Cyber Threat Detection Using Deep Learning in IoT Networks

[1] D.SandhyaRani, [2] Y. SAI, [3] Y. VASANTH KUMAR, [4] S. NANDINI, [5] T REVATHI
[1] Assistant Professor, Department of ECE, Sri Indu College of Engineering & Technology, Hyderabad.
[2,3,4,5] U.G. Scholar, Department of ECE, Sri Indu College of Engineering & Technology, Hyderabad.

ABSTRACT
With the rapid expansion of digital systems and internet connectivity, cyber threats have become more advanced and frequent, creating serious risks for individuals, organizations, and critical infrastructure. Traditional signature-based detection techniques often struggle to identify new or evolving attacks, emphasizing the need for more intelligent and adaptive security solutions.
This study proposes a deep learning-based cyber threat detection system that utilizes neural networks to automatically learn complex patterns from network traffic and system logs. This enables the system to detect anomalies and malicious activities in real time. The model integrates feature extraction, classification, and predictive analytics to identify threats such as malware, ransomware, phishing, and Distributed Denial-of-Service (DDoS) attacks with high accuracy. Experimental results show that the proposed system performs better than conventional approaches in detecting both known and zero-day attacks. This demonstrates its effectiveness as a robust and proactive cybersecurity solution capable of enhancing overall system protection.

Keywords: Cyber Threat Detection, Deep Learning, Neural Networks, Anomaly Detection, Intrusion Detection System (IDS), Malware Detection, Real-Time Security, Network Security, Zero-Day Attack Detection

1. INTRODUCTION

In the digital era, the increasing reliance on internet-connected systems and cloud-based services has made cybersecurity a critical concern for organizations and individuals alike. Cyber threats, including malware, ransomware, phishing, and distributed denial-of-service (DDoS) attacks, are becoming more sophisticated, frequent, and damaging. Traditional security measures, such as signature-based intrusion detection systems (IDS), often struggle to detect novel or evolving threats, leaving networks vulnerable to exploitation.

Deep learning offers a promising solution by enabling systems to automatically learn complex patterns and relationships from large volumes of data. Unlike traditional rule-based methods, deep learning models can identify anomalies, predict malicious activities, and adapt to new attack patterns in real-time. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks have been widely applied in analyzing network traffic, system logs, and user behavior to detect cyber threats effectively.

The objective of this project is to develop a deep learning-based cyber threat detection system capable of identifying both known and unknown attacks with high accuracy. By leveraging neural network architectures for feature extraction and classification, the system aims to provide a robust, real-time defense mechanism that enhances network security and minimizes the impact of cyber attacks on critical infrastructures and sensitive data.

2. LITERATURE REVIEW

Deep learning has transformed cyber threat detection by enabling systems to automatically learn complex patterns from network traffic and system logs. Convolutional Neural Networks (CNNs) are used to analyze traffic patterns, while Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks effectively process sequential data, detecting attacks like DDoS and malware. Recent studies show that deep learning-based Intrusion Detection Systems (IDS) outperform traditional signature-based methods by identifying both known and unknown threats. However, challenges remain, including the

need for large datasets, high computational resources, and vulnerability to adversarial attacks. Despite these challenges, deep learning provides a robust framework for accurate and real-time cyber threat detection.

3. EXISTING SYSTEM

Existing cyber threat detection systems mainly rely on **signature-based** or **rule-based** approaches, which identify attacks by comparing network activity to a database of known threat signatures. While effective for known attacks, these systems fail to detect **new or evolving threats** such as zero-day exploits and sophisticated malware. Some systems use traditional machine learning models like Support Vector Machines (SVM) or Random Forests on extracted features, but their accuracy is limited and they often require manual feature engineering. Additionally, these systems struggle with real-time detection in large-scale networks due to computational constraints and lack adaptability to dynamic cyber environments.

4. PROPOSED SYSTEM

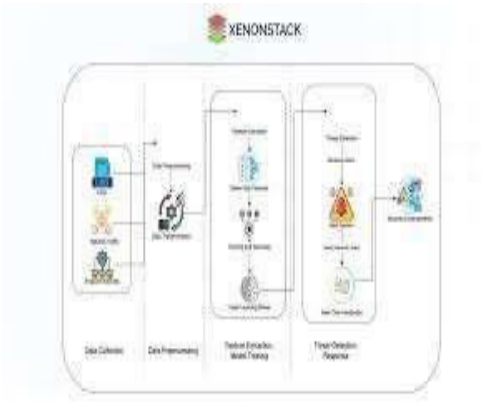
The proposed system employs **deep learning techniques** to enhance cyber threat detection, overcoming the limitations of traditional methods. By using architectures like CNNs, RNNs, and LSTMs, the system automatically learns complex patterns from network traffic and system logs, enabling it to detect both known and unknown attacks in real-time. Unlike signature-based systems, this approach does not rely on predefined rules or manual feature extraction, making it more adaptive and robust. The system can identify threats such as malware, phishing, and DDoS attacks with higher accuracy and reduced false positives, providing a scalable and efficient solution for modern cybersecurity challenges.

5. METHODOLOGY

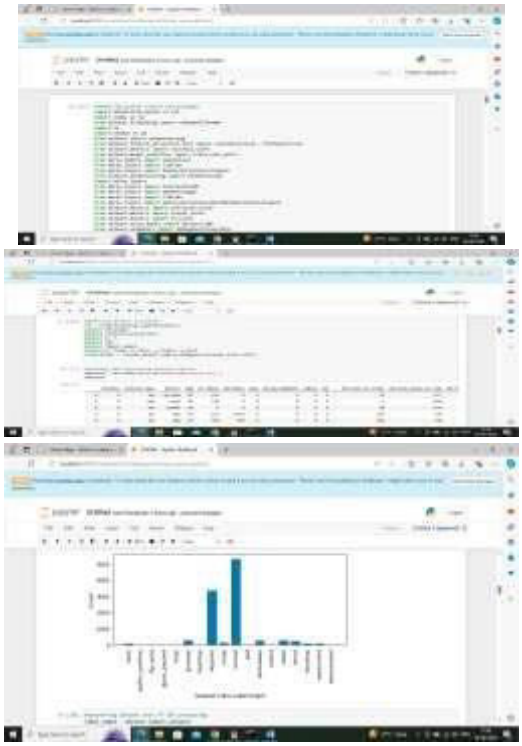
The methodology of the proposed system involves collecting a **dataset of network traffic and system logs** containing both normal and malicious activities. The data is **preprocessed** to remove noise, normalize features, and convert it into a suitable format for deep learning models. A **deep learning architecture**—such as CNN, RNN, or LSTM—is then trained to automatically extract features and classify network behavior as normal or malicious. Techniques like **data augmentation, dropout, and batch normalization** are applied to improve model accuracy and prevent overfitting. Once trained, the system performs **real-time threat detection**, identifying attacks such as malware, phishing, and DDoS with high accuracy, and its performance is evaluated using metrics like accuracy, precision, recall, and F1-score.

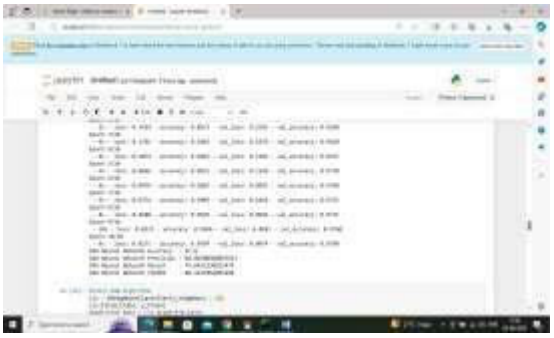
6. System Model

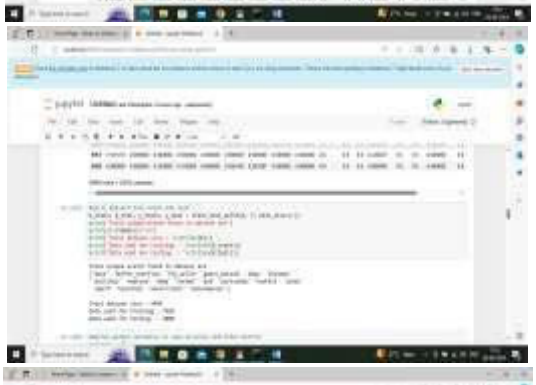
SYSTEM ARCHITECTURE

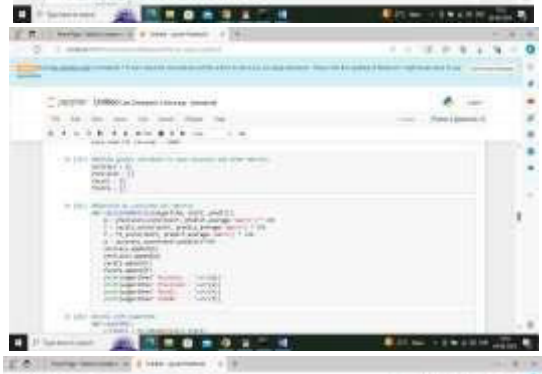


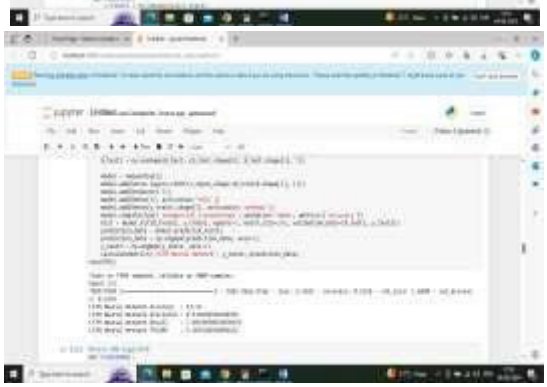
7. Results and Discussions

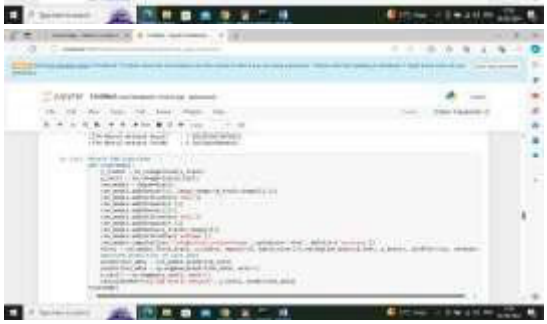


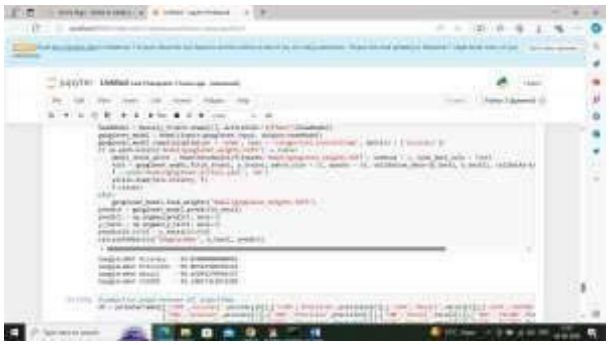


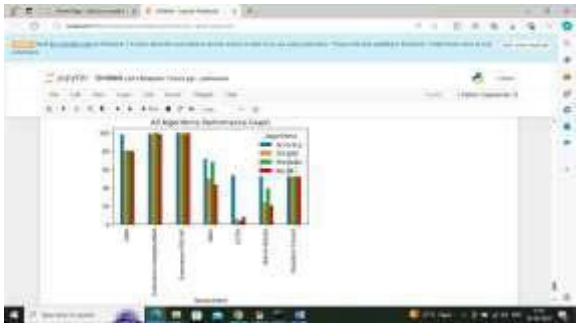












8. CONCLUSION

In conclusion, the proposed deep learning-based cyber threat detection system provides an effective and adaptive solution to modern cybersecurity challenges. By leveraging architectures like CNNs, RNNs, and LSTMs, the system can automatically learn complex patterns from network traffic and system logs, enabling accurate detection of both known and unknown threats in real-time. Compared to traditional signature-based and machine learning approaches, this method improves detection accuracy, reduces false positives, and adapts to evolving attack patterns. Overall, deep learning offers a robust framework for enhancing network security, safeguarding critical systems, and mitigating the impact of cyber attacks. In conclusion, the proposed deep learning-based cyber threat detection system provides a comprehensive and adaptive solution to the growing challenges in cybersecurity. By leveraging advanced neural network architectures such as CNNs, RNNs, and LSTMs, the system can automatically extract meaningful patterns from vast amounts of network traffic and system log data, enabling the accurate identification of both known and unknown threats. This approach significantly improves upon traditional signature-based and conventional machine learning methods by reducing false positives, detecting zero-day attacks, and adapting to dynamic cyber environments. Moreover, the system's capability for real-time monitoring and analysis allows organizations to respond swiftly to security incidents, minimizing potential damage and downtime. The integration of deep learning also opens opportunities for future enhancements, including combining threat intelligence, anomaly detection, and federated learning to create more robust, scalable, and privacy-preserving cybersecurity solutions. Overall, this work demonstrates the critical role of deep learning in safeguarding digital infrastructures, protecting sensitive data, and building resilient security frameworks against increasingly sophisticated cyber attacks.

9. REFERENCES

1. A. Aldhaheri, "Deep learning for cyber threat detection in IoT networks," *ScienceDirect*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000512. [Accessed: Oct. 23, 2025].
2. P. Santos, "A Systematic Review of Cyber Threat Intelligence," *PubMed Central*, 2025. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC12300000/. [Accessed: Oct. 23, 2025].
3. ECP Neto, "Deep learning for intrusion detection in emerging IoT environments," *SpringerLink*, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s10462-025-11346-z. [Accessed: Oct. 23, 2025].
4. A. H. Salem, "Advancing cybersecurity: a comprehensive review of AI-driven threat detection," *Journal of Big Data*, 2024. [Online]. Available: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00957-y. [Accessed: Oct. 23, 2025].
5. A. Alabdulatif, "A Novel Ensemble of Deep Learning Approach for Intrusion Detection," *MDPI Electronics*, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/14/7984. [Accessed: Oct. 23, 2025].

6. T. S. Oyinloye, "Enhancing cyber threat detection with an improved artificial neural network," *ScienceDirect*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666764924000316. [Accessed: Oct. 23, 2025].
7. M. Rahmati, "Towards Explainable and Lightweight AI for Real-Time Cyber Threat Hunting in Edge Networks," *arXiv*, 2025. [Online]. Available: https://arxiv.org/abs/2504.16118. [Accessed: Oct. 23, 2025].
8. Y. Chen, "A survey of large language models for cyber threat detection," *ScienceDirect*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404824003213. [Accessed: Oct. 23, 2025].
9. A. H. Salem, "Artificial intelligence and machine learning in cybersecurity," *SpringerLink*, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s10115-025-02429-y. [Accessed: Oct. 23, 2025].
10. M. Schmitt, "Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection," *arXiv*, 2023. [Online]. Available: https://arxiv.org/abs/2401.01342. [Accessed: Oct. 23, 2025].