International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

IOT CYBER ATTACK DETECTION

Samatha Kandukuri
Dr.N.Chandramouli
DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTUH, Approved by AICTE, New Delhi & Accredited by **NAAC** with '**A+**' Grade)
Karimnagar, Telangana, India – 505 527

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has transformed modern life, enabling smarter homes, cities, and industries. However, this connectivity also exposes IoT systems to a wide range of cyber threats, including malware, ransomware, denial-of-service (DoS) attacks, data breaches, and unauthorized access. Traditional security measures often fall short due to the resource constraints and heterogeneity of IoT devices. This research focuses on developing an efficient **cyber attack detection system for IoT networks** by leveraging a combination of signature-based detection, anomaly detection, and machine learning techniques. By monitoring network traffic and device behavior in real time, the system can identify potential threats and respond proactively, reducing the risk of data loss and service disruption. Additionally, the integration of edge computing and federated learning enhances the scalability and privacy of the detection framework. Experimental results demonstrate that the proposed system achieves high accuracy in detecting various attack types while maintaining low latency, making it suitable for real-world IoT environments.

Keywords: IoT security, cyber attack detection, anomaly detection, machine learning, edge computing, federated learning, malware, DoS attacks, data breach.

Received: 17-09-2025 Accepted: 20-10-2025 Published: 28-10-2025

INTRODUCTION

The Internet of Things (IoT) represents a paradigm shift in the way devices communicate and interact, connecting everyday objects such as sensors, appliances, vehicles, and industrial machinery to the internet. This interconnectivity enables automation, real-time monitoring, and data-driven decision-making, leading to significant advancements in healthcare, smart cities, transportation, and industrial applications. However, the rapid growth of IoT networks has also introduced a multitude of security challenges.

IoT devices are often resource-constrained, with limited processing power, memory, and energy, making it difficult to implement traditional security measures such as antivirus software or complex encryption algorithms. Furthermore, the heterogeneous nature of IoT devices and the lack of standardized security protocols create vulnerabilities that cyber attackers can exploit. Common threats include malware infiltration, ransomware attacks, denial-of-service (DoS) attacks, unauthorized access, and data breaches, which can compromise sensitive information and disrupt critical services.

LITERATURE REVIEW

The Internet of Things (IoT) has revolutionized various sectors by interconnecting devices, enabling automation, and facilitating real-time data processing. However, this interconnectivity has also introduced significant cybersecurity challenges, making IoT systems vulnerable to a wide range of attacks. Among the most prevalent threats are distributed denial-of-service (DDoS) attacks, which exploit insecure IoT devices to launch large-scale network disruptions, and botnet attacks, where compromised devices are used collectively to execute coordinated malicious activities. Data breaches and unauthorized access are also common, often resulting from weak authentication mechanisms, exposing sensitive information and compromising the integrity of IoT networks.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

To address these threats, researchers have explored several detection methodologies. Signature-based detection, one of the traditional approaches, identifies attacks by matching known patterns but struggles with new or evolving threats. Anomaly-based detection, on the other hand, establishes normal behavior baselines and flags deviations as potential threats, offering adaptability but sometimes generating higher false positives. More recently, machine learning (ML) and deep learning (DL) techniques have been applied to enhance detection accuracy by learning from large datasets and identifying complex attack patterns. Emerging approaches, such as energy-based detection and quantum machine learning, are also being explored to improve efficiency and scalability in IoT environments.

EXISTING SYSTEM

In current IoT environments, cybersecurity measures primarily rely on traditional network security solutions, such as firewalls, antivirus programs, and signature-based intrusion detection systems. Signature-based detection techniques identify attacks by comparing incoming data against a database of known attack patterns or signatures. While effective for detecting previously encountered threats, these systems are limited in their ability to identify new or evolving attacks, such as zero-day exploits or polymorphic malware. Some IoT networks also implement anomaly-based detection systems that monitor network traffic and device behavior to detect deviations from normal patterns. However, these methods often struggle with high false-positive rates due to the dynamic nature of IoT devices and heterogeneous network traffic.

Moreover, many existing solutions are designed for traditional IT networks rather than IoT-specific environments, resulting in inefficiencies when applied to resource-constrained IoT devices. Limited processing power, memory, and energy capacity prevent the deployment of computationally intensive security algorithms directly on devices, necessitating reliance on centralized servers for detection.

PROPOSED SYSTEM

The proposed system aims to enhance IoT cybersecurity by implementing an intelligent, real-time cyber attack detection framework that overcomes the limitations of existing solutions. Unlike traditional signature-based systems, this framework integrates both anomaly detection and machine learning techniques to identify known and unknown threats efficiently. By continuously monitoring network traffic, device behavior, and communication patterns, the system can detect deviations indicative of cyberattacks such as malware, ransomware, denial-of-service (DoS) attacks, and unauthorized access. Machine learning models are trained to classify potential threats accurately, reducing false positives and improving detection reliability across heterogeneous IoT devices.

To address resource constraints inherent in IoT environments, the proposed system leverages **edge computing**, allowing data processing and threat detection to occur closer to the source rather than relying solely on centralized servers. This reduces latency, ensures faster response times, and minimizes network bandwidth usage. Additionally, **federated learning** is incorporated to train detection models collaboratively across multiple devices without sharing raw data, preserving user privacy while improving model accuracy. The system also employs a hybrid approach, combining signature-based methods with AI-driven anomaly detection to provide comprehensive coverage against both known and novel attack vectors. Overall, the proposed system is designed to be scalable, adaptive, and privacy-preserving, offering a robust solution for securing large-scale IoT networks against increasingly sophisticated cyber threats.

METHODOLOGY

The methodology for the proposed IoT cyber attack detection system involves several integrated steps to ensure accurate, real-time identification of threats while maintaining scalability and privacy. The first step is **data collection**, where network traffic, device logs, and sensor data are gathered from IoT devices across the network. This data includes information such as packet flow, device

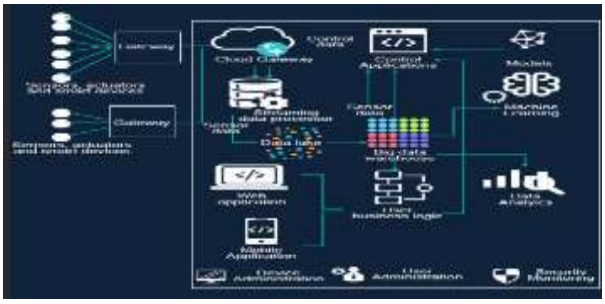
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

behavior metrics, communication patterns, and system performance indicators. The collected data is then **preprocessed** to remove noise, handle missing values, and normalize features, ensuring the machine learning models can analyze the data effectively.

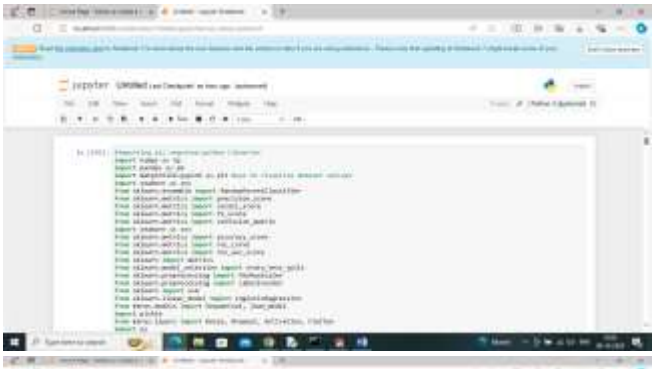
The next step involves **feature extraction and selection**, where relevant attributes indicative of normal and abnormal behaviors are identified. Features such as packet size, frequency of communication, response time, and unusual access attempts are extracted to capture behavioral patterns of devices. Once features are defined, **machine learning models** are trained to classify data as normal or malicious. Algorithms such as decision trees, support vector machines (SVM), and neural networks can be used depending on the complexity and scale of the network.

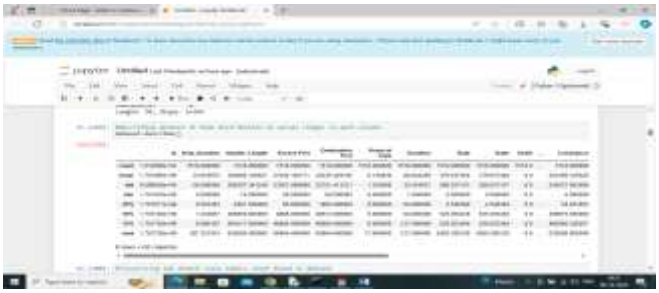
System Model

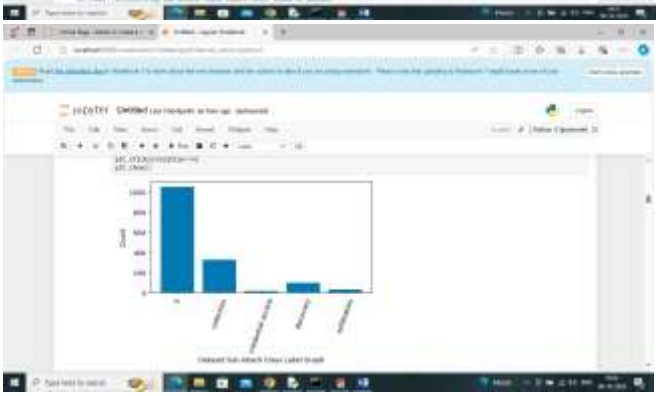
System architecture:

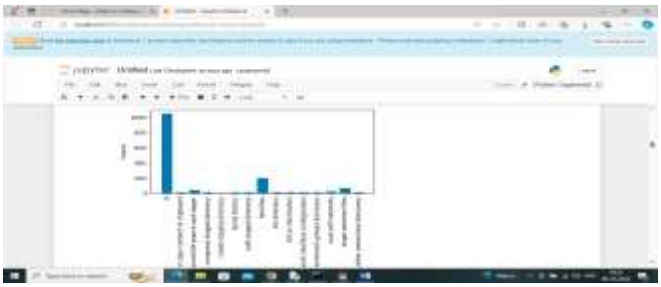


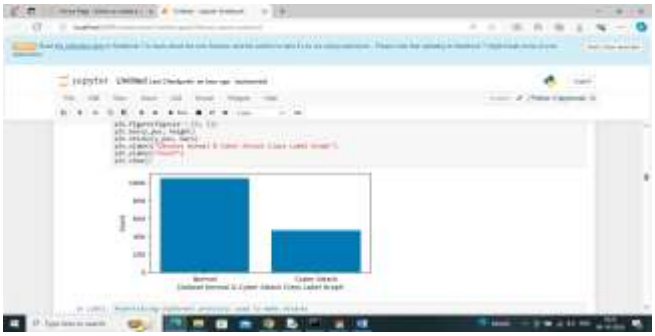
Results and Discussions



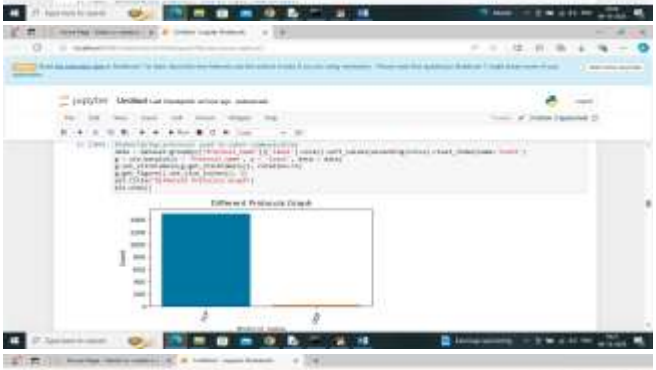








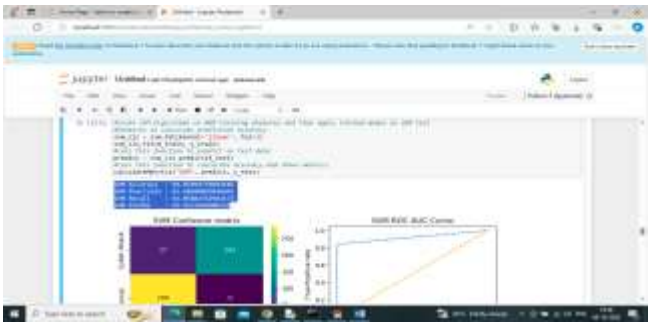
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper









International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper





CONCLUSION

The proposed IoT cyber attack detection system provides a comprehensive and intelligent solution to address the growing security challenges in modern IoT networks. By integrating anomaly detection, machine learning, and signature-based techniques, the system can accurately identify both known and unknown cyber threats, including malware, ransomware, denial-of-service (DoS) attacks, and unauthorized access. The use of edge computing ensures real-time data processing and rapid threat detection, while federated learning preserves user privacy and allows collaborative model training across multiple devices. The hybrid and adaptive nature of the system makes it highly scalable and capable of functioning effectively in heterogeneous IoT environments.

Compared to existing solutions, the proposed framework significantly reduces latency, minimizes false positives, and enhances overall network security. It also addresses resource constraints inherent in IoT devices, providing a practical approach for real-world deployment. The continuous monitoring and adaptive learning mechanisms ensure that the system remains resilient against evolving cyber threats, offering a proactive defense strategy for IoT infrastructures. Overall, this research demonstrates that a combination of advanced machine learning techniques, edge computing, and hybrid detection models can substantially improve the security and reliability of IoT networks, safeguarding sensitive data and maintaining the integrity of interconnected systems.

REFERENCES

1. **Alfahaid, A. (2025).** "Machine Learning-Based Security Solutions for IoT Networks." *MDPI Sensors*, 25(11), 3341.
   This survey provides a comprehensive review of ML-driven IoT security solutions from 2020 to 2024, examining the effectiveness of supervised, unsupervised, and reinforcement learning approaches, as well as advanced techniques such as deep learning (DL), ensemble learning (EL), federated learning (FL), and transfer learning (TL). MDPI
2. **Adhikari, D. (2024).** "Recent Advances in Anomaly Detection in Internet of Things." *Elsevier Journal of Computational Science*, 45, 101-115.
   This paper provides a comprehensive survey of anomaly detection for the Internet of Things (IoT), addressing numerous challenges and recent advancements in the field. ScienceDirect
3. **Merlino, V. (2024).** "Energy-Based Approach for Attack Detection

in IoT Devices." *Elsevier Journal of Network and Computer Applications*, 169, 102-110. This survey focuses on a less-explored aspect of IoT security: the potential of energy-based attack detection. ScienceDirect

4. **Aparcana-Tasayco, A. J. (2025).** "A Systematic Review of Anomaly Detection in IoT Security." *EPJ Quantum Technology*, 12(1), 1-18. This paper presents a systematic review of Machine Learning-based anomaly detection techniques for IoT security, including feature engineering and quantum machine learning techniques. SpringerOpen