İSTANBUL UNIVERSITY CERRAHPAŞA

ORIGINAL ARTICLE
Electrica 2025; 25: 1-8

Enhancing Zero-Day Attack Detection in IoT Networks via Isolation Forest and Ensemble Tree Models

Serpil Üstebay

Department of Computer Software, İstanbul Medeniyet University Faculty of Engineering and Natural Sciences, İstanbul, Türkiye

Cite this article as: S. Üstebay, "Improving zero-day attack detection accuracy in IoT networks with isolation forest and tree-based models," *Electrica*, 25, 0177, 2025. doi: 10.5152/electrica.2025.24177.

WHAT IS ALREADY KNOWN ON THIS TOPIC?

- *IoT devices are increasingly targeted by cyberattacks due to their exposure to sensitive data, and traditional signature-based intrusion detection systems (IDS) struggle to detect zero-day attacks.*

WHAT DOES THIS STUDY ADD ON THIS TOPIC?

- *This study introduces a two-layer IDS architecture that integrates supervised tree-based models with the Isolation Forest algorithm to improve detection of both known and zero-day attacks.*
- *The proposed method achieves up to 99% accuracy for known attacks and demonstrates promising detection rates (30–62%) for zero-day threats across three diverse IoT datasets.*
- *The research empirically validates the Isolation Forest method as an effective anomaly detection technique for identifying previously unseen cyber threats in IoT environments.*

Corresponding author:
Serpil Üstebay

E-mail:
serpil.ustebay@medeniyet.edu.tr

Received: November 27, 2024
Revision Requested: January 5, 2025
Last Revision Received: January 27, 2025
Accepted: March 3, 2025
Publication Date: August 11, 2025

DOI: 10.5152/electrica.2025.24177

ABSTRACT

The Internet of Things (IoT) devices perform critical functions such as sensitive data collection, storage, and processing, which make them vulnerable to malicious attacks. In this study, a Network Intrusion Detection System was designed to enhance the security of IoT devices. Data sets obtained from three different IoT environments (CICEVSE2024, CICIoT2023, and RT-IoT2022) were utilized for attack detection using tree-based machine learning methods. Experimental results demonstrated that attacks were detected with an average accuracy of 99%. Additionally, a second security layer was implemented to identify zero-day attacks. Analyses showed that the Isolation Forest algorithm detected zero-day attacks with accuracies ranging from 30% to 62%. This proposed approach shows promise in enhancing security against known and unknown attacks.

Index Terms—Cyber-security, Internet of Things, isolation forest, zero-day attack, zero-shot learning

I. INTRODUCTION

The Internet of Things (IoT) has seamlessly integrated into daily life, fueled by rapid advancements in technology and internet infrastructure. The Internet of Things devices connect physical objects to the internet, enabling data collection, recording, analysis, and sharing for various purposes. These devices often process sensitive data critical for managing business operations across sectors such as education, healthcare, industry, and agriculture.

However, increasing demand for IoT devices has made them prime targets for cyber threats. Such threats exploit IoT system vulnerabilities to cause data theft, service interruptions, malware spread, physical damage, and reputational harm to companies. For example, in the healthcare sector, a vulnerability in an IoT device could result in unauthorized access to patient information, while in industrial settings, it could lead to production line disruptions or workforce losses. Therefore, developing robust Intrusion Detection Systems (IDS) to detect and prevent cyber threats is essential.

The evolving nature of cyber threats necessitates continuous updates to IDS systems and the integration of multiple approaches to ensure robust defense. Three fundamental approaches are commonly employed in Network Intrusion Detection Systems (NIDSs) [1]: Signature-based IDS, Anomaly-based IDS, and Stateful Protocol Analysis.

Signature-based IDS systems detect known attacks by matching observed activities against a database of stored patterns. Observed activities are checked against these stored patterns. While these systems are highly effective at identifying known attacks, they struggle to detect new or variant attack types [2-4]. Anomaly-based IDS uses rules representing normal system behavior, often created using statistical methods, to identify anomalies. Observed activities are evaluated against these rules to identify anomalies [5-7].

Stateful protocol analysis records generally accepted normal protocol activities for each protocol state. Profiles outline appropriate protocol usage, and anomalies are detected by comparing observed events to predefined profiles [8].

In recent years, machine learning (ML) has been increasingly applied to enhance the performance and efficiency of many technological applications by extracting and learning complex data patterns that are otherwise difficult for experts to observe. Machine learning's capabilities have also been leveraged to detect threats in NIDS. In [9], Distributed Denial of Service (DDoS) attacks were detected using the CICDDoS2019 dataset, various machine learning algorithms such as artificial neural networks, support vector machines (SVM), Naive Bayes (NB) variants, logistic regression (LR), k-nearest neighbors (KNN), decision trees (DT), and random forests (RFs), achieved high accuracy rates of 98%–99%.

Similarly, [10] investigated the impact of data issues such as missing values, outliers, and imbalanced records on machine learning model performance using the CICIDS2017 dataset. Pre-processing steps included data cleaning, matching, normalization, outlier detection, sampling, and dimensionality reduction. DT, RF, NB, and LR models were trained for six different attack types. Random forest achieved the highest accuracy of 99.94% on the processed dataset.

Despite their effectiveness, signature-based NIDS systems are limited in detecting zero-day attacks, which target undiscovered vulnerabilities [11]. Zero-day attacks pose a particularly severe threat to networks. These are carried out by targeting vulnerabilities in the software of devices that have not yet been discovered. Zero-day vulnerabilities can cause huge financial and intangible damage when exploited before being noticed by device manufacturers.

This work aims to improve IoT security by developing a NIDS that combines ML models with the Isolation Forest (iForest) algorithm to detect known and zero-day attacks. The study aims to fill a critical gap in the existing cybersecurity literature by demonstrating the high accuracy of machine learning models in detecting known attacks and the potential of Isolation Forest to address zero-day attacks.

The paper is structured as follows: Section II provides a comprehensive review of the existing literature related to zero-day attack detection and the application of iForest in cybersecurity. Section III details methods and experimental setups. Section IV presents the proposed approach's results and discusses the findings. Finally, Section V concludes the study.

II. LITERATURE REVIEW

Zero-day attacks are difficult to detect as they exploit unknown vulnerabilities, making them a critical concern for cybersecurity researchers. To address this, researchers are analyzing outlier-based methods for zero-day attack detection. Two common approaches utilized in this context are the One-Class SVM and autoencoders [12]. Analyzing both approaches, [13] shows that detection accuracy ranges from 89% to 99% for the NSL-KDD and from 75% to 98% for the CICIDS2017. Research highlights that both models have a low miss rate (false positives) in zero-day attack detection, but the accuracy of autoencoders is higher compared to One-Class SVM. In addition to that, [14] analyzed Snort's, an open-source NIDS and intrusion prevention system, performance in detecting zero-day attacks. It was tested on 183 previously unseen attack vectors, achieving an accuracy of 17%. It was emphasized that, although this detection rate is low, it is not zero.

[15] developed a security system for attack detection in a fog environment by combining Autoencoder and iForest methods in fog computing. The research achieved a 95.4% accuracy rate in tests conducted with the NSL-KDD dataset. Since their proposed system supports binary classification, it is insufficient to determine the attack type. Besides, no analysis is presented about the contributions or support level of the iForest method to the autoencoder method. Similarly, [16] used the iForest method to detect anomalies in web traffic and achieved a high accuracy rate of 93%. The low computational complexity of the iForest model enables it to detect anomalies very quickly. No analysis is included in this study to detect zero-day attacks.

iForest-based outlier detection model [17] is used to detect outliers in the training set. Before outlier detection, the dataset is reduced using feature elimination methods. Then, all outliers are detected and removed to make the intrusion detection model more effective. The research achieved an average of 3% increase in precision, recall, F1 score, and accuracy values using LR, SVM, AdaBoost, NB, and KNN methods.

This study analyzes tree-based ML models' success in detecting cyber-attacks in different IoT environments. Three different IoT environments (CICEVSE2024, CICIoT2023, and RT-IoT2022) are used in this context. Logistic regression, DT, KNN, SVM, AdaBoost, RF, and XGBoost methods were compared for detecting attacks in Electric Vehicle Charging Equipment (EVSE) networks [18]. Methods such as XGBoost and AdaBoost proved effective in distinguishing the complex attack patterns of EVSE networks. XGBoost demonstrated superior accuracy and a lower false alarm rate compared to other methods. Tree-based ensemble learning techniques have emerged as powerful tools for enhancing the security of EVSE networks and optimizing attack detection. The Federated Learning-Based Anomaly Detection System (FL-EVCS) [19] aims to protect data privacy by sharing model parameters, avoiding the centralized data collection used in traditional ML approaches, which is considered insecure. Researchers obtained 97% accuracy from the CICEVSE2024 dataset. Results underscore FL-EVCS's ability to establish a secure and resilient charging infrastructure while maintaining strict privacy standards. In addition, [20] achieved an average accuracy of 94.23% was achieved on the CICEVSE dataset using deep learning-based AutoKeras and genetic programming-based TPOT frameworks.

[21] developed IDS systems using the CICIoT2023 dataset, which includes 33 different attack types. Three classification strategies were applied: 34 classes, 8 classes, and a binary class. These scenarios were analyzed using DT, RF, LR, AdaBoost, and SVM. Among all scenarios, while SVM demonstrated the lowest accuracy (76.09%), RF emerged as the most robust model, achieving 99% accuracy across all scenarios. [22] focused on detecting DDoS attacks using two-stage deep learning models such as Deep Neural Networks (DNN), Convolutional Neural Networks, and Long short-term memory networks (LSTM). Firstly, the models determined whether the network flood was malicious, and subsequently, they identified whether the malicious activity constituted a DDoS attack in the CICIoT2023 dataset. Long short-term memory stood out as the best model, achieving 94% accuracy in the first stage and 90% accuracy in the second stage. The researchers highlighted that, although the two-stage model enhanced accuracy, its computational complexity posed challenges for real-time application, necessitating further improvements. Likewise, [23] implemented various machine learning algorithms, including LR, KNN, and DNN, on the CIC2023 dataset to identify attack patterns. Across all models, a precision of 0.9999 was achieved, along with equally high recall, accuracy, and F1 scores.

[24] developed IDS systems for IoT environments using the RT-IoT2022 dataset and various machine learning methods, including KNN, SVM, DT, Gradient Boosting (GB), XGBoost, RF, and Extremely Randomized Trees (ERT). Random forest and XGBoost models stood out, achieving 99% accuracy. These models demonstrated their reliability for real-time IoT attack detection by excelling across multiple metrics, such as F1 score, recall, precision, and accuracy.

[25] presented a two-stage feature selection approach that reduces computational load while maintaining IoT system security. They achieved 98.8% accuracy by reducing the RT-IoT2022 dataset by 62%, using an enhanced whale optimization algorithm (WOA-HA) that incorporates a chaotic Hénon map mechanism, an adaptive coefficient vector, and a binary operator. However, the complexity of the parameter settings in this approach requires domain-specific knowledge. Additionally, while the algorithm performs well with large IoT datasets, its efficiency may decrease with extremely large-scale data.

[26] study in context employed the Quantized Autoencoder model for detecting network anomalies in edge devices through unsupervised learning. The model integrates optimization techniques such as pruning, clustering, and quantization. Experimental studies conducted with the 2022 RT-IoT dataset to train the model achieved an average accuracy of 98%.

III. MATERIALS AND METHODS

In this section, we provide a comprehensive overview of the datasets, machine learning techniques, and the proposed methodology for ensuring secure IoT systems.

A. Datasets

Three different datasets, CICEVSE2024, CICIoT2023, and RT-IoT2022 were used from different IoT environments. Each dataset includes network traffic floods and has its own domain-specific protocols and attacks.

CICEVSE2024 [27] is designed to contribute to cybersecurity research on EV charging stations, considering the increasing use of electric vehicles. It includes various attack scenarios, covering both network and host attacks on EVSE when idle and during charging. Researchers can assess the suitability of specific features by utilizing the dataset for tasks such as statistical analysis, behavioral profiling, and anomaly detection. Detailed information on the types of attacks performed is provided in Table I. In this work, we used CICEVSE-A device network flood.

CICIoT2023 [28] aims to enhance security analytics applications in real IoT operations, with 33 attacks performed on an IoT topology consisting of 105 devices. Generating large-scale data for IoT security is a costly and complex process. The Canadian Cybersecurity Institute has established a laboratory to develop IoT security solutions and made this data available to improve cybersecurity practices and support the development of new solutions to address these challenges. Table II lists the attack scenarios performed in the test environment.

RT-IoT2022 [29] contains data from a testbed representative of the real world created by combining different IoT devices such as Thing Speak-LED, Wipro-Bulb, and MQTT-Temp. Attacks in the dataset are categorized in Table III.

B. Methods

In this study, zero-day attacks are examined by defining an outlier as an observation that deviates from generally expected behavior [30]. Anomalies can be described as abnormal behaviors (attacks) generated by different processes that do not conform to the system's normal (benign) structure. iForest assumes that outliers are rare and tend to be located far from the centers of normal clusters. This technique relies on a partitioning process using a random tree structure. For each dataset, a random feature is selected, and a random partition value is chosen between the minimum and maximum values

TABLE I. CICEVSE DATASET DESCRIPTION

Attack Group	Number of Records	Types
Benign	68	Normal traffic
Recon	98 547	Aggressive-scan, vulnerability-scan, os-fingerprinting, portscan, service-detection, slowloris-scan, SYN-stealth-scan, synonymous-IP
Dos	131 094	ICMP-fragmentation, SYN-flood, TCP-flood

TABLE II. CICIOT2023 DATASET DESCRIPTION

Attack Group	Number of Records	Attack Types
Benign	295 585	Normal traffic
DDoS	109 996	ACK fragmentation, UDP flood, SlowLoris, ICMP flood,RSTFIN flood, PSHACK flood, HTTP flood, UDP fragmentation, TCP flood, SYN flood, SynonymousIP flood
Brute Force	10 000	Dictionary brute force
Spoofing	10 000	ARP spoofing, DNS spoofing
DoS	39 999	TCP flood, HTTP flood, SYN flood, UDP flood
Recon	42 262	Ping sweep, OS scan, Vulnerability scan, Port scan, Host discovery
Web-based	24 828	Sql injection, Command injection, Backdoor malware, Uploading attack, XSS, Browser hijacking
Mirai	29 999	GREIP flood, Greeth flood, UDPPlain

TABLE III. RT-IOT2022 DATASET DESCRIPTION

Attack Group	Number of Records	Attack Types
Benign	12 507	
DoS	94 659	DOS_SYN_Hping
DDoS	534	DDOS_Slowloris
Recon	7602	Nmap_Udp_Scan, Nmap_Xmas_Tree_Scan, Nmap_Os_Detection, Nmap_Tcp_Scan, Nmap_Fin_Scan
Spoofing	7750	ARP_poisoning
Brute Force	37	Metasploit_Brute_Force_SSH

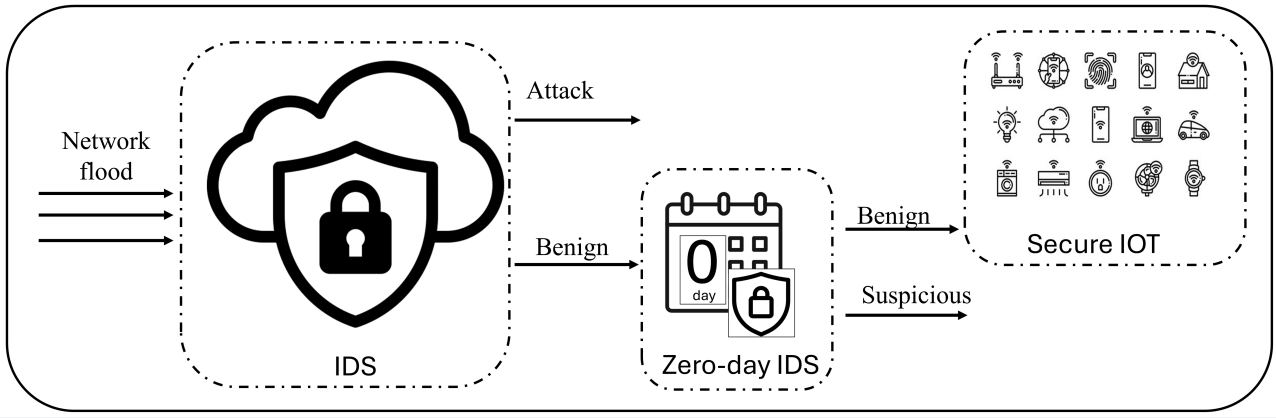

Fig. 1. Proposed NIDS system architecture.

of that feature to construct the tree structures. Outliers are isolated with fewer partitions compared to normal data points, resulting in shorter paths for outliers. To achieve this, an anomaly score is calculated for each sample based on (1).

$$S(x) = 2^{-H(x)/c(n)} \quad (1)$$

H(x) represents the isolation depth for sample x, while c(n) is the normalization factor, calculated based on the size of the dataset. S(x) denotes the anomaly score of the sample, with higher scores indicating a greater likelihood of the sample being anomalous.

The proposed IDS system incorporates a two-stage security mechanism, as illustrated in Fig. 1. The first stage employs supervised machine learning methods to detect known attacks originating from previously identified vulnerabilities. In this stage, widely adopted models from the literature are utilized for security detection. The second stage focuses on identifying potential zero-day attacks using iForest. Network flows that pass through the first stage are analyzed by iForest to assess their likelihood of being zero-day attacks. Normal flows are forwarded to the secure IoT environment, while suspicious flows are directed to the appropriate security officer for further investigation.

TABLE IV. PERFORMANCE METRICS OF ML MODELS

Dataset	ML Model	Accuracy	Precision	Recall	F1 Score
CICEVSE2024	DT	1	1	1	1
	RF	0.99	0.99	0.99	0.99
	GB	0.99	0.99	0.99	0.99
	ET	0.99	0.99	0.99	0.99
	XGB	0.99	0.99	0.99	0.99
CICIoT2023	DT	0.76	0.76	0.76	0.76
	RF	0.81	0.81	0.81	0.81
	GB	0.79	0.79	0.79	0.79
	ET	0.74	0.74	0.74	0.74
	XGB	0.82	0.82	0.82	0.81
RT-IoT2022	DT	0.99	0.99	0.99	0.99
	RF	0.99	0.99	0.99	0.99
	GB	0.99	0.99	0.99	0.99
	ET	0.99	0.99	0.99	0.99
	XGB	0.99	0.99	0.99	0.99

IV. RESULTS AND DISCUSSION

This study used Python 3.11, Pandas 2.0, and scikit-learn 1.4 libraries on a Windows 11 operating system with a 2nd Generation Intel® Core™ i5-1240P processor. All datasets were divided into 70:30 training and test sets. Models were optimized using a probability-based Bayesian method. Hyperparameters tested with the Bayesian method include the number of estimators (50, 500), maximum depth (10, 100), learning rate (1e-4, 1e-1), subsample (0.5, 1.0), colsample bytree (0.5, 1.0), gamma (0, 10), and minimum child weight (1, 10). These values were tested to optimize the balance between overfitting and generalization, with the best model being selected. Records containing missing values were removed from the study. Raw data was used without any preprocessing. Accuracy, precision, recall, and F1-score were used to evaluate the performance of the models. Accuracy represents the ratio of correctly predicted samples to all test samples. Precision measures the proportion of positive predictions that were actually correct. Recall (also known as Sensitivity) indicates how many of the actual positive samples were correctly identified by the model. F1-Score is the harmonic mean of Precision and Recall. It is often preferred over accuracy when dealing with imbalanced data.

Since tree-based ML models are known for their robustness in handling noisy data and their ability to model complex relationships [31-32]. In this work, we used DT, RF, GB, ET, and XGB models to analyze IoT security challenges. Table IV presents a comparison of testing performance metrics for three different datasets: RT-IoT2022, CICEVSE2024, and CICIoT2023. While models achieved high performance in RT-IoT2022 and CICEVSE2024 environments, as shown in Table IV, performance metrics in CICIoT2023 are insufficient for a robust NIDS when compared to the works in [21], [22], and [23]. This could be due to the dataset's complexity, which may be related to

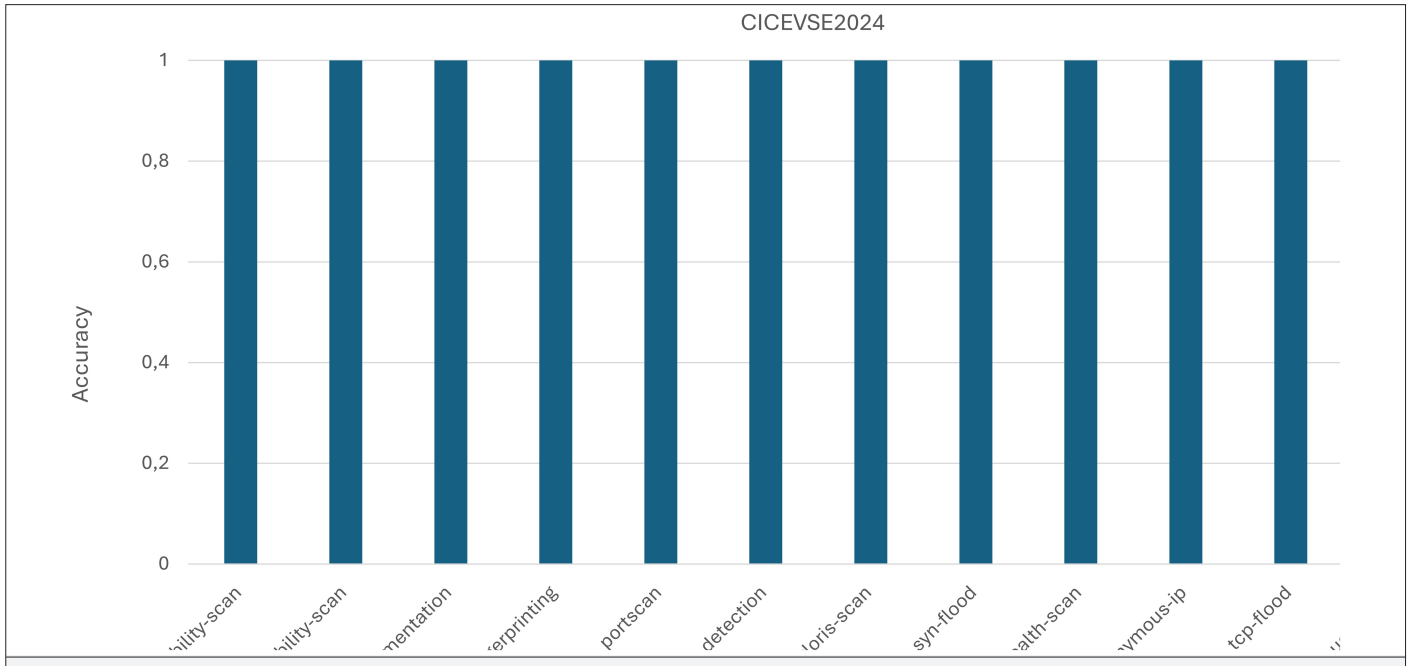

Fig. 2. Zero-day attack detection accuracy of iForest algorithm according to different attack scenarios by using CICEVSE2024.

its device variety, number of devices, attack types, and other factors. Commonly, as the complexity of the dataset increases, it becomes more challenging for machine learning models to identify the relationship between benign and attack data [33-34]. [21] achieved 99% accuracy in detecting attack samples using RF. In contrast, we obtained a lower accuracy of 81% with RF. Since no information regarding the hyperparameters of the RF model was provided in [21], a comparative analysis could not be conducted. Although high accuracy was reported in [23], the study focused on developing an NIDS using binary classification, where network floods are predicted as either malicious or benign. This approach does not provide information about specific attack types. However, since the primary goal of the study was to demonstrate the effectiveness of the iForest method against zero-day attacks, the analysis showed that the iForest method improved security by an average of 62% for CICIoT2023.

Each dataset contains different attack scenarios based on its structure. Consequently, separate iForest models were trained for each dataset. Since zero-day attacks are those that have not been seen before, the iForest model was trained by excluding these attack data from the training set during the training phase. Each attack type was assumed to be a zero-day attack and presented to the iForest

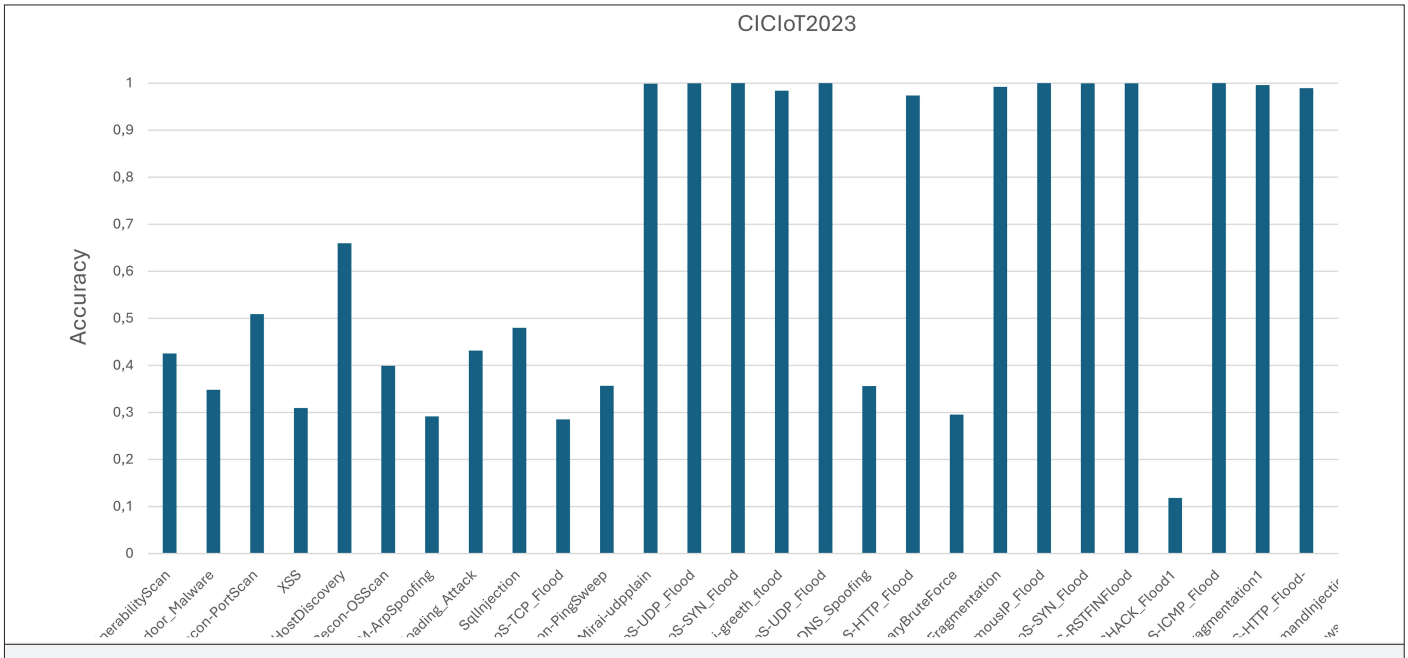

Fig. 3. Zero-day attack detection accuracy of iForest algorithm according to different attack scenarios by using CICIoT2023.

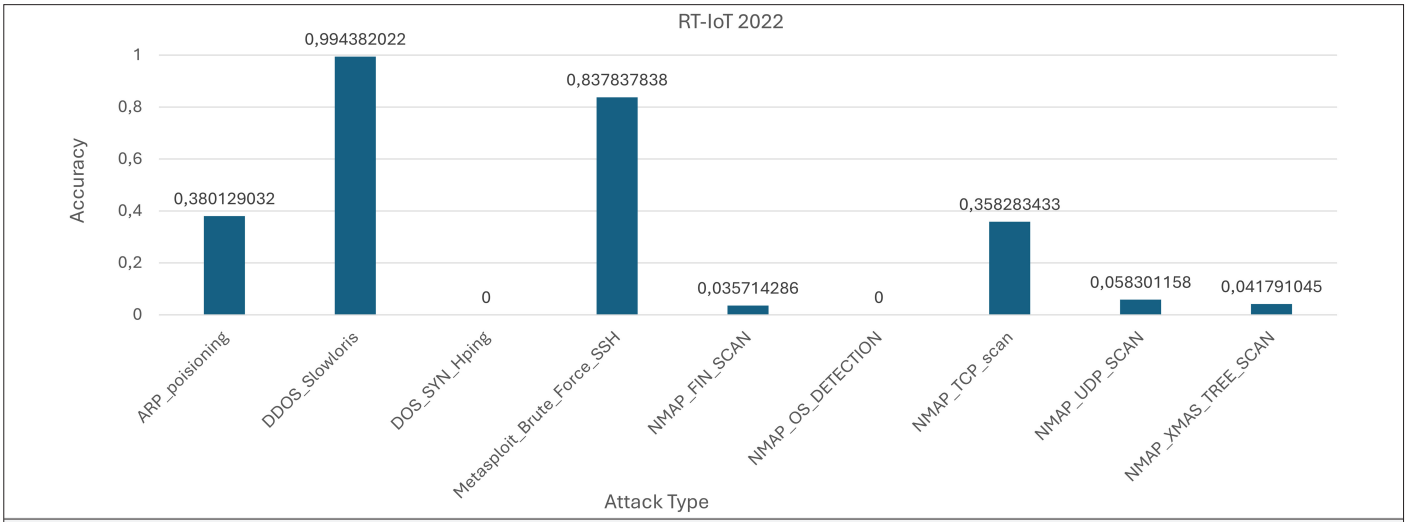

Fig. 4. Zero-day attack detection accuracy of iForest algorithm according to different attack scenarios by using RT2022.

method for testing within the corresponding dataset. The model's performance, evaluated in terms of accuracy, is presented in Figs. 2-4.

The use of EVs in the transportation sector is increasing [35]. In addition to serving as an alternative for transportation, the integration of green energy sources has made these vehicles a key component of energy management systems [36]. The increasing number of charging stations has also introduced new security challenges. While ML has demonstrated its effectiveness in cybersecurity within other IoT environments [37], research in this area is limited. This study shows that ML can enhance cybersecurity for EVs. In addition to addressing known attacks, it was found that the iForest method provides high accuracy in detecting zero-day attacks. For a more robust defense, these methods should be further tested on diverse datasets.

This study adopted a similar approach to [16] and [17] in terms of zero-day attack detection and utilized the iForest method. A key distinction between our study and theirs is that we demonstrate the effectiveness of iForest in zero-day detection through comparative analyses involving different scenarios, where the iForest method was both used and not used. [17] observed an average performance increase of 3% in detecting zero-day attacks using iForest, which is lower than the performance of the model we presented. Furthermore, [15] was designed to analyze possible attack types, including zero-day attacks, separately, considering the problem beyond a general classification task. Known attack types were taught to existing tree-based ML algorithms, achieving 99% accuracy. iForest was used to reconsider the possible 0.1% error margin. An average accuracy of 62% was obtained for CICIoT2023, and an average of 30% accuracy was obtained for RT2022. Each attack includes different attack vectors targeting various vulnerabilities. When Fig. 2 is examined, the Mirai-great-flood attack was detected at a rate of 100%, while Recon-OsScan was detected at a rate of 39%. This is related to how different attack vectors can be from the system's normal state. Some attacks were not detected at all in the RT-IoT2022 dataset, which is an expected outcome.

V. CONCLUSION

The Internet of Things devices are used in critical processes such as collecting, storing, routing, and managing sensitive data, enabling revolutionary developments in many sectors. However, the sensitive data they contain and their widespread usage have made IoT devices open targets for malicious people. NIDS systems are essential to ensure the security of IoT environments. Although these systems effectively detect known vulnerabilities with traditional methods, they can be vulnerable to zero-day attacks. In this study, a NIDS system was designed to ensure the security of different IoT environments. The iForest method was used to detect zero-day attacks. Obtained results are promising, and there is a need to develop more secure systems. There is no silver bullet in cybersecurity.

In the future, we aim to maximize the accuracy rate of detection of zero-day attacks based on a hybrid system that uses iForest and neural networks.

Data Availability Statement: The data that support the findings of this study are available on request from the corresponding author.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – S.Ü.; Design – S.Ü.; Supervision – S.Ü.; Resources – S.Ü.; Materials – S.Ü.; Data Collection and/or Processing – S.Ü.; Analysis and/or Interpretation – S.Ü.; Literature Search – S.Ü.; Writing – S.Ü.; Critical Review – S.Ü.

Declaration of Interests: The author has no conflicts of interest to declare.

Funding: The author declare that this study has received no financial support.

REFERENCES

1. M. S. Ozkan-Okay, "A comprehensive systematic literature review on intrusion detection systems," *IEEE Access*, vol. 9, pp. 157727–157760, 2021. [CrossRef]
2. K. Rai, M. S. Devi, and A. Guleria, "Decision tree based algorithm for intrusion detection," *Int. J. Adv. Netw. Appl.*, vol. 7, no. 4, p. 2828, 2016.
3. N. Hubballi, and V. Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey," *Comput. Commun.*, vol. 49, pp. 1–17, 2014. [CrossRef]
4. M. Uddin, A. A. Rahman, N. Uddin, J. Memon, R. A. Alsaqour, and S. Kazi, "Signature-based multi-layer distributed intrusion detection system using mobile agents," *Int. J. Netw. Secur.*, vol. 15, no. 2, pp. 97–105, 2013.

5. F. Geramiraz, A. S. Memaripour, and M. Abbaspour, "Adaptive anomaly-based intrusion detection system using fuzzy controller," *Int. J. Netw. Secur.*, vol. 14, no. 6, pp. 352–361, 2012.
6. R. Samrin, and D. Vasumathi, 2017, "Review on anomaly based network intrusion detection system," *In 2017 international conference on electrical, electronics, communication, computer, and optimization techniques* (ICEECCOT) (pp. 141–147).
7. W. Yassin, N. I. Udzir, Z. Muda, and M. N. Sulaiman, *Anomaly-Based Intrusion Detection through k-Means Clustering and Naives Bayes Classification*, 2013.
8. D. Seo, and H. L. (tarih yok), "SIPAD: SIP-VoIP anomaly detection using a stateful rule tree," *Comput. Commun.*, vol. 36, no. 3, p. 562574, 2013.
9. T. Aytaç, M. A. AYDIN, and A. H. ZAİM, "Detection DDOS attacks using machine learning methods," *Electrica*, vol. 20, no. 2, pp. 159–167, 2020. [CrossRef]
10. E. Y. Guven, S. Gulgun, C. Manav, B. Bakir, and Z. G. Aydin, "Multiple classification of cyber-attacks using machine learning," *Electrica*, vol. 22, no. 2, pp. 313–320, 2022. [CrossRef]
11. M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, "From zero-shot machine learning to zero-day attack detection," *Int. J. Inf. Sec.*, vol. 22, no. 4, pp. 947–959, 2023. [CrossRef]
12. Y. Guo, "A review of Machine Learning-based zero-day attack detection: Challenges and future directions," *Comput. Commun.*, vol. 198, pp. 175–185, 2023. [CrossRef]
13. H. Hindy, R. Atkinson, C. Tachtatzis, J.-N. Colin, E. Bayne, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," *Electronics*, vol. 9, no. 10, p. 1684, 2020. [CrossRef]
14. H. Holm, "Signature based intrusion detection for zero-day attacks:(not) a closed chapter?," In 47th Hawaii international conference on system sciences. New York: IEEE, 2014, pp. 4895–4904. [CrossRef]
15. K. Sadaf, and J. Sultana, "Intrusion detection based on autoencoder and isolation forest in fog computing," *IEEE Access*, vol. 8, pp. 167059–167068, 2020. [CrossRef]
16. W. Chua et al., "Web traffic anomaly detection using isolation forest," *Informatics*, vol. 11, no. 4, p. 83, 2024. [CrossRef]
17. R. C. Ripan et al., "An isolation forest learning based outlier detection approach for effectively classifying cyber anomalies," In *Hybrid, J. Intell. Syst.*: 20th International Conference on Hybrid Intelligent Systems (HIS 2020), Springer International Publishing, 2021, pp. 270–279.
18. S. R. Hegde, V. V., K. R. M. V. Chandrakala, G. K. T., and V. K. A. Shankar, "Enhancing anomaly detection in Electric Vehicle Supply Equipment (EVSE) networks using classical and ensemble learning approaches," Control Instrumentation System Conference (CISCON), Manipal, India, 2024, pp. 1–5. [CrossRef]
19. S. Purohit, and M. Govindarasu, "FL-EVCS: Federated Learning based Anomaly Detection for EV Charging Ecosystem," 33rd International Conference on Computer Communications and Networks (ICCCN). Kailua-Kona: HI, pp. 1–9. [CrossRef]
20. D. Vasan, E. J. S. Alqahtani, M. Hammoudeh, and A. F. Ahmed, "An AutoML-based security defender for industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 47, 100718, 2024. [CrossRef]
21. A. G. Kumar, A. Rastogi, and V. Ranga, "Evaluation of different machine learning classifiers on new IoT dataset CICIoT2023," International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India, 2024, pp. 1–6. [CrossRef]
22. S. Hizal, U. Cavusoglu, and D. Akgun, "A novel deep learning-based intrusion detection system for IoT DDoS security," *Internet Things*, vol. 28, 101336, 2024. [CrossRef]
23. A. Berqia, H. Bouijij, A. Merimi, and A. Ouaggane, "Detecting DDoS attacks using machine learning in IoT environment," In International Conference on Intelligent Systems and Computer Vision (ISCV). New York: IEEE, 2024, pp. 1–8. [CrossRef]
24. N. U. Sama, S. Ullah, S. M. A. Kazmi, and M. Mazzara, "Cutting-edge intrusion detection in IoT networks: A Focus on ensemble models," in *IEEE Access*, vol. 13, pp. 8375–8392, 2025. [CrossRef]
25. K. Zhang, Y. Liu, X. Wang, F. Mei, G. Sun, and J. Zhang, "Enhancing IoT (Internet of Things) feature selection: A two-stage approach via an improved whale optimization algorithm," *Expert Syst. Appl.*, vol. 256, 124936, 2024. [CrossRef]
26. B. S. Sharmila, and R. Nagapadma, *Quantized Autoencoder (QAE) Intrusion Detection System for Anomaly Detection in Resource-Constrained IoT Devices Using RT-IoT2022 Dataset. Cybersecurity*, 2023.
27. E. D. Buedi, A. A. Ghorbani, S. Dadkhah, and R. L. Ferreira, "Enhancing ev charging station security using a multi-dimensional dataset": Cicevse2024, In IFIP Annual Conference on Data and Applications Security and Privacy. Cham: Springer Nature Switzerland, 2024, pp. 171–190.
28. E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors (Basel)*, vol. 23, no. 13, 5941, 2023. [CrossRef]
29. B. S. Sharmila, and R. Nagapadma, "Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset," *Cybersecurity*, vol. 6, no. 1, p. 41, 2023. [CrossRef]
30. A. Blázquez-García, A. Conde, U. Mori, and J. A. Lozano, "A review on outlier/anomaly detection in time series data," *ACM Comput. Surv. (CSUR)*, vol. 54, no. 3, pp. 1–33, 2022. [CrossRef]
31. T. Chen, and C. Guestrin, "Xgboost: A scalable tree boosting system," In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, NY, USA: ACM, 2016, pp. 785–794. [CrossRef]
32. M. Rashid, J. Kamruzzaman, T. Imam, S. Wibowo, and S. Gordon, "A tree-based stacking ensemble technique with feature selection for network intrusion detection," *Appl. Intell.*, vol. 52, no. 9, pp. 9768–9781, 2022. [CrossRef]
33. S. Uddin, and H. Lu, "Dataset meta-level and statistical features affect machine learning performance," *Sci. Rep.*, vol. 14, no. 1, p. 1670, 2024. [CrossRef].
34. M. Z. Naser, and A. Alavi, 2020, *Insights into Performance Fitness and Error Metrics for Machine Learning. arXiv Preprint ArXiv:2006.00887*.
35. S. Aggarwal, and A. K. Singh, "Electric vehicles the future of transportation sector: A review," *Energy Sources A*, pp. 1–21, 2021. [CrossRef]
36. A. M. Al-Ghaili, H. Kasim, H. Aris, and N. M. Al-Hada, "Can electric vehicles be an alternative for traditional fossil-fuel cars with the help of renewable energy sources towards energy sustainability achievement?," *Energy Inform.*, vol. 5 (Suppl 4), p. 60, 2022. [CrossRef]
37. A. Thakkar, and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges," *Arch. Comp. Methods Eng.*, vol. 28, no. 4, pp. 3211–3243, 2021. [CrossRef]

Serpil Üstebay received the Ph.D. degree from İstanbul University in 2018. She currently works as an Assistant Professor in the Department of Computer Engineering at Istanbul Medeniyet University, Türkiye. Her research interests include IoT, cybersecurity, machine learning, and deep neural networks.