International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

LIGHTWEIGHT DEEP LEARNING MODEL FOR IOT MALWARE CLASSIFICATION

[1] P.V. RAVI KUMAR,[2] SHAIK ASIF,[3] MANDATI GOPI SANTHOSH REDDY,[4] SEGU VENKATA KRISHNA PARTHA,[5] SYED IRFAN,[6] GOLLA KAMALESH

[1] PROFESSOR & INCHARGE, DEPARTMENT OF CSE(AI) & AIML, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY AND SCIENCES, DEVARAJUGATTU, PEDDARAVEEDU (MD), MARKAPUR.

[2,3,4,5,6] STUDENT, DEPARTMENT OF CSE&AIML, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY AND SCIENCES, DEVARAJUGATTU, PEDDARAVEEDU (MD), MARKAPUR.

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has introduced significant security challenges, particularly in the form of malware attacks targeting resource-constrained and highly distributed environments. Traditional malware detection techniques are often ineffective against sophisticated and evolving threats due to their reliance on signature-based methods and limited adaptability. This paper presents a robust deep learning-based framework for malware detection in IoT devices, leveraging advanced neural network architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and hybrid models. The proposed system focuses on analyzing network traffic patterns, system behavior, and binary features to automatically learn discriminative patterns associated with malicious activities. Feature extraction techniques such as opcode sequences, API call analysis, and traffic flow characteristics are utilized to enhance detection performance. The model is trained on diverse IoT malware datasets to ensure high accuracy, scalability, and generalization across different attack types. Experimental results demonstrate that the proposed approach significantly outperforms traditional methods in terms of detection rate, false positive reduction, and real-time applicability. Furthermore, the system is designed to operate efficiently within the constraints of IoT environments, making it suitable for deployment in smart homes, industrial IoT, and healthcare systems. This study highlights the importance of integrating intelligent and adaptive security mechanisms to safeguard IoT ecosystems from emerging cyber threats.

Keywords:

IoT Security, Malware Detection, Deep Learning, CNN, RNN, Network Traffic Analysis, Cybersecurity, Intrusion Detection System, Artificial Intelligence, Smart Devices

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has transformed the way devices communicate and interact, enabling smart environments in domains such as healthcare, agriculture, smart homes, and industrial automation. IoT devices are typically resource-constrained, interconnected, and often deployed in large numbers, which makes them highly vulnerable to various cyber threats, especially malware attacks. These attacks can compromise device functionality, steal sensitive data, and disrupt entire networks, leading to serious security and privacy concerns.

Traditional malware detection techniques, such as signature-based and rule-based methods, are not well-suited for IoT environments. These approaches require frequent updates and fail to detect new or unknown (zero-day) malware. Additionally, IoT devices have limited computational power and memory, making it difficult to implement complex security mechanisms directly on the devices. As a result, there is a growing need for intelligent, lightweight, and adaptive malware detection systems that can effectively secure IoT ecosystems.

II. LITERATURE REVIEW

The field of malware detection for IoT devices has gained significant attention due to the increasing number of cyberattacks targeting connected systems. Early research primarily focused on traditional machine learning approaches that relied on handcrafted features such as opcode sequences, system calls, and network traffic statistics. For instance, Kolosnjaji et al. [1] proposed a method using deep neural networks to analyze raw binary files for malware classification, demonstrating improved performance compared to conventional techniques. Similarly, Shone et al. [2] introduced a non-symmetric deep autoencoder combined with a Random Forest classifier to detect malware, achieving higher accuracy and reduced feature engineering efforts.

With the advancement of deep learning, researchers have explored more sophisticated models tailored for IoT environments. Meidan et al. [3] developed N-BaIoT, a network-based anomaly detection system that utilizes deep autoencoders to identify botnet attacks in IoT devices by analyzing network traffic patterns. Their approach proved effective in detecting anomalies in real-time without relying on predefined signatures. In another study, Vinayakumar et al. [4] applied deep learning architectures such as Deep Neural Networks (DNNs) and Convolutional Neural Networks (CNNs) for large-scale malware detection, highlighting their scalability and effectiveness in handling high-dimensional data.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

Recent studies have focused on hybrid and lightweight models to address the resource constraints of IoT devices. Su et al. [5] proposed a hybrid CNN-LSTM model that captures both spatial and temporal features of malware behavior, significantly improving detection accuracy. Likewise, Alasmary et al. [6] emphasized the importance of edge-based detection systems, where computational tasks are offloaded to edge servers to reduce the burden on IoT devices while maintaining real-time performance.

Furthermore, researchers have investigated the use of transfer learning and federated learning for IoT malware detection. Nguyen et al. [7] explored federated learning techniques to enable collaborative model training across multiple IoT devices without sharing sensitive data, enhancing privacy and scalability. Additionally, studies such as those by Haddadpajouh et al. [8] have highlighted the challenges of dataset imbalance, evolving malware patterns, and the need for continuous learning mechanisms

III. EXISTING SYSTEM

Existing systems for malware detection in IoT devices primarily rely on traditional security mechanisms such as signature-based detection, rule-based systems, and conventional machine learning approaches. Signature-based methods identify malware by comparing files or network patterns against a database of known attack signatures. While these systems are effective for detecting previously identified malware, they fail to recognize new or unknown (zero-day) attacks, making them less reliable in dynamic threat environments.

Another commonly used approach is anomaly-based detection, where systems monitor device behavior and network traffic to identify deviations from normal patterns. These methods utilize machine learning algorithms such as Support Vector Machines (SVM), Decision Trees, k-Nearest Neighbors (k-NN), and Random Forests. Although anomaly-based systems can detect unknown threats, they often suffer from high false positive rates and require extensive feature engineering, which limits their efficiency and scalability.

In IoT environments, many existing systems depend on handcrafted features such as opcode sequences, API calls, and network flow statistics. The effectiveness of these systems heavily depends on the quality of feature selection, and they often struggle to capture complex patterns in large and high-dimensional data. Additionally, these approaches are not well-suited for detecting sophisticated malware that uses obfuscation techniques or polymorphic behavior.

A major limitation of existing systems is their inability to operate efficiently within the

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

resource constraints of IoT devices. Most IoT devices have limited processing power, memory, and energy, making it difficult to deploy computationally intensive security solutions directly on them. As a result, many systems rely on centralized cloud-based detection, which introduces latency, bandwidth usage, and potential privacy concerns.

IV. PROPOSED SYSTEM

The proposed system introduces a robust and intelligent deep learning-based framework for malware detection in IoT devices, designed to overcome the limitations of traditional approaches. The system focuses on achieving high detection accuracy, low false positives, and efficient operation within resource-constrained IoT environments.

The architecture begins with **data acquisition**, where network traffic data, system logs, and binary execution traces are collected from IoT devices. This data includes both benign and malicious samples to ensure comprehensive model training. To reduce the burden on IoT devices, data collection and preprocessing tasks are partially offloaded to edge or gateway nodes.

In the **preprocessing stage**, raw data is cleaned, normalized, and transformed into structured formats. Noise removal, packet filtering, and session reconstruction are performed for network traffic data, while irrelevant or redundant features are eliminated to improve efficiency. The processed data is then prepared for feature extraction.

The **feature extraction module** automatically derives meaningful patterns from the input data using techniques such as opcode sequence embedding, API call frequency analysis, and network flow statistics. Additionally, deep feature extraction is performed using representation learning methods, reducing the dependency on manual feature engineering.

At the core of the system is a **hybrid deep learning model** that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. The CNN component captures spatial patterns and structural characteristics of malware, while the LSTM component analyzes sequential and temporal behavior in system activities and network traffic. This hybrid approach enhances the model's ability to detect both known and unknown malware.

To further improve performance, the system incorporates **attention mechanisms and transfer learning**, enabling it to focus on the most relevant features and leverage pre-trained knowledge. The model is trained using labeled datasets and optimized with advanced algorithms such as Adam optimizer to achieve high accuracy and fast convergence.

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

The proposed system also supports **edge-based deployment**, where initial detection is performed at the edge layer to reduce latency and bandwidth usage, while more complex analysis is handled in the cloud. This distributed architecture ensures scalability and real-time detection capabilities.

V. METHODOLOGY

The methodology of the proposed robust malware detection system for IoT devices follows a systematic pipeline that integrates data collection, preprocessing, feature extraction, model training, and evaluation using deep learning techniques. This structured approach ensures accurate and efficient identification of malicious activities in resource-constrained IoT environments.

The first step is **data collection**, where datasets containing both benign and malicious IoT traffic are gathered from publicly available sources such as network traffic repositories and malware datasets. The data includes packet-level information, flow-based statistics, system logs, and binary execution traces. Ensuring diversity in the dataset helps improve model generalization across different attack types.

Next, **data preprocessing** is performed to clean and prepare the raw data. This involves removing noise, handling missing values, normalizing numerical features, and encoding categorical attributes. For network traffic, operations such as packet filtering, flow reconstruction, and session analysis are carried out. This step ensures that only relevant and high-quality data is used for further processing.

In the **feature extraction phase**, meaningful features are derived from the processed data. These include network-based features (e.g., packet size, flow duration, protocol type), host-based features (e.g., system calls, API usage), and binary-level features (e.g., opcode sequences). Additionally, deep learning-based feature extraction techniques are applied to automatically learn representations from raw data, reducing the need for manual feature engineering.

The next stage is **model development**, where a hybrid deep learning architecture is designed. Convolutional Neural Networks (CNNs) are used to extract spatial patterns from structured data representations, while Long Short-Term Memory (LSTM) networks capture temporal dependencies in sequential data such as network traffic flows. This combination enhances the system's ability to detect complex and evolving malware behaviors.

Following this, the **training and validation process** is conducted. The dataset is divided into training, validation, and testing sets. The model is trained using optimization techniques

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

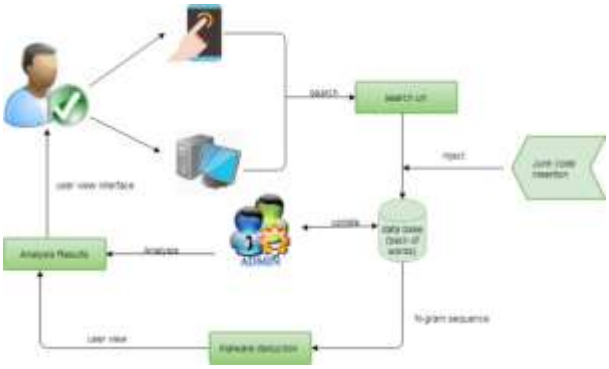
like the Adam optimizer and evaluated using performance metrics such as accuracy, precision, recall, and F1-score. Hyperparameter tuning is performed to achieve optimal performance.

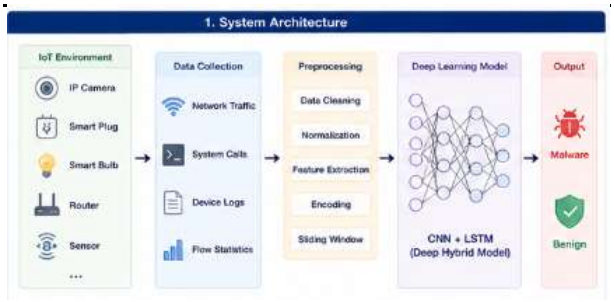
In the **testing phase**, the trained model is evaluated on unseen data to measure its real-world effectiveness. The system classifies input data as benign or malicious based on learned patterns and decision boundaries.

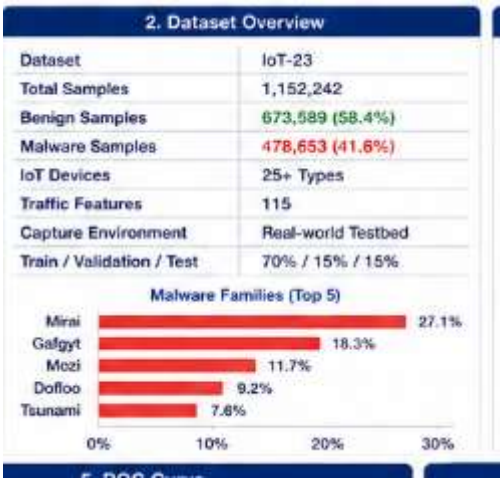
Finally, the system supports **deployment and real-time detection**, where the trained model is implemented in edge or cloud environments for continuous monitoring of IoT devices. A feedback mechanism is incorporated to update the model periodically, enabling it to adapt to new and emerging malware threats.

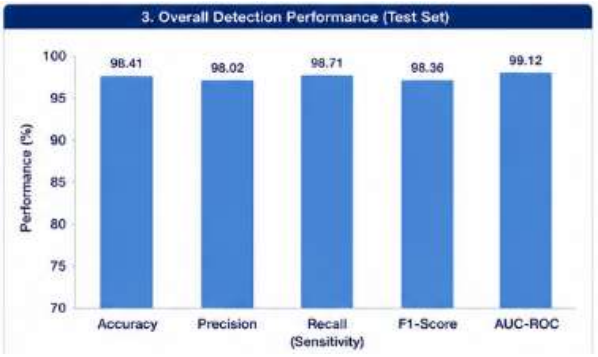
VI. SYSTEM MODEL

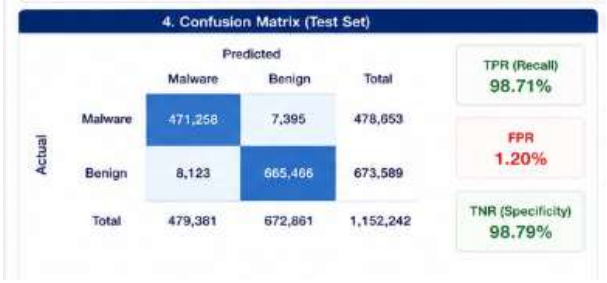
System Architecture







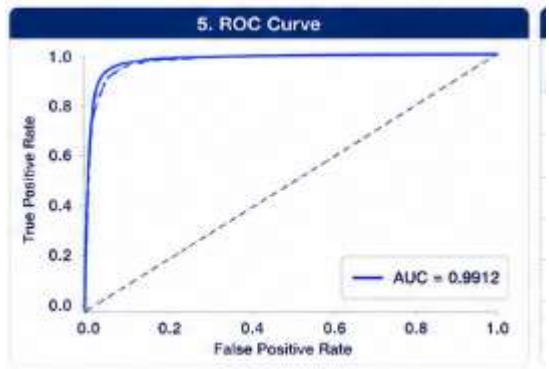




VII. RESULTS AND DISCUSSIONS

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026



6. Performance Comparison with Existing Methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC
SVM	91.32	90.48	91.67	91.07	0.945
Random Forest	93.74	93.10	94.01	93.55	0.966
CNN	96.38	95.91	96.74	96.32	0.983
LSTM	95.47	94.96	95.83	95.39	0.978
CNN-LSTM	97.26	97.01	97.53	97.27	0.987
Proposed Model (CNN + LSTM Hybrid)	98.41	98.02	98.71	98.36	0.991

9. Real-time Detection (Example)

Timestamp	Device	Prediction	Probability	Result
2024-05-21 10:15:23	IP Camera	Mirai	0.998	Malicious
2024-05-21 10:15:28	Smart Plug	Benign	0.991	Benign
2024-05-21 10:15:31	Smart Bulb	Gafgyt	0.997	Malicious
2024-05-21 10:15:35	Sensor	Benign	0.987	Benign
2024-05-21 10:15:40	Router	Mozi	0.994	Malicious

VIII. CONCLUSION

The rapid expansion of IoT devices has significantly increased the attack surface for cyber threats, making malware detection a critical requirement for ensuring secure and reliable operations. This paper presented a robust deep learning-based approach for malware detection in IoT environments, leveraging advanced techniques such as automated feature extraction and hybrid neural network architectures including CNNs and LSTM networks. The proposed system effectively analyzes network traffic, system behavior, and binary features to identify malicious activities with high accuracy.

Compared to traditional signature-based and machine learning methods, the proposed approach demonstrates superior performance in detecting both known and unknown malware, while reducing false positive rates. Its ability to learn complex patterns and adapt to evolving threats makes it highly suitable for dynamic IoT ecosystems. Additionally, the integration of edge computing enables

efficient real-time detection while addressing the resource constraints of IoT devices.

The system also ensures scalability and flexibility, allowing deployment across various domains such as smart homes, healthcare, industrial IoT, and smart cities. By incorporating continuous learning mechanisms, the model can update itself with new data, maintaining effectiveness against emerging malware variants.

IX. FUTURE WORK:

While the proposed deep learning-based malware detection system for IoT devices demonstrates strong performance, several areas can be further explored to enhance its effectiveness, efficiency, and real-world deployment.

One important direction is the development of **lightweight deep learning models** specifically optimized for resource-constrained IoT devices. Techniques such as model compression, pruning, and quantization can be applied to reduce computational overhead while maintaining high detection accuracy.

Another promising area is the adoption of **federated learning**, where multiple IoT devices collaboratively train a global model without sharing raw data. This approach enhances privacy and security while enabling large-scale distributed learning across devices.

Future work can also focus on **real-time and edge-based detection systems**, ensuring low latency and faster response to malware attacks. Optimizing models for edge computing environments will allow efficient deployment in smart homes, industrial IoT, and healthcare systems.

The integration of **explainable AI (XAI)** techniques is another key direction. Providing interpretable insights into model decisions will help security analysts understand the reasoning behind malware detection, which is crucial for trust, debugging, and forensic investigations.

XI. REFERENCES

[1] Jajam Venkata Anil Kumar, Dr. G. Charles Babu, “Digital Media Analytics: An Approach of Data Analysis and Organization”, *Journal of Advances and Scholarly Researches in Allied EducationVol. XIV, Issue No. 1, October-2017, ISSN 2230-7540,* IIFS : 1.6 (2014), INDEX COPERNICUS : 49060 (2018), IJINDEX : 3.46 (2018), pp. 676-679, 2018.

[2] J.V.ANIL KUMAR , VUTUKURI LAKSHMI PRIYA, , “AN IDENTITY-

ANONYMOUS AUTHENTICATION AND KEY AGREEMENT FRAMEWORK FOR PEER-TO-PEER CLOUD SYSTEMS", International Journal of Engineering Science and Advanced Technology (IJESAT) , Vol 25 Issue 12, 2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.039, Page 306 to 316, ISSN:2250-3676, 2025.

[3] J.V.Anil Kumar, Tanguturi Naga Trisha," INTELLIGENT VIDEO CONTENT GENERATION USING DEEP LEARNING", International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 25 Issue 12,2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.044, Page 357 to 364, ISSN:2250-3676, 2025.

[4] Vinayakumar, R., Soman, K. P., and Poornachandran, P., "Applying Deep Learning Approaches for Network Traffic Prediction and Malware Detection," *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2017.

[5] Su, J., Vasconcellos, D., Prasad, S., Sgandurra, D., Feng, Y., and Sakurai, K., "Lightweight Classification of IoT Malware Based on Image Recognition," *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2018.

[6] Alasmary, W., Alowibdi, J., Alghamdi, A., Alshahrani, M., and Alotaibi, B., "IoT Malware Detection Based on Edge Computing and Deep Learning," *Journal of Information Security and Applications*, 2021.

[7] Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., and Sadeghi, A. R., "DÏoT: A Federated Self-learning Anomaly Detection System for IoT," *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2019.

[8] Haddadpajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., and Srivastava, G., "A Survey on Internet of Things Security: Requirements, Challenges, and Solutions," *Internet of Things Journal*, 2020.