IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204357 |

Enhancing Intrusion Detection in IoT Systems

Harshitha S, Cinchana S, Deeksha H.V., Divyashree H.R., Gagana B.S.

Assistant Professor, Department of CSE, Malnad College of Engineering, Hassan, India

Department of CSE, Malnad College of Engineering, Hassan, India

Department of CSE, Malnad College of Engineering, Hassan, India

Department of CSE, Malnad College of Engineering, Hassan, India

Department of CSE, Malnad College of Engineering, Hassan, India

ABSTRACT: The Internet of Things (IoT) has revolutionized technology, but it also presents a vast attack surface for malicious actors. Traditional network intrusion detection systems are often insufficient for IoT environments due to resource constraints, heterogeneous communication protocols, and device diversity. This research aims to enhance network intrusion detection for IoT systems by combining machine learning algorithms with domain-specific knowledge of IoT traffic patterns. Real-time analysis helps identify threats, mitigates risks, and demonstrates the efficacy and resilience of the proposed solution.

KEYWORDS: CNN, LSTM, IoT, Intrusion Detection

I. INTRODUCTION

Network Intrusion Detection (NID) is crucial in IoT systems for safeguarding against unauthorized access and malicious activities. By monitoring network traffic, NID identifies suspicious patterns and anomalies, enhancing security in interconnected environments. Leveraging advanced algorithms, NID adapts to the dynamic nature of IoT, providing real-time analysis and alerts for timely threat mitigation. As a cornerstone of IoT security, NID plays a pivotal role in protecting sensitive data and preserving operational integrity.

II. OBJECTIVE

1.Identifying Anomalies
2.Preventing Unauthorized Access
3.Protecting Data Integrity
4.Mitigating Cyber Threat
5.Improving Incident Response
6.Optimizing Resource Utilizations

III. LITERATURE SURVEY

The study focuses on optimizing the Internet of Things intrusion detection system using the LM-BP neural network model. The model improves detection rates of DOS, R2L, U2L, and Probing attacks and reduces false alarm rates. This approach can be used for smart homes, campuses, and supply chains, accelerating the deployment of the global Internet of Things and promoting efficient economic industry development. However, the LM-BP model has some defects, such as a relatively low overall detection rate and a limited data set, KDD CUP 99. Future research will focus on improving the overall detection rate and integrating the algorithm into the intrusion detection system. [1]

This work presents an intrusion detection system architecture for IoT environments that uses a large computational capacity infrastructure like the public cloud and distributed resources at the edge of the network. Classification is performed at the edge near devices and sensors to reduce processing latency, while the cloud is used for model enhancement and dissemination. The system can be used for different types of IoT networks while maintaining control over task distribution. The proposed logical scheme is generic and can be adapted to other Natural Language Processing (NLP) techniques. Experiments demonstrate the feasibility of the NLP technique in intrusion detection, identifying trade-offs for feedback requirements and results quality. The method uses as little as possible to generate

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204357 |

good results, and a device with reduced resources can perform classification and detection of noveltieswith a flow rate of 450Kb per second. Huan Hui Yan et.al. [2]

The article presents a new method for generating adversarial net- work packets and invalidating DL-based NIDSs. It uses model extraction techniques to attack adversaries even when DL models are black- boxes. The saliency map is used to identify critical features and packet attributes for AE generation. The solution successfully attacks the state-of-the-art NIDS, Kitsune, in the Mirai Botnet and video streaming scenarios. Future research will focus on mitigation solutions to enhance DL models' robustness in intrusion detection. [3]

The system used intersection operation to identify 16 and 19 features for detecting DDoS and DoS attacks on BoT-IoT and KDD Cup 1999 datasets. The system achieved higher accuracy and
detection rates of 99.9993 percentage and 99.5798 percentage, respectively, with JRip using 16 features on BoT-IoT. The KDD Cup 1999 dataset also improved accuracy and detection rates to 99.9920percentage and 99.9943percentage. The work aims to find optimal features for IDS using a combination of bio-inspired algorithms. [4]

The paper introduces Realguard, a DNN-based intrusion detection system for IoT network gateways. It uses a lightweight feature extraction algorithm and an efficient attack detection model based on a damped incremental statistic algorithm and a deep neural network model. Realguard accurately detects 10 attack types with a small computational footprint and is efficient enough to run on a Raspberry PI in real time. [5]

IV. SYSTEM DESIGN

1.Data Pre-processing: Prepare datasets (UNSW-NB15 and IoT 23) for training and evaluation, including cleaning and normalization.
2. Train/Validation/Test Split: Divide pre-processed datasets into training, validation, and testing sets for model training, hyperparameter tuning, and final evaluation.
3. Deep Learning Model Construction: Build CNN and LSTM classifiers for intrusion detection.
4. Model Training: Train CNN and LSTM models to distinguish normal from anomalous network traffic.
5. Model Evaluation: Assess model performance using metrics like accuracy, recall, precision, loss, and F1-score.
6. Performance Evaluation: Calculate various metrics to gauge the effectiveness of the proposed IDS based on deep learning methods.

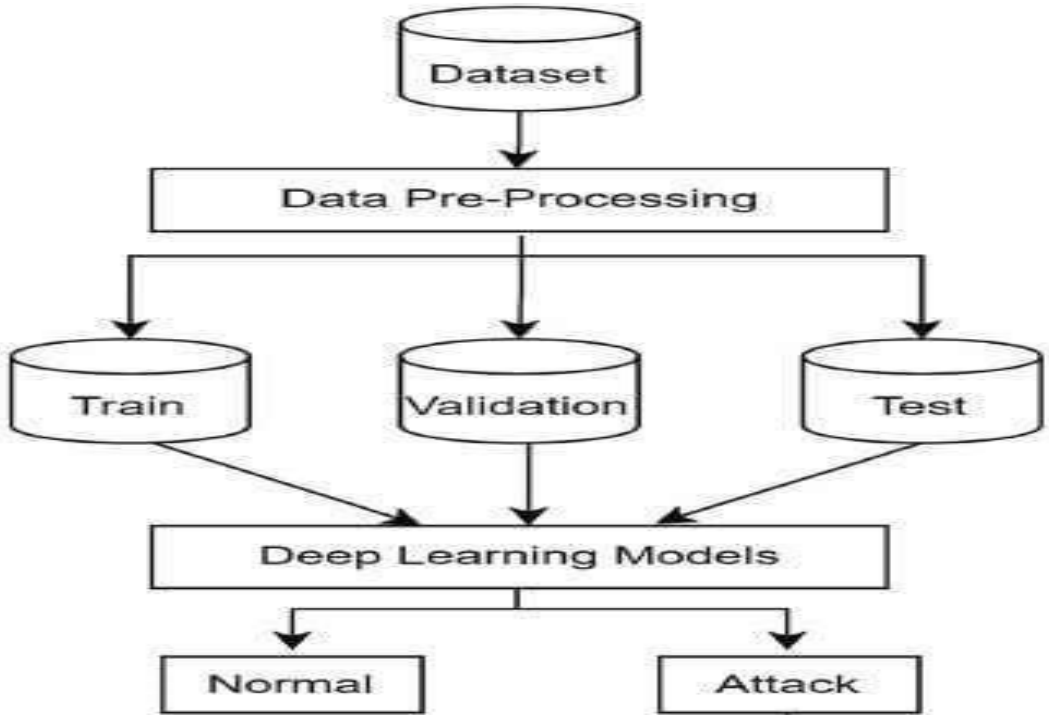

Figure 1. System Design

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204357 |

V. IMPLEMENTATION

1. Problem Definition: Clearly define objectives, types of intrusions, performance metrics, and deployment scenarios for IoT intrusion detection.
2. Data Collection and Preprocessing: Collect raw data, preprocess it by removing noise, handling missing values, and normalizing features.
3. Model Design: Design CNN and LSTM architectures for intrusion detection, capturing spatial and temporal patterns in network traffic.
4. Model Training and Evaluation: Train models with labelled datasets to distinguish between normal and anomalous activities, evaluate performance using metrics like accuracy, precision, recall, and F1-score.
5. System Integration: Integrate trained models into IoT infrastructure for real-time intrusion detection, configuring them to process data and generate alerts.
6. Deployment and Monitoring: Deploy the system in production IoT environments, continuously monitoring network traffic for security threats and sending alerts for investigation.
7. Fine-Tuning and Maintenance: Periodically fine-tune and maintain the system to address emerging threats, optimize parameters, and adapt to changes in the environment.

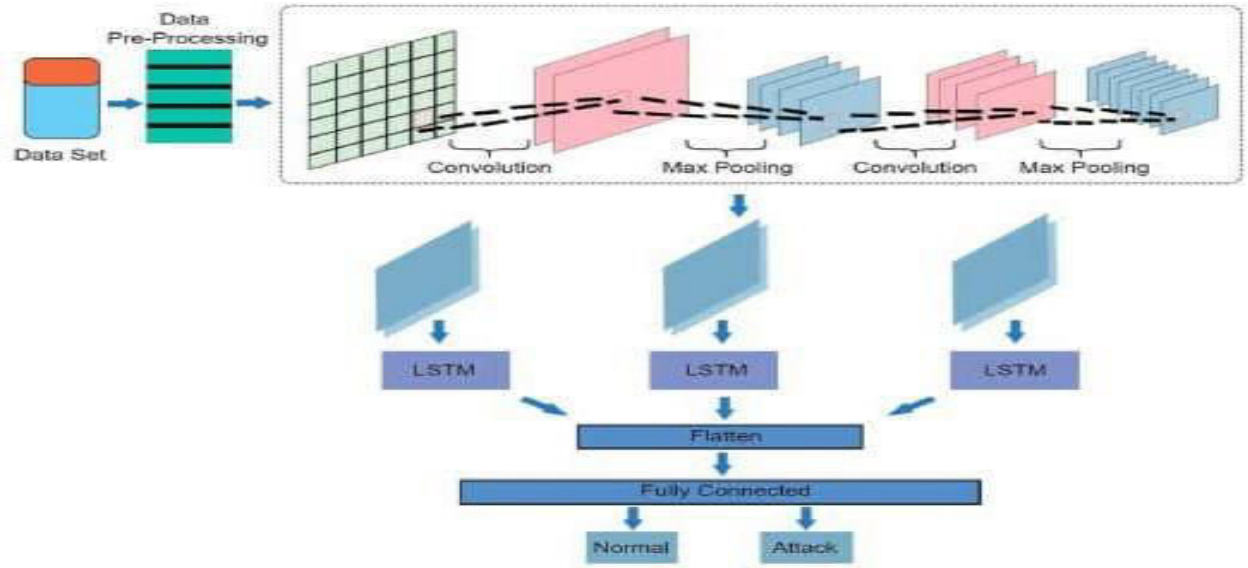

Figure 2. CNN+LSTM Architecture

VI. RESULT

- CNN-LSTM achieves the highest accuracy at 97.82%, followed by CNN at 96.62%, and LSTM at 96.437%.
- CNN-LSTM outperforms the other models in loss, with a value of 5.35%, compared to CNN's 5.85%, and LSTM's 6.64%.
- Both CNN-LSTM and CNN exhibit the highest precision at around 99%, indicating robust confidence in their predictions.
- CNN-LSTM leads in recall with 96.94%, followed closely by CNN at 96.62%, and LSTM at 96.24%.
- The F1 score, balancing precision and recall, is highest for CNN-LSTM at 97.34%, followed by CNN at 96.98%, with LSTM also at 96.98%.
- AUCROC, measuring the ability to distinguish classes, is highest for CNN-LSTM and CNN at 99.64%, while LSTM trails slightly behind at 99.47%.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204357 |

Model Performance Metrics Table

Model Name	Accuracy	Loss	Precision	Recall	F1 Score	AUCROC
CNN_LSTM	97.82%	5.35%	99.09%	96.94%	97.34%	99.64%
CNN	96.62%	5.85%	99.00%	96.62%	96.98%	99.64%
LSTM	96.437%	6.64%	99.16%	96.24%	96.98%	99.47%

Figure 3: Model Performance Metrics Table

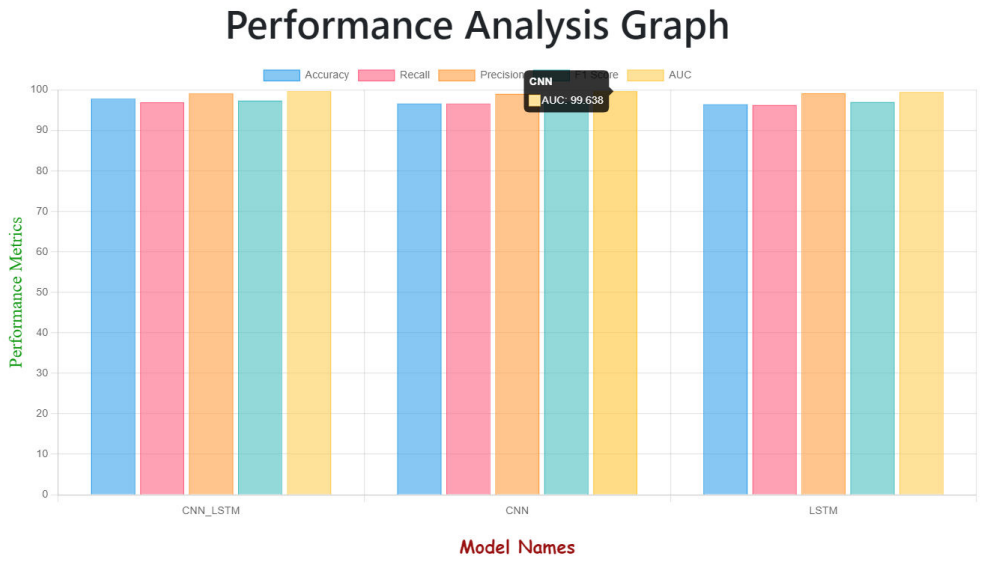

Figure 4: Performance Analysis

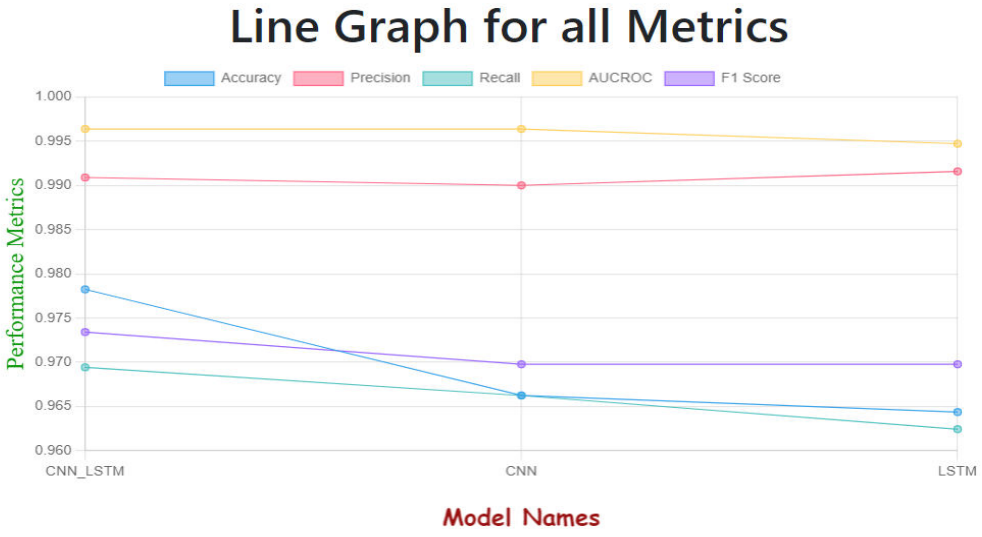

Figure 6: Line Graph

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204357 |

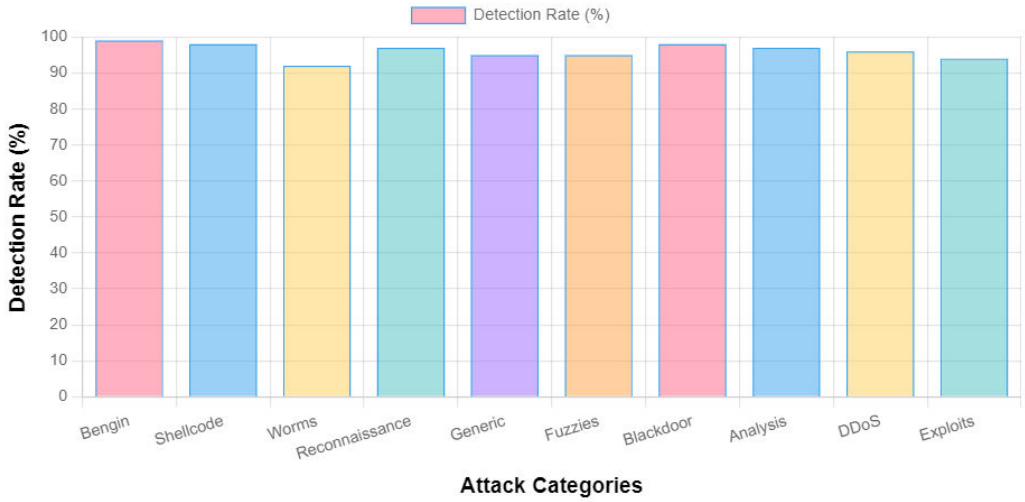

Figure 5: Detection Rate of Attack Types

VII. CONCLUSION

The proposed intrusion detection system uses Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to enhance cybersecurity in IoT environments. The system accurately detects abnormal behaviors and security threats by capturing spatial patterns in network traffic data. Its adaptability, scalability, and efficiency make it suitable for deployment in dynamic IoT environments. The system continuously monitors network traffic, generates alerts, and facilitates proactive response and mitigation actions.

REFERENCES

1. Aimin Yang, Yunxi Zhuansun, Chenshuai Liu, Jie Li, and Chunying Zhang. Design of intrusion detection system for internet of things based on improved bp neural network. Ieee Access, 7:106043–106052, 2019.
2. Guilherme Weigert Cassales, Hermes Senger, Elaine Ribeiro de Faria, and Albert Bifet. Idsa-iot: an intrusion detection system architecture for iot networks. In 2019 IEEE Symposium on Computers and Communications (ISCC), pages 1–7. IEEE, 2019.
3. Pushparaj Nimbalkar and Deepak Kshirsagar. Feature selection for intrusion detection system in internet-of-things (iot). ICT Express, 7(2):177–181, 2021.
4. Pavlos Papadopoulos, Oliver Thornewill von Essen, Nikolaos Pitropakis, Christos Chrysoulas, Alexios Mylonas, and William J Buchanan. Launching adversarial attacks against network intrusion detection systems for iot. Journal of Cybersecurity and Pri- vacy, 1(2):252–273, 2021.
5. Xuan-Ha Nguyen, Xuan-Duong Nguyen, Hoang-Hai Huynh, and Kim-Hung Le. Re- alguard: A lightweight network intrusion detection system for iot gateways. Sensors, 22(2):432, 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details