Edge AI–Based Real-Time Intrusion Detection System for Secure IoT Networks

Prof. Aarti R. Jaiswal[1], Hasib Nisar Baig[2], Hamza Ali Quazi[3], Himanshi Bhandekar[4], Himanshu Dhongade[5], Ishwari Thakare[6], Janhavi Jadhao[7], Jayash Rathod[8], Karan Rathod[9]

[1]*Assistant Professor, Jagadambha College of Engineering and Technology, Yavatmal, Maharashtra, India*

[2,3,4,5,6,7,8,9]*Student, Jagadambha College of Engineering and Technology, Yavatmal, Maharashtra, India*

Abstract— The rapid growth of Internet of Things (IoT) devices has greatly improved automation, connectivity, and data-driven services. However, the increasing number of connected devices also raises their vulnerability to cyberattacks. Traditional intrusion detection systems depend on centralized cloud processing, which can introduce delays and may not respond quickly enough to immediate threats. This research proposes a system based on Edge Artificial Intelligence (Edge AI) specifically designed for IoT networks. This framework deploys lightweight machine learning models at edge nodes to detect abnormal traffic patterns and malicious activities in real time. The system analyzes network traffic locally, which cuts down communication delays and improves detection speed. Experimental evaluation shows that the proposed architecture increases detection accuracy while reducing latency and bandwidth use. The results highlight the potential of combining edge computing with artificial intelligence to create secure, scalable, and efficient IoT infrastructures.

Index Terms— Edge Computing, Intrusion Detection System, IoT Security, Machine Learning, Cybersecurity.

I. INTRODUCTION

The Internet of Things has become one of the most impactful technological advances in modern computing. IoT systems connect sensors, smart devices, industrial machines, and consumer electronics over the internet to enable automation and smart decision-making. Examples of IoT applications include smart homes, healthcare monitoring systems, industrial automation platforms, and intelligent transportation networks. Despite their advantages, IoT devices often have limited resources and lack strong security measures. Many IoT devices run with minimal processing power and limited memory, making it hard to implement traditional security solutions. Because of this, attackers frequently take advantage of these weaknesses to launch distributed denial-of-service attacks, steal data, inject malware, and gain unauthorized access. Large-scale cyber incidents like botnet attacks show how insecure IoT devices can serve as entry points for widespread network threats. Intrusion Detection Systems (IDS) are commonly used to monitor network traffic and spot suspicious activities. Conventional IDS architectures heavily rely on centralized cloud servers for analyzing network data. However, this cloud-based detection can introduce delays and use significant bandwidth since all network data must be sent to remote servers for analysis. Edge computing offers a promising alternative by processing data closer to where it originates. By integrating machine learning algorithms at edge nodes, security threats can be detected in real time without fully depending on centralized infrastructure. This research aims to design an Edge AI-based intrusion detection framework that can enhance security in IoT networks while also maintaining efficiency and scalability.

II. RELATED WORK

Several studies have examined intrusion detection methods for IoT environments. Traditional signature-based systems depend on predefined patterns of known attacks. While these systems can effectively detect previously identified threats, they often struggle with new or evolving attacks. Machine learning-based detection methods have become more popular because they can identify anomalies and unknown attack patterns. Prior research has put forward cloud-based

machine learning models to analyze IoT traffic. These methods commonly use algorithms like Support Vector Machines, Random Forest, and Neural Networks. While these models achieve high detection rates, their reliance on cloud processing increases network delays and raises potential privacy issues. Recent advances in edge computing allow machine learning models to run directly on local gateways or edge devices. This method cuts down latency and enables quicker response times. Some studies have explored lightweight deep learning models optimized for edge devices. However, many systems still face challenges related to model efficiency, data privacy, and scalability. The proposed research builds on earlier efforts by merging edge-based machine learning with distributed monitoring mechanisms. The goal is to create a system that balances detection accuracy with computational efficiency so it can function effectively in real-world IoT settings.

III. SYSTEM ARCHITECTURE

The proposed intrusion detection framework consists of four main layers: Device Layer, Edge Processing Layer, Detection Layer, and Management Layer. The Device Layer includes IoT sensors, smart appliances, cameras, and industrial devices that generate network traffic. These devices connect with local gateways or routers that serve as edge nodes. The Edge Processing Layer performs initial data filtering and feature extraction. Instead of sending raw traffic to the cloud, edge nodes analyze packets locally to identify key traffic features such as packet size, protocol type, and connection frequency. The Detection Layer consists of machine learning models trained to classify network behavior as normal or malicious. These models run directly on the edge nodes and continuously monitor traffic patterns. If abnormal activity is detected, alerts are generated immediately. The Management Layer oversees updates, maintains logs, and conducts system monitoring. Security administrators can use this layer to analyze attack trends, update detection models, and manage network policies. This layered structure ensures efficient monitoring while minimizing communication overhead.

IV. METHODOLOGY

The methodology of the proposed research includes data collection, feature extraction, model training, and system deployment. First, network traffic datasets, representing both normal and malicious behavior, were collected from public cybersecurity repositories and simulated IoT environments. Feature extraction techniques were used to convert raw network packets into structured datasets suitable for machine learning analysis. Indicators of abnormal activity included connection duration, packet rate, and protocol distribution. During experimentation, several machine learning algorithms were assessed, including Decision Trees, Random Forest classifiers, and lightweight neural networks. The models were trained with labeled datasets and validated through cross-validation techniques to ensure reliability. To support edge deployment, the trained models were optimized to minimize memory usage and computational complexity. Techniques like model compression and pruning were used to ensure the detection system could run efficiently on resource-limited edge devices. Finally, the optimized models were deployed on edge nodes where they monitored live network traffic and generated alerts whenever suspicious patterns were detected. V. RESULTS AND ANALYSIS An experimental evaluation was conducted to assess the performance of the proposed system. Metrics such as detection accuracy, precision, recall, latency, and resource utilization were considered during the analysis. The edge-based intrusion detection model achieved high accuracy in identifying common attack types, including denial of service attacks, port scanning attempts, and malware communication patterns. Compared to centralized cloud-based detection systems, the proposed approach significantly reduced response times. Latency measurements indicated that analyzing traffic locally at the edge reduced detection delays by nearly fifty percent in many cases. This improvement allows for quicker responses to cyber threats and stops the spread of malicious activities across networks. The system also showed efficient resource usage. Only summarized alerts were sent to the cloud, which significantly reduced network bandwidth consumption. These results confirm that edge-based detection can provide both security enhancements and operational efficiency.

V. RESULTS AND ANALYSIS

An experimental evaluation was conducted to assess the performance of the proposed system. Metrics such as detection accuracy, precision, recall, latency, and resource utilization were considered during the analysis. The edge-based intrusion detection model achieved high accuracy in identifying common attack types, including denial of service attacks, port scanning attempts, and malware communication patterns. Compared to centralized cloud-based detection systems, the proposed approach significantly reduced response times. Latency measurements indicated that analyzing traffic locally at the edge reduced detection delays by nearly fifty percent in many cases. This improvement allows for quicker responses to cyber threats and stops the spread of malicious activities across networks. The system also showed efficient resource usage. Only summarized alerts were sent to the cloud, which significantly reduced network bandwidth consumption. These results confirm that edge-based detection can provide both security enhancements and operational efficiency.

VI. ADVANTAGES AND LIMITATIONS

The proposed system offers several benefits for modern IoT networks. First, real-time detection leads to quicker responses to cyber threats. Second, edge processing decreases reliance on centralized cloud infrastructure, improving scalability and resilience. Third, local data processing boosts privacy because sensitive traffic data does not need to be sent to external servers. Despite these benefits, some limitations still exist. Edge devices generally have limited computing power, which restricts the complexity of machine learning models that can be deployed. Additionally, keeping training datasets updated is crucial to ensure the system continues to recognize new types of cyberattacks. Another issue is securely updating machine learning models across distributed edge nodes. Future systems must include secure update methods to prevent attackers from tampering with detection models.

VII. FUTURE SCOPE

Future research can further improve edge-based intrusion detection by integrating advanced deep learning models specifically designed for embedded hardware. Techniques like federated learning may allow multiple edge nodes to collaboratively train detection models without sharing raw data. Linking with blockchain-based logging systems could also enhance the integrity of security event records. Such integration would ensure that intrusion alerts cannot be altered after they are generated. Another promising area is the use of adaptive learning algorithms that automatically update themselves based on changing attack patterns. This capability would help intrusion detection systems remain effective against emerging cybersecurity threats. Moreover, combining intrusion detection with automated response mechanisms could lead to fully autonomous security frameworks able to isolate compromised devices without human intervention.

VIII. CONCLUSION

This research presented an Edge AI-based intrusion detection framework aimed at improving the security of IoT networks. By deploying lightweight machine learning models directly on edge nodes, the proposed system enables real-time monitoring and quick detection of malicious activities. Experimental analysis showed improvements in detection speed, reduced latency, and efficient resource use compared to traditional cloud-based detection systems. The results underscore the effectiveness of merging edge computing with artificial intelligence for modern cybersecurity applications. As IoT ecosystems expand across various industries, ensuring secure communication among devices becomes increasingly important. The proposed approach contributes to building scalable and intelligent security solutions capable of protecting next-generation connected environments.

REFERENCES

[1] D. Evans, 'The Internet of Things: How the Next Evolution of the Internet Is Changing Everything,' Cisco White Paper.

[2] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press.

[3] S. Sicari et al., 'Security, Privacy and Trust in Internet of Things: The Road Ahead,' Computer Networks.

[4] W. Stallings, Network Security Essentials: Applications and Standards.

[5] A. Al-Fuqaha et al., 'Internet of Things: A Survey on Enabling Technologies and Security Issues,' IEEE Communications.