Smart Internet of Things

www.siot.reapress.com

Smart. Internet. Things. Vol. 1, No. 3 (2024) 198–202.

Paper Type: Original Article

Hybrid Machine Learning Models for IoT Security

Nihar Ranjan Sahu*

Department of Computer Science,KIIT(Deemed to Be) University,Bhubneswar-751024,Odisha,India; 22051696@kiit.ac.in.

Citation:

Received: 10 July 2024 *Revised: 12 September 2024* *Accepted: 16 November 2024*	Sahu, N. R. (2024). Hybrid Machine Learning Models for IoT Security. *Smart internet of things, 1*(3), 198-202.

Abstract

The swift growth of the Internet of Things (IoT) brings forth considerable security challenges due to the variety of connected devices and their limited resources. Conventional security strategies are unable to keep pace with evolving cyber threats, rendering the IoT ecosystem susceptible to attacks. This paper introduces a hybrid machine-learning framework aimed at enhancing IoT security. Our method merges supervised and unsupervised techniques to detect both known and unknown (zero-day) threats. This hybrid framework utilizes fuzzy detection along with classification algorithms to recognize malicious activities while reducing false positives. We assess the performance of the model using publicly available IoT datasets and compare it to other Machine Learning (ML) models. The findings reveal notable improvements in precision, accuracy, recall, and response time. These results suggest that the hybrid model establishes a more robust basis for safeguarding the IoT environment against threats.

Keywords: Hybrid machine learning, IoT security, Anomaly detection, Threat classification, Zero-day attacks, Traffic analysis, Real-time detection.

1 | Introduction

The Internet of Things (IoT) is expanding and transforming industries from healthcare to smart cities. However, IoT devices' increasing connectivity and diversity still raise significant security concerns. Traditional security systems make networks more resilient to distributed and resource-constrained IoT [1].

environments. Attacks such as Distributed Denial of Service (DDoS), ransomware, and unauthorized data deletion are becoming increasingly frequent and sophisticated, posing significant challenges to the IoT ecosystem. These challenges require new solutions. Machine Learning (ML) holds promise for improving IoT security by detecting malicious activity from data patterns [2]. However, relying solely on supervision or unsupervised training can be limiting. Pattern tracking is good at identifying known attack patterns but struggles to detect new, unseen threats [3]. On the other hand, unsupervised models can flag anomalies without prior knowledge of attack patterns, but they are more likely to be negative. Supervised and unsupervised techniques are used to develop threats in IoT systems. Using both methods, hybrid models can

Corresponding Author: 22051696@kiit.ac.in

https://doi.org/10.22105/siot.v1i3.271

detect various threats, from stealth attacks to zero-day attacks. Our solutions are evaluated using a real-world IoT dataset, and the results are evaluated using traditional machine-learning methods [4].

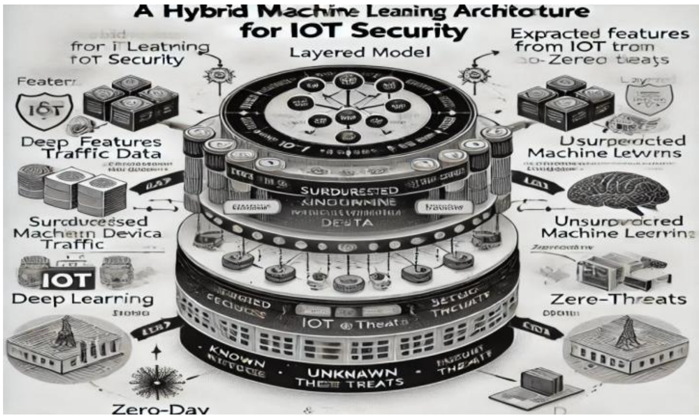

Fig. 1 . Hybrid ML architecture for IoT security.

Table 1. Performance comparison of different ML models for IoT security.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional ML model	85.2	83.5	81.3	82.4
Anomaly Detection only	88.7	87.1	85.4	86.2
Hybrid ML model	92.3	91.8	90.5	91.1

Table 2. System performance metrics for hybrid ML model.

Metric	Description	Measured Value
Accuracy (%)	Percentage of correctly identified threats	92.3
Precision (%)	True positive rate out of all detected positives	91.8
Recall (%0)	True positive rate out of actual positive instances	90.5
F1-Score (%)	The harmonic mean of precision and recall	91.1
Detection Latency (ms)	Time taken to detect threats in real-time	120

Let X represent the input data, the IoT traffic features extracted from the devices. Let y represent the known traffic labels (e.g., normal or malicious). Y' is the predicted label from the ML model. f(X) is the decision function applied by the supervised learning model. L(y,y') is the loss function that minimizes the error between the actual and predicted values. Z represents the latent features from the unsupervised learning module (e.g., for anomaly detection). D(X, Z) represents the decision function of the hybrid model combining supervised and unsupervised results. The basic prediction of a supervised model can be represented as

$$Y' = f(X), \tag{1}$$

where f(X) is the function learned by the supervised classifier to predict the output based on input features X. For the loss function that measures the error between actual and predicted values, the cross-entropy loss is commonly used in classification problems:

$$L(y,y') = -\sum y \log (y'). \tag{2}$$

In a hybrid model, the anomaly detection function (unsupervised) for IoT traffic can be defined as

$$Z=g(X), \quad (3)$$

where g(X) extracts latent variables or anomalies in the data. The final decision function in the hybrid model, combining supervised and unsupervised techniques, can be written as

$$D(X, Z)=\alpha f(X)+\beta g(X), \quad (4)$$

where α and β are weights assigned to supervised and unsupervised learning components, depending on their contribution to the overall prediction.

These equations explain the relationships between various components of your hybrid ML model for IoT Security and how supervised and unsupervised techniques work together for threat detection.

2 | Related Work

Many studies have applied ML techniques to IoT security. Supervised learning algorithms such as random forest and Support Vector Machines (SVM) have been used in intrusion detection and have shown high accuracy in classifying known threats [5]. For example, Fleury et al. [6] used SVM to analyze network connections in a smart home environment and obtain high-level classification. However, this technique requires logging and cannot detect zero-day attacks. This model works well without log information but often suffers from unpleasant consequences. Priyadarshini et al. [7] investigate the use of autoencoders to identify vulnerabilities in smart city infrastructure, highlighting the potential and challenges of vulnerability. Promise. The hybrid model provides the advantages of supervised and unsupervised learning. Mirsky et al. [8] demonstrated the potential of hybrid models in detecting known and unknown threats in critical systems. Based on this process, our model aims to improve detection accuracy further while reducing the vulnerability in the IoT environment.

3 | Proposed Hybrid ML Model

The proposed hybrid model consists of two primary components: anomaly detection and supervised classification. These components are integrated to detect known and unknown threats in IoT traffic.

3.1 | Feature Extraction

The model begins with feature extraction from IoT traffic. The features used in this study include:

Packet size: size of the data packets exchanged between devices. Flow duration: duration of each data flow between devices. Inter-arrival time: time between consecutive packets.

Source/destination IP: identifiers of devices communicating over the network. Traffic volume: the overall traffic volume generated within a specific time window [9].

3.2 | Anomaly Detection

The unsupervised learning component of the model uses K-means clustering to group normal IoT traffic and identify outliers. These outliers represent potential anomalies that correspond to unknown attacks. The decision function for anomaly detection is given by

$$Z=g(X), \quad (5)$$

where Z is the anomaly score, and g(X) represents the transformation of input features X using the anomaly detection algorithm.

3.3 | Supervised Classification (Supervised Learning)

We employ a Random Forest classifier for the known attack patterns, which is trained on labeled IoT traffic data. The model learns to classify data as normal or malicious based on predefined labels. The classification decision function is

$$y\hat{} = f(X), \tag{6}$$

where y^ is the predicted label, and f(X) is the decision function derived from the supervised classifier.

3.4 | Hybrid Decision Function

The final decision for each data point is made by combining the results of the anomaly detection and supervised classification components:

$$D(X,Z) = \alpha f(X) + \beta g(X), \tag{7}$$

where α and β are weight coefficients that balance the contributions of supervised and unsupervised learning models, these coefficients are optimized to minimize the number of false positives while maintaining high detection accuracy.

4 | Experimental Setup and Dataset

4.1 | Dataset

We used the IoT-23 dataset, which contains real-world traffic from various IoT devices, including benign and malicious activities. The Dataset includes several attacks, such as DDoS, ransomware, and port scanning [10].

4.2 | Evaluation Metrics

The performance of the hybrid model was evaluated using the following metrics:

Accuracy: the proportion of correctly identified instances (normal and malicious).

Precision: the proportion of true positives among all predicted positives.

Recall: the proportion of true positives among all actual positives.

F1-score: the harmonic mean of precision and recall, balancing false positives and false negatives.

Detection latency: the time taken to detect and respond to threats in real time.

Acknowledgments

The author would like to thank Kiit university for providing support and resources that played a significant role in completing the research on hybrid ML models for IoT security. We are particularly grateful to Hitesh Mahapatra for his expert guidance and thoughtful approach, which played a significant role in developing the established standard of research and practice. The staff for assistance in setting up and maintaining the necessary IoT infrastructure for operational testing. We would also like to thank our colleagues for their collaboration and suggestions, whose comments helped improve our process and contributed to all this great work.

Funding

This research received no specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors carried out all work independently in their respective institutional research activities. KIIT University provided the infrastructure and computational resources for this research.

Data Availability

The data used in this research, including the IoT-23 dataset, is publicly available and can be accessed from the Stratosphere Laboratory at the following link: https://www.stratosphereips.org/datasets-iot23. Any additional data generated or analyzed during this study is available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper. They have no financial, personal, or professional relationships that could be perceived as influencing the research presented here. Additionally, the authors confirm that no competing interests from any third-party organizations or funding sources could have affected the design, execution, or reporting of the findings. This study was conducted independently as part of the authors' academic work, with no external influence or bias. All conclusions drawn are based solely on the data and analysis performed.

References

[1] Sayeed Anwar, Ujjeisheei Panda, & Hitesh Mohapatra. (2024). Legal and ethical issues in IoT based smart city: data privacy, surveillance, and citizen rights. *Journal of computer science engineering and software testing*, *10*(2), 17–26. https://matjournals.net/engineering/index.php/JOCSES/article/view/617

[2] Mishra, S. R., & Mohapatra, H. (2024). Enhancing money laundering detection through machine learning: A comparative study of algorithms and feature selection techniques. In *AI and blockchain applications in industrial robotics* (pp. 300–321). IGI Global. https://www.igi-global.com/chapter/enhancing-money-laundering-detection-through-machine-learning/336091

[3] Mahesh, B. (2020). Machine learning algorithms-a review. *International journal of science and research (IJSR).[internet]*, *9*(1), 381–386. https://www.researchgate.net/profile/Batta-Mahesh/publication/344717762_Machine_Learning_Algorithms_-A_Review/links/5f8b2365299bf1b53e2d243a/Machine-Learning-Algorithms-A-Review.pdf?eid=5082902844932096t

[4] Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of things (IoT): A literature review. *Journal of computer and communications*, *3*(5), 164–173. https://www.scirp.org/journal/paperinformation?paperid=56616

[5] Steinwart, I., & Christmann, A. (2008). *Support vector machines*. Springer Science & Business Media.

[6] Fleury, A., Vacher, M., & Noury, N. (2009). SVM-based multimodal classification of activities of daily living in health smart homes: sensors, algorithms, and first experimental results. *IEEE transactions on information technology in biomedicine*, *14*(2), 274–283. https://doi.org/10.1109/TITB.2009.2037317

[7] Priyadarshini, I. (2024). Anomaly detection of IoT cyberattacks in smart cities using federated learning and split learning. *Big data and cognitive computing*, *8*(3), 21. https://doi.org/10.3390/bdcc8030021

[8] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). *Kitsune: An ensemble of autoencoders for online network intrusion detection*. ArXiv Preprint ArXiv:1802.09089.

[9] Wang, X., Chen, M., Xing, C., & Zhang, T. (2016). Defending DDoS attacks in software-defined networking based on legitimate source and destination IP address database. *IEICE transactions on information and systems*, *99*(4), 850–859. https://search.ieice.org/bin/summary.php?id=e99-d_4_850

[10] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM sigcomm computer communication review*, *34*(2), 39–53. https://dl.acm.org/doi/abs/10.1145/997150.997156