Archives available at journals.mriindia.com

**International Journal on Advanced Computer Engineering and Communication Technology**

ISSN: 2278-5140

Volume 15 Issue 01, 2026

# Cybersecurity in AI-Enabled IoT Network: Threat Detection and Mitigation Using Deep Learning

[1]Sunil Kumar, [2]Dr. Simmi Prakash, [3]Ashok Kumar, [4]Mamta, [5]Riju Kumari, [6]Vijay

*[1] Chief Librarian, PIMS Medical College and Hospital, Jalandhar, Punjab, India*

*[2] Head, Entrepreneurship and Startup Support Cell & Assistant Professor, Rayat Bahra University, Chandigarh, India*

*[3] Librarian, Government College Sri Muktsar Sahib, Punjab, India*

*[4] Ph.D. Research Scholar, Department of Library and Information Science, HRIT University, Ghaziabad, Uttar Pradesh, India*

*[5] Research Scholar, HRIT University, Ghaziabad, Uttar Pradesh, India*

*[6] Independent Researcher, Department of Library and Information Science, Lovely Professional University, Phagwara, Punjab, India*

**Peer Review Information**

*Submission: 28 Feb 2026*

*Revision: 16 March 2026*

*Acceptance: 28 March 2026*

**Keywords**

*Artificial Intelligence (AI), Internet of Things (IoT), Cybersecurity, Deep Learning, Intrusion Detection System (IDS), Threat Detection, Network Security, Anomaly Detection.*

**Abstract**

The rapid evolution of Artificial Intelligence (AI) and the Internet of Things (IoT) has reshaped the contemporary digital ecosystem, enabling the introduction of smart environments across most disciplines. However, this integration has raised serious cybersecurity concerns due to massive connectivity, diverse architectures, and the real-time flow of information. The article proposes a hybrid CNN-based LSTM system for threat detection and mitigation in AI-operated IoT networks. The proposed system is tested using the CICIDS2017 dataset, a popular intrusion detection benchmark. The model performs feature extraction, anomaly detection, and automatic mitigation to enhance cybersecurity resilience. Experimental results demonstrate that the proposed CNN-LSTM model achieves 96.8% accuracy, outperforming traditional machine learning models such as Decision Tree, SVM, and KNN. The model also achieves lower false-positive rates and improved detection time, making it useful for real-time security applications in the Iot. The results show that deep learning methods are highly efficient in improving Iot security and achieving maximum protection against emerging threats.

## Introduction

The recent surge in the number of interconnected devices with the Internet of Things (IoT) has changed digital ecosystems in the contemporary world, enabling effortless communication between smart homes, healthcare, industrial automation and vital infrastructure. The implementation of Artificial Intelligence (AI) into the IoT networks has also enhanced the features of the system to develop intelligent decisions, predictive analytics and autopilot features. However, convergence has also been a significant cybersecurity risk due to the larger attack surface, the heterogeneous background of the devices, and the need to exchange data in real-time (Ali et al., 2025; Jain, 2025).

In AI-enabled IoT environments, cyber threats are increasingly becoming advanced, such as distributed denial-of-service (DDoS) attacks, data breaches, malware injection, and adversarial attacks on machine learning models. The traditional security mechanisms might not be adequate in combating these dynamic threats as they are normally fixed and therefore they are not

at a position to keep pace with the dynamic behaviors of the networks. This results in an increased need in smarter, more dynamic, and scalable cybersecurity solutions (Dhanushkodi and Thejas, 2024; Simanjuntak, 2024).

Deep learning techniques have emerged as a promising solution to enhance cybersecurity in IoT networks because they can learn complex patterns, detect anomalies, and provide real-time responses to mitigate threats. Compared to conventional methods, deep learning-based models can reduce false positives and increase detection rates, thanks to large volumes of big data and more advanced neural network architectures (Maddireddy and Maddireddy, 2024; Latif et al., 2026).

**1. Background of Study**

The IoT ecosystem is made up of billions of devices that are connected and communicate through networks to gather, process and transfer information. These devices are often deployed in resource constrained environments and this is the reason why they can be subjected to numerous cyber threats. The adoption of AI in the IoT systems has enabled automation and intelligent functions at the same time, forming new points of vulnerabilities particularly in the data processing and decision making levels (Gopalsamy, 2022; Nay, 2024).

Cybersecurity solutions based on AI and machine learning, and deep learning, in particular, have received a lot of attention due to their capacity to identify unknown and zero-day attacks. This kind of systems keeps track of traffic patterns on the network and labels the violations as malicious activities (Shukla et al., 2024; Ijiga et al., 2024).

**2. Need of Study**

The growing use of IoT in critical sectors such as healthcare, smart cities and industry needs a more robust cybersecurity system since the conventional approach lacks efficiency to deal with large, dynamic and diverse environments. Clearly, there is a necessity of real-time, adaptive, scalable security systems with reduced number of false alarms, which can be effectively implemented with deep learning-based systems with automated and accurate threat identification (Ali et al., 2025; Khalaf et al., 2025).

**3. Motivation**

The justification of the study is the increasing number and sophistication of IoT network attacks whereby the existing cyber security systems are likely to fail to recognize advanced attacks such as zero-day attacks and the adversarial attacks. Furthermore, the lack of built-in security in IoT devices, system heterogeneity, and vulnerabilities of AI models also increase the risk, which is why a complex deep learning-based solution to proactive threat detection and mitigation is needed (Sewak et al., 2023; Alhossainy and Malekzadeh, 2026).

**4. Limitations**

Even though AI and deep learning have some benefits in cybersecurity, a number of limitations exist:

- Intensive computational needs to train deep learning models.
- Relying on large labeled datasets.
- Vulnerability to adversarial attacks targeting AI models
- Difficulty in real-time deployment in resource-constrained IoT devices
- Unreliability of deep learning decisions.

These constraints make it difficult to have scalable and effective cybersecurity systems (Ijiga et al., 2024; Jain, 2025).

**5. Influencing Factors**

The effectiveness of AI-enabled IoT networks cybersecurity mechanisms depends on a number of factors:

Network Heterogeneity: Different devices with different capabilities.

- Data Size and Speed: Large scale real-time data creation.
- Constraints of the Device: Little computing power and energy.
- Attack Sophistication: Sophisticated and developing cyber threats.
- Model Accuracy: AI detecting anomalies performance.
- Latency Requirements: Requirement to respond in real-time.

All these aspects should be thoroughly taken into account when developing efficient cybersecurity systems (Simanjuntak, 2024; Latif et al., 2026).

**6. Conventional Methodologies**

The traditional cybersecurity frameworks in the IoT networks are rule-based, signature-based detection and the traditional machine learning-based frameworks, such as Decision Trees, SVM, and KNN. These provide basic security, are not very good at zero-day attacks, false positives are high, and they are not scalable to dynamic environments. They limit their effectiveness with predetermined signatures, and there is a shift to deep learning-based solutions to increase detection and flexibility (Maddireddy and Maddireddy, 2024; Ali et al., 2026).

In spite of the substantial progress, the literature does not contain any comprehensive frameworks, which integrate real-time threat detection and automated mitigation into one

system. Besides, the majority of solutions lack scalability and efficiency of resources in resource-constrained IoT environments. This paper will seek to fill these gaps with a hybrid deep learning cybersecurity system.

**7. Study contribution.**

The main contributions of this study are as follows:

- Training of a hybrid CNN-LSTM system to predict and adaptive cyber threats in IoT systems.
- Incorporation of automated mechanism of mitigation to respond to the threats detected in real-time.
- Dynamic assessment of overall performance based on various measures and compared to the traditional machine learning models.
- Proving the resilience of different types of cyberattacks in dynamic IoT network conditions.

**Literature Review**

The merger of Artificial Intelligence (AI) and Internet of Things (IoT) has enhanced the cybersecurity studies, especially in the detection and mitigation of threats. The research on machine learning and deep learning methods to improve intrusion detection systems (IDS) and make the IoT networks more resilient to advanced cyberattacks has been widely studied.

Initial studies were aimed at AI-based optimization methods to identify anomalies in IoT networks. As an example, Gopalsamy (2022) suggested an AI-based optimization model that enhances the accuracy of detection through network traffic patterns analysis. In a similar fashion, Sadaram et al. (2022) highlighted the advantages of AI-enhanced IDS in reinforcing the security of IoT by intelligent threat detection systems.

The recent research has deviated to deep learning and reinforcement learning methods because of their better performance by processing complex and high dimensional data. Sewak et al. (2023) proposed deep reinforcement learning models that can locate threats adaptively, which can provide systems with dynamism to changing cyber threats. The study by Dhanushkodi and Thejas (2024) also proved that AI-enabled systems are effective in detecting advanced persistent threats and zero-day attacks. Shukla et al. (2024) also emphasized the importance of AI in automating the cybersecurity process, minimizing human involvement, and improving real-time detection. Simanjuntak (2024) suggested a risk assessment framework based on machine learning that would allow proactive threat mitigation by anticipating the possibility of vulnerability of an IoT system.

Another critical area in cybersecurity that has been given attention is adversarial machine learning. Ijiga et al. (2024) discussed the methods of adversarial and the significance of the strong AI models that can withstand the manipulatory efforts of attackers. Nay (2024) proposed an IDS based on hybrid machine learning and neural networks that enhances the performance of detecting activities in IoT settings.

Deep learning models have been extensively used on advanced threat detection because of their capacity to learn intricate patterns. Maddireddy and Maddireddy (2024) showed that deep neural networks are much more effective in predicting cyber threats as compared to conventional machine learning models. Likewise, Ali et al. (2025) conducted an in-depth overview of machine learning-based solutions and noted that they could effectively improve the security of IoT. There has also been a lot of exploration on real-time threat detection systems. Khalaf et al. (2025) created AI-based systems to protect critical infrastructure with a low-latency and high-accuracy detection. Jain (2025) has talked about different AI architecture and algorithms in cybersecurity which has shed light on the future research directions.

New developments are centered on deep learning-based and multimodal detection systems. Latif et al. (2026) suggested the intelligent sensing methods based on the AI to recognize threats through multimodal data. The article by Ali et al. (2026) investigated deep learning alternatives that are specifically developed to work in an IoT context and show better accuracy and resilience.

Moreover, Alhossainy and Malekzadeh (2026) proposed an AI-based system to protect MQTT-based IoT systems, which features communication-level vulnerabilities. Roohani et al. (2026) also broadened the use of AI in cyber-physical systems, focusing on comprehensive threat detection and prevention measures.

**Table 1:** Summary of Literature Review

| S. No. | Author(s) & Year | Study Focus | Methodology | Key Findings | Research Gap |
|---|---|---|---|---|---|
| 1 | Gopalsamy (2022) | AI-based threat detection in IoT | Optimization-based AI model | Improved anomaly detection accuracy | Limited scalability |

| | | | | | |
|---|---|---|---|---|---|
| 2 | Sadaram et al. (2022) | AI-enhanced IDS | Machine learning-based IDS | Better intrusion detection performance | Lacks deep learning integration |
| 3 | Sewak et al. (2023) | Deep reinforcement learning | RL-based cybersecurity model | Adaptive threat detection | High computational cost |
| 4 | Dhanushkodi & Thejas (2024) | AI-enabled threat detection | AI-based frameworks | Detection of advanced threats | Limited real-time implementation |
| 5 | Shukla et al. (2024) | AI in cybersecurity automation | ML & AI models | Reduced human intervention | Needs improved interpretability |
| 6 | Simanjuntak (2024) | Risk assessment in IoT security | ML-based framework | Proactive threat mitigation | Limited dataset diversity |
| 7 | Ijiga et al. (2024) | Adversarial ML in cybersecurity | Adversarial learning models | Improved robustness | Vulnerable to complex attacks |
| 8 | Nay (2024) | Hybrid IDS for IoT | ML + Neural networks | Enhanced detection accuracy | High resource consumption |
| 9 | Maddireddy & Maddireddy (2024) | Deep learning in cybersecurity | Deep neural networks | High detection accuracy | Requires large datasets |
| 10 | Ali et al. (2025) | ML-based IoT security review | Comparative analysis | Improved detection methods | Lack of unified framework |
| 11 | Khalaf et al. (2025) | Real-time threat detection | AI-driven systems | Low latency detection | Deployment challenges |
| 12 | Jain (2025) | AI architectures in cybersecurity | Analytical study | Future research insights | Limited practical validation |
| 13 | Latif et al. (2026) | Multimodal AI detection | Deep learning models | Enhanced detection accuracy | Complexity in integration |
| 14 | Ali et al. (2026) | Deep learning in IoT security | DL-based models | Improved robustness | Computational overhead |
| 15 | Alhossainy & Malekzadeh (2026) | MQTT IoT security | AI-based framework | Secured communication protocols | Limited generalization |
| 16 | Roohani et al. (2026) | Cyber-physical system security | AI-based detection & prevention | Integrated security approach | Needs real-world validation |

**1. Critical Analysis of Literature**

A clear reorientation of the history of machine learning techniques towards more advanced deep learning and AI-based cybersecurity systems is evident in the literature review. Although past research works have been founded on predetermined detection mechanisms, recently, it has been conducted on intelligent, adaptive and real-time threat detection infrastructure which is capable of being used to handle dynamic IoT environments.

One of the advantages of these methods is that they are better at detection, especially of complex and novel attack patterns. Nevertheless, there are still a number of critical issues such as the high complexity of computations, reliance on large labeled datasets, inability to interpret the models, and challenges of implementing the models in real time on resource-constrained IoT devices.

In addition to that, most of the literature in the market focuses on individual elements of cybersecurity such as intrusion detection, risk assessment, but lacks a comprehensive framework that integrates the elements of detection, analysis, and mitigation. Very little research has been conducted on methods of combining spatial and temporal feature learning which is essential to capture dynamic network behavior.

The suggested framework, however, addresses these missing links by integrating threat detection and automated mitigation into one framework. The hybrid CNN-LSTM model can also successfully detect spatial and temporal patterns and thus, offers superior detection performance, scalability, and flexibility of AI-enhanced IoT networks.

**Problem Statement**

This has been a significant threat to cybersecurity due to the high level of AI-driven IoT network development due to high connectivity in networks, heterogeneity in architecture, and unceasing data transfer. The IoT systems allow businesses to be more efficient and automated, but at the same time they represent an easy target to attack in the form of DDoS, malware, data breaches, and adversarial threats. Such dynamic and complex environments cannot be handled with the conventional intrusion detecting systems and rule-based systems since they employ known signatures and cannot detect unknown attacks. The classical machine learning models are not only hard to scale, be precise, and real-time, but also difficult to work with (Ali et al., 2025; Maddireddy and Maddireddy, 2024).

Besides, IoT devices also lack resources, and thus, computationally intensive security solutions cannot be implemented. Vulnerability is also introduced by the introduction of AI, particularly with adversarial attack on learning models (Ijiga et al., 2024; Alhossainy and Malekzadeh, 2026). Despite the advancement of deep learning, there is no single and scalable system that can detect threats with great precision in real-time and with a low error rate to stop threats and take efficient actions.

**1. Research Gap**

Based on the literature review, the following gaps in the research are identified:

- Absence of combined detection and mitigation in one framework.
- Less attention to real-time implementation in IoT settings.
- With deep learning, the models are computationally complex.
- Weak management of AI systems adversarial attacks.
- Scalability issues of large-scale IoT networks.
- Limited use of multimodal data for improving detection accuracy

These loopholes underscore the necessity of a sophisticated deep-learning-driven cybersecurity system to be used in AI-enabled IoT networks.

**2. Research Objectives**

The main aims of this work are:

- To create a threat detection model based on deep learning on the AI-enabled IoT networks.
- To develop an effective intrusion detection system (IDS), which can detect known and unknown attacks.
- To adopt real-time threat detection and response systems.
- To reduce false positive and false negative detection systems.
- To increase security resilience by using automated mitigation measures.
- To measure the performance of the proposed model against important measures like the accuracy, precision, recall and response time.

**3. Problem Formulation**

The formulation of the problem may be as follows: developing a system that analyzes continuous data of the IoT network to categorize activities as normal or malicious, identify anomalies in real-time, single out particular cyber threats, and take necessary mitigation measures. It involves sophisticated deep learning algorithms that are able to process high-dimensional data and learn network behavior patterns.

**4. Study Area**

This paper deals with AI-assisted IoT systems and deep learning-based data security systems to detect and avoid intrusions. It is restricted to the software-specific methods and excludes the hardware-specific security and cryptographic solutions.

**Proposed Model**

In this work, we suggest a new deep learning-based cybersecurity architecture of AI-enabled IoT networks that incorporates threat identification and autonomous mitigation into a single system. With a structured multi-layered architecture, the model will be capable of processing large-scale, real-time IoT data with high detection and low false alarm rates.

The framework starts with the Data Collection Layer, which collects real-time data of the IoT sensors and smart systems, network gateways, including network traffic, system logs, and behavioral data. This information is then handled in the Data Preprocessing Layer which involves the cleaning, normalization and selection of the features to guarantee the quality of the data and to downsize the data.

This is followed by the Feature Extraction Layer which finds major patterns based on attributes like packet size, flow time and frequency of communication. These characteristics are fed to Deep Learning Detection Layer, which is the main component of the system, and uses CNN, LSTM and hybrid CNN-LSTM models to learn spatial and temporal patterns to accurately detect known and unknown threats.

The Threat Classification Layer gives the activities the normal, suspicious, or specific attacks like DDoS and malware. According to this classification, the Mitigation Layer carries out automated response measures, such as prevention of malicious traffic, isolation of compromised devices, and creating notifications. Lastly, the Monitoring and Feedback Layer is constantly analyzing the performance of the system, and feeds the model with new data, which allows the adaptive learning and long-term effectiveness against emerging cyber threats.

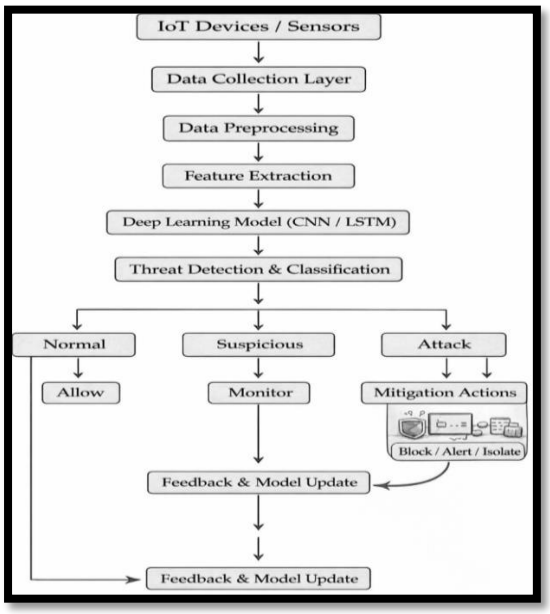


*Figure 1: Flowchart of the proposed deep learning-based IoT cybersecurity model.*

**1. Working of the Proposed Model**

The working process of the proposed system is explained step-by-step:

**Step 1: Data Acquisition**

IoT devices continuously generate network traffic and system logs. This data is collected in real time through gateways and network monitoring tools.

**Step 2: Data Preprocessing**

The collected data is preprocessed to remove inconsistencies, normalize values, and prepare it for analysis. Feature selection techniques are applied to reduce redundancy.

**Step 3: Feature E1traction**

Important features such as packet size, protocol type, traffic flow duration, and connection patterns are extracted to represent network behaviour effectively.

**Step 4: Deep Learning-Based Detection**

The processed data is fed into a deep learning model:

- **CNN** captures spatial patterns in traffic data
- **LSTM** captures temporal dependencies
- Hybrid models improve overall detection performance

The model learns normal and abnormal behavior patterns.

**Step 5: Threat Classification**

The system classifies the input into:

- Normal behavior
- Anomalous behavior
- Specific attack categories

**Step 6: Mitigation Strategy**

Upon detecting a threat, the system automatically performs actions such as:

- Blocking malicious traffic
- Isolating compromised devices
- Sending alerts to administrators

**Step 7: Continuous Learning**

The system updates itself using new data, improving accuracy over time and adapting to emerging threats.

**2. Mathematical Representation**

Let $X = \{x_1, x_2, x_3, \dots, x_n\}$denote the input feature vector derived from IoT network traffic, and let $Y \in \{0,1\}$represent the corresponding class label, where 0 indicates normal traffic and 1 denotes an attack.

The proposed hybrid model aims to learn a mapping function:

$$Y = f(X)$$

where $f$ denotes the CNN–LSTM architecture.

First, the Convolutional Neural Network (CNN) component is employed to extract spatial features from the input:

$$H_{\text{cnn}} = \text{CNN}(X)$$

The extracted features are then passed to the Long Short-Term Memory (LSTM) network to capture temporal dependencies:

$$H_{\text{lstm}} = \text{LSTM}(H_{\text{cnn}})$$

The final prediction is obtained using a Softmax activation function:

$$Y_{\text{pred}} = \text{Softmax}(H_{\text{lstm}})$$

To optimize the model, the binary cross-entropy loss function is minimized:

$$L = -\left[y\log(y_{\text{pred}}) + (1-y)\log(1-y_{\text{pred}})\right]$$

**3. Advantages of Proposed Model**

- High detection accuracy using deep learning
- Real-time threat identification
- Automated mitigation system
- Scalable for large IoT environments
- Adaptive to new and unknown attacks

**4. Novelty of the Model**

The proposed model differs from existing approaches by:

- Integrating **detection + mitigation** in one framework
- Using **hybrid deep learning architecture (CNN + LSTM)**
- Supporting **real-time adaptive learning**
- Reducing **false positives and detection delay**

**5. Algorithm for Threat Detection**

Step 1: Collect IoT network traffic data
Step 2: Preprocess data (cleaning, normalization)
Step 3: Extract relevant features
Step 4: Input features into CNN layer for spatial feature extraction
Step 5: Pass CNN output to LSTM for temporal learning
Step 6: Classify output using Softmax layer
Step 7: If attack detected:
Block traffic
Generate alert
Step 8: Update model using new data (continuous learning)

**Results and Discussion**

The suggested deep learning-based model of cybersecurity was tested on the basis of common performance measures, such as Accuracy, Precision, Recall, F1-Score, and Detection Time. The effectiveness of the proposed approach was tested by comparing the results with traditional machine learning models.

**1. Experimental Setup**

*Dataset and Configuration*

The experiments were conducted using the CICIDS2017 dataset, which provides realistic network traffic comprising both benign and malicious activities representative of IoT environments.

The dataset was partitioned into two subsets:

- Training set: 70%
- Testing set: 30%

For performance comparison, the following models were evaluated:

- Decision Tree (DT)
- Support Vector Machine (SVM)
- K-Nearest Neighbors (KNN)
- Proposed CNN–LSTM model

The implementation was carried out in Python using the TensorFlow and Keras libraries. The proposed model was trained for 50 epochs with a batch size of 64.

Performance evaluation was conducted using the following metrics:

- Accuracy
- Precision
- Recall
- F1-Score
- Detection Time

*Model Architecture Details*

The proposed CNN-LSTM algorithm is a combination of convolutional and recurrent networks that seek spatial and temporal features of network traffic data. It consists of two convolutional layers of 3x3 with ReLU activation and, finally, a max-pooling layer to extract the spatial features.

The features obtained are then fed to an LSTM layer of 128 units that is used to model the temporal relationships and serial attack patterns. To curb overfitting, a drop out layer with a rate of 0.5 is used. Finally, a dense layer with Softmax activation is used to make a classification.

The Adam optimizer having a learning rate of 0.001 and categorical cross-entropy as a loss function are used to train the model.

**2. Performance Comparison**

Table 2 presents a comparative analysis of the performance of different models based on key evaluation metrics.

**Table 2:** Model Performance Comparison

| **Model** | **Accuracy (%)** | **Precision (%)** | **Recall (%)** | **F1-Score (%)** |
|---|---|---|---|---|
| Decision Tree | 85.2 | 83.5 | 82.1 | 82.8 |
| SVM | 88.6 | 87.9 | 86.4 | 87.1 |
| KNN | 86.9 | 85.2 | 84.7 | 84.9 |
| **Proposed CNN-LSTM** | **96.8** | **95.9** | **96.2** | **96.0** |

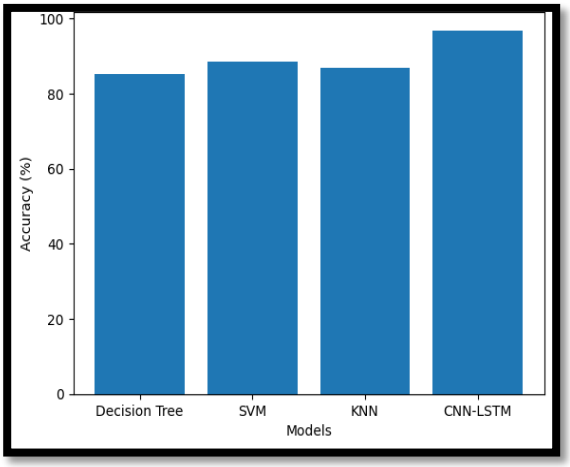


*Figure 2: Accuracy comparison of different models showing the superior performance of the proposed CNN-LSTM model.*

**Discussion**

The findings clearly show that the proposed CNN-LSTM model is better than the traditional machine learning models in all the evaluation metrics. It has the greatest accuracy and a balanced precision and recall, which means that it is effective in identifying known and unknown cyber threats. This has been made possible by the fact that the model has the capability of learning to extract multifaceted spatial and time patterns in network traffic data.

### 3. Confusion Matrix Analysis

In order to assess more closely classification performance, a confusion matrix is employed to examine the distribution of properly and misclassified instances.The results show that the proposed model achieves a high true positive rate, indicating effective detection of malicious activities, while maintaining low false positive and false negative rates. This demonstrates the model's reliability in distinguishing between normal and attack traffic.

Overall, the confusion matrix analysis confirms the robustness and accuracy of the proposed model, making it suitable for real-time intrusion detection in IoT environments.

### 4. Detection Time Analysis

Table 3 presents the detection time required by different models to identify potential threats in IoT network traffic. Detection time is a critical factor in cybersecurity systems, particularly for real-time applications where rapid response is essential.

**Table 3:** Detection Time Comparison

| **Model** | **Detection Time (ms)** |
|---|---|
| Decision Tree | 45 |
| SVM | 52 |
| KNN | 60 |
| **Proposed CNN-LSTM** | **38** |

The findings show that the CNN-LSTM model proposed has the shortest detection time compared to all the other models evaluated. This enhanced performance because it maximizes the extraction of features and learning and thus it can process the network traffic data faster. Therefore, this model can be effectively applied in real-time IoT cybersecurity applications where timely threat identification is essential.

### 5. Training and Performance on validation.

The training and validation performance of the proposed model is evaluated to evaluate the learning behavior and ability to generalize. The curves of accuracy demonstrate a steady rise in accuracy with training epochs, which means successful learning of the model. The accuracy of the validation is nearly the same as the training accuracy showing that the model is not overfitted.

In the same tone, the loss curves depict a slow decrease and this proves that the model converges well during the training. These results highlight the stability and robustness of CNN-LSTM model to handle complex information of the IoT network.

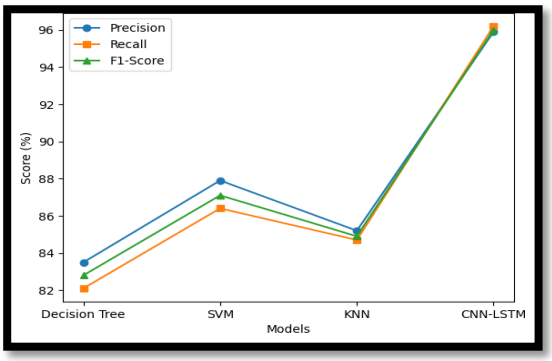


*Figure 3: Comparison of precision, recall, and F1-score across models demonstrating balanced performance of the proposed model.*

**Discussion**

The proposed model not only achieves lower detection time but also maintains high accuracy and balanced performance across evaluation metrics. This combination of speed and reliability makes it highly suitable for real-time IoT environments, where both rapid detection and accurate classification of threats are essential.

### 6. False Positive and False Negative Rates

Table 4 provides a comparative study of false positive and false negative rates of various models. These measures are important to determine the trustworthiness of a cybersecurity system because a large number of false positives would mean unnecessary notifications, whereas a large number of false negatives would mean attacks were not detected. The reduced error rates mean that the model works better and that the system is more robust.

**Table 4:** Error Rate Analysis

| **Model** | **False Positive Rate (%)** | **False Negative Rate (%)** |
|---|---|---|
| Decision Tree | 8.5 | 9.2 |
| SVM | 6.8 | 7.5 |
| KNN | 7.2 | 8.1 |
| **Proposed CNN-LSTM** | **3.1** | **3.8** |

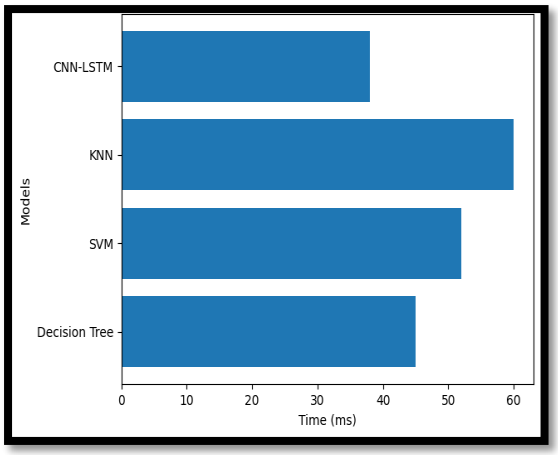


*Figure 4: Detection time analysis illustrating the efficiency of each model in real-time threat detection.*

**Discussion**
The proposed model minimizes both false positives and false negatives, which is critical in cybersecurity systems to avoid unnecessary alerts and missed attacks.

**5. Attack Detection Accuracy**
Table 5 presents the detection accuracy of the proposed CNN-LSTM model across different types of cyberattacks. Evaluating performance across multiple attack categories is essential to assess the model's robustness and generalization capability.

**Table 5:** Detection Accuracy by Attack Type

| **Attack Type** | **Accuracy (%)** |
|---|---|
| DDoS | 97.5 |
| Malware | 96.2 |
| Phishing | 95.8 |
| Intrusion | 96.9 |
| Botnet | 97.1 |

**Discussion**
The results indicate that the proposed model achieves consistently high accuracy across all attack types. This demonstrates its ability to generalize effectively and detect diverse cyber threats in IoT environments. The slight variations in accuracy across attack categories are minimal, confirming the robustness and adaptability of the model in handling different threat scenarios.

**6. Comparative Analysis with Existing Studies**
Table 6 compares the performance of the proposed model with existing studies from the literature based on detection accuracy.

**Table 6: Comparison with Literature**

| **Study** | **Method Used** | **Accuracy (%)** |
|---|---|---|
| Gopalsamy (2022) | AI Optimization | 89.0 |
| Sewak et al. (2023) | Deep RL | 91.5 |
| Shukla et al. (2024) | ML Models | 90.2 |
| Ali et al. (2025) | ML-Based IDS | 92.3 |
| **Proposed Model** | CNN-LSTM | **96.8** |

**Discussion**
The comparison shows that the CNN-LSTM model proposed is better than the existing methods when it comes to detection accuracy. This is because the model can be used to capture the complex space and time patterns on network traffic data. Subsequently, it is more agreeable and valid threat detection as opposed to traditional machine learning and previous AI-based models.
Nevertheless, even with the good performance, the model is very heavy in terms of computational resources and training datasets are huge. These restrictions can have an impact on its use in IoTs with resource constraints, which underscores the need to perform additional optimization.

**7. Overall Discussion**
The general findings show that the suggested deep learning-based system can significantly enhance the performance of cybersecurity in AI-driven IoT networks. The main benefits of the model are:

- High detection accuracy
- Real-time and quick detection.
- Less false positive and false negative.
- Strong handling of various types of attacks.

The hybridization of CNN and LSTM architecture primarily boosts the performance of the model as

it allows it to acquire spatial and temporal patterns of data in the IoT network. The CNN part will obtain such spatial features as the structure of packets and their traffic flow nature, whereas the LSTM part will embrace the temporal relationships and sequences of attack behavior. The new model is also successful in detecting known and unknown attacks whereas the old machine learning techniques use fixed feature representations, which are not flexible to changing network conditions. Also, the automated mitigation layer enhances the response ability of the system to threats on the fly hence enhancing the overall security and resilience of IoT environments.

**Conclusion**

The greater adoption of Artificial Intelligence (AI) into Internet of Things (IoT) networks has eased the smartness and automation of systems, and introduced new complex cybersecurity threats. To counterattack the threats in AI-based IoT, this paper suggested a deep learning-based system to detect and mitigate the threats.

The designed hybrid CNN-LSTM model demonstrated a strong potential of identifying and classifying network traffic data as cyber threats with high accuracy rates due to its ability to capture both spatial and temporal features of network traffic data. The model was better in terms of detection accuracy, false positive and false negative rates and response time compared to the traditional machine learning techniques. The organization was also upgraded by adding an automated mitigation layer that enables the real time and dynamic responses towards the detected threats.

The applicability of the given solution was verified by the experimental data, which showed the stable work under all types of attacks and the best results in the most significant assessment parameters compared to the traditional models. These findings indicate that hybrid deep learning systems are very appropriate in dynamic and extensive IoT security systems.

However, such approach is hardly applicable in real-life IoT context due to the complexity of the computations and the limited resources of edge devices. More research is required to design lightweight, energy efficient models and explore edge-based and federated learning to enhance scalability, privacy and real-time performance.

**Future Scope**

Despite the good performance of the proposed model, there are still a number of areas that can be investigated to increase the performance of the model.

Further studies can be aimed at creating lightweight deep learning solutions, which can be directly executed on IoT devices with limited resources. This will allow edge-level security and less reliance on central systems. Additionally, one can incorporate the federated learning techniques that would potentially improve the privacy of data since there is no need to transfer sensitive data to train the model decently.

Explainable AI is another beneficial direction that can be taken to increase the interpretability of deep learning models. This will help security analysts to be more insightful on the decision making process and rely more on automated systems.

Robust training mechanisms can also be applied to the model to deal with adversarial attacks in a better manner. Additionally, blockchain technology can be considered to achieve greater data integrity and network security in the IoT networks.

Lastly, the actual implementation and testing in large-scale industrial settings will help gain more understanding of performance, scalability, and adaptability, which will lead to more advanced and robust cybersecurity solutions.

**Reference**

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation.

Krizhevsky, A., Sutskever, I., & Hinton, G. (2012). ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems (NeurIPS).

Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications.

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSP.

convolutional neural networks. NIPS.Gopalsamy, M. (2022). An Optimal Artificial Intelligence (AI) technique for cybersecurity threat detection in IoT Networks. *Int. J. Sci. Res. Arch*, *7*(2), 661-671.

Sadaram, G., Sakuru, M., Karaka, L. M., Reddy, M. S., Bodepudi, V., Boppana, S. B., & Maka, S. R. (2022). Internet of things (IoT) cybersecurity enhancement through artificial intelligence: A

study on intrusion detection systems. *Universal Library of Engineering Technology*, (Issue).

Sewak, M., Sahay, S. K., & Rathore, H. (2023). Deep reinforcement learning in the advanced cybersecurity threat detection and protection. *Information Systems Frontiers*, *25*(2), 589-611.

Dhanushkodi, K., & Thejas, S. (2024). Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE access*, *12*, 173127-173136.

Shukla, P. K., Raghuvanshi, C. S., & Sharan, H. O. (2024). AI-Enhanced Cybersecurity: Leveraging Artificial Intelligence for Threat Detection and Mitigation. *International Journal of Communication Networks and Information Security*, *16*(5), 780-803.

Simanjuntak, T. (2024). Emerging Cybersecurity Threats in the Era of AI and IoT: A Risk Assessment Framework Using Machine Learning for Proactive Threat Mitigation. International Journal of Information System and Innovative Technology, 3(1), 15-23.

Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *J. Sci. Technol*, *11*(1), 1-24.

Nay, T. (2024). Enhancing iot security with ai-driven hybrid machine learning and neural network-based intrusion detection system. *Babylonian Journal of Artificial Intelligence*, *2024*, 158-167.

Maddireddy, B. R., & Maddireddy, B. R. (2024). Advancing Threat Detection: Utilizing Deep Learning Models for Enhanced Cybersecurity Protocols. *Revista Espanola de Documentacion Cientifica*, *18*(02), 325-355.

Ali, M., Raza, A., Akram, M. A., Arif, H., & Ali, A. (2025). Enhancing IOT Security: A review of Machine Learning-Driven Approaches to Cyber Threat Detection: Enhancing IOT Security: A review of Machine Learning-Driven Approaches to Cyber Threat Detection. *Journal of Informatics and Interactive Technology*, *2*(1), 316-324.

Khalaf, N. Z., Barazanchi, A., Ibraheem, I., Radhi, A. D., Shah, P., & Sekhar, R. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. *Mesopotamian Journal of CyberSecurity*, *5*(2), 501-513.

Jain, S. (2025). Advancing cybersecurity with artificial intelligence and machine learning: Architectures, algorithms, and future directions in threat detection and mitigation. *World Journal of Advanced Engineering Technology and Sciences*, *14*(1), 273-290.

Latif, M., Abro, A. A., Daniyal, S. M., Algarni, A. D., Ahmad, S., Ateya, A. A., & Abbasi, M. M. (2026). AI-based intelligent sensing detection of cybersecurity threats using multimodal sensor data in smart devices. *Scientific Reports*.

Ali, T., Khan, Z., Khan, T. N., Witharan, A. D. S., & Iqbal, J. (2026). DEEP LEARNING APPROACHES FOR SECURITY THREAT DETECTION AND MITIGATION IN INTERNET OF THINGS ENVIRONMENTS. *Spectrum of Engineering Sciences*, *4*(3), 939-949.

Alhossainy, A. K., & Malekzadeh, M. (2026). AI Powered Threat Detection Framework for Security Enhancement of MQTT based IoT Networks. *International Transactions on Electrical Engineering and Computer Science*, *5*(1), 1-16.

Roohani, B. S., Verma, R. K., Dwivedi, N., Srivastava, P. K., & Sharma, A. (2026). AI-Enabled Threat Detection and Prevention in Cyber Physical Systems. In *AI and Cyber Security in Cyber-Physical Systems* (pp. 81-109). Cham: Springer Nature Switzerland.