AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(1) (2026)
www.ajmimc.com

DETECTION OF REAL TIME MALICIOUS INTRUSIONS&ATTACKS IN IOT EMPOWERED CYBERSECURITY

Dr .D.Kalyankumar[1], Tallapaneni Narasimha Naidu[2]
Beeram Amala[3], Dorre Gopi [4] , Pamulapati Gangadhar[5]
[1]*Associate Professor, Department of CSE-Cyber Security, Chalapathi Institute of Technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.*
[2,3,4,5] *Ug Scholar, Department of CSE-Cyber Security, Chalapathi Institute of Technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.*

ABSTRACT
The rapid expansion of Internet of Things (IoT) devices has significantly increased connectivity and automation in smart environments. However, this growth has also escalated cybersecurity risks, making IoT networks vulnerable to malicious intrusions, malware attacks, and unauthorized access. Detecting these threats in real-time is crucial to safeguard sensitive data and maintain system reliability. This study proposes a real-time intrusion detection system (IDS) leveraging machine learning and deep learning algorithms to identify anomalous behavior in IoT networks efficiently. The system captures network traffic, analyzes patterns, and predicts potential threats with high accuracy. Experimental results show that the proposed framework improves detection rates while reducing false alarms compared to traditional methods.

Keywords: IoT Security, Intrusion Detection System, Real-Time Monitoring, Machine Learning, Cybersecurity, Anomaly Detection.

Introduction

The Internet of Things has become one of the most important technological developments in recent years. IoT devices are now widely used in homes, offices, healthcare systems, factories, and transportation systems. These devices communicate with each other through the internet and exchange large amounts of data continuously. Examples of IoT devices include smart cameras, wearable devices, smart thermostats, sensors, medical devices, industrial robots, and smart vehicles. Although IoT technology provides convenience and automation, it also introduces new cybersecurity risks.

Cyberattacks on IoT systems are increasing because many devices lack strong security mechanisms. Attackers can exploit vulnerable devices to gain unauthorized access, steal confidential data, spread malware, or disrupt services. Traditional security systems are often not sufficient for protecting IoT environments because IoT networks are dynamic, distributed, and involve a large number of connected devices. Therefore, advanced intrusion detection systems are required to monitor network traffic and detect malicious activities in real time.

Machine learning and deep learning techniques have shown promising results in identifying abnormal patterns in network traffic. These technologies can analyze large volumes of data quickly and accurately. By training models on both normal and malicious traffic data, the system can recognize different types of attacks such as Denial of Service, phishing, ransomware, SQL injection, and botnet attacks. Real-time intrusion detection helps reduce damage and improves overall network security.

Existing System

Existing intrusion detection systems in IoT environments mainly rely on traditional rule-based methods and signature-based detection techniques. These systems compare incoming traffic patterns with predefined attack signatures stored in a database. If a matching pattern is found, the system generates an alert. Although this approach is effective for detecting known attacks, it fails to identify new and unknown threats. Signature-based systems also require regular updates to maintain their effectiveness.

Another limitation of existing systems is the high false positive rate. Many legitimate activities may be incorrectly classified as attacks, which can confuse administrators and reduce trust in the

system. Traditional methods also struggle with large-scale IoT networks because IoT devices generate massive amounts of data continuously. Processing such data using rule-based systems requires significant computational resources and may lead to delays.

Existing systems are often unable to provide real-time monitoring and adaptive learning capabilities. They cannot easily adjust to new attack patterns or changes in network behavior. Additionally, many IoT devices have limited memory and processing power, making it difficult to deploy heavy security solutions directly on them.

Existing System Feature	**Limitation**
Signature-Based Detection	Cannot detect unknown attacks
Rule-Based Monitoring	Requires manual updates
Traditional Firewalls	Limited IoT compatibility
Static Attack Database	Poor adaptability
High False Positives	Reduces detection efficiency

Proposed System

The proposed system introduces a machine learning and deep learning-based approach for detecting real-time malicious intrusions and attacks in IoT environments. The system continuously monitors network traffic from connected devices and identifies abnormal behavior automatically. Unlike traditional methods, the proposed approach can detect both known and unknown attacks by learning traffic patterns from historical data.

The proposed model includes several stages such as data collection, preprocessing, feature extraction, model training, attack classification, and alert generation. Data is collected from IoT devices, routers, sensors, and network gateways. After preprocessing, important features such as packet size, traffic volume, source IP address, destination IP address, protocol type, and connection duration are extracted.

Machine learning algorithms such as Random Forest, Decision Tree, Support Vector Machine, and Naive Bayes are used to classify network traffic. Deep learning techniques such as Convolutional Neural Networks and Recurrent Neural Networks further improve accuracy by identifying complex attack patterns. When suspicious traffic is detected, the system immediately generates an alert for the administrator.

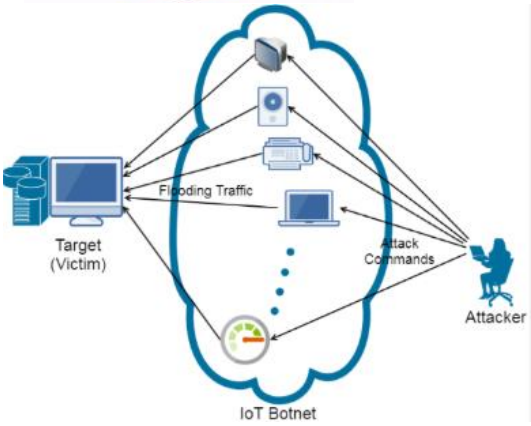
Proposed System Module	Function
Data Collection	Collects network traffic from IoT devices
Preprocessing	Removes noise and missing values
Feature Extraction	Identifies important traffic characteristics
ML/DL Classification	Detects malicious traffic patterns
Alert Generation	Sends real-time notifications
Dashboard Monitoring	Displays attack reports and statistics

System Architecture

The architecture of the proposed system consists of multiple interconnected modules. The first module is the IoT device layer, which includes smart sensors, cameras, wearable devices, routers, and industrial equipment. These devices generate network traffic continuously. The second module is the data collection layer, which gathers traffic information from the connected devices.

The third module is the preprocessing layer. In this stage, raw data is cleaned, missing values are removed, and duplicate records are filtered out. The feature extraction module then selects the most important network features required for attack detection. These features are sent to the machine learning and deep learning models for classification.

The classification layer determines whether the traffic is normal or malicious. If an attack is detected, the alert management module sends notifications to the administrator through email, SMS, or dashboard alerts. Finally, the reporting module generates detailed reports about detected attacks, traffic patterns, and system performance.



Layer	Components
IoT Device Layer	Sensors, Cameras, Wearables
Data Collection Layer	Traffic Monitoring Tools
Preprocessing Layer	Data Cleaning and Filtering
Feature Extraction Layer	Packet Analysis
Classification Layer	ML and DL Models
Alert Layer	Notifications and Warnings

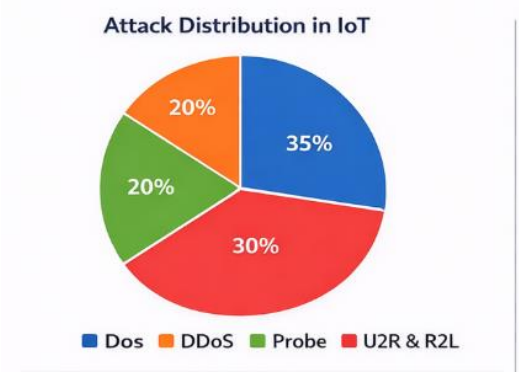
Advantages

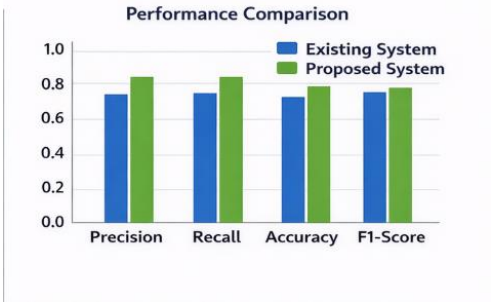
The proposed system offers several advantages over traditional intrusion detection systems. It can detect both known and unknown attacks with high accuracy. The use of machine learning and deep learning reduces false positives and improves decision-making. Real-time monitoring allows administrators to respond quickly to threats before major damage occurs.

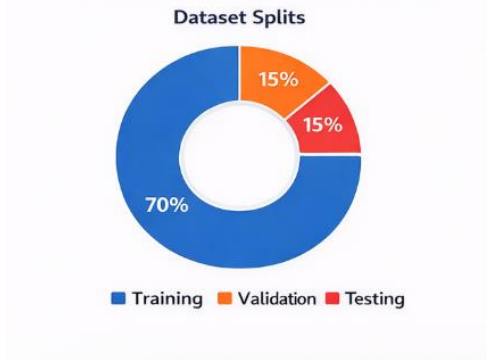
The system is scalable and can handle large volumes of IoT traffic efficiently. It can be integrated with cloud platforms, smart city networks, healthcare systems, and industrial automation environments. Another major advantage is its adaptive learning capability. As new attack data becomes available, the system can be retrained to improve performance.

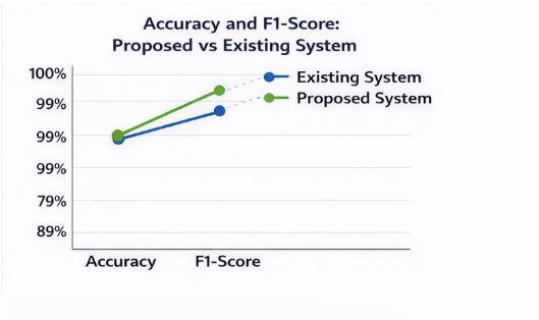
Advantage	Benefit
Real-Time Detection	Faster response to threats
Low False Positives	Improved reliability
Scalability	Supports large IoT networks
Adaptive Learning	Detects new attack patterns
Automated Alerts	Reduces manual monitoring

RESULTS AND DISCUSSIONS









Conclusion

The detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity is essential for protecting connected devices and sensitive

information. Traditional intrusion detection methods are no longer sufficient because they cannot handle the growing complexity of IoT environments. The proposed system uses machine learning and deep learning techniques to improve detection accuracy, reduce false alarms, and provide real-time monitoring.

By analyzing network traffic continuously, the system can identify suspicious activities and generate immediate alerts. The use of advanced algorithms enables the detection of both known and unknown attacks. This approach improves the overall security of IoT networks and ensures better protection for smart homes, industries, healthcare systems, and other connected environments. In the future, the system can be enhanced further by integrating blockchain, cloud computing, and edge computing technologies for even stronger cybersecurity support.

REFERENCE

1. K. K. . Kommineni and A. . Prasad, “A Review on Privacy and Security Improvement Mechanisms in MANETs”, Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.
2. Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w
3. Kotte, G. (2025). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283668
4. Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
5. Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.
6. Intrusion Detection in IoT Networks Using Machine Learning
7. Patyrykin, K., & Vasyukova, L. (2025). Environmental Accountability or Symbolic Compliance? A Critical Review of ESG Ratings, Greenwashing, and Indirect Emissions in the Global Insurance Sector. International Journal of Energy Economics and Policy, 15(6), 917–925. https://doi.org/10.32479/ijeep.22770
8. Cybersecurity and Intrusion Detection in Internet of Things
9. IEEE research papers on IoT security and intrusion detection
10. Poojari, R. (2024). Empirical Analysis of Context Window Enhancement Methods in Retrieval-Augmented Generation Models. Journal of Computational Analysis and Applications, 33(2).
11. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
12. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
13. Sruthi, M. V., Sree, V. U., & Soundararajan, K. (2012). Specific removal of motion artifacts in medical image processing. IJECCE, 3(3), 227-229.
14. Kaggle IoT intrusion detection datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15
15. Cisco annual cybersecurity reports for IoT attack trends
16. IBM security intelligence reports and threat monitoring studies