International Journal of Technology, Leadership and Sciences (IJTLS)

ISSN: 3107-9083
www.ijtls.com
Research Paper
DOI: https://doi.org/10.5281/zenodo.20799849

# REAL-TIME MALWARE DETECTION FOR IOT SYSTEMS USING DEEP LEARNING TECHNIQUES

**GOPALAKRISHNA KAJA[1], M.ANUSHA[2], DR.VUNNAVA DINESH BABU[3], Dr.CHAVA HARI BABU[4], R.VAMSI KRISHNA[5], D.SRIDHAR[6]**

[1]*M.Tech Student,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[2]*Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[3]*Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[4]*Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[5]*Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[6]*Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

**ABSTRACT:**

Security vulnerabilities, especially malware attacks on resource-constrained systems, have arisen due to the development of Internet of Things (IoT) devices. The dynamic characteristics of contemporary threats render conventional malware detection methods sometimes inadequate for ensuring full protection. This research proposes a solution for virus detection in IoT devices using deep learning techniques.The suggested method employs advanced neural network models to independently identify intricate patterns and features from data on network traffic and device activities. The model attains high precision in identifying both established and novel malware variants by the use of architectures like Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN). The framework is designed to be versatile and adaptive, geared for efficient operation within the constrained processing capabilities of IoT devices.The proposed approach exhibits markedly improved detection accuracy, precision, and a reduced false positive rate compared to traditional machine learning methods, as shown by the experimental results. Moreover, the technology can identify attacks in real-time, hence enhancing the overall security of IoT ecosystems.

**Keywords:** Internet of Things (IoT), Malware Detection, Deep Learning, Cybersecurity, Network Traffic Analysis, Anomaly Detection, Cyber Threat Intelligence, Resource-Constrained Devices.

**Received Date:** 5 June 2026; **Accepted Date:** 15 June 2026; **Published Date:** 20 June 2026;



## I. INTRODUCTION

The Internet of Things (IoT) has revolutionized device communication and interaction across several industries, including transportation, smart homes, healthcare, and industrial automation. The incorporation of IoT devices over networks enables astute decision-making and effortless data interchange. Malware attacks provide a considerable security risk to IoT devices due to their enhanced connection. Such attacks may endanger essential data, interrupt services, and cause substantial financial and operational harm.

IoT devices often demonstrate limitations in processing power, memory, and energy capacity relative to conventional computer systems. Traditional security methods, like signature-based malware detection and intricate encryption techniques, are hindered by these constraints. The fast increase of malware

variants and the diverse characteristics of IoT systems complicate detection efforts, making conventional methods less effective.

Advanced deep learning algorithms provide potential solutions to these difficulties. Unlike traditional models, deep learning algorithms may independently extract representations and patterns from large datasets without requiring human intervention in feature engineering. To identify malicious activity in real-time, techniques like as Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) analyze code patterns, system behavior, and network traffic.

This project intends to use deep learning methodologies to create an effective virus detection solution for Internet of Things devices. The suggested method seeks to improve detection precision while reducing computing expenses and false positives. The solution utilizes powerful algorithms to detect both known and unknown threats, ensuring maximum security of IoT environments.

## II.LITERATURE REVIEW

S. Kumar and R. Patel suggested a virus detection methodology for IoT networks using machine learning methods, including Support Vector Machine (SVM) and Decision Tree. Their methodology enhanced the precision of malware detection compared to traditional techniques. Nonetheless, the system's ability to combat emerging malware threats was constrained by its significant dependence on human feature extraction.

A. Sharma and P. Singh used deep learning models, namely Convolutional Neural Networks (CNN), to independently identify relevant aspects from malware data. Their methodology exceeded conventional machine learning techniques in detection accuracy owing to its less dependence on manually crafted characteristics.

M. Zhang and L. Wang concentrated on virus detection with neural networks, leveraging data obtained from Internet of Things (IoT) network traffic. While requiring substantial datasets for effective model training, their techniques enhanced detection rates and classification effectiveness.

K. Lee and J. Kim created a hybrid deep learning framework that combines Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) architectures to extract temporal and geographical features from IoT malware data. The hybrid approach significantly improved the accuracy of malware detection and categorization.

R. Gupta and N. Verma tackled the issue of limited computing resources in IoT devices by developing a lightweight malware detection method. Their method enabled effective functioning in resource-limited IoT environments while maintaining sufficient detection precision.

## III.EXISTING SYSTEM

Contemporary malware detection solutions for IoT devices mostly rely on traditional machine learning approaches and signature-based detection. The simplicity and ease of execution of these treatments make them extensively used.

Signature-based detection techniques may recognize malware by using a repository of established malware signatures. This method is proficient in identifying existing dangers, although it is unable to detect novel types of malware. Thus, zero-day attacks continue to pose a substantial threat in Internet of Things environments.

The anomaly-based detection method is a common choice; it observes system activity and detects any deviations. This approach, although proficient in identifying unknown threats, often proves inaccurate in real-time applications due to its high false positive rates.

The precision of detection has improved owing to the use of machine learning systems, including techniques such as Support Vector Machines (SVM), Decision Trees, and Random Forests. To determine whether an action is harmless or harmful, these systems evaluate characteristics derived from data, such as network traffic and device behavior. In contrast, they are insufficient for handling intricate, large-scale IoT data and need substantial human feature engineering.

Furthermore, the majority of current systems were not designed for IoT applications.

Implementing intricate security frameworks on IoT devices is challenging due to their limited compute capability, memory, and energy resources. Many current solutions lack real-time detection capabilities or are too resource-intensive.

**DISADVANTAGES**

- The amount and velocity of data produced by the Internet of Things provide challenges for current systems.
- Traditional methods may inadequately identify threats in real-time, leading to unmitigated assaults.

## IV.PROPOSED SYSTEM

The suggested approach utilizes sophisticated deep learning techniques to provide a comprehensive malware detection framework for Internet of Things devices, addressing the limitations of standard malware detection methods. The system autonomously pulls significant features from raw data, differentiating it from traditional methods that rely on human feature engineers. This examination of spatial and temporal patterns in IoT data utilizes deep learning architectures, including CNN and RNN. CNN is used for feature extraction from binary data and network traffic, while RNN or LSTM collects sequential activity and detects abnormalities over time. This architecture analyzes data obtained from Internet of Things devices, including system logs, executable files, and network traffic, for categorization and training by feeding it into a deep learning model. Upon concluding training, the model can accurately and immediately categorize incoming data as either benign or malicious. We use lightweight model optimization strategies to guarantee that IoT devices execute tasks efficiently with little computing cost, hence adapting their limited resources. The system may be easily expanded to accommodate the growing number of IoT devices and the changing nature of malware threats. Moreover, it enables continuous learning and real-time monitoring, hence improving security in IoT ecosystems by detecting both established and novel malware variants with reduced false positives.

**ADVANTAGES**

- Capable of effectively handling dynamic malware assaults and vast IoT networks.
- Augments Internet of Things (IoT) security by identifying and countering advanced threats via continuous learning.

## V.SYSTEM MODEL

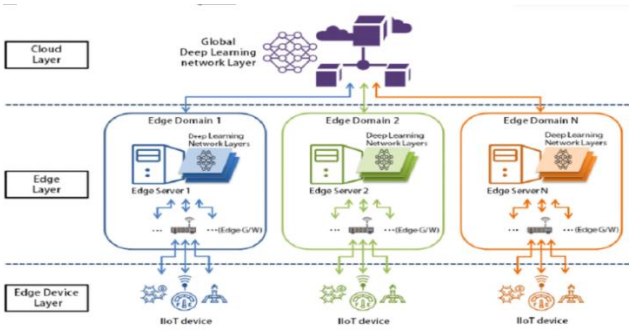



**Fig 1.System Model**

## VI.MODULES

- **IoT Devices Module:**

This category includes Internet of Things (IoT) gadgets, including cameras, smart appliances, and sensors. These devices provide data on device activities, system logs, and network traffic. Malware detection relies on these devices as its main data source.

- **Data Collection Module:**

The data collection module acquires varied information, including network packets, traffic logs, executable files, and system activity records, from IoT devices. A dataset is used to save the gathered data for further study.

- **Data Preprocessing Module:**

This segment prepares the raw data for deep learning model training by cleaning, filtering, normalizing, and transforming. Data preprocessing and feature extraction are then performed to enhance the model's efficacy.

- **Deep Learning Model / Malware Detection Module:**

The system's primary module acquires and classifies data using deep learning techniques, including CNN and RNN/LSTM. The model assesses incoming data for harmful or benign

patterns using geographical and temporal analysis.

- **Classification Module:**

The system then classifies the recognized activity into normal or dangerous categories based on the model's analysis. The detection outcome is generated by the trained deep learning model.

- **Alert System Module:**

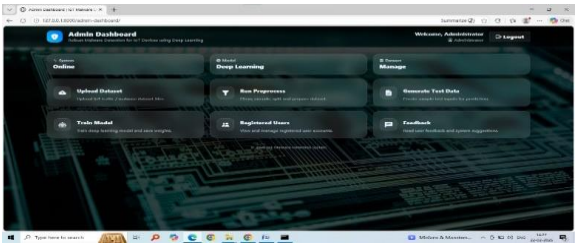
Upon detecting hazardous behavior, the alert system promptly creates warning notifications and relays the findings of malware identification to the monitoring system.

- **User/Admin Notification Module:**

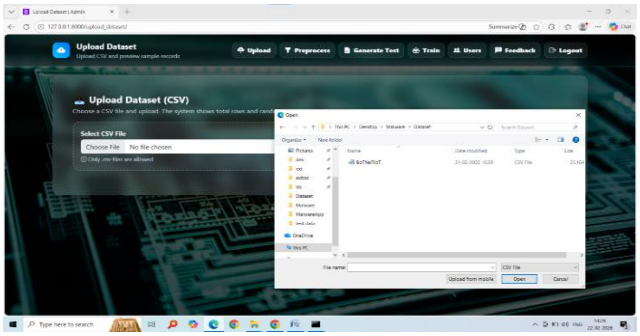
This module's alert notifications facilitate immediate intervention to avert malware assaults and bolster IoT security for the user or system administrator.

## VII.SCREENSHOTS

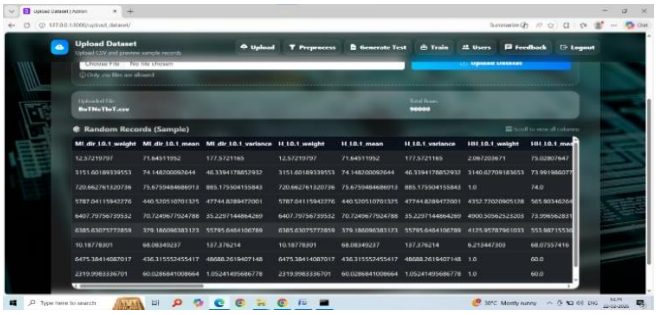

Just click the "Administrator Interface" option. The administrator's login credentials include just "admin" for both the username and password.



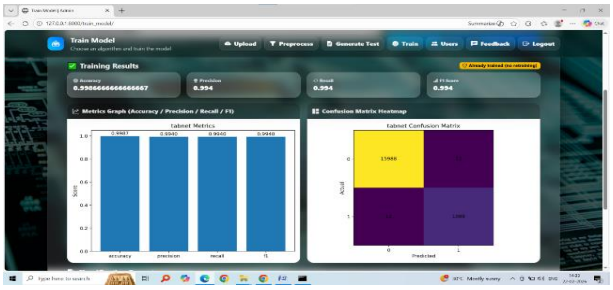

Access the upload dataset module from the admin dashboard.



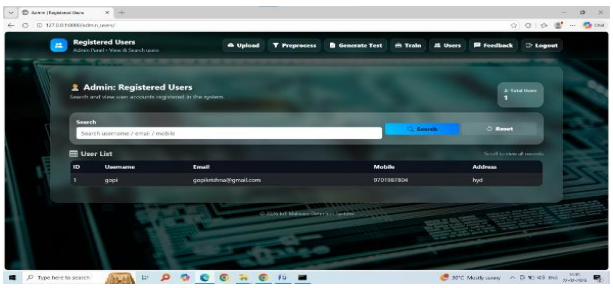

The result shown below is what you may expect after the dataset upload.



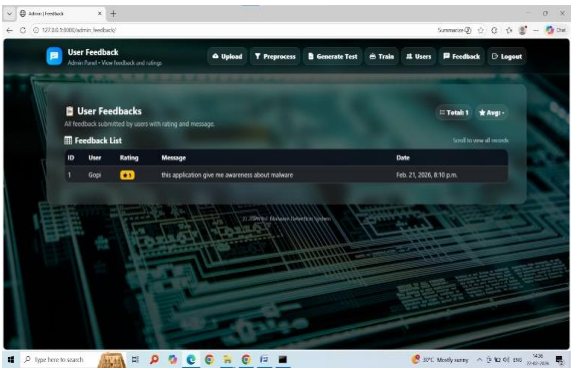

Engage the preprocess module button



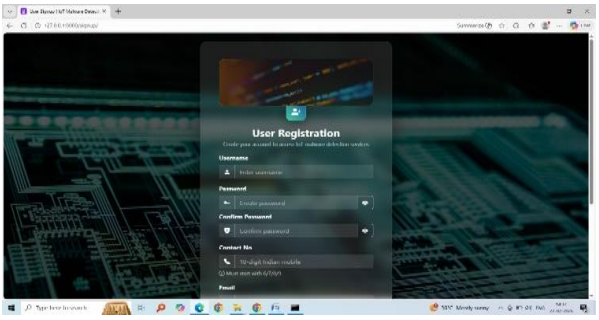

Data obtained during the training phase of the IoT malware detection system using the TabNet deep learning algorithm. The model attained precision, recall, and F1-score around 99.4%, yielding an accuracy of about 99.86%, signifying the system's proficiency in differentiating between IoT devices compromised by malware and those that are uninfected.



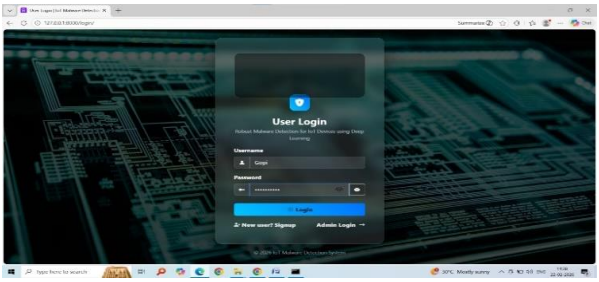
All registered users are available to the administrator. Advance to the next lesson by selecting the button.



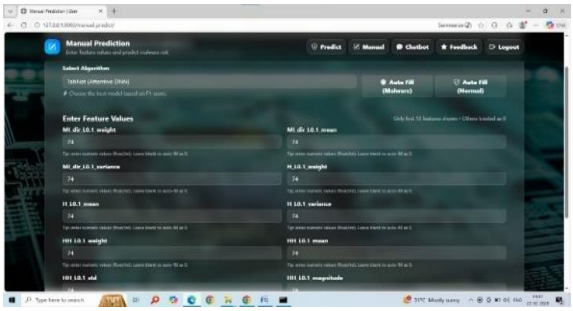

Management have the power to evaluate user-submitted comments.



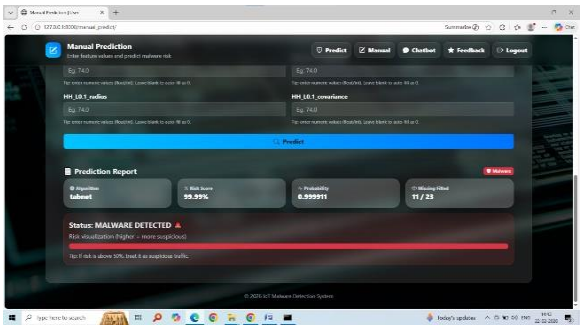

User registration page. After completing your registration, choose "User Login.



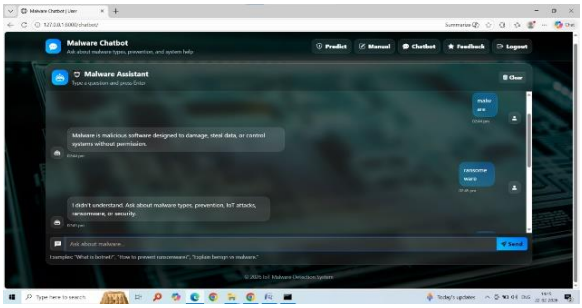

To access the user's application, provide their username and password.

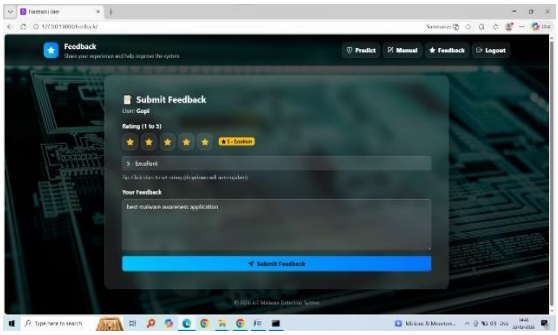



To produce a forecast, insert the data from the text file containing the manual testing information.




This is the outcome for the given parameters. Feel free to ask any questions you may have about malware to increase awareness.




## VIII.CONCLUSION

An advanced and efficient method for detecting harmful actions in IoT settings is Robust Malware Detection for IoT Devices using a Deep Learning algorithm. The system can assess extensive volumes of data from devices and precisely categorize them as benign or harmful using deep learning methodologies. This considerably enhances detection precision relative to conventional signature-based approaches, which often neglect novel or unfamiliar threats.

The integration of components such as data collection, preprocessing, model training, and alarm production guarantees a comprehensive end-to-end security architecture. Decisions are made immediately, and data moves through the

system clearly via sequential and collaborative processes. Automated alert systems significantly improve security by allowing users or administrators to respond promptly upon detecting a danger.

## IX.FUTURE ENHANCEMENTS

The Deep Learning approach for Robust Malware Detection in IoT Devices might be improved to augment its applicability, scalability, and efficiency. The use of edge computing for real-time detection is a promising new avenue. One approach to improve reaction speed and minimize latency is to implement lightweight deep learning models directly on IoT devices or edge gateways. This allows the system to swiftly identify malware without significant need on cloud infrastructure.

Federated Learning is an innovative methodology that allows several IoT devices to jointly train a model without the need to upload any raw data. This method improves security and privacy while maintaining the advantages of collaborative learning. This functionality is advantageous when it is impractical to transport sensitive information to remote servers.

To enhance the system's detection accuracy for intricate and dynamic malware patterns, it may be supplemented by including sophisticated deep learning architectures, such as CNN-LSTM hybrids or Transformer-based models. Furthermore, zero-day attacks not present in the training sample may be detected by combining behavioral analysis with anomaly detection methods.

## X.REFERENCES

[1] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[2] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, “Kitsune: An ensemble of autoencoders for online network intrusion detection,” in Proc. Network and Distributed System Security Symp. (NDSS), 2018.

[3] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, and Y. Elovici, “N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.

[4] R. Vinayakumar, K. P. Soman, and P. Poornachandran, “Applying deep learning approaches for network traffic prediction and intrusion detection,” IEEE Access, vol. 7, pp. 41582–41598, 2019.

[5] K. Alrawashdeh and C. Purdy, “Toward an online anomaly intrusion detection system based on deep learning,” in Proc. IEEE SoutheastCon, 2016, pp. 1–6.

[6] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” IEEE Trans. Emerging Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.

[7] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” in Proc. 9th EAI Int. Conf. Bio-inspired Information and Communications Technologies (BICT), 2016, pp. 21–26.

[8] R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning DDoS detection for consumer Internet of Things devices,” in Proc. IEEE Security and Privacy Workshops (SPW), 2018, pp. 29–35.

[9] A. Sivanathan, D. Sherratt, H. H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, “Characterizing and classifying IoT traffic in smart cities and campuses,” in Proc. IEEE INFOCOM, 2018, pp. 559–567.

[10] Y. Zhang, X. Chen, L. Li, D. Zhang, and Y. Wang, “A survey on deep learning for IoT security,” IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020.