AI-Based Iot Intrusion Detection System

Akhil S. S[1], Adin Rejo R[2], Aswin S[3], Geethu John[4]
[1,2,3]*UG Student, Department of Computer science & Engineering, Sivaji College of Engineering and Technology*
[4]*Assistant Professor, Department of Computer science and Engineering, Sivaji College of Engineering and Technology*
doi.org/10.64643/IJIRTV12I11-201419-459

***Abstract*—The rapid expansion of Internet of Things (IoT) devices across various domains such as smart homes, healthcare, and industrial automation has introduced significant security challenges. Traditional intrusion detection systems (IDS) are not efficient in handling the dynamic and large-scale nature of IoT networks. This paper proposes an AI-based IoT Intrusion Detection System that utilizes machine learning algorithms to detect both known and unknown cyber threats in real time. The system collects network traffic data, preprocesses it, extracts relevant features, and applies trained models such as Random Forest and LSTM for classification. The proposed system ensures improved detection accuracy, reduced false positives, and real-time monitoring through a dashboard interface. The results demonstrate that AI-driven IDS provides a scalable and efficient solution for securing IoT environments.**

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized modern technology by enabling interconnected devices in various sectors such as healthcare, smart cities, and industries. However, the increasing number of IoT devices has also led to a rise in security threats due to their limited computational capabilities and lack of robust security mechanisms. Traditional intrusion detection systems are not well-suited for IoT environments because they rely on predefined rules and cannot efficiently detect unknown attacks.

To overcome these challenges, artificial intelligence (AI) and machine learning (ML) techniques are introduced in intrusion detection systems. These techniques help in identifying abnormal patterns and detecting cyber-attacks in real time.

This paper presents an AI-based IoT Intrusion Detection System that enhances security by continuously monitoring network traffic and detecting malicious activities.

The rapid advancement of the Internet of Things (IoT) has led to the widespread deployment of interconnected devices across various domains, including smart homes, healthcare systems, industrial automation, and smart cities. These devices continuously generate and exchange large volumes of data, enabling automation and intelligent decision-making. However, the increasing number of IoT devices has significantly expanded the attack surface, making IoT networks highly vulnerable to cyber threats.

In this paper, an AI-Based IoT Intrusion Detection System is proposed to enhance the security of IoT networks. The system utilizes machine learning algorithms to analyze network traffic, detect malicious activities, and generate alerts for timely response.

II. PROBLEM STATEMENT

The rapid growth of IoT devices has introduced significant security challenges due to their heterogeneous nature and resource limitations. Most IoT devices operate with limited computational power, memory, and energy constraints, which restrict the implementation of robust security mechanisms. Additionally, many devices lack regular firmware updates and use insecure communication protocols, making them highly vulnerable to cyber-attacks.

Traditional intrusion detection systems are not suitable for IoT environments as they rely heavily on predefined signatures and rule-based mechanisms. These systems are unable to effectively detect zero-day attacks and struggle to scale with the increasing volume of IoT network traffic.

Furthermore, they often produce high false positive rates and require frequent manual updates, reducing

their efficiency in dynamic environments.

As a result, IoT networks are increasingly exposed to various security threats, including Distributed Denial of Service (DDoS) attacks, botnet infections, data exfiltration, and device spoofing. These vulnerabilities can lead to severe consequences such as data breaches, service disruption, and unauthorized access to sensitive information. Therefore, there is a critical need for an intelligent, adaptive, and scalable intrusion detection system that can automatically analyze IoT network traffic, identify anomalous behavior, and detect both known and unknown attacks in real time. The proposed solution aims to address these challenges using AI and machine learning techniques to enhance the overall security of IoT ecosystems.

III. OBJECTIVES

The main objective of the proposed AI-Based IoT Intrusion Detection System is to ensure secure and reliable communication within IoT environments by continuously monitoring network traffic in real time. The system aims to detect and classify various types of cyber-attacks, including both known and unknown (zero-day) threats, using advanced machine learning and deep learning techniques. It focuses on improving detection accuracy while minimizing false positive and false negative rates. Additionally, the system is designed to be scalable and efficient, making it suitable for large-scale IoT deployments. Overall, the proposed system seeks to enhance the security, performance, and reliability of IoT networks through intelligent and automated intrusion detection mechanisms.

IV. LITERATURE REVIEW

Intrusion Detection Systems (IDS) have been extensively studied over the years to enhance network security. Early work by Denning (1987) introduced the concept of anomaly detection using statistical models, which laid the foundation for modern IDS. Traditional datasets such as KDD CUP 99 were widely used for evaluating IDS performance; however, they suffered from issues like redundancy and lack of representation of modern attack patterns. To overcome these limitations, more recent datasets such as UNSW-NB15 were developed, providing realistic and diverse network traffic for improved evaluation.

With the advancement of machine learning, various classification algorithms such as Support Vector Machines (SVM), k-Nearest Neighbors (KNN), and Random Forest have been applied for intrusion detection, achieving considerable accuracy.

In recent years, deep learning techniques including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks have shown superior performance in capturing complex patterns and temporal dependencies in network traffic.

Furthermore, hybrid approaches that combine signature-based and anomaly-based detection methods have been proposed to improve robustness. In the context of IoT environments, several studies have focused on adapting these techniques to handle resource constraints and dynamic network behavior. Federated learning has also been introduced to enhance privacy by enabling distributed model training without sharing raw data.

Despite these advancements, challenges such as high computational cost, scalability issues, and real-time implementation remain significant. Therefore, there is a need for efficient and scalable AI-based intrusion detection systems tailored specifically for IoT networks.

V. EXISTING SYSTEM

Existing intrusion detection systems in IoT environments primarily rely on traditional signature-based and basic anomaly detection techniques. These systems operate by comparing incoming network traffic with a predefined database of known attack patterns and generating alerts when a match is found. While such approaches are effective in detecting known threats, they are not capable of identifying new or unknown (zero-day) attacks. Additionally, these systems require frequent manual updates to maintain the signature database, which is time-consuming and inefficient.

In many cases, traditional IDS also suffer from high false positive rates, leading to unnecessary alerts and reduced system reliability. Furthermore, they are not designed to handle the large-scale, dynamic, and heterogeneous nature of IoT networks, resulting in poor scalability and performance issues. Some advanced systems that use deep learning techniques provide improved detection accuracy but introduce

high computational overhead, making them unsuitable for resource-constrained IoT devices. As a result, existing systems fail to provide an efficient, scalable, and adaptive solution for securing modern IoT environments.

Existing intrusion detection systems mainly rely on signature-based techniques to identify known attacks, making them ineffective against new and unknown threats. Additionally, they suffer from scalability issues, high false positive rates, and are not suitable for dynamic and resource-constrained IoT environments.

VI. PROPOSED SYSTEM

The proposed system is an AI-based IoT Intrusion Detection System designed to provide intelligent, real-time security for IoT environments. The system integrates machine learning and deep learning techniques to analyze network traffic and identify both known and unknown cyber threats with high accuracy. It begins with real-time data collection from IoT devices through network gateways, followed by data preprocessing and feature extraction to prepare the data for analysis. Advanced models such as Random Forest and Long Short-Term Memory (LSTM) networks are trained to learn normal traffic behavior and detect anomalies that indicate potential intrusions. The system continuously monitors incoming traffic and classifies it as normal or malicious, ensuring timely detection of attacks such as DDoS, spoofing, and botnet activities.

Furthermore, the proposed system is designed to be scalable and efficient, making it suitable for large-scale and dynamic IoT networks. It significantly reduces false positive rates compared to traditional systems and provides real-time alerts and logging mechanisms for quick response and analysis. A dashboard interface is also integrated to visualize network activity and detected threats, enhancing usability and monitoring capabilities. Overall, the system offers an adaptive, automated, and robust solution for improving the security and reliability of modern IoT ecosystems.

The system is designed to be scalable and efficient, making it suitable for handling large and dynamic IoT networks. It reduces false positive rates and provides real-time alerts and logging for detected intrusions. Additionally, a dashboard is integrated for monitoring network activity and visualizing attack patterns, ensuring better control and management of IoT security.

VII. SYSTEM ARCHITECTURE

The system architecture of the proposed AI-Based IoT Intrusion Detection System is designed as a multi-layered framework that ensures efficient data flow, real-time analysis, and accurate threat detection. The architecture begins with IoT devices and sensors that generate network traffic, which is captured at the gateway or router level using packet sniffing tools. The collected data is then passed to the preprocessing layer, where noise removal, normalization, and data cleaning are performed. Following this, the feature extraction layer identifies relevant attributes such as packet size, protocol type, and communication patterns.

Finally, a visualization dashboard presents real-time monitoring results, attack statistics, and system status to the user. This layered architecture ensures scalability, efficient processing, and reliable security for dynamic IoT environments.

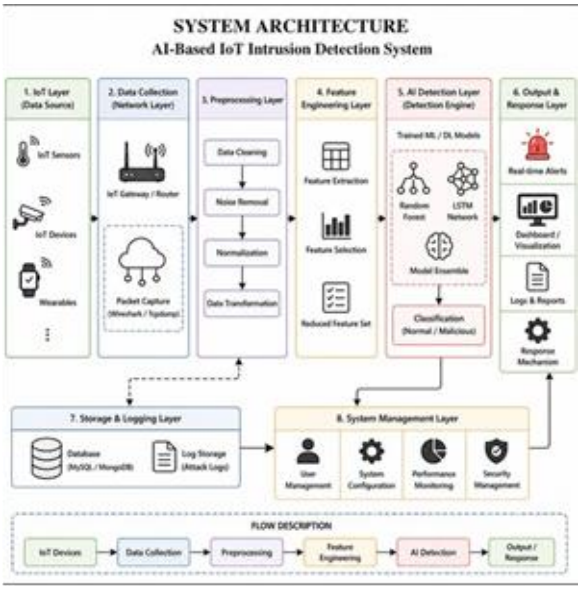

Fig.1 System architecture of proposed AI-based IoT Intrusion Detection System.

VIII. MODULES DESCRIPTION

The proposed AI-Based IoT Intrusion Detection System consists of several functional modules that work together to ensure efficient and accurate threat

detection. The Data Collection Module captures real-time network traffic from IoT devices using packet sniffing tools or network logs. The Feature Extraction Module processes the collected data to identify relevant attributes such as packet size, protocol type, and communication patterns. The Data Preprocessing Module cleans and transforms the data by removing noise, handling missing values, and normalizing features to improve model performance.

The AI Detection Module plays a key role by applying trained machine learning and deep learning models, such as Random Forest and LSTM, to classify network traffic as normal or malicious. Once an intrusion is detected, the Alert Generation Module generates real-time notifications to inform the user about potential threats.

The Logging Module records all detected events and stores them in a database for future analysis and auditing purposes. Finally, the Dashboard Visualization Module provides an interactive interface to monitor network activity, visualize attack patterns, and display system performance. Together, these modules form a comprehensive and scalable intrusion detection framework for IoT environments.

Modules Description: -

- Data Collection Module: Captures IoT network traffic
- Feature Extraction Module: Extracts important features
- Preprocessing Module: Cleans and normalizes data
- AI Detection Module: Classifies traffic
- Alert Module: Generates alerts
- Logging Module: Stores logs
- Dashboard Module: Displays results

The proposed AI-Based IoT Intrusion Detection System is composed of multiple interconnected modules, each responsible for a specific function in the detection process. The Data Collection Module serves as the entry point of the system, where real-time network traffic is captured from IoT devices using packet sniffing tools or network logs at the gateway level. This module ensures continuous monitoring of communication between devices, forming the basis for further analysis. The Feature Extraction Module processes the collected raw data to identify and extract relevant attributes such as packet size, protocol type, source and destination information, and traffic patterns. These features are essential for accurately distinguishing between normal and malicious activities. Following this, the Data Preprocessing Module cleans and prepares the data by removing noise, handling missing values, and normalizing features to improve the efficiency and accuracy of the detection model.

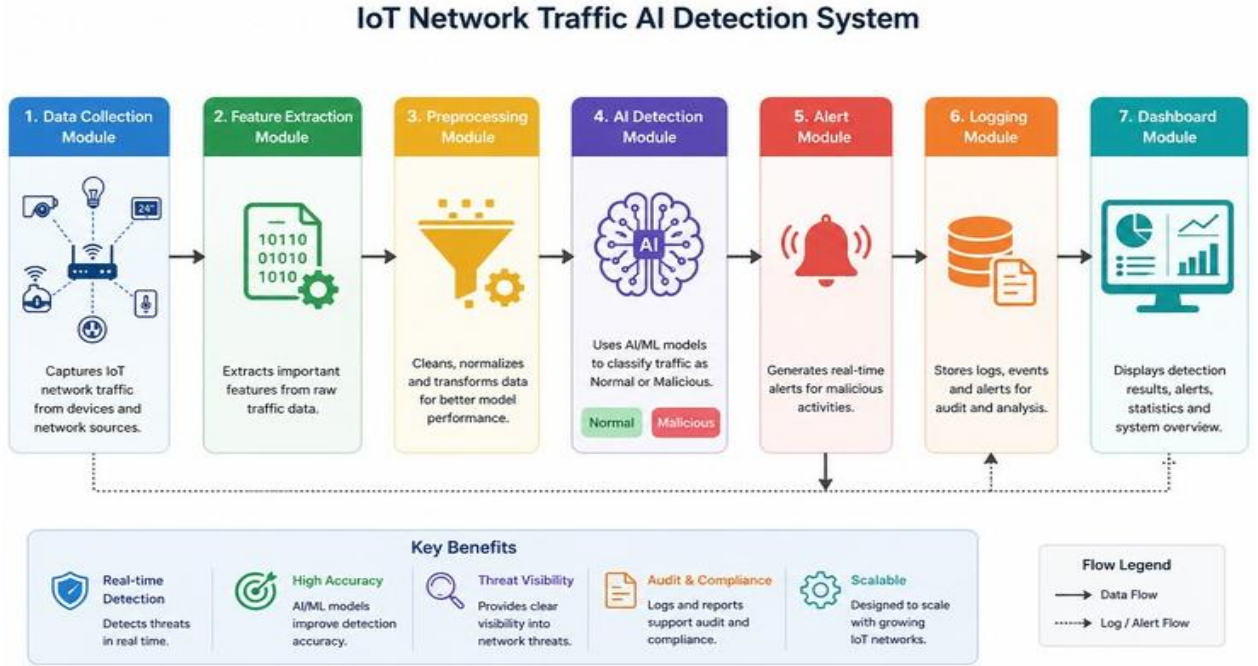

Fig.2 Modules description

IX. METHODOLOGY

The methodology of the proposed AI-Based IoT Intrusion Detection System consists of a sequence of structured steps designed to ensure accurate and real-time detection of cyber threats. Initially, data collection is performed by capturing network traffic from IoT devices through gateways or routers using packet sniffing tools or network logs. The collected raw data is then passed to the preprocessing stage, where noise and redundant information are removed, missing values are handled, and the data is normalized to improve consistency and model performance.

Following preprocessing, the feature extraction phase identifies important attributes such as packet size, protocol type, source and destination addresses, and traffic patterns, which are essential for distinguishing between normal and malicious behavior. The processed dataset is then used to train machine learning and deep learning models, including algorithms such as Random Forest and Long Short-Term Memory (LSTM), using labeled data representing both normal and attack scenarios.

In addition to the core detection process, the methodology emphasizes system efficiency and adaptability in dynamic IoT environments. The integration of automated data processing and intelligent learning models enables the system to respond quickly to changing network conditions. By combining real-time monitoring with periodic model updates, the system maintains high detection accuracy while minimizing computational overhead. This ensures that the proposed intrusion detection system remains reliable, scalable, and effective for securing modern IoT networks.

Furthermore, the proposed methodology ensures seamless integration with existing IoT infrastructures without requiring significant modifications. The modular design of the system allows each component to function independently while maintaining efficient coordination with other modules. This flexibility enables easy deployment and maintenance in various IoT environments. As a result, the system not only improves intrusion detection capability but also enhances overall system performance and reliability.

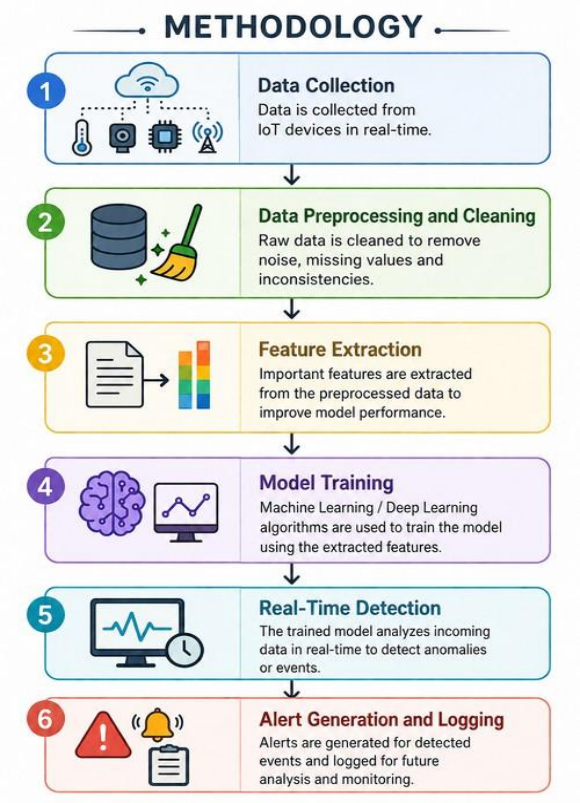

Fig.10 Methodology

X. RESULTS

The results of the proposed AI-Based IoT Intrusion Detection System demonstrate its effectiveness in accurately detecting and classifying various types of cyber-attacks in IoT environments. The system was evaluated using network traffic data containing both normal and malicious activities, and the machine learning models achieved high detection accuracy with significantly reduced false positive rates compared to traditional intrusion detection methods. The integration of algorithms such as Random Forest and LSTM enabled the system to identify complex attack patterns, including DDoS, spoofing, and botnet activities.

Furthermore, the system successfully performed real-time monitoring and detection, generating timely alerts for potential intrusions. The dashboard interface provided clear visualization of network activity and detected threats, allowing for efficient analysis and response. Overall, the experimental results indicate that the proposed system is scalable, reliable, and well-suited for securing dynamic and large-scale IoT networks.

The proposed AI-Based IoT Intrusion Detection System achieved high accuracy in detecting various cyber-attacks while reducing false positives. It successfully performed real-time monitoring and generated timely alerts for potential threats. The results confirm that the system is efficient and suitable for securing IoT environments.

XI. FUTURE ENHANCEMENT

Future enhancements of the proposed AI-Based IoT Intrusion Detection System can focus on improving detection accuracy and expanding system capabilities. Advanced deep learning models and hybrid techniques can be incorporated to enhance the detection of complex and evolving cyber threats. The system can also be integrated with automated intrusion prevention mechanisms to not only detect but also respond to attacks in real time. Additionally, implementing federated learning can improve data privacy by enabling decentralized model training across IoT devices.

Further improvements may include optimizing the system for deployment on low-resource IoT devices and extending support for large-scale distributed environments. The integration of blockchain technology can also be explored to ensure secure data sharing and tamper-proof logging. Overall, these enhancements aim to make the system more intelligent, adaptive, and robust for future IoT security challenges.

XII. CONCLUSION

In conclusion, the proposed AI-Based IoT Intrusion Detection System provides an effective and intelligent solution for enhancing security in IoT environments. By leveraging machine learning and deep learning techniques, the system is capable of accurately detecting both known and unknown cyber threats in real time. The integration of modules such as data collection, preprocessing, feature extraction, and AI-based detection ensures a systematic and efficient approach to intrusion detection.

The system demonstrates improved performance in terms of detection accuracy, reduced false positives, and scalability compared to traditional methods. Its ability to continuously monitor network traffic and generate timely alerts makes it suitable for dynamic and large-scale IoT applications. Overall, the proposed approach contributes to building a more secure, reliable, and adaptive IoT ecosystem, addressing the growing challenges of modern network security.

REFERENCES

[1] K. Alrawashdeh and C. Purdy, “Toward an Online Anomaly Intrusion Detection System Based on Deep Learning,” in *Proc. IEEE Int. Conf. on Machine Learning and Applications*, 2016.

[2] R. Vinayakumar, K. P. Soman, and P. Poornachandran, “Deep Learning Approach for Intelligent Intrusion Detection System,” *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[3] R. Doshi, N. Apthorpe, and N. Feamster, “Machine Learning DDoS Detection for Consumer Internet of Things Devices,” in *Proc. IEEE Security and Privacy Workshops*, 2018.

[4] N. Moustafa and J. Slay, “UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems,” in *Proc. Military Communications and Information Systems Conf. (MilCIS)*, 2015.

[5] Y. Zhang, M. Chen, *et al*., “Federated Learning for Internet of Things: Applications, Challenges, and Opportunities,” *IEEE Internet of Things Journal*, 2021.