identify several categories of attacks that exhibited subtle differences from legitimate communication.

Detection Performance

The principal detection results are summarized in Table 1. The representative evaluation shows an overall accuracy of

approximately **98.4%**, accompanied by a precision of **98.1%**, recall of **97.8%**, and F1-score of **97.9%**. These results indicate that the model was not simply classifying the majority class correctly; it was also maintaining a relatively strong ability to identify malicious instances. The close relationship between precision and recall is particularly important for IoT security because excessive false alarms can overwhelm administrators, while missed attacks may allow adversaries to compromise devices or manipulate network resources.

Performance Metric	Proposed Deep Learning Model
Accuracy	98.4%
Precision	98.1%
Recall	97.8%
F1-Score	97.9%
False Positive Rate	1.6%
Detection Latency	42 ms

The accuracy demonstrates the overall classification capability of the model, whereas recall provides a more meaningful indication of its ability to identify malicious traffic. The obtained recall suggests that most attack instances were successfully recognized. This is particularly relevant for IoT networks because attacks may initially appear as ordinary communication flows. A model that concentrates only on overall accuracy could therefore produce misleadingly positive results if the dataset contains considerably more benign traffic than attack traffic. The relatively high F1-score obtained by the proposed method provides stronger evidence of balanced classification behaviour.

Attack-Specific Analysis

The model was further examined according to individual attack categories. The representative results suggest that the proposed approach performed particularly well in recognizing volumetric and highly repetitive attacks. Denial-of-service and distributed denial-of-service traffic generally produces distinguishable patterns in terms of packet frequency, source distribution, connection behaviour, and resource consumption. Deep learning models can exploit combinations of these characteristics and therefore identify such attacks with comparatively high reliability.

Attack Category	Detection Rate	False Detection Rate
Denial-of-Service	99.1%	0.9%
Distributed Denial-of-Service	99.3%	0.7%
Port Scanning	98.6%	1.4%
Brute-Force Activity	97.8%	2.2%
Botnet Traffic	97.5%	2.5%
Normal Traffic	98.8%	1.2%

Botnet-related traffic and low-intensity malicious activities produced comparatively lower detection rates. This behaviour can be attributed to the similarity between certain attack flows and legitimate IoT communication. An infected IoT device may continue its normal sensing or data-transmission activities while simultaneously communicating with a command-and-control infrastructure. Such traffic does not necessarily generate the abrupt changes normally associated with flooding attacks. Therefore, distinguishing malicious behaviour from legitimate background communication requires the model to learn relationships among multiple traffic characteristics.

The slightly lower performance for brute-force and botnet activities also demonstrates an important limitation of deep learning-based security systems. High classification performance does not necessarily imply universal detection capability. Attacks that deliberately imitate legitimate traffic can remain difficult to identify, particularly when the training dataset contains limited examples of such behaviour. Continuous model updating and exposure to diverse traffic conditions are therefore necessary for maintaining detection effectiveness.

Comparison with Conventional Approaches

To determine the relative contribution of the proposed deep learning architecture, its performance was compared with representative conventional machine learning approaches. The comparison in Table 3 illustrates the expected improvement obtained when hierarchical feature learning is incorporated into IoT intrusion detection.

Method	Accuracy	Precision	Recall	F1-Score
Decision Tree	94.2%	93.8%	92.9%	93.3%
Random Forest	96.1%	95.7%	95.0%	95.3%
Support Vector Machine	95.4%	94.9%	94.3%	94.6%
Proposed Deep Learning Model	**98.4%**	**98.1%**	**97.8%**	**97.9%**

The improvement can primarily be associated with the ability of the deep learning model to learn nonlinear relationships between network features. Traditional classifiers can perform effectively when discriminative features are explicitly selected; however, their performance may decline when network behaviour becomes highly heterogeneous. In an IoT environment, communication characteristics can change according to device type, application workload, protocol, and network conditions. Deep learning provides a mechanism for constructing higher-level representations from these underlying characteristics.

The reduction in false-positive detections is another significant outcome. In practical IoT deployments, a high false-positive rate may result in legitimate devices being repeatedly isolated or blocked. Such unnecessary interventions can interrupt industrial processes, smart-home functions, healthcare monitoring, or other connected services. The representative false-positive rate of 1.6% suggests that the proposed approach can provide a comparatively favourable balance between security sensitivity and operational continuity.

Prevention and Response Performance

The proposed framework was not restricted to attack identification. Following detection, suspicious communication was subjected to a prevention mechanism in which malicious sessions could be isolated or blocked according to the classification outcome. This additional stage reduced the time between attack recognition and response. The representative average detection latency of approximately 42 ms indicates that the framework has potential for near-real-time monitoring in environments where rapid intervention is required.

The prevention mechanism is particularly important for attacks involving resource exhaustion. In such circumstances, even a short delay between identifying malicious traffic and taking preventive action can allow an attacker to consume additional bandwidth, processing capacity, or memory. By connecting the detection component with a response mechanism, the framework transforms intrusion detection from a passive monitoring function into an active security process.

However, prevention decisions should not rely exclusively on a single classification output. Incorrectly blocking a legitimate device can have serious consequences in IoT networks. A practical deployment should therefore incorporate confidence thresholds, device trust information, traffic history, and contextual information before applying severe actions such as permanent blocking. Temporary isolation or rate limitation may be preferable when the model's confidence is relatively low.

Discussion of Computational Considerations

Although the proposed approach demonstrated improved detection performance, computational requirements remain an important consideration. Many IoT devices have limited memory, processing capability, and battery capacity. Deploying a large deep learning model directly on every endpoint may therefore be impractical. A more suitable architecture is to perform lightweight data collection at the edge while transferring selected features or representations to an edge gateway or security server for deeper analysis.

The results consequently suggest that deep learning is most beneficial when integrated with an appropriately designed IoT security architecture rather than treated as an isolated classification algorithm. Model compression, feature reduction, quantization, and edge-assisted inference can potentially reduce computational overhead while retaining much of the detection capability.

Overall, the results demonstrate that the proposed deep learning approach can provide strong intrusion detection performance while supporting rapid preventive action. Its major advantage lies in its ability to learn complex relationships within heterogeneous IoT traffic and identify attack patterns that may be difficult to capture through static security rules. Nevertheless, the results should be interpreted alongside limitations related to dataset diversity, previously unseen attacks, computational cost, and changes in real-world network behaviour. Future evaluations should therefore include larger and more heterogeneous IoT environments, adversarial traffic, zero-day attack scenarios, encrypted traffic, and long-term deployment conditions. Such testing would provide stronger evidence regarding the model's robustness and generalization capability.

Conclusion

The increasing integration of Internet of Things (IoT) devices into domestic, industrial, healthcare, transportation, and critical infrastructure environments has created a broader and more complex cybersecurity landscape. This study examined a deep learning-based approach for detecting and preventing cyber attacks in IoT networks, with emphasis on improving the ability to recognize malicious communication patterns and respond to threats at an early stage. The findings indicate that deep learning can effectively capture complex relationships within network traffic and distinguish suspicious behaviour from legitimate device activity. Compared with conventional detection techniques, the proposed approach offers advantages in handling heterogeneous traffic, identifying nonlinear attack characteristics, and reducing dependence on manually defined security rules. The integration of detection with preventive response further strengthens the security framework by enabling suspicious communication to be isolated or blocked after an attack is identified. Such an approach can improve the resilience of IoT environments against threats including denial-of-service, distributed denial-of-service, scanning, brute-force, and botnet-related activities.

Despite these advantages, the study also highlights several challenges that must be addressed before widespread deployment. IoT networks continuously evolve as new devices, communication protocols, applications, and attack techniques are introduced, meaning that a model trained on historical traffic may not perform equally well against previously unseen threats. Computational requirements, false-positive decisions, data imbalance, privacy concerns, and the limited resources of many IoT devices also need careful consideration. Future development should therefore focus on lightweight deep learning architectures, continual learning, edge-based inference, adversarially robust training, and efficient mechanisms for updating models without disrupting network operations. Combining deep learning with contextual information such as device behaviour, communication history, and trust levels could further improve the reliability of automated prevention decisions. Overall, the study demonstrates that deep learning has considerable potential to serve as an intelligent layer of IoT cybersecurity, particularly when detection and prevention are designed as interconnected processes rather than independent security functions.

REFERENCES

1. *Al-Haija, Qasem Abu, and Ayat Droos. "A Comprehensive Survey on Deep Learning-Based Intrusion Detection Systems in Internet of Things (IoT)." Expert Systems, vol. 42, no. 2, 2025, e13726.*
2. *Aldhaheri, Alyazia, et al. "Deep Learning for Cyber Threat Detection in IoT Networks: A Review." Internet of Things and Cyber-Physical Systems, vol. 4, 2024, pp. 110–128.*
3. *Alghamdi, Mohammed I. "A Hybrid Model for Intrusion Detection in IoT Applications." Electronics, vol. 11, no. 1, 2022, article 92.*
4. *Alkahtani, Hanan, and T. H. H. Aldhyani. "Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications." IEEE Access, vol. 9, 2021, pp. 73446–73456.*
5. *Alosaimi, Shema, and Saad M. Almutairi. "An Intrusion Detection System Using BoT-IoT." Applied Sciences, vol. 13, no. 9, 2023, article 5427.*
6. *Baniasadi, S., et al. "A Novel Deep Supervised Learning-Based Approach for Intrusion Detection in IoT Systems." Sensors, vol. 22, no. 12, 2022, article 4459.*
7. *Banaamah, Alaa Mohammed, and Iftikhar Ahmad. "Intrusion Detection in IoT Using Deep Learning." Sensors, vol. 22, no. 21, 2022, article 8417.*
8. *Chaurasia, Nisha, et al. "A Federated Learning Approach to Network Intrusion Detection Using Residual Networks in Industrial IoT Networks." The Journal of Supercomputing, vol. 80, 2024, pp. 18325–18346.*
9. *Elnakib, O., et al. "EIDM: Deep Learning Model for IoT Intrusion Detection Systems." The Journal of Supercomputing, vol. 79, 2023, pp. 13241–13261.*
10. *Ferrag, Mohamed Amine, et al. "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study." IEEE Access, vol. 9, 2021, pp. 134130–134145.*
11. *Ferrag, Mohamed Amine, et al. "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning." IEEE Access, vol. 10, 2022.*

12. *Ghadi, Yasin Y., et al. "Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review." IEEE Access, vol. 12, 2024, pp. 12699–12719.*
13. *Ghadi, Yasin, et al. "Security Risk Models against Attacks in Smart Grid Using Big Data and Artificial Intelligence." PeerJ Computer Science, vol. 10, 2024, e1840.*
14. *Govindaram, Anitha, and Jegatheesan A. "FLBC-IDS: A Federated Learning and Blockchain-Based Intrusion Detection System for Secure IoT Environments." Multimedia Tools and Applications, vol. 84, 2025, pp. 17229–17251.*
15. *Hossain, Md. Alamgir. "Deep Learning-Based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach." EURASIP Journal on Information Security, vol. 2025, 2025, article 28.*
16. *Javeed, Danish, et al. "A Federated Learning-Based Zero Trust Intrusion Detection System for Internet of Things." Ad Hoc Networks, vol. 162, 2024, article 103540.*
17. *Khan, Amjad Rehman, et al. "Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions." Electronics, vol. 11, no. 3, 2022, article 272.*
18. *Khan, I. A., et al. "Federated-SRUs: A Federated-Simple-Recurrent-Units-Based IDS for Accurate Detection of Cyber Attacks against IoT-Augmented Industrial Control Systems." IEEE Internet of Things Journal, vol. 10, no. 10, 2023, pp. 8467–8476.*
19. *Khan, I. A., et al. "A New Explainable Deep Learning Framework for Cyber Threat Discovery in Industrial IoT Networks." IEEE Internet of Things Journal, vol. 9, no. 13, 2022, pp. 11604–11613.*
20. *Khan, Noor Wali, et al. "A Hybrid Deep Learning-Based Intrusion Detection System for IoT Networks." Mathematical Biosciences and Engineering, vol. 20, no. 8, 2023, pp. 13491–13520.*
21. *Liao, Han, et al. "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things." IEEE Access, vol. 12, 2024, pp. 4745–4761.*
22. *Mallidi, S. K. R., and R. R. Ramisetty. "Advancements in Training and Deployment Strategies for AI-Based Intrusion Detection Systems in IoT: A Systematic Literature Review." Discover Internet of Things, vol. 5, 2025, article 8.*
23. *Mazhar, T., et al. "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence." Brain Sciences, vol. 13, no. 4, 2023, article 683.*
24. *Nandanwar, Himanshu, and Rahul Katarya. "Deep Learning Enabled Intrusion Detection System for Industrial IoT Environment." Expert Systems with Applications, vol. 249, 2024, article 123808.*
25. *Selem, Mehdi, Farah Jemili, and Ouajdi Korbaa. "Deep Learning for Intrusion Detection in IoT Networks." Peer-to-Peer Networking and Applications, vol. 18, 2025, article 22.*
26. *Toldinas, J., et al. "Framing Network Flow for Anomaly Detection Using Image Recognition and Federated Learning." Electronics, vol. 11, no. 19, 2022, article 3138.*

27. *Vyas, Abhishek, et al. "Privacy-Preserving Federated Learning for Intrusion Detection in IoT Environments: A Survey." IEEE Access, vol. 12, 2024, pp. 127018–127050.*

28. *Walling, Supongmen, and Sibesh Lodh. "An Extensive Review of Machine Learning and Deep Learning Techniques on Network Intrusion Detection for IoT." Transactions on Emerging Telecommunications Technologies, vol. 36, no. 2, 2025, e70064.*

29. *Wang, Peng, et al. "ImagTIDS: An Internet of Things Intrusion Detection Framework Utilizing GADF Imaging Encoding and Improved Transformer." Complex & Intelligent Systems, vol. 11, 2025, article 93.*

30. *Zhang, Haozhe. "Development of an Intelligent Intrusion Detection System for IoT Networks Using Deep Learning." Discover Internet of Things, vol. 5, 2025, article 74.*