ISSN 2277-2685
IJESR/June. 2025/ Vol-15/Issue-3s/39-46
D Bhavya Sree *et. al.*, / International Journal of Engineering & Science Research

Anomaly Detection Model in IoT Networks

A Hima Bindu, D Bhavya Sree, Mittapelli Hasmitha

[1]Assistant Professor, Department Of Cse, Bhoj Reddy Engineering College For Women, India.

[2,3]B. Tech Students, Department Of Cse, Bhoj Reddy Engineering College For Women, India.

ABSTRACT

The growing development of IoT (Internet of Things) devices creates a large attack surface for cybercriminals to conduct potentially more destructive cyberattacks; as a result, the security industry has seen an exponential increase in cyber-attacks. Many of these attacks have effectively accomplished their malicious goals because intruders conduct cyber-attacks using novel and innovative techniques. An anomaly-based IDS (Intrusion Detection System) uses machine learning techniques to detect and classify attacks in IoT networks. In the presence of unpredictable network technologies and various intrusion methods, traditional machine learning techniques appear inefficient. In many research areas, deep learning methods have shown their ability to identify anomalies accurately. Convolutional neural networks are an excellent alternative for anomaly detection and classification due to their ability to automatically categorize main characteristics in input data and their effectiveness in performing faster computations.

We design and develop a novel anomaly-based intrusion detection model for IoT networks. First, a convolutional neural network model is used to create a multiclass classification model. The proposed model is then implemented using convolutional neural networks in 1D. The proposed convolutional neural network model is validated using the, IoT Network Intrusion, and IoT-23 intrusion detection, MQTT-IoT-IDS2020 datasets. Transfer learning is used to implement binary and multiclass classification using a convolutional neural network multiclass pre-trained model. Our proposed binary and multiclass classification models have achieved high accuracy, precision, recall, and F1 score compared to existing deep learning implementations.

1-INTRODUCTION

Cybersecurity has become a cornerstone in managing information across today's rapidly expanding Internet of Things (IoT) environment. With IoT devices now deeply integrated into homes, industries, healthcare, transportation, and security systems, their widespread distribution and complex communication protocols have introduced significant vulnerabilities. As the number of devices grows—from 16 billion in 2015 to an expected 83 billion by 2024—the risk of cyber-attacks also escalates. While IoT enhances efficiency and productivity through automation and remote access, it simultaneously increases the attack surface for threats such as Distributed Denial of Service (DDoS), ransomware, and botnet attacks, all of which exploit weaknesses in network infrastructure and unencrypted systems.Despite the benefits that IoT offers, its architecture lacks unified security standards, making these systems especially difficult to safeguard.Traditional intrusion detection systems (IDS), reliant on signature-based or heuristic approaches, struggle to identify emerging threats due to the need for constant updates and domain expertise.To address these challenges, this study proposes a deep learning-based IDS using Convolutional Neural Networks (CNNs) for both binary and multiclass traffic classification. This

advanced system distinguishes between 15 different attack types and legitimate network behavior using CNN architecture and transfer learning techniques. Furthermore, the research introduces a strategy for generating enriched datasets from existing traffic data, enhancing the detection accuracy and robustness of the models. The system's effectiveness in identifying anomalies supports its practical application in securing dynamic IoT environments, paving the way for more resilient and intelligent cybersecurity frameworks.

Existing System

Anomaly detection in IoT networks employs various methods to identify deviations from normal behavior. Rule-based systems rely on predefined rules or thresholds, making them simple to implement and interpret. These systems are particularly suitable for use cases where anomalies are well-defined and straightforward. Statistical methods, on the other hand, analyze the properties of data, such as mean, variance, and probability distributions, often using techniques like time-series analysis to detect deviations from expected patterns.

Proposed System

The proposed system for anomaly detection in IoT networks utilizes a deep learning-based Convolutional Neural Network (CNN) model. . It automatically extracts features from raw data, eliminating the need for manual feature engineering. It begins with preprocessing IoT data, transforming it into a format compatible with the CNN1D model. The architecture includes convolutional layers for feature extraction, normalization layers for output standardization, and pooling layers for dimensionality reduction.

2-REQUIREMENT ANALYSIS

Functional Requirements

Modules:

- User:

Inputs the Data : User inputs test file data Views Result: Model gives result of anomalies

Non-Functional Requirements

- **Performance**: The system's performance is measured by its response time and throughput, ensuring fast and efficient processing of user requests and predictions.
- **Reliability**: The system guarantees high availability, fault tolerance, and robust backup and recovery mechanisms to ensure continuous operation and minimize downtime.
- **Security**: The system incorporates data encryption, access control measures, and audit logging to protect sensitive information and monitor user activities for potential security breaches.
- **Usability**: The system is designed with an intuitive user interface, complemented by comprehensive documentation and training materials to enhance user experience and ease of use.
- **Maintainability**: The system is built with modularity, high code quality, and thorough testing to facilitate easier maintenance and quick updates or fixes.
- **Portability**: The system ensures platform independence, allowing it to run on different operating systems, and provides flexibility in deployment across diverse environments.

3-DESIGN

An architecture description is a formal description and representation of a system organized in a way that supports reasoning about the structure of the system.

Software Architecture

Software architecture defines the high-level

structure of a software system, outlining components, their interactions, and technology choices. It ensures the system is scalable, maintainable, and aligned with business needs.

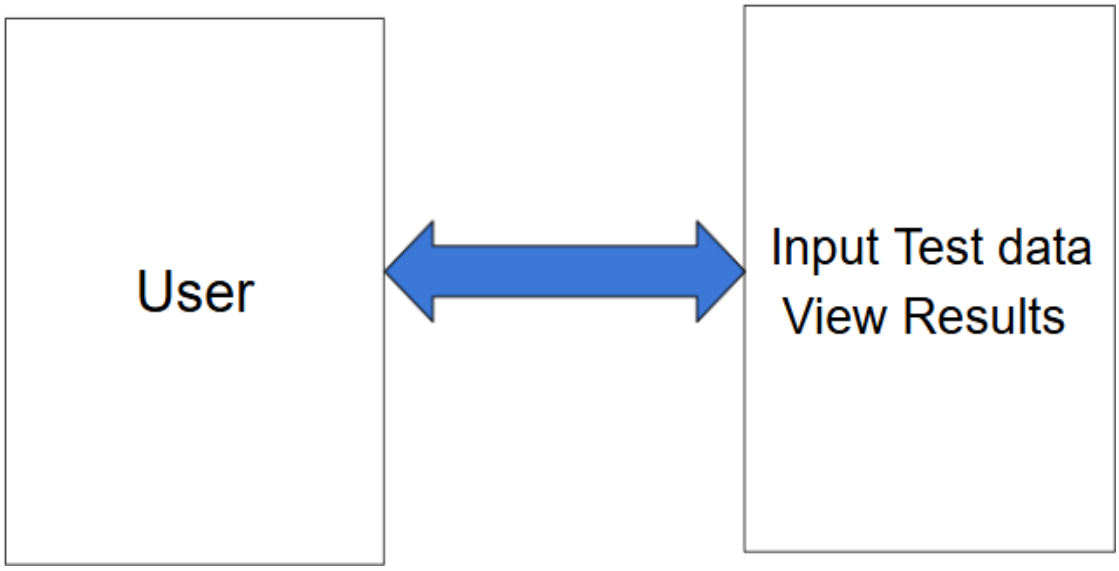

Fig 3.1 Software Architecture

Technical Architecture

It refers to the design and organization of the physical components of a system, including processors, memory, and input/output devices. It defines how these components interact to support system functionality and performance.

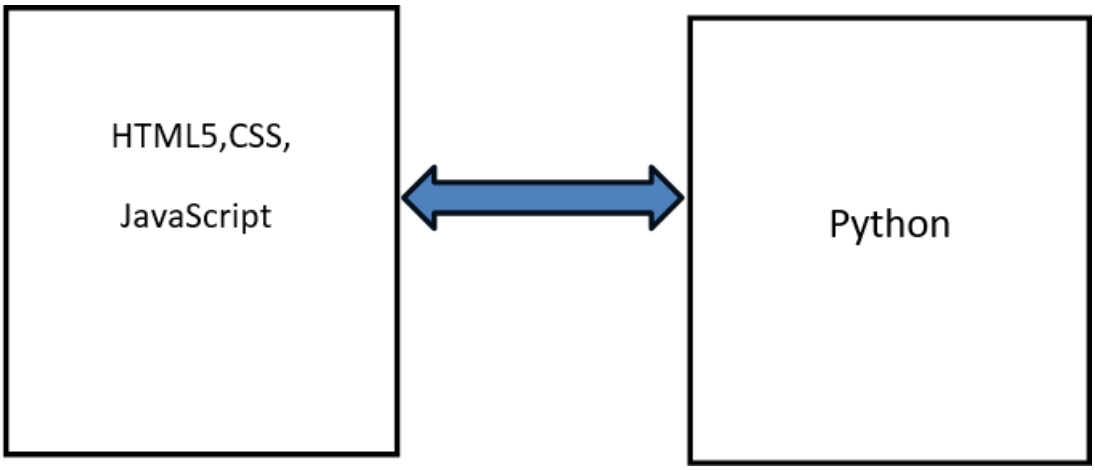

Fig 3.2 Technical Architecture

The proposed Anomaly Detection Model for IoT Networks begins by taking IoT network traffic data

as input, which includes attributes such as packet size, source and destination IP addresses, protocol types, port usage, connection duration, and frequency of data transmission. The data is pre-processed to handle missing values, reduce noise, and normalize feature scales to ensure consistency and quality across diverse IoT devices.

Feature selection techniques such as Mutual Information, Chi-square test, or PCA (Principal Component Analysis) are employed to identify the most significant attributes that contribute to anomalous behavior. These selected attributes are then used to train various machine learning and anomaly detection algorithms, including One-Class SVM, Isolation Forest, Autoencoders, and K-Means clustering.

The model performance is evaluated using metrics such as **accuracy**, **recall**, **precision**, **F1-score**, and **AUC-ROC** to determine its effectiveness in distinguishing between normal and anomalous network behaviors. Based on the evaluation results, the most efficient and robust model is selected for real-time anomaly detection in IoT networks to enhance security and prevent potential cyber threats.

Convolutional Neural Network :

In this project, a Convolutional Neural Network (CNN) is the core deep learning algorithm to detect anomalies in IoT network traffic. The CNN model processes the extracted features from datasets such as IoT-23 by capturing spatial and sequential patterns in the data using 1D convolutional layers. The architecture includes a series of layers such as Conv1D, LayerNormalization, MaxPooling1D, Dropout, and Dense layers.

Algorithm:

1. Input Feature Processing: Accept input features extracted from IoT network traffic (e.g., packet size, flow duration, protocol type).
2. Convolution Operation: Apply 1D convolutional filters over the input sequences to detect local patterns (e.g., repeated spikes, unusual flow behavior).
3. Activation Function: Use ReLU (Rectified Linear Unit) after each convolutional layer to introduce non-linearity and enable the model to learn complex patterns.
4. Pooling: Use MaxPooling1D to reduce feature dimensionality while retaining the most important information.
5. Dropout (optional): Apply dropout to prevent overfitting by randomly turning off neurons during training.

4-IMPLEMENTATION

Python

Python is one of the most popular programming languages today, known for its simplicity and extensive features.It was created by Guido van Rossum, and released in 1991. Its clean and straightforward syntax makes it beginner-friendly, while its powerful libraries and frameworks makes it perfect for developers. It can be used on a server to create web applications. It can be used to handle big data and perform complex mathematics.Python runs on an interpreter system, meaning that code can be executed as soon as it is written. This means that prototyping can be very quick.Python can be treated in a procedural way, an object-oriented way or a functional way.Python relies on indentation, using whitespace, to define scope; such as the scope of loops, functions and classes. Other programming languages often use curly-brackets for this purpose.Python is a versatile, high-level programming language that emphasizes simplicity and readability. It is widely used in various fields,

including web development, data science, artificial intelligence, and machine learning, making it ideal for projects

Features of Python

Ease of Use and Readability: Python's syntax is simple and closely resembles English, making it beginner-friendly and efficient for rapid development.

Interpreted Language: Python executes code line by line, allowing easier debugging and testing during development.

Extensive Libraries: Python offers a rich ecosystem of libraries like NumPy, Scikit-learn, Pandas, and Matplotlib, which simplify complex tasks in data science and machine learning.

Cross-Platform Compatibility: Python runs on various platforms (Windows, macOS, Linux) without requiring significant changes to the code.

Support for Multiple Paradigms: Python supports procedural, object-oriented, and functional programming styles, making it versatile for diverse applications.

Community Support: With an extensive global community, Python developers have access to vast resources, tutorials, and forums.

Advantages:

1. Python's simple and readable syntax makes it easy for beginners and professionals to quickly develop and debug programs.
2. Python provides a rich set of libraries and frameworks, such asScikit-learn, NumPy, Pandas, Matplotlib.
3. Python programs can run seamlessly across multiple platforms without modification, ensuring portability of your project.
4. Python's concise syntax and dynamic nature reduce development time, allowing faster prototyping and implementation of our project modules, such as feature selection and MLP classifier development.
5. Python's modular design makes it scalable for future expansions, such as handling larger datasets or adding new functionalities.

5-RESULTS

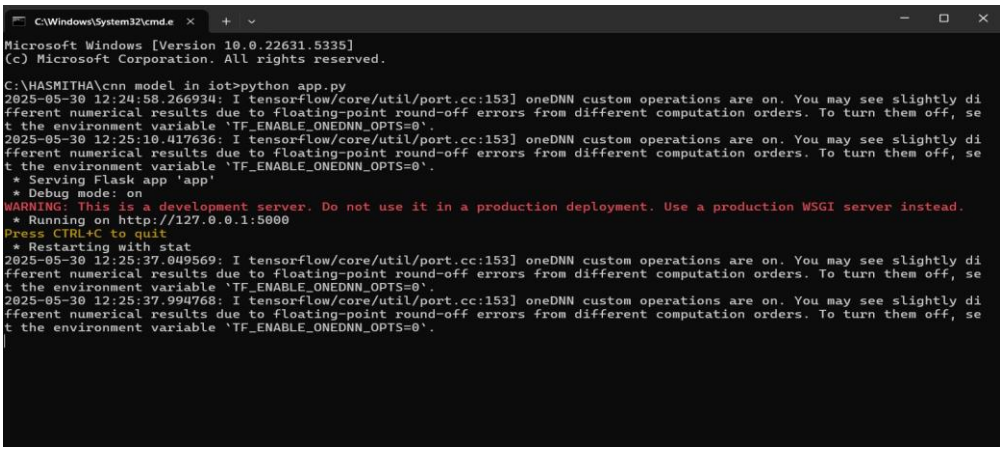

Fig 1 Terminal to run code and get URL

Fig 2 To choose file for Anomaly Detection

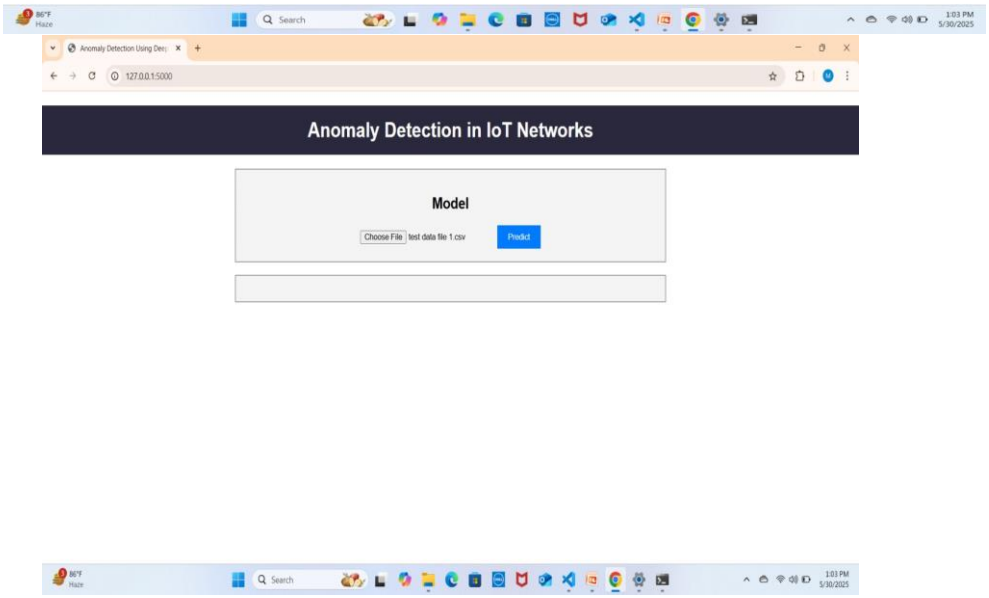

Fig 3 Test file has been choosen

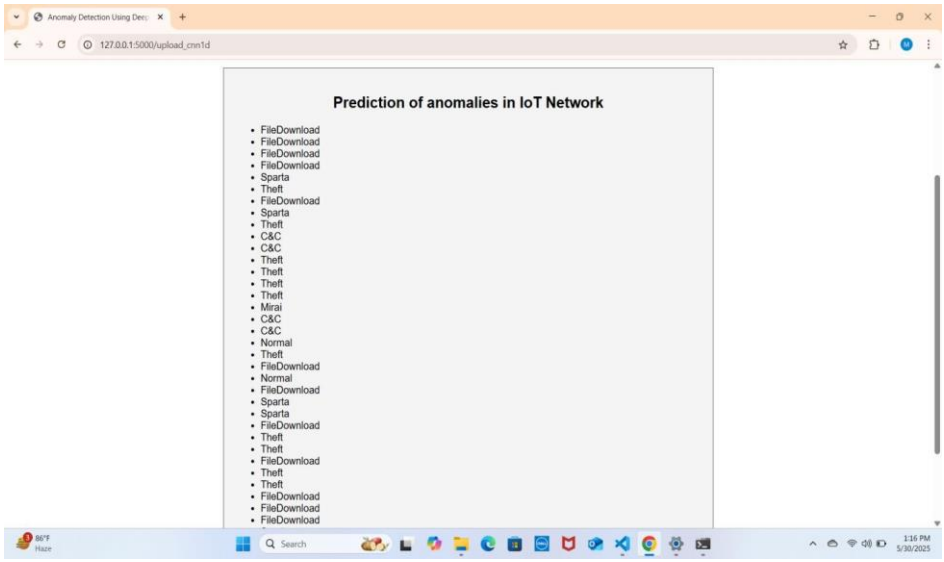

Fig 4 Result of test data file

6-CONCLUSION

The project presents a deep learning-based anomaly detection model for IoT networks using convolutional neural networks (CNNs) to classify both binary and multiclass anomalies. Recognizing that cyber attackers continually develop new methods—such as DDoS and botnet attacks—the study proposes generating a new dataset by combining and transforming existing datasets. This technique enhances the model's ability to detect a wider range of threats. Three datasets were created and merged to expand the number of attack categories, and the model was validated using multiple established intrusion detection datasets, including BoT-IoT, MQTT-IoT-IDS2020, IoT-23, IoT Network Intrusion, IoT-DS-1, and IoT-DS-2. Various CNN architectures (1D, 2D) were used to effectively classify different types of anomalies in IoT traffic. By validating the model on well-known datasets like BoT-IoT, IoT- 23, and MQTT-IoT-IDS2020, the study demonstrates the scalability and reliability of its approach. This project highlights the importance of adaptive, data-driven models in enhancing the security posture of evolving IoT ecosystems.

REFERENCES

[1] S. Smith. (2023). IoT Connections To Reach 83 Billion By 2024, Driven By Maturing Industrial Use Cases. Accessed: Apr. 10, 2023. [Online]. Available: https://www.juniperresearch.com/press/press-releases/iot-conn ections-to-reach-83-billion-by-2024-driven

[2] A. Mukherjee. (2022). IoT Growth Demands Rethink of Long-Term Storage Strategies, Says IDC. Accessed: Apr. 4, 2022. [Online]

[3] C. Robberts and J. Toft, Finding vulnerabilities in IoT devices?: Ethical hackingofelectronic locks, dissertation, School Elect. Eng. Comput.Sci., KTHRoy. Inst. Technol., Stockholm, Sweden, 2021.

[4] C. Meffert, D. Clark, I. Baggili, and F. Breitinger, Forensic state acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition, in Proc. 12th Int. Conf. Availability, Rel. Secur., Aug. 2022, pp. 1 11, doi:

10.1145/3098954.3104053.

[5] S.N.Firdous,Z.Baig,C.Valli,andA.Ibrahim , Modellingandevaluation of malicious attacks against the IoT MQTT protocol, in Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (Green Com) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData), Jun. 2017, pp. 748755, doi: 10.1109/iThings-GreenCom CPSCom-SmartData.2023.115.

[6] I. Ullah and Q. H. Mahmoud. (2021). IoT Intrusion Detection Datasets. Accessed: Apr. 10, 2021. [Online]. Available: https://sites.google. com/view/iotdataset1