Journal of Computer and Electrical Sciences (JCES)- Volume-1 Issue-4, April 2026
ISSN: 3049-2602

AI-BASED ROBUST NETWORK INTRUSION DETECTION SYSTEM

J. Rohitha[1], Mrs. Mary Lavanya[2]

[1]Student, Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada, NTR, Andhra Pradesh, India
[2]Assistant Professor, Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada, NTR, Andhra Pradesh, India

Email: rohithajunapudi1610@gmail.com

Abstract*: With the rapid growth of computer networks and internet-based services, protecting systems from cyberattacks has become a critical challenge. Traditional security mechanisms such as firewalls and signature-based intrusion detection systems are limited in detecting new and evolving attacks. This project proposes a Robust Network Intrusion Detection System (NIDS) based on Machine Learning to enhance network security by accurately identifying both known and unknown intrusions. The proposed system monitors network traffic and extracts relevant features from packet and flow-level data. Machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and Decision Tree are trained on benchmark intrusion datasets to classify network activities as normal or malicious. The model learns traffic patterns and detects anomalies with high accuracy while reducing false positive rates. Performance is evaluated using metrics such as accuracy, precision, recall, and F1-score. This ML-based approach improves adaptability, scalability, and detection efficiency compared to traditional methods. The proposed NIDS can be effectively deployed in enterprise networks, cloud environments, and critical infrastructures to strengthen overall cybersecurity.*

Keywords: **Network Intrusion Detection, Machine Learning, Cybersecurity, Anomaly Detection, Traffic Analysis, Risk Assessment, Web-Based Security Support, Threat Classification, Network Safety.**

1. INTRODUCTION

The rapid growth of computer networks and internet-based services has significantly increased the risk of cyber attacks and security threats. Organizations depend heavily on network systems for communication, data storage, financial transactions, and daily operations. As a result, protecting these networks from malicious activities such as unauthorized access, malware infections, denial-of-service attacks, and data theft has become a major concern in the field of cybersecurity.

Traditional security mechanisms such as firewalls and signature-based intrusion detection systems provide only a basic level of protection. These systems are mainly effective in identifying known threats because they rely on predefined signatures. However, they often fail to detect new or unknown attacks, which makes modern networks vulnerable to advanced and evolving cyber threats.

To overcome these limitations, intrusion detection systems supported by machine learning techniques have gained importance. Machine learning enables the system to learn patterns from large volumes of network traffic data and classify activities as normal or malicious. This helps in improving detection accuracy, identifying unknown attacks, and reducing false alarms.

2. LITERATURE SURVEY

The literature on network security shows that intrusion detection has become an important research area because of the increasing number of cyber threats in modern communication systems. Traditional intrusion detection systems mainly use signature-based and anomaly-based approaches to identify malicious activities in network traffic. Signature-based systems are effective for known attacks, but they cannot detect new or unknown threats. Anomaly-based systems can identify unusual behaviour, but they often suffer from high false positive rates.

Recent studies have introduced machine learning techniques such as Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbour, and Artificial Neural Networks for intrusion detection. These methods analyze network traffic data, learn hidden patterns, and classify activities as normal or malicious. Researchers commonly use benchmark datasets such as KDD Cup 1999, NSL-KDD, CICIDS, and UNSW-NB15 to evaluate the performance of these models.

Although many machine learning-based systems have improved intrusion detection accuracy, existing approaches still face limitations such as high computational complexity, inefficient feature selection, limited real-time capability, and difficulty in adapting to evolving attack patterns. Based on these observations, the proposed system is designed to provide a more robust and scalable intrusion detection framework using machine learning for accurate and efficient cyber attack detection.

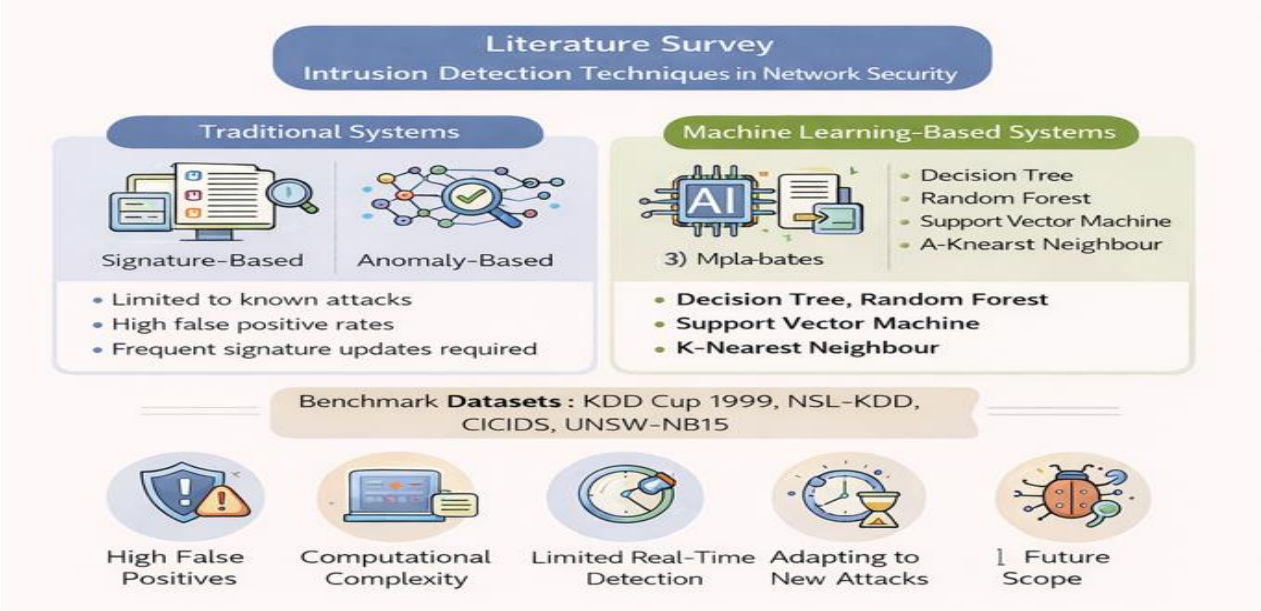

Fig 1: Comparisons Between two systems

3. PROPOSED SYSTEM

The proposed **ML-Based Robust Network Intrusion Detection System** is designed in a modular and scalable manner so that network traffic monitoring, preprocessing, feature extraction, model prediction, and alert generation can work together efficiently. The system aims to detect both known and unknown intrusions by using machine learning techniques on structured network traffic data.

The major components of the proposed system are:

3.1 System Components

- **Presentation Layer:** User interface for monitoring network traffic and viewing alerts
- **Application Layer:** Backend logic for preprocessing, feature extraction, model execution, and alert handling
- **Data Layer:** Database and intrusion datasets used for storing traffic logs and training records

3.2 Functional Modules

1. Data Collection Module
Collects network traffic data from datasets or monitoring tools. The data contains both normal and malicious traffic records.

2. Data Preprocessing Module
Cleans the collected data by removing duplicates, handling missing values, and converting categorical values into machine-readable form.

3. Feature Extraction Module
Selects important attributes such as protocol type, packet size, source and destination addresses, connection duration, and failed login attempts.

4. Prediction Engine
Uses trained machine learning algorithms such as Random Forest, Decision Tree, and Support Vector Machine to classify traffic as normal or malicious.

5. Alert Generation Module
Generates alerts whenever suspicious or malicious network activity is detected.

6. Log Management Module
Stores detected intrusion records and system logs for future analysis and monitoring.

The system follows a machine learning-based approach in which the trained model learns patterns from historical network traffic and applies this knowledge to detect cyber threats in incoming data. This improves detection efficiency, adaptability, and overall network security.

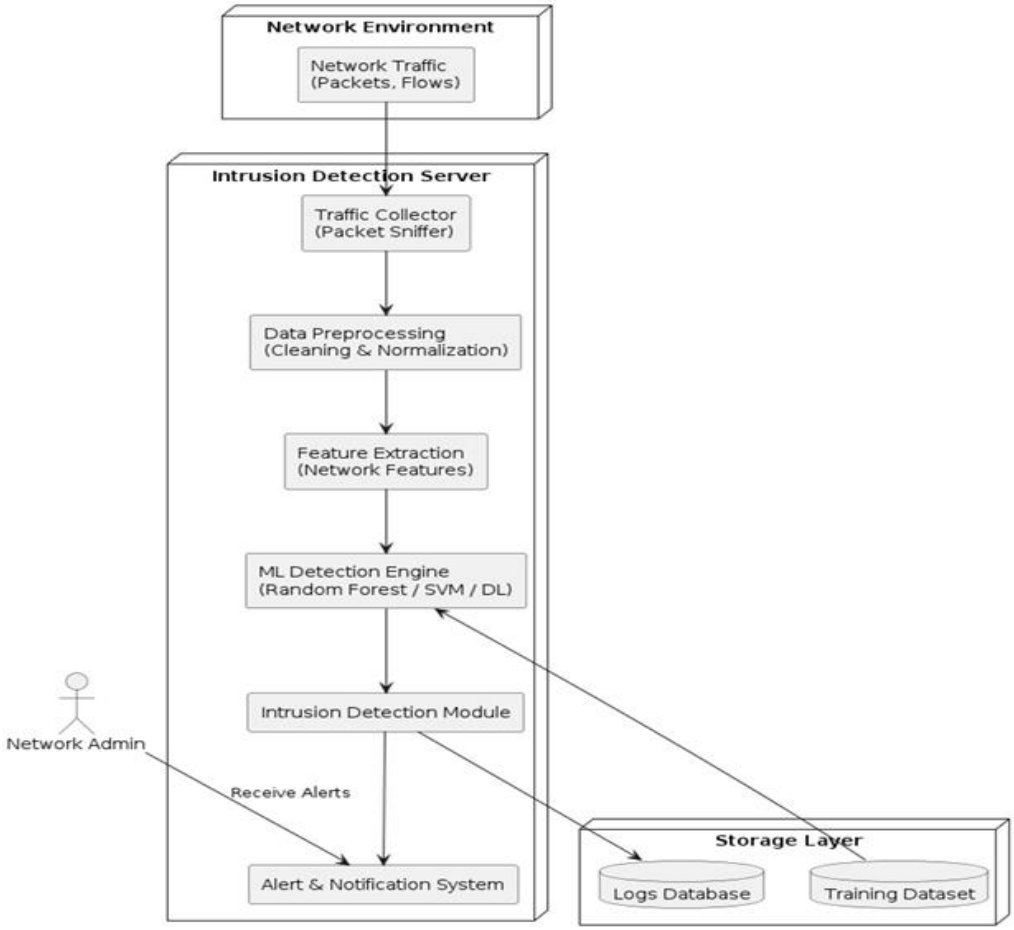

Fig 2: System Architecture

4. METHODOLOGY

The methodology of the proposed system is as follows:

1. Data Collection:
The system collects network traffic data from standard intrusion detection datasets containing both normal and attack-related records.
2. Data Preprocessing:
The collected data is cleaned by removing duplicate values, handling missing data, encoding categorical features, and normalizing input values where required.
3. Feature Extraction:
Important features such as protocol type, connection duration, packet size, source address, destination address, and failed login attempts are selected for analysis.
4. Model Training:
Machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine, and

K-Nearest Neighbour are trained using the processed dataset.

5. Intrusion Detection:

The trained model analyzes incoming network traffic and predicts whether the activity is normal or malicious.

6. Alert Generation:

If suspicious behaviour is detected, the system generates alerts to notify the network administrator for immediate response.

This methodology helps improve intrusion detection accuracy, reduces manual monitoring effort, and supports efficient network security management..

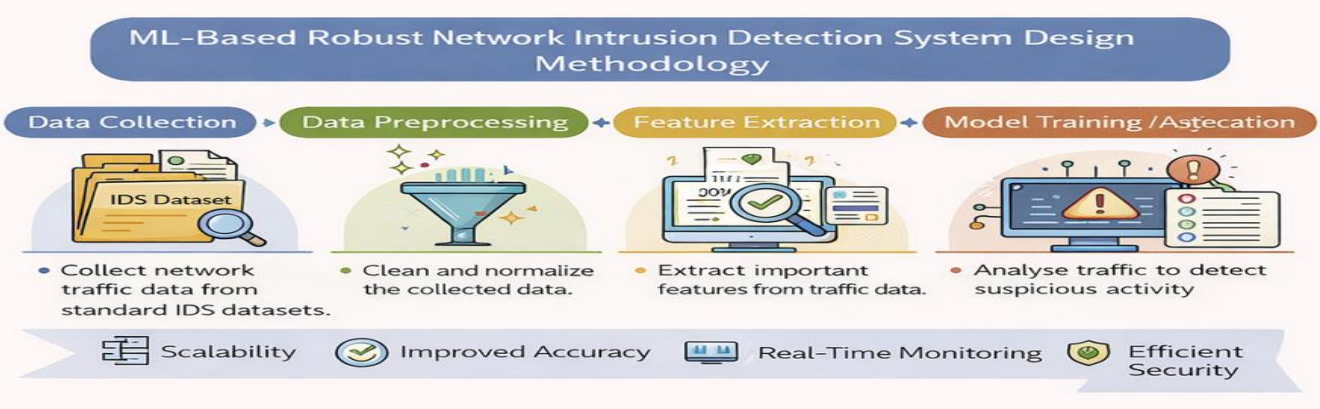

Fig 3: Design Methodology

IMPLEMENTATION AND RESULTS

The proposed ML-Based Robust Network Intrusion Detection System is implemented as a machine learning-based security solution for detecting cyber attacks in network environments. The system is developed using Python and related machine learning libraries for preprocessing, classification, and evaluation. The model is trained using benchmark intrusion detection datasets and tested on different categories of network traffic.

The implementation includes modules for data collection, preprocessing, feature extraction, machine learning model training, intrusion detection, and alert generation. The system uses algorithms such as Random Forest, Decision Tree, and Support Vector Machine to classify traffic patterns. The prediction results are used to determine whether the observed activity is normal or malicious.

Experimental results show that the proposed system improves intrusion detection accuracy and reduces false positive rates compared to traditional rule-based approaches. The system can identify suspicious traffic effectively and provide timely alerts, making it useful for practical cybersecurity applications.

The system is implemented using:

- **Frontend:** User monitoring interface
- **Backend:** Python-based processing and prediction
- **Database:** MySQL / traffic log storage

Key features include:

- Network traffic monitoring
- Data preprocessing and feature extraction
- Machine learning-based classification
- Intrusion alert generation
- Log storage and analysis

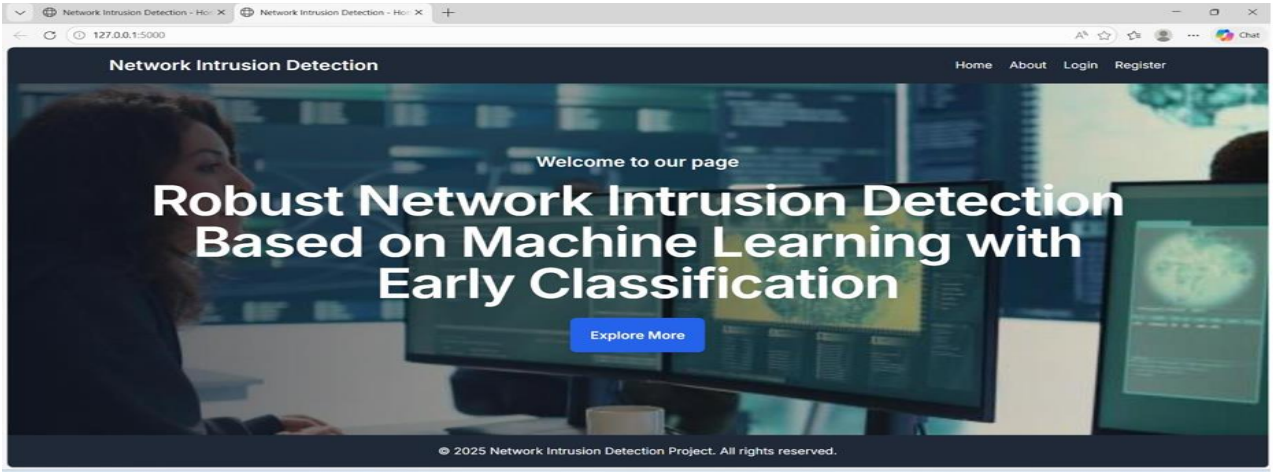

Fig 4: Index Interface

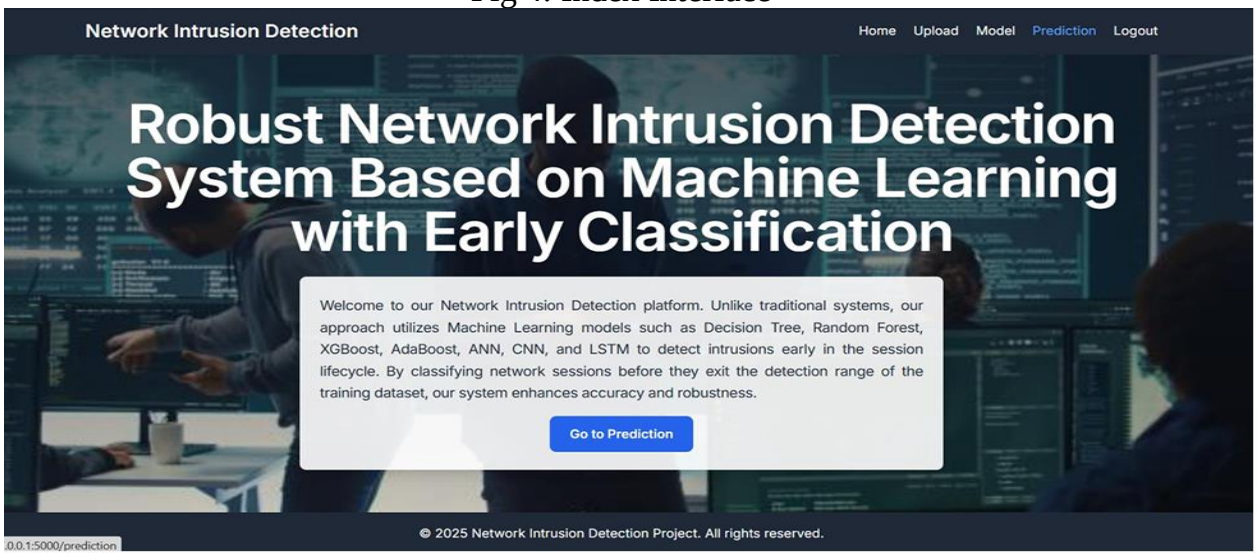

Fig 5: Login Page

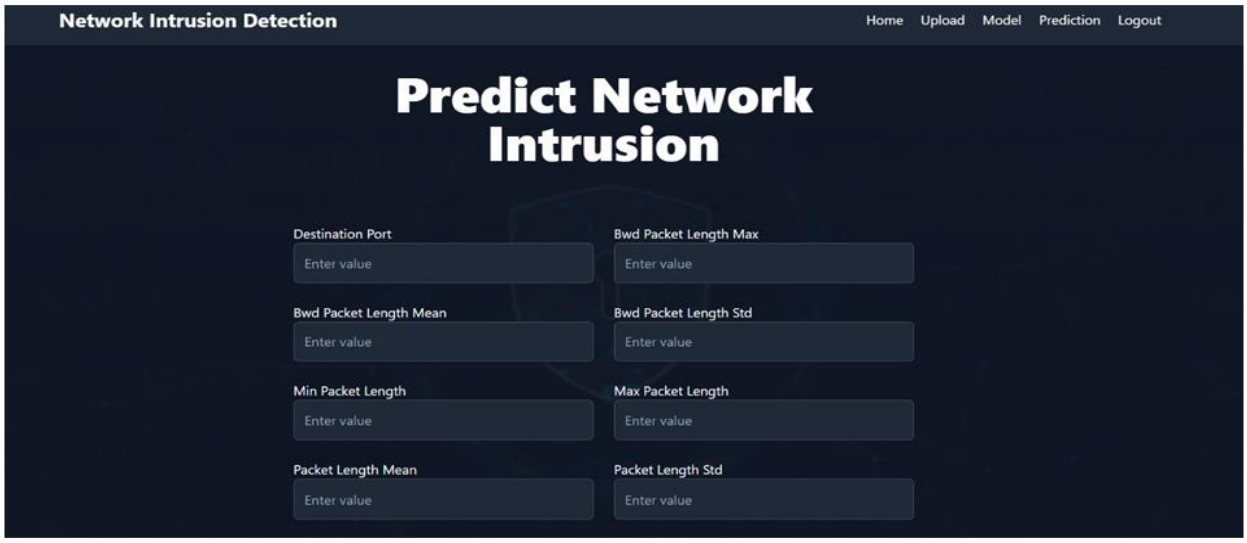

Fig 6: Prediction Page

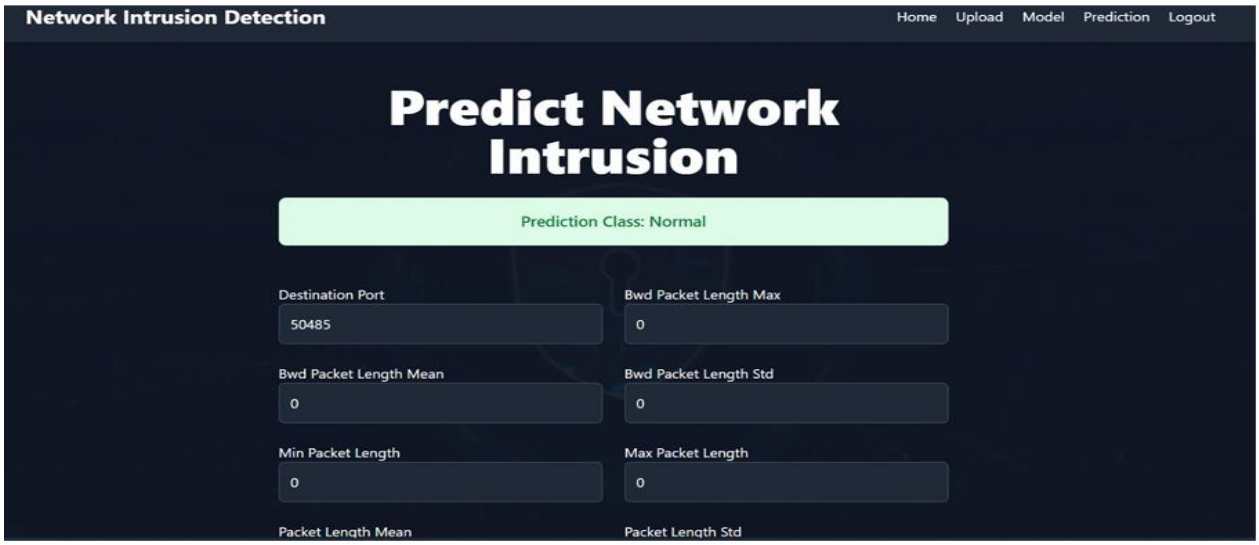

Fig 7: Results Page

5. FUTURE SCOPE

The proposed system can be further enhanced by using larger and more diverse intrusion datasets for better model generalization. Advanced deep learning techniques can also be applied to improve detection of complex and evolving cyber attacks. Real-time deployment in live network environments can make the system more practical for enterprise and cloud security applications.

In future versions, the project can be extended with automated response mechanisms, cloud-based intrusion monitoring, IoT security support, and advanced visualization dashboards. Continuous retraining and adaptive learning can further improve system accuracy and efficiency.

6. CONCLUSION

In this paper, an **ML-Based Robust Network Intrusion Detection System** is presented as an intelligent cybersecurity solution for detecting malicious activities in network traffic. By applying machine learning techniques to intrusion detection, the system can identify both known and unknown attacks more effectively than traditional methods. The proposed approach improves detection accuracy, reduces false alarms, and supports timely alert generation for administrators.The system provides a scalable and efficient framework for strengthening network security in modern digital environments. Overall, the proposed project demonstrates how machine learning can enhance intrusion detection and contribute to improved cybersecurity management.

REFERENCES

[1] Machine Learning – Tom M. Mitchell, McGraw-Hill Education, 1997.
[2] Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow – Aurélien Géron, O'Reilly Media, 2019.
[3] Artificial Intelligence: A Modern Approach – Stuart Russell and Peter Norvig, Pearson Education.
[4] Node.js Official Documentation – https://nodejs.org
[5] React Official Documentation – https://react.dev
[6] MySQL Official Documentation – https://www.mysql.com
[7] Scikit-learn Documentation – https://scikit-learn.org
[8] IEEE Research papers on Network Intrusion Detection Systems.
[9] KDD Cup Network Intrusion Detection Dataset.