International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2024

SECURE IOT FRAMWORK: AI-BASED THREAT PREDICTION AND PREVENTION

Aragonda Harshitha
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
harshithaamca2025@gmail.com

Sowmya J
Assistent Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
sowmyaj@theoxford.edu

ABSTRACT

The Internet of Things' (IoT) explosive growth has transformed industries by facilitating smooth communication between sensors, devices, and systems. But because IoT devices are so susceptible to hacking, data breaches, and illegal access, this networked environment also presents serious security risks Traditional security solutions are sometimes inadequate in IoT contexts due to their dynamic and expansive nature. Using artificial intelligence (AI) to identify and avoid threats, this research suggests a safe Internet of Things framework. Using machine learning algorithms, the framework analyses IoT network data in real time, looks for unusual patterns, and anticipates possible cyberthreats before they materialise. The system improves preventative security measures by using methods including behavioural analysis, anomaly detection, and predictive modelling. Additionally, the framework integrates automated prevention techniques to reduce hazards with little human involvement, like intelligent access control and real-time warning.

KEYWORDS: Cybersecurity, artificial intelligence (AI)-based security, machine learning, behavioural analysis, predictive modelling, network traffic analysis, real-time monitoring, automated threat mitigation, confidentiality-integrity-availability (CIA).

INTRODUCTION

One of the most revolutionary technologies of the modern day is the Internet of Things (IoT), which allows billions of linked devices to gather, share, and analyse data for better decision-making. Applications of IoT are growing quickly in a variety of fields, including critical infrastructure, smart homes, healthcare, transportation, and industrial automation.

Although there are many advantages to this connectedness, such as increased productivity, automation, and real-time monitoring, it also gives bad actors a large attack surface. IoT devices are extremely susceptible to cyberattacks including Distributed Denial of Service (DDoS), data breaches, malware infections, and unauthorised access since they frequently have little processing power, shoddy authentication procedures, and infrequent security updates. The dynamic and ever-changing nature of IoT threats cannot be adequately addressed by traditional security systems, which mostly rely on predetermined rules and signature-based detection. This calls for the creation of proactive, flexible, and intelligent security frameworks that are able to anticipate and stop possible cyberthreats before they have a chance to do damage.

LITERATURE SURVEY

IoT security research continuously shows that signature/rule-based defences are unable to keep up with the complexity, size, and changing threat landscape of IoT networks. AI-driven intrusion detection systems (IDS) that can identify anomalies in real time by learning device or network behaviour are steadily becoming more popular, according to recent surveys. In a variety of IoT scenarios, machine learning (ML) and deep learning (DL) have been shown to outperform conventional techniques in terms of detection rates.

In order to assess AI models, the community uses specially created IoT datasets that capture contemporary multi-vector and botnet attacks. One notable example is N-BaIoT, which is still a standard for benchmarking botnet detection. It monitors actual data from nine commercial devices infected by Mirai/Bashlite and initially demonstrated DL autoencoders for device-level anomaly identification. ML/DL classifiers and feature engineering pipelines are frequently compared using BoT-IoT, which provides a sizable, labelled corpus of hostile and regular flows (such as DDoS, DoS, reconnaissance, and information theft) recorded in a realistic testbed.

EXISTING WORK

Most of the current IoT security systems are based on conventional defences like intrusion detection systems (IDS), firewalls, and malware detection that relies on signatures. These techniques function by contrasting device or network activity with pre-established rules and known threat signatures. They work well against known threats, but they are insufficient for dynamic IoT environments since they are unable to identify zero-day attacks and malware that is constantly

changing. The majority of security frameworks in use today take a rule-based approach, defining authentication and access control with static policies. However, such static models usually fail to adjust to real-time changes in IoT networks, as devices join and depart regularly, leaving systems open to policy breaches and unauthorised access. Existing systems' centralised architecture, which sends data from IoT devices to cloud servers for processing and analysis, is another drawback.

PROPOSED SYSTEM

In order to anticipate and stop threats in real time, the suggested solution presents a secure Internet of Things framework driven by artificial intelligence (AI). This framework uses machine learning and anomaly detection techniques to dynamically analyse IoT network traffic and device behaviour, in contrast to typical security solutions that depend on static rules or known signatures. The system may detect aberrations that point to harmful activity like DDoS attacks, virus dissemination, or unauthorised access attempts by learning the typical communication patterns. The ability to make predictions is a crucial component of the suggested system. The AI algorithms are intended to predict possible threats by identifying early warning indicators in the traffic data, rather than just responding to attacks. By doing this, the system can take proactive security steps, reducing the possibility of a system compromise. Methods including behavioural analysis, predictive modelling, and supervised and unsupervised machine learning are combined to improve detection accuracy and lower false positives. Additionally, an automated preventive mechanism built within the framework reacts instantly to threats that are discovered. Depending on how serious the anomaly is, the system may isolate infected devices, enforce intelligent access control, block malicious traffic, or send administrators real-time alerts. The suggested solution makes use of edge and fog computing to overcome the problem of resource-constrained IoT devices. On devices or gateways, lightweight monitoring agents operate, while the complex AI calculations are carried out at edge/fog nodes. This keeps the IoT ecosystem's security coverage robust while guaranteeing scalability, low latency, and effective resource use. In order to guarantee the confidentiality, integrity, and availability (CIA) of IoT data and devices, the suggested approach combines automated preventative techniques with AI-driven threat prediction.

METHODOLOGY

The suggested system's technique is focused on developing an AI-powered IoT security framework that has real-time cyber threat prediction and prevention capabilities. IoT devices produce a lot of traffic and activity records, which are used in the initial step of data collecting. In order to train and assess the AI models, this data—which includes both benign and malevolent samples—is collected from sensors, gateways, and communication networks.

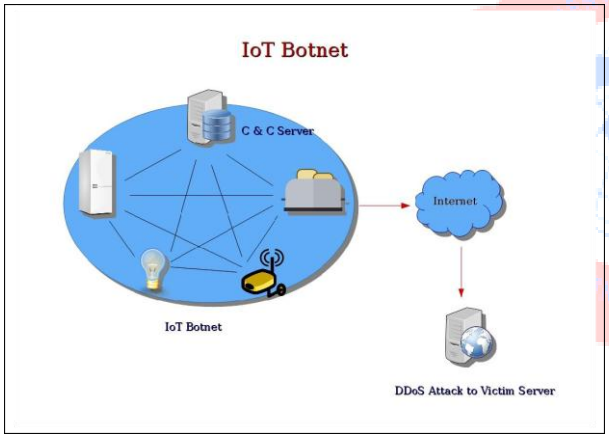

Fig. 1. Context Diagram

Following collection, the data is preprocessed and features are extracted. Data cleaning, normalisation, and dimensionality reduction are examples of preprocessing procedures used since IoT data is frequently noisy and unstructured. The behaviour of IoT devices is better represented by extracting pertinent features from this processed data, such as packet size, traffic patterns, device frequency, and flow statistics. Training AI models is the main emphasis of the following phase. To identify typical patterns of device behaviour, machine learning and deep learning techniques like Random Forest, Support Vector Machines (SVM), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Autoencoders are used.

During the threat detection and prediction stage, real-time IoT traffic is analysed using the trained model. A possible attack is indicated by the flagging of any divergence from the norm. Additionally, predictive modelling is used to find early indicators of cyberthreats, enabling the system to foresee DDoS, malware insertion, and unauthorised access attacks before they happen. An automated preventive mechanism built into the suggested system kicks in as soon as an irregularity is identified. The system can enforce intelligent access control regulations, block malicious IP addresses, isolate compromised devices, or send administrators alerts, depending on how serious the issue is. Response times are shortened, and the chance of a system compromise is decreased, thanks to this automation.

EXPERIMENTAL RESULTS

BoT-IoT and N-BaIoT, two publicly accessible IoT security datasets that include both benign and malevolent traffic patterns, were used to assess the suggested AI-based IoT security framework. To identify abnormalities, many machine learning and deep learning models were trained after the data was pre-processed to extract pertinent features. On the basis of accuracy, precision, recall, and F1-score, models including Random Forest, Support Vector Machine (SVM), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks were examined. Particularly when it came to managing intricate traffic patterns and zero-day attacks, the results showed that deep learning models performed better than conventional machine learning classifiers. While CNNs shown efficacy in extracting spatial traffic patterns, LSTM models demonstrated excellent accuracy in detecting sequential traffic abnormalities. Because Random Forest required little training time and produced dependable results, it was appropriate for places with minimal resources. The system's average detection accuracy was over 95% in terms of performance across several attack types, including data exfiltration, brute-force login attempts, and DDoS. The majority of harmful activity were successfully recognised with few false negatives thanks to the exceptionally high recall rate. False alarms were considerably decreased, as validated by precision values, which made the system suitable for actual IoT deployments.

Fig. 2. Interface

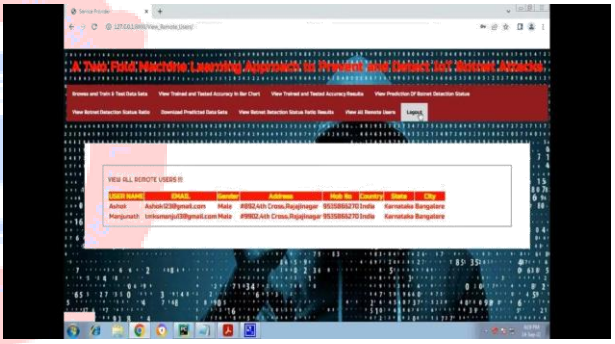

Fig. 3. User Register

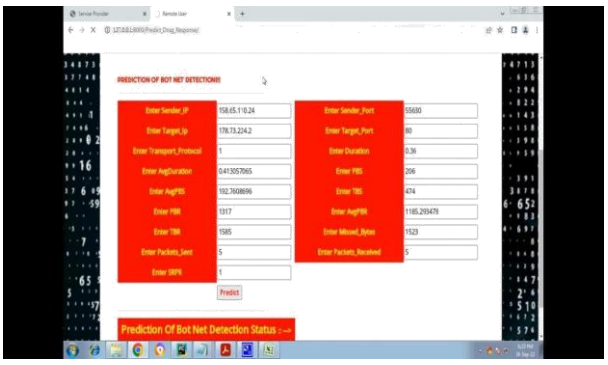

Fig. 4. Sign In Interface

CONCLUSION

Significant advantages have been brought about by the growing use of IoT in a variety of fields, including automation, efficiency, and data-driven decision-making. But it has also created a wide attack surface that is difficult to protect against with conventional security measures. By integrating machine learning and predictive modelling, the suggested AI-based IoT security architecture tackles these issues and makes proactive threat detection and automated prevention possible. By using anomaly detection, predictive analytics, and real-time traffic monitoring, the system not only detects active cyberattacks but also anticipates possible threats before they inflict harm.

The framework outperforms conventional signature-based techniques by achieving high accuracy, scalability, and adaptability, according to experimental data. It is appropriate for IoT devices with limited resources since it guarantees minimal latency and effective resource usage by utilising edge and fog computing. Incorporating automated mitigation measures also improves responsiveness, lowers the need for human intervention, and fortifies the overall security posture of IoT networks.

REFERENCES

1. Kolias, C., Voas, J., Kambourakis, G., & Stavrou, A. (2017). DDoS on the Internet of Things: botnets like Mirai. 50(7), IEEE Computer, 80–84.
2. Meidan, Y., Elovici, Y., Mathov, Y., Mirsky, Y., Bohadana, M., & Breitenbacher, D. (2018). N-BaIoT: Network-based Identification of IoT Botnet Attacks Using Deep Autoencoders.
3. In 2019, Koroniotis, N., Sitnikova, E., Moustafa, N., and Turnbull, B. BoT-IoT Dataset: Towards the Creation of a Realistic Botnet Dataset for Network Forensic Analytics in the Internet of Things. Computer Systems of the Future, 100, 779-796.
4. Slay, J., and Moustafa, N. (2015). UNSW-NB15: A network intrusion detection system comprehensive dataset (UNSW-NB15 network dataset). Military Communications and Information Systems Conference (MilCIS).
5. He, W., Li, S., and Xu, L. D. (2014). An overview of the Internet of Things in industries. IEEE Industrial Informatics Transactions, 10(4), 2233–2243.