Dean&Francis
ISSN 2959-6157

AI-based IoT Intrusion Detection Using Machine Learning

Yinpeng Yu

Bachelor of information Technology, University of Technology Sydney, Sydney, Australia, 14374274
392563611@qq.com

Abstract:

The development of smart home technology offers an unprecedented level of convenience, fundamentally transforming traditional home environments, but it also introduces the system to various cybersecurity risks such as unauthorized access and data leakage. With the expansion of the application scope of the Internet of Things network and the increase in the number of device deployments, traditional static defense methods have proven inadequate in the timely identification of complex intrusion behaviors and protecting network security. In response to this situation, this study proposes an intrusion detection system based on artificial intelligence, which can autonomously identify abnormal network traffic and isolate infected devices. The study used the CIC-IoT2023 and IoT-23 datasets to train and evaluate three machine learning models: logistic regression, support vector machine (RBF kernel), and random forest. The research results indicate that all three models exhibit high performance in terms of accuracy, robustness, and response speed, verifying the feasibility of applying artificial intelligence and machine learning to the security monitoring system of smart home systems. This study proposes a novel approach for constructing intelligent Internet of Things systems with self-defense capabilities.

Keywords: IoT security, machine learning, intrusion detection, Random Forest, SVM, Logistic Regression

1. Introduction

The rapid development of smart home technology and the significant increase in the deployment of Internet of Things devices have fostered a highly interconnected ecosystem where that integrates the Internet with smart home devices. This interconnection brings unprecedented convenience to life, but it also introduces potential cybersecurity risks, such as unauthorized access, data leakage, and remote contro [1]. In recent years, multiple incidents of smart camera intrusions and distributed denial-of-service attacks (DDOS) based on the Internet of Things have underscored the critical need for enhancing system

ISSN 2959-6157

security.

In the field of the Internet of Things (IoT), traditional static defense mechanisms usually rely on preset feature detection or static firewall policies. These mechanisms exhibit significant limitations in detecting complex and dynamically changing attack patterns. To address these challenges and mitigate potential losses, this study investigates the application of artificial intelligence (AI) and machine learning (ML) in adaptive intrusion detection systems. By learning the behavior of network traffic, it is capable of distinguishing between normal connections and malicious connections [2].

This study selected two representative public datasets - CIC-IoT2023 and IoT-23 - to train and evaluate the performance of various machine learning models. By integrating artificial intelligence-based anomaly detection and automatic disconnection mechanisms, this study proposes a dynamic self-defense framework tailored for smart home environments. The research results aim to provide theoretical and practical support for the construction of an IoT system with self-learning and defense capabilities.

2. Smart Home Security Threat Analysis (Network Intrusion, Hacking Manipulation, and Privacy Breach)

2.1 Main Types and Characteristics of Network Intrusions

In smart home environments, network intrusion has become one of the most common and highly destructive attack vectors. Intrusion activities manifest in various forms, typically by exploiting insecure Wi-Fi connections, outdated firmware, or weak authentication protocols to gain unauthorized system access. Once successful, attackers can manipulate devices by intercepting communication packets or tampering with control commands. As Wu et al. [1] noted in their literature review, the exponential growth of IoT devices has expanded the attack surface. Furthermore, the prevalence of users unfamiliar with networking and cybersecurity exacerbates the vulnerability of home networks to infiltration. Furthermore, intrusions are not limited to external attacks; some originate from compromised internal IoT devices. Once compromised, these devices form a "botnet" [3]. These compromised nodes are leveraged by attackers to participate in distributed denial-of-service (DDoS) attacks, causing traffic disruption and system paralysis. Consequently, defending against cyber intrusions necessitates a dynamic and adaptive security system that provides safeguards through real-time anomaly detection and traffic filtering.

2.2 Hacking Manipulation and Privacy Data Leakage

Hacker manipulation is another critical threat that IoT systems need to guard against. Without the users' knowledge, attackers remotely invade devices such as smart cameras, voice assistants, or thermostats, turning them into "monitoring tools". Such intrusions lead to the leakage of sensitive information, such as audio recordings, video images, and user behavior data [4]. Moreover, attackers can perpetrate ransomware attacks by encrypting user data and demanding a ransom. Kumar et al. [2] pointed out that one of the challenges faced by current practitioners is ensuring the integrity and confidentiality of data transmitted between IoT devices, attackers can easily steal data by exploiting insecure communication channels. Solving this problem requires the introduction of an artificial intelligence-based monitoring mechanism that enables real-time anomaly detection and behavior recognition by learning normal communication patterns, thereby effectively preventing manipulation and information leakage.

3. AI-Driven Anomaly Detection Techniques

3.1 Application of Machine Learning Algorithms in Anomaly Detection

In this study, machine learning is instrumental in identifying abnormal traffic and attack behaviors within IoT environments. Through training, the system can instantly recognize potential attacks and anomalous patterns. The research references several commonly used algorithms, including Logistic Regression (LR), Support Vector Machines (SVM), and Random Forests (RF). Artificial Intelligence of Things (AIoT) systems process complex network data through these models, achieving high-pre-

cision differentiation between normal and malicious behavior [4]. Logistic regression is characterized by its rapid inference speed and high interpretability, rendering it suitable for lightweight IoT applications that require real-time detection. Support Vector Machines based on Radial Basis Functions (RBF) excel at detecting nonlinear attack patterns by mapping data to high-dimensional spaces to distinguish complex boundaries [2]. Random forests mitigate overfitting risks by integrating multiple decision trees, offering significant advantages in terms of model stability and robustness [5]. All three approaches can construct intrusion detection systems with adaptive learning and efficient response capabilities.

3.2 Model Performance Comparison and Evaluation Results

To verify whether the model performance is applicable to IoT, this study conducted experiments based on the two public datasets, CIC-IoT2023 and IoT-23. The evaluation metrics for each model include accuracy, Precision, recall rate, F1-score, and AUC, ensuring a comprehensive assessment of model performance. According to the charts and results, the accuracy of all three models is above 99%, with the Random Forest model showing the most stable performance across all metrics. Logistic Regression has an advantage in computational efficiency, while SVM with the RBF kernel has stronger adaptability in identifying complex nonlinear intrusion behaviors.

The research findings align with existing studies. The ensemble learning method such as Random Forest has stronger generalization ability in an unknown network environment [2]. The AI-driven anomaly link detection technology demonstrates high feasibility, capable of reducing false alarm rates and enhancing dynamic defense capabilities.

4. Research Methodology and Experimental Design

4.1 Dataset Selection and Preprocessing

The study selected two publicly available IoT security datasets - CIC-IoT2023 and IoT-23 - to ensure the reliability and reproducibility of the experiments.

CIC-IoT2023 contains various normal and malicious traffic samples from different IoT devices, while IoT-23 focuses on real attack behaviors, such as Mirai botnet activities, denial-of-service (DoS) attacks, and data leaks. During the data preparation phase, the data underwent preprocessing. The main steps included: removing duplicates, filling in missing values, normalizing numerical features, and one-hot encoding the categorical features. Subsequently, the data was stratified and divided in a 80/20 ratio, ensuring a balanced distribution of normal and abnormal samples in both sets.

4.2 Model Training and Parameter Configuration

This study implemented and compared three machine learning algorithms: logistic regression (LR), support vector machine with RBF kernel (SVM), and random forest (RF). All models were trained using the same training and test sets to ensure the consistency and reproducibility of the experimental results.

For logistic regression, the liblinear solver was used to accelerate the convergence speed. SVM (RBF): Set parameter C = 1.0 and gamma = ‘scale’ to handle non-linear distributions. Random forest: Contains 100 decision trees (n_estimators = 100), with a maximum depth of 10 to balance accuracy and efficiency. Training and evaluation were conducted using the Scikit-learn library within a Python (Jupyter Notebook) environment. Performance metrics include accuracy, precision, recall, F1 value, and AUC.

4.3 Evaluation and Visualization

The model performance is visualized through confusion matrices and ROC curves. These visualizations provide an intuitive representation of the accuracy and robustness of each model in distinguishing between normal and malicious connections. Based on the results, the random forest shows the most stable performance, while SVM-RBF performed exceptionally well in capturing samples near complex decision boundaries. These experimental results directly validate the effectiveness and feasibility of the artificial intelligence-based anomaly detection method in IoT security.

ISSN 2959-6157

5. Design and Optimization of Intelligent Security Mechanisms

5.1 Design of Adaptive Defense Systems

The IoT environment is becoming increasingly complex and dynamic, making traditional static defense mechanisms ill-suited for the rapidly evolving IoT industry. This reality necessitates a shift from static strategies to intelligent dynamic defenses. AIoT systems possess self-learning and decision-making capabilities, making them highly suitable for intrusion detection and response [1]. Based on this principle, this study designs an AI-driven dynamic defense mechanism that can identify abnormal network traffic in real time and automatically isolate infected devices. This framework incorporates modules for real-time data collection, anomaly detection, and device disconnection. When machine learning models (e.g., random forests) detect abnormal behavior, the system automatically executes isolation and disconnection operations, severing affected IoT device nodes from the network to ensure cybersecurity. This automated defense mechanism significantly reduces response times and effectively mitigates the risk of cascading failures caused by malware propagation [2]. By integrating data-driven learning with autonomous control mechanisms, the research framework achieves anomaly link detection capabilities, enabling self-defense functions that empower IoT device clusters to maintain the security of the entire smart home ecosystem.

5.2 System Optimization and Future Improvements

Although the AI-driven defense framework performs well in terms of accuracy and adaptability, several challenges remain Firstly, the system relies on labeled datasets (such as CIC-IoT2023 and IoT-23), resulting in limited capability to identify unknown attack vectors. Future IoT security systems should introduce unsupervised or semi-supervised learning to enhance detection capabilities for zero-day attacks [6]. Another possible challenge is related to hardware. IoT devices usually have limited processing capabilities and may struggle to deploy complex AI models locally. Additionally, current research has not been fully tested and deployed in actual smart homes, leaving uncertainty about potential issues that may arise in complex and dynamic real-world environments. Overall, future research should focus on developing lightweight, easy-to-deploy, and privacy-protected AI systems to adapt to the still-developing IoT architecture.

6. Conclusion

This study explores the application of machine learning algorithms in the security intrusion detection of the Internet of Things. By comparing logistic regression, support vector machine based on RBF kernel, and random forest models, the results demonstrate that machine learning-based AI can effectively capture complex traffic patterns and identify malicious behaviors in IoT environments. The study used a combination of the CIC-IoT2023 and IoT-23 datasets, which cover a wide range of attack scenarios, making the model performance evaluation more representative. The experimental results show that all models achieved high accuracy and stability, proving that machine learning has significant potential in the IoT field, especially in cybersecurity. The findings of this study help to further understand the role of intelligent algorithms real-time security protection and abnormal traffic detection.

This study is not without its limitations. The research primarily focused on traditional machine learning models, without conducting an in-depth exploration of deep learning or AIoT adaptive systems. Additionally, the experimental data came from public datasets, which may have overlooked the diversity of real networks. Future research should therefore prioritize exploring deep learning methods, AIoT adaptive frameworks based on edge computing, and lightweight models suitable for real-time IoT deployment, in order to enhance the scalability, adaptability, and energy efficiency of the system.

References

[1] Wu, J., Li, W., & Cao, J. (2021). AIoT: a taxonomy, review and future directions. Telecommunications Science, 37(8), 1–17. https://doi.org/10.11959/j.issn.1000-0801.2021204

[2] Kumar, A., & Singh, R. (2023). Machine Learning for IoT Intrusion Detection: A Comprehensive Survey. Journal of Network and Computer Applications, 222, 103526.

[3] Liu, Y., & Xu, C. (2021). Lightweight Anomaly Detection in

IoT Networks Using Ensemble Models. Information Sciences, 580, 345–360.

[4] Zhou, Y., & Chen, X. (2022). Deep Learning Approaches for IoT Security: Challenges and Opportunities. IEEE Internet of Things Journal, 9(5), 4152–4167.

[5] Li, P., & Zhao, T. (2021). Random Forest-based Intrusion Detection for IoT Networks. Sensors, 21(19), 6382.

[6] Zhang, Q., & Hu, J. (2022). Adaptive Edge Intelligence for IoT Security Management. Future Generation Computer Systems, 134, 223–235.