January
March 26

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

Vol - 2
Issue - 1

AI-Driven Security Framework for IoT Networks

Ayushi Nagar
Assistant Professor
School of Science
Aryavart University, Sehore (M.P.)

ABSTRACT

Billions of smart devices talk to each over the highly connected digital ecosystem that has been created by the rapid rise of Internet of Things (IoT). While IoT enhances automation, efficiency and decision-making, it has also brought security threats of grave import. Due to the limited memory, low processing power and weak authentication systems of IoT devices traditional security mechanisms are unable to provide an effective solution. Consequently, IoT networks are susceptible to cyber-attacks like DDoS (Distributed Denial of Service) attacks, data theft, malware injections, and unauthorized access.

This work introduces a new AI-based security framework specifically for IIoT networks. By incorporating machine learning models, the framework is equipped to provide real-time analysis of potential threats, detecting anomalies and adapting response strategies. Unlike rule-based systems, AIs can learn patterns from the experiments that take place on the network and therefore pick up unknown/zero-day attacks. The given approach enhances all-around protection by using layered security architecture, edge-level monitoring and cloud-based intelligence analysis.

They design and implement the framework, evaluate its performance in simulated IoT environments. The results show better detection accuracy, lower response time, and higher scalability. This research work demonstrates implementing artificial intelligence to enhance IoT security without losing efficiency and flexibility.

KEYWORDS

Artificial Intelligence, Internet of Things (IoT), Cybersecurity, Machine Learning, Intrusion Detection System (IDS), Network Security, Anomaly Detection, Edge Computing, DDoS Attacks, Smart Devices

1. INTRODUCTION

The Internet of Things (IoT) the ecosystem that connects devices to each other and the internet, enabling them to share information is revolutionizing how we communicate. Interconnected sensors and devices are heavily relied within smart homes, healthcare systems, industrial automation and smart cities. But the growth of IoT networks has opened up security weaknesses too. Most IoT devices are probably working with little to no security configurations; thus, they become an easy target toy for cyber-criminals.

Conventional cybersecurity solutions are primarily built for high-performance computing systems like servers and PCs. These approaches also need a lot of computation resources and constant manual maintenance. In contrast, IoT devices are resource-constrained and cannot support complex security software. Furthermore, the highly dynamic environment of IoT networks makes it challenging to employ static rule-based protection systems.

AI (Artificial Intelligence) can be a great help to overcome this setback. Artificial intelligence (AI)-based systems can process huge amounts of network traffic, detect anomalies in data packets, and take actions against such threats without manual intervention. Detection techniques aided by machine learning algorithms can learn from new data continuously. Such adaptability allows AI to be deployed effectively in contemporary IoT settings where threats can change quickly.

To this end, a complete AI-based security structure is envisioned to protect IoT generated content while providing IoT system performance in terms of confidentiality, integrity and availability.

2. RESEARCH METHODOLOGY

In this section, we describe the research methodology used to systematically design and implement the AI-powered security system for IoT networks. It is presented in a way that breaks the work into four main topics: system architecture design, data collection and preprocessing, machine learning model implementation, and finally performance evaluation. First, using the device, edge and cloud layers of a cross layer IoT security architecture to distribute security tasks. Then, by simulating some IoT environments, network traffic data is generated and used after go through cleaning and feature selection methods so that data are ready for analysis. Subsequently, appropriate types of machine learning algorithms are generated and trained to properly identify anomalies in the system and categorize cyberattacks accordingly. In the end, we evaluate the proposed framework in different attacking scenarios to measure both detection accuracy over various attack cases and response time efficiency as well as resource-efficiency. We believe that the described iterative approach, based on assessing trust-relevant entities in a systematic manner results provides success factors for reliable allocation of security into large scale and practice-oriented environments.

2.1 System Architecture Design

The initial phase of the research focuses on creating a multi-layered AI-driven security framework specifically for IoT networks. Architecture: Three Layers The architecture is separated into three layers as shown below device layer, edge layer and cloud layer. The device layer (or smart devices layer) is mainly composed of IoT sensors and various smart devices responsible for data acquisition. To minimize latency, the edge layer filters data and performs lightweight anomaly detection. Deep learning analysis and extensive threat intelligence processing are done through the cloud layer.

This layered architecture improves efficiency as sensitive data can be computed at the source to avoid communication latency. It also allows scalability since new devices can be added seamlessly, without impacting the overall system. This architecture allows secure communication protocols and the transferring of encrypted data. The framework ensures robust protection by spreading the security works onto different layers, minimizing computational burden on small IoT devices.

2.2 Data Collection and Preprocessing

Network Traffic Data Collection from IoT Environments Simulation tools as well as public datasets are employed to collect normal and malicious traffic patterns. The data preprocessing is vital to clear the noise and deal with missing values in addition to normalizing network parameters such as packet size, frequency, and protocol type.

Feature selection techniques are used for disciplinary changing and identifying those features which are useful for prediction of network security. This is less computationally expensive and more accurate model. How do we use the data to test our machine learning performance? With appropriate preprocessing, the AI model is not fed garbage in but rather high-quality input directly affecting detection accuracy and false alarm rates.

2.3 Machine Learning Model Implementation

At this stage, machine learning based algorithms like Decision Trees, Random Forest and Neural Networks are applied to perform anomaly detection and attack classification. The training method relies on supervised learning techniques trained on labelled datasets. It teaches the system to differentiate between real and malicious traffic.

To assess the efficacy of different algorithms, performance metrics like accuracy, precision, recall and F1-score are computed. The top performing model gets embeded into the framework. [14] The sensitivity of MLP is with respect to Scheduled updates This system can periodically update itself using new training sets to adapt and learn about any emerging threat on the internet.

2.4 Performance Evaluation and Testing

Lastly, the proposed approach is evaluated in a simulated IoT environment. It proposes different types of attacks scenarios including DDoS, spoofing and malware injection. The detection speed, response time, and resource consumption of the system are calculated.

A comparison is made with classical rule-based systems and the AI framework. The evaluation shows higher detection rates and fewer false positives. The proposed solution is verified and proving to work in this testing phase.

3. PROBLEM SOLVING APPROACH

Some of the major challenges faced in the IoT networks are weak authentication, no encryption, processing power limitations and non-real-time monitoring. The vulnerabilities enable attackers to compromise devices and interfere with network operations.

Intelligent automation in the proposed AI-driven framework overcomes these issues. It does more than rely on static rules of behaviour, the system monitors traffic across a network and identifies patterns which are out of place. For instance, if a device generates an abnormally high number of data packets in a short amount of time the system would be able to detect the anomaly and isolate it before the attack can spread.

Edge computing in IoT ensures faster detection of any incidents that happened by processing data at the edge rather than sending it to a cloud server. This minimizes reliance on centralized servers and enhances response time. In addition, the adaptive learning enables the model to identify new types of attacks without manual reprogramming.

Incorporating layered architecture, machine learning, and the automated response mechanism brings scalable and efficient solutions through the proposed framework. Along with being an attack detector, it prevents catastrophic network failures due to attacks on the IoT communication.

4. ADDITIONAL CONTRIBUTION: EXPLAINABLE AI FOR IOT SECURITY

Why not combine the proposed in this study with Explainable Artificial Intelligence (XAI). Many AI-powered security systems are “black boxes,” which means that users don’t know the rationale behind a particular decision. That opacity fosters distrust and complicates troubleshooting.

The Framework utilizes explanatory AI techniques, providing explicit reasoning for why a device is determined to be malicious. For instance, the system displays which traffic characteristics caused the alert. This same transparency enables network admins to make informed decisions and verify alerts quickly.

Explainable AI also help comply to regulations and bring clarification in systems. Since IoT systems are being used in critical infrastructure including healthcare and smart cities, the security mechanisms of these systems need to be transparent. The integration of both technical reliability and user trust is thus strengthened.

5. CONCLUSION

IoT networks are rapidly expanding and thus require new, intelligent forms of security solutions. So the basic security methods are not enough because the capabilities of your devices are limited, and so is their adaptability to emerging threats. The work proposed an AI driven security framework tailored for IoT domains.

In this proposed system, we have used a layered architecture which will integrate the machine learning algorithms in combination with edge-cloud coordinated model for real time

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

threat detection and effective resource utilization. A comparative experiment was performed to evaluate detection performance and response time relative to existing systems.

Moreover, integrating explainable AI adds an extra layer of transparency and trust to automated security decisions. Artificial intelligence significantly increases the protection level of an IoT network without loss in terms of scalability and adaptability.

Further research can investigate deep learning optimization, federated learning for data privacy preserving and integrate it well with blockchain for better information security. Such AI-enabled security structures can offer a solid approach to constructing robust and secure IoT networks.

REFERENCES

1. Datta, A., Baral, C. (2014). Internet of Things: A survey. Computer Networks, 54(15), 2787–2805.
2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M.(2015). IoT: A survey on enabling technologies. Charles E. Perkins, “IP Mobility Support for IPv4,” July 8, 1996 (https://tools.ietf.org/html/rfc2002) Accessed: October 1, 2023.
3. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A security challenges roadmap in the Internet of Things (IoT). Digital Communications and Networks, Volume 4, Issue 2, pp118–137.
4. Doshi, R., Apthorpe, N., & Feamster, N. (2018). IoT devices DDoS detection using machine learning IEEE Security and Privacy Workshops.
5. M. Conti, A. Dehghantanha, K. Franke and S. Watson (2018). Security and forensics for Internet of Things. Future Generation Computer Systems 78, 544–546 (2018).