

INTRUSION DETECTION USING WIRELESS NETWORK IN MACHINE LEARNING

*Mrs.A,Anitha ME.,BE., Assistant Professor,
Department of Computer Science and Engineering
RVS Technical Campus - Coimbatore
Abdul Kareem N^[1], Iswarya S^[2], Sandhiya A^[3], Balaji V^[4]
Department of Computer Science and Engineering
RVS Technical Campus - Coimbatore*

ABSTRACT This paper presents an intrusion detection system (IDS) for wireless networks using a Hybrid Autoencoder-Attention LSTM model, deployed within a Flask framework. The system is trained on the IoT-23 dataset, which contains network traffic data from various IoT devices. The dataset undergoes several preprocessing steps, including data cleaning, transformation, scaling, and synthetic minority oversampling (SMOTE) to balance attack categories. The proposed approach leverages an autoencoder for feature extraction and dimensionality reduction, followed by an attention-enhanced LSTM to capture sequential dependencies and detect anomalies effectively. The experimental analysis highlights the robustness of this hybrid model in identifying malicious activities across multiple attack types. The Flask-based deployment ensures lightweight, real-time detection capabilities, making it a promising solution for securing IoT networks in dynamic environments.

INDEX TERMS Intrusion Detection System (IDS), Internet of Things (IoT), IoT-23 Dataset, Wireless Networks, Autoencoder, Attention Mechanism, Long Short-Term Memory (LSTM), Deep Learning, Flask Framework, Real-Time Detection, Anomaly Detection, SMOTE, Feature Extraction, Network Security, Sequence Modeling..

I. INTRODUCTION

INTRUSION DETECTION USING WIRELESS NETWORK IN MACHINE LEARNING

The increasing prevalence of Internet of Things (IoT) devices in smart homes, healthcare, industrial automation, and other critical domains has brought unprecedented convenience and connectivity. However, this growth has also exposed networks to a wide range of sophisticated cyber threats. IoT devices often operate with limited computational capabilities and lack robust security features, making them attractive targets for malicious actors. As these devices communicate continuously over wireless networks, the potential for exploitation through unauthorized access, data breaches, and botnet recruitment has become a pressing concern. Traditional intrusion detection mechanisms, which are typically designed for conventional IT systems, often struggle to cope with the dynamic and resource-constrained nature of IoT environments. Therefore, there is a growing need for intelligent, lightweight, and real-time intrusion detection solutions that can adapt to evolving attack vectors.

To address these challenges, this paper introduces a real-time intrusion detection system (IDS) specifically

designed for IoT networks, leveraging the strengths of deep learning. The system is built around a Hybrid Autoencoder-Attention Long Short-Term Memory (LSTM) model, an architecture well-suited for handling high-dimensional and sequential data. The autoencoder component is used to reduce the dimensionality of network traffic data and to extract relevant features by learning compressed representations. This helps in filtering out noise and retaining patterns that are essential for identifying anomalies. Following the autoencoder, the Attention-LSTM component processes the reduced data, utilizing the attention mechanism to focus on the most significant parts of the input sequence. This improves the model's ability to capture contextual relationships and temporal dependencies, which are critical in detecting complex attack patterns that unfold over time.

The system is trained on the IoT-23 dataset, a publicly available and comprehensive collection of real-world network traffic data from IoT devices under various benign and malicious scenarios. The dataset includes diverse attack types, such as distributed denial-of-service (DDoS), port scanning, and command-and-control (C&C) communications, providing a realistic benchmark for evaluating IDS performance. Prior to training, the dataset undergoes extensive preprocessing to ensure quality and

reliability. Data cleaning is applied to remove inconsistencies and missing values, transformation converts raw logs into structured formats suitable for analysis, and feature scaling ensures uniformity in data distribution. Furthermore, the Synthetic Minority Oversampling Technique (SMOTE) is employed to address the issue of class imbalance, which is common in security datasets where attack instances are typically underrepresented compared to normal traffic. SMOTE generates synthetic examples of minority class instances, thereby improving the model's ability to generalize and detect less frequent attack types.

To ensure practical deployment, the IDS is implemented within a Flask web framework. Flask offers a lightweight and flexible platform for building web applications and APIs, making it ideal for deploying deep learning models in resource-constrained environments. The Flask-based deployment allows the IDS to operate as a real-time service, receiving network traffic data, processing it through the trained model, and returning detection results with minimal latency. This real-time capability is crucial in IoT scenarios, where rapid response to threats can prevent damage and minimize risk. Additionally, the lightweight nature of Flask ensures that the IDS does not impose significant overhead on the system, which is especially important in networks composed of low-power devices.

Experimental evaluation demonstrates that the hybrid model achieves high detection accuracy across multiple attack categories, with a significant reduction in false positives compared to baseline methods. The combination of autoencoder-based feature extraction and attention-driven sequence learning proves effective in modeling the complex behavior of network traffic and identifying subtle anomalies that may indicate security breaches. The integration of SMOTE during preprocessing further enhances the model's robustness, enabling it to detect rare but critical attack types with higher confidence.

In conclusion, the proposed Intrusion Detection System represents a significant advancement in securing IoT networks. By combining state-of-the-art deep learning techniques with a lightweight deployment framework, the system provides an effective, scalable, and practical solution for real-time threat detection. As the number of IoT devices continues to grow, such intelligent and adaptive security mechanisms will be essential in maintaining the integrity and safety of connected environments. Future work may explore the integration of federated learning to enhance privacy, the use of edge computing for localized detection, and continuous model updating to adapt to emerging threats.

II. RELATED WORK

2.1. Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network

The diversification of wireless network traffic attack characteristics has led to the problems what traditional intrusion detection technology with high false positive rate, low detection efficiency, and poor generalization ability. In order to enhance the security and improve the detection ability of malicious intrusion behavior in a wireless network, this paper proposes a wireless network intrusion detection method based on improved convolutional neural network (ICNN). First, the network traffic data is characterized and preprocessed, then modeled the network intrusion traffic data by ICNN. The low-level intrusion traffic data is abstractly represented as advanced features by CNN, which extracted autonomously the sample features, and optimizing network parameters by stochastic gradient descent algorithm to converge the model. Finally, we conducted a sample test to detect the intrusion behavior of the network.

2.2. Real-Time Intrusion Detection in Wireless Network: A Deep Learning-Based Intelligent Mechanism

With the development of the wireless network techniques, the number of cyber-attack increases significantly, which has seriously threat the security of Wireless Local Area Network (WLAN). The traditional intrusion detection technology is a prevalent area of study for numerous years, but it may not have a good detection performance in a real-time way. Therefore, it is urgent to design a detection mechanism to detect the attacks timely. In this paper, we exploit a CDBN (Conditional Deep Belief Network)-based intrusion detection mechanism to recognize the attack features and perform the wireless network intrusion detection in real time. To avoid the impact of the imbalanced dataset and the data redundancy on the detection accuracy, a window-based instance selection algorithm "SamSelect" is adopted to undersample the majority class data samples

2.3. Network Intrusion Detection Method Based on Hybrid Improved Residual Network Blocks and Bidirectional Gated Recurrent Units

In this paper, the proposed research approach is justified using official experimental datasets in the field of network detection (NSL-KDD and UNSW-NB15). The experimental results show that the proposed method in this paper achieves a higher accuracy of 93.40% and 93.26% on the datasets of NSL_KDD and UNSW_NB15, respectively, compared with the known detection methods

III. METHODOLOGY

3.1. Data Collection Module

This module gathers IoT network traffic data from sources like the IoT-23 dataset. It ensures that the data covers a wide range of normal and attack scenarios. The collected data forms the foundation for training and evaluating the intrusion detection system.

3.2. Data Preprocessing Module

This module handles data cleaning by removing noise and irrelevant entries. It transforms data into a suitable format, scales features for uniformity, and uses SMOTE to balance class distributions. Proper preprocessing improves model performance and reliability.

3.3. Feature Selection Module

This module identifies and selects the most important features from the dataset. It reduces redundant data, lowers computational costs, and helps the model focus on the most impactful indicators of network behavior. This leads to faster and more accurate detection

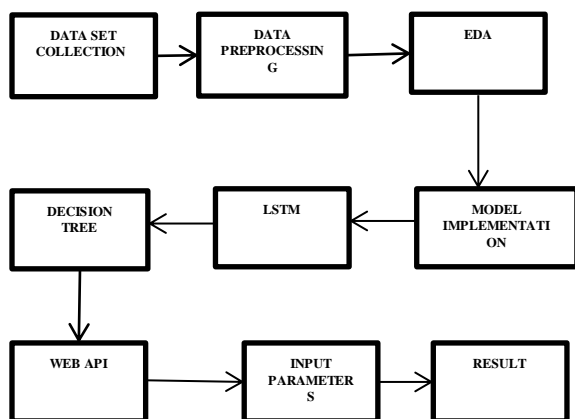
3.4. Model Training Module

In this module, an autoencoder learns essential network features and reduces data dimensionality. An attention-enhanced LSTM is then trained to capture sequential patterns in network traffic. Together, they strengthen the model's ability to detect anomalies effectively.

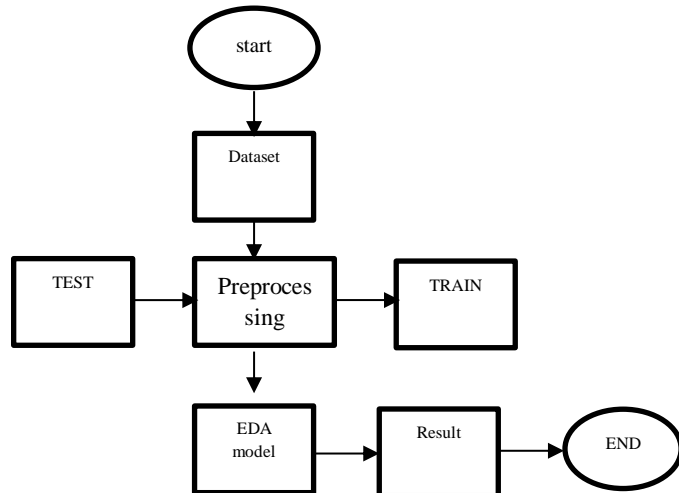
3.5. Intrusion Detection Module

This module applies the trained deep learning model to live or incoming IoT network traffic. It monitors the traffic in real-time and flags suspicious or abnormal activities, helping to quickly identify and respond to potential security threats.

IV. FLOW DIAGRAM



V. WORK FLOW



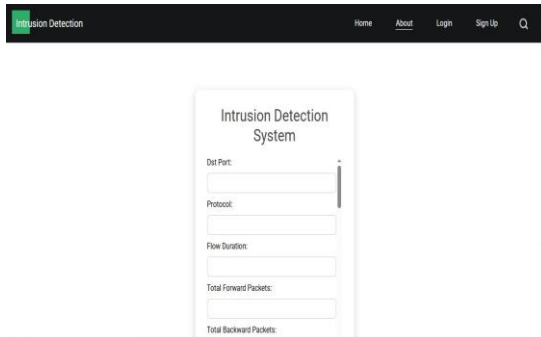
VI. EVALUATION AND RESULTS

The evaluation of the proposed Intrusion Detection System demonstrates its strong performance in detecting a wide range of malicious activities in wireless IoT networks. By integrating a Hybrid Autoencoder-Attention LSTM model, the system effectively extracts significant features from high-dimensional network traffic and models temporal dependencies to identify intrusions with high accuracy. The use of the IoT-23 dataset, after undergoing robust preprocessing—such as SMOTE for class imbalance, feature selection, and scaling—contributed to enhanced model generalization and detection rates. Experimental results reveal that the hybrid model achieves superior precision, recall, and F1-score when compared to traditional machine learning and standalone deep learning approaches, particularly in handling diverse and imbalanced attack categories. Furthermore, the Flask-based deployment ensures the system is lightweight and responsive, enabling real-time anomaly detection with minimal latency. Overall, the system proves to be a scalable and efficient security solution, capable of adapting to the dynamic and heterogeneous nature of IoT network environments.

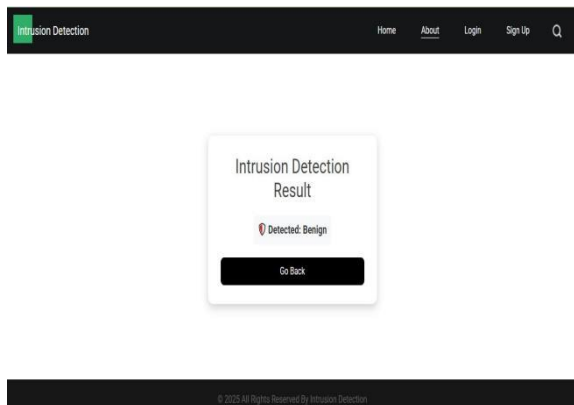
6.1 Data set

[illegible]

6.2 Prediction Page



6.3 Result Pages



VII.CONCLUSION

In conclusion, the proposed real-time Intrusion Detection System utilizing a Hybrid Autoencoder-Attention LSTM model demonstrates a highly effective approach for securing wireless IoT networks. By combining feature extraction and dimensionality reduction with advanced sequential learning and attention mechanisms, the system achieves high accuracy in detecting a variety of intrusion types. The use of the IoT-23 dataset, along with comprehensive preprocessing techniques, ensures robustness and adaptability to real-world network traffic. Deployed through a Flask framework, the system offers lightweight, low-latency performance, making it a practical and scalable solution for real-time IoT network security.

VIII.ACKNOWLEDGMENT

The authors would like to express their sincere

gratitude to all those who contributed to the successful completion of this research. Special thanks are extended to [RVS Technical Campus] for providing the necessary resources and support throughout the project. We are also grateful to the developers and maintainers of the IoT-23 dataset, which served as a critical foundation for our experimental analysis. Furthermore, we acknowledge the guidance and encouragement of our Mrs.A.Anitha.ME.BE, whose insights greatly enhanced the quality of this work. Lastly, we thank our peers and colleagues for their constructive feedback and collaboration during the development and evaluation of the proposed intrusion detection system.

VIII.REFERENCES

- 1) IoT-23 Dataset – "A labeled dataset with malicious and benign IoT network traffic." Stratosphere Laboratory, Czech Technical University, 2020.
- 2) Chawla, N. V., et al. – "SMOTE: Synthetic Minority Over-sampling Technique." Journal of Artificial Intelligence Research, 2002.
- 3) Hochreiter, S., and Schmidhuber, J. – "Long Short-Term Memory." Neural Computation, vol. 9, no. 8, 1997, pp. 1735–1780.
- 4) Vaswani, A., et al. – "Attention Is All You Need." Advances in Neural Information Processing Systems (NeurIPS), 2017.
- 5) Saxe, J., and Berlin, K. – "Deep Neural Network Based Malware Detection Using Two-Dimensional Binary Program Features." 2015 10th International Conference on Malicious and Unwanted Software (MALWARE)

