Black Sea Journal of Engineering and Science
doi: 10.34248/bsengineering.1353999

Open Access Journal
e-ISSN: 2619 – 8991

Research Article
Volume 7 - Issue 3: 488-494 / May 2024

THE IMPACT OF DEVICE TYPE NUMBER ON IOT DEVICE CLASSIFICATION

Ahmet Emre ERGÜN[1]*, Özgü CAN[2]

[1]İzmir Katip Çelebi University, Faculty of Engineering and Architecture, Department of Computer Engineering, 35620, İzmir, Türkiye
[2]Ege University, Faculty of Engineering, Department of Computer Engineering, 35100, İzmir, Türkiye

Abstract: Today, connected systems are widely used with the recent developments in technology. The internet-connected devices create data traffic when communicating with each other. These data may contain extremely confidential information. Observers can obtain confidential information from the traffic when the security of this traffic cannot be adequately ensured. This confidential information can be personal information as well as information about the type of device used by the person. Attackers could use machine learning to analyze encrypted data traffic patterns from IoT devices to infer sensitive information, even without decrypting the actual content. For example, if someone uses IoT devices for health monitoring or smoke detection, attackers could leverage machine learning to discern victims' habits or identify health conditions. An increase in the number of IoT devices may decrease the accuracy of classification when using machine learning. This paper presents the importance of the effect of device type number on the classification of IoT devices. Therefore, inference attacks on privacy with machine learning algorithms, attacks on machine learning models, and the padding method that is commonly used against such attacks are presented. Moreover, experiments are carried out by using the dataset of the traffic generated by the Internet of Things (IoT) devices. For this purpose, Random Forest, Decision Tree, and k-Nearest Neighbors (k-NN) classification algorithms are compared, and the accuracy rate changes according to the number of devices are presented. According to the results, the Random Forest and Decision Tree algorithms are found to be more effective than the k-NN algorithm. When considering a scenario with two device types, the Random Forest and Decision Tree algorithms achieved an accuracy rate of 98%, outperforming the k-NN algorithm, which had an accuracy rate of 95%.

Keywords: Classification, Internet of things (IoT), Machine learning, Padding, Privacy, Trade-off

***Corresponding author:** İzmir Katip Çelebi University, Faculty of Engineering and Architecture, Department of Computer Engineering, 35620, İzmir, Türkiye
E mail: ahmetemreergun95@gmail.com (A. E. ERGÜN)
Ahmet Emre ERGÜN https://orcid.org/0000-0002-3025-5640
Özgü CAN https://orcid.org/0000-0002-8064-2905

Received: September 01, 2023
Accepted: April 26, 2024
Published: May 15, 2024
Cite as: Ergün AE, Can Ö. 2024. The impact of device type number on IoT device classification. BSJ Eng Sci, 7(3): 488-494.

1. Introduction

The use of Internet of Things (IoT) devices is higher than it has ever been, and it is expanding rapidly. The number of cyber threats has increased considerably with the widespread use of these IoT devices. In particular, devices such as cameras, sensors, smartphones, smart clocks, heat meters that are connected to the Internet create various security problems. These devices create data traffic when communicating with each other. If the security and privacy of this data traffic cannot be ensured sufficiently, threats may occur. Attackers who observe data traffic can infer highly confidential information from that traffic (Ergün and Can, 2022a). For this purpose, machine learning algorithms are used to classify the IoT devices and also the type of these devices. Thus, devices that are used in the traffic can be detected and their device models or manufacturer information can be identified. Thereupon, attackers gain large amounts of sensitive information as IoT devices collect significant amount of data. For example, the privacy of personal health information may be violated by detecting wearable devices that measure blood pressure and pacemakers. Also, the location information tracked from a detected device such as a smartphone or a smartwatch may also result in a privacy violation (Kröger, 2018). Similarly, the smoke sensor information can be used to obtain the smoking habit of the individual.

The machine learning techniques used by the traffic observer extract packet features from encrypted IoT device traffic as input. The encrypted packets' transmission time and packet size characteristics are visible to the observer. Additionally, the observer uses them to categorize IoT devices and anticipates having a high probability of success in accessing accurate data about different device types in the traffic. The fundamental concept behind deploying machine learning is the attacker model's capacity to learn data characteristics like packet size and transmission time, even when the traffic is encrypted. As a result, privacy leakage occurs. Therefore, obfuscating the traffic is needed to falsify the machine learning algorithms. Enhancing communication privacy without degrading network performance is crucial. For this purpose, the padding method is used to prevent traffic classification, to improve the communication privacy and preserve user privacy.

The goal of the packet padding mechanism is to mitigate the challenges in preserving privacy in IoT (Pinheiro et al., 2020). Thus, padding is applied to the packet size to disguise the packet size. The goal of this study is to present the privacy threats in IoT traffic, privacy attacks against internet-connected devices, the padding method that is widely used against these attacks, and an evaluation based on Random Forest, Decision Tree and k-NN classification algorithms that are widely used in attacks. For this purpose, the experimental results are compared by the device type number and the related machine learning algorithms that are used for the classification. Thus, the study shows the effect of the number of device types and the chosen machine learning method on the accuracy rates. The organization of this study is as follows: In Section 2, the commonly used machine learning methods, the padding method used to preserve privacy, and attacks on machine learning methods are explained. In Section 3, Random Forest, Decision Tree and k-NN algorithms are evaluated to infer device type. Results and the accuracy rates are presented in Section 4. Finally, Section 4 concludes and outlines the future work.

2. Materials and Methods

2.1. Machine Learning Methods Commonly Used in Attacks

Machine learning methods can be used for inferences made from the traffic of devices connected to the Internet, and the rate of inference can vary according to the selected algorithm. Machine learning algorithms commonly used in attacks on privacy are Random Forest, Decision Tree, and k-NN. Random Forest, as the name suggests, consists of a large number of individual decision trees that work as a community (Abdulkareem and Abdulazeez, 2021). Each tree in the Random Forest predicts a class and the class with the most votes becomes the model's prediction. Using the Random Forest algorithm, in the work of (Dogru and Subasi, 2018), they reached 92% accuracy. Decision Tree algorithm deals with developing decision making models based on the true values of data features (Alghuried, 2017). These algorithms work by teaching the system how to classify and predict data (Charbuty and Abdulazeez, 2021). The algorithms look for the tree structure until a selection is made. (Aksoy and Gunes, 2019) used the Decision Tree algorithm to identify 33 IoT devices with a high accuracy of 98%. k-Nearest Neighbor (k-NN) algorithm is a widely used non-parametric classification method (Wang et al., 2021). It is used for classification and regression of data. An important feature of any kNN technique for classification or regression is to find the k-NN that allows us to estimate the value or class for a given point (Gawri et al., 2022). Pinheiro et al. (2020) has achieved 94% accuracy rate by using the k-NN algorithm in their studies.

The model in which the traffic observer (attacker) observes the data transmission between the victim and the IoT device and obtains data after taking the resulting data into the machine learning process is shown in Figure 1. The attacker first gathers encrypted data and analyzes traffic using packet sent times and packet sizes. The attacker classifies the data with machine learning algorithms, allowing him/her to infer the types of devices the victim uses.

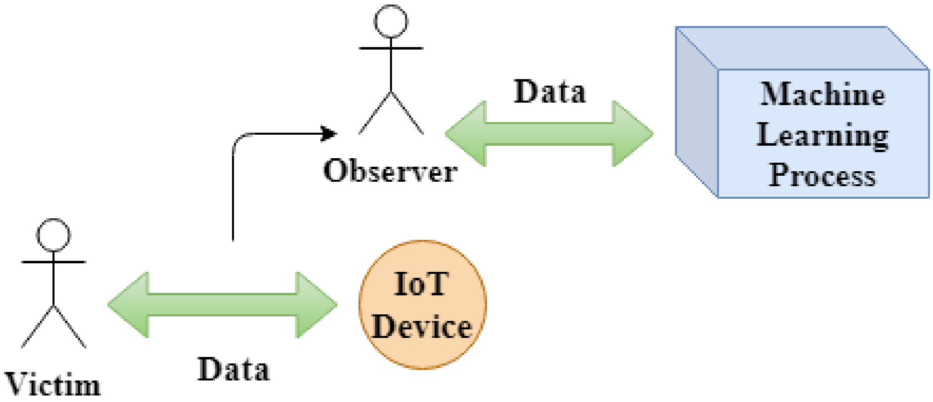


Figure 1. Attack model

2.2. Padding Method

An attacker watching the traffic can make inferences about the traffic even though the traffic is encrypted. This can create serious threats to privacy. The attacker can optimize the packet sizes in the traffic using machine learning algorithms. Packet sizes can cause information leakage about the device type. Therefore, these packets appear as larger bytes than they originally were, thanks to the padding method based on changing traffic packet sizes. It is a very effective method in reducing the accuracy of the attacker's machine learning. Adding the least amount of padding while determining the amount of padding is extremely important for the utility of traffic. Therefore, the amount of pad should be the minimum required. Strategies aiming to maintain the privacy-utility trade-off against different scenarios and data types have been discussed in the literature (Ergün and Can, 2022b). But, despite these various strategies aiming to maintain the privacy-utility trade-off against different scenarios and data types, there is no single optimal padding strategy in the literature that can be applied for every scenario and data type. The visualized version of the model in which the size of the original packet is increased in the padding method is shown in Figure 2. Packet size may vary depending on the determined padding strategy.

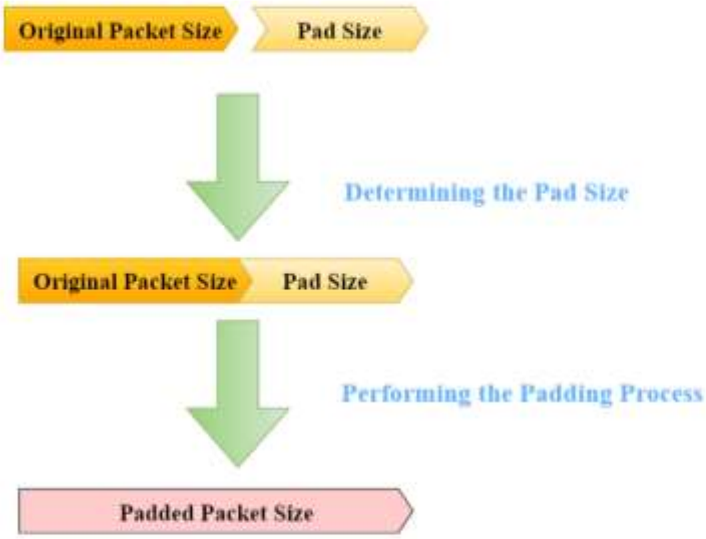


Figure 2. Padding model.

2.3. Attacks against Machine Learning

As the opposite of the scenario in Section 2.1, the roles of attacker and victim are reversed. In this situation, the attacker represents the person owning IoT devices, while the victim is the one aiming to deceive the attacker's machine learning-based classification system. The victim uses techniques to mislead the attacker's model, causing misclassification or a drop in performance. In Adversarial Examples, also known as Evasion Attack, the attacker can mislead the victim’s machine learning model with incorrect training data (Kwon et al., 2018). The correct prediction percentage of the machine learning model, which uses adversarial examples in the training data, is reduced. In order to carry out this attack, the attacker trains his own Generative Adversarial Network with the victim’s model. It then corrupts the inputs at the time of the test, allowing the victim model to make the wrong decision (Biggio et al., 2013).

Poisoning Attack increases the errors in the testing phase of the machine learning model with the training data produced by the attacker (Biggio et al., 2012). Tolpegin et al. (2020) are used data poisoning attack against federated learning systems. They also proposed defense system against this attack. In the work of Yerlikaya and Bahtiyar (2022), various machine learning algorithm’s robustness and performance against adversarial examples are analyzed. In their work, for almost all datasets, some machine learning algorithms exhibit superior robustness and performance results against adversarial attacks.

3. Results

In this section, the findings obtained by using commonly used machine learning algorithms and the dataset of Sivanathan et al. (2018) are evaluated. In the work of (Alex et al., 2023), it is shown that Sivanathan et al. (2018) dataset large in terms of size, with tens of millions of records, while the others remained in the hundreds of thousands. It was observed in which algorithm the attacker achieved higher results. Experiments were carried out on the data set that Sivanathan et al. (2018) created in his study. From this data set, 3 different experiments were carried out using 2, 4 and 6 IoT devices. 80% of the data was used as training data and 20% as test data. Sivanathan et al. (2018) dataset consists of 10 attributes, one of which is the target attribute. Since encrypted IoT traffic contains only time and packet size features to predict target attribute, our results are lower than those in Sivanathan et al. (2018) work. The test results are shown in Table 1. In the first experiment in which 6 devices were used, 84% accuracy rate was obtained with the Random Forest algorithm, which is widely used in classification, 84% with the Decision Tree algorithm, and 71% with the k-NN algorithm. In the second experiment, 4 devices were used and it was observed that the accuracy rates increased for all 3 algorithms. In the experiment with 4 devices, 88% accuracy rate was obtained with the Random Forest algorithm, 88% with the Decision Tree algorithm, and 85% with the k-NN algorithm. In the third experiment, 2 devices were used. In Random Forest and Decision Tree algorithms, 98% accuracy rate, and 95% accuracy rate in k-NN algorithm has been achieved. The devices used in the experiments are ’Amazon Echo’, ’Belkin wemo switch’, ’Insteon camera’, ’Netatmo welcome’, ’Smart things’, ’Withings smart baby monitor’.

In Figure 3, the device types and packet numbers in the experiment in which 2 devices were used are shown. The device types and packet numbers in the experiment in which 4 devices were used are shown in Figure 4. In Figure 5, the types and numbers of devices in the experiment in which 6 devices were used are shown. In three different scenarios, IoT devices with the data numbers closest to each other in Sivanathan et al. (2018) dataset were selected. Having data numbers close to each other during the classification process allows more reliable inferences to be made about the performance and accuracy of machine learning algorithms.

The confusion matrices of Random Forest, Decision Tree and k-NN algorithms in experiments using 2, 4 and 6 device types are shown in Figure 6, 7, 8. These matrices showcase the accuracy of each algorithm by showing the numbers of true and predicted labels for each type of device. The results show that the number of accurate predictions declines with increasing device kinds. In particular, confusion increases with four and six device types, indicating that these circumstances involve more complexity and uncertainty in prediction, but confusion decreases and classification accuracy increases with only two devices.

As seen in Table 1, the accuracy rates of the Random Forest and Decision Tree algorithms are higher than the k-NN algorithm in experiments where 2, 4 and 6 devices are used. As the number of devices increases, accuracy decreases as the diversity in classification increases.

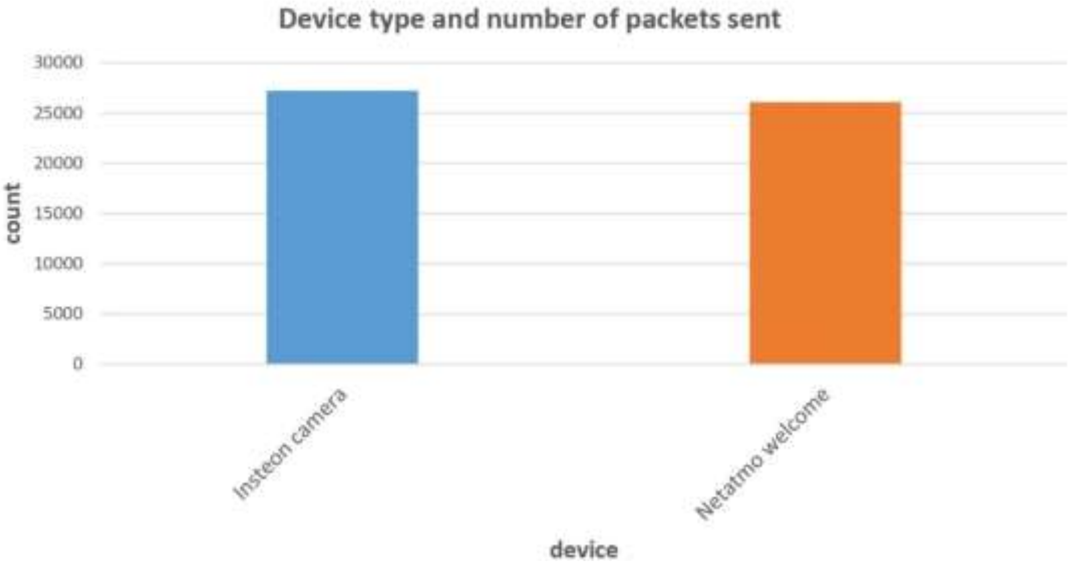


Figure 3. 2 device types and number of packets sent.

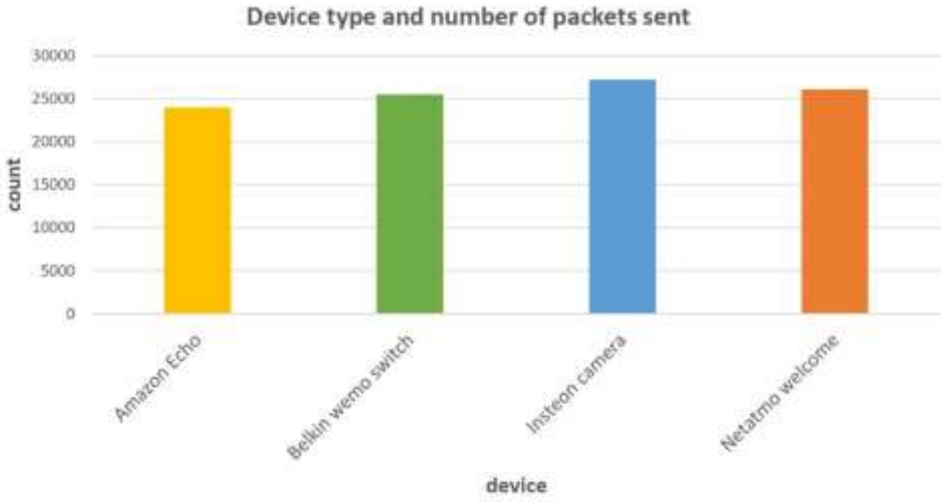


Figure 4. 4 device types and number of packets sent

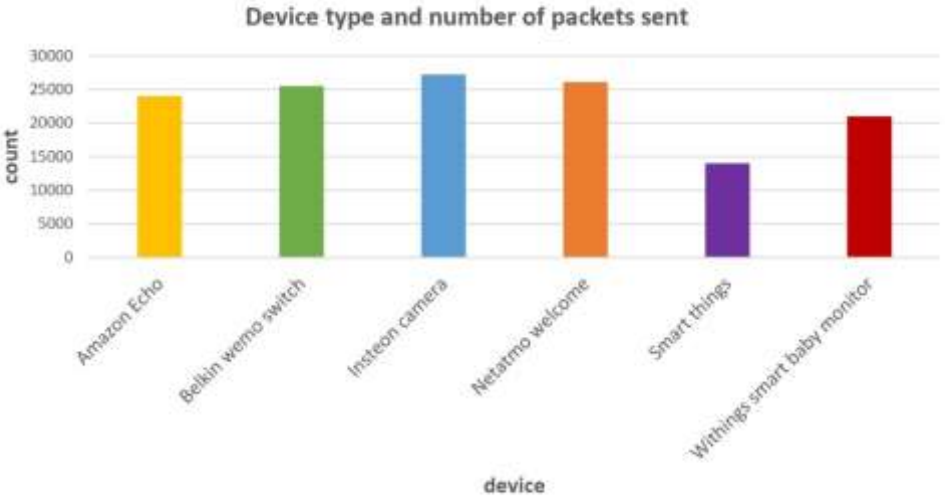
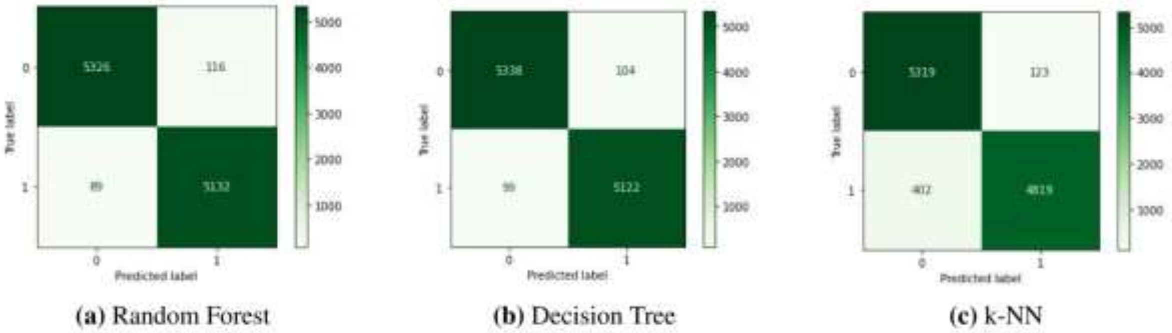
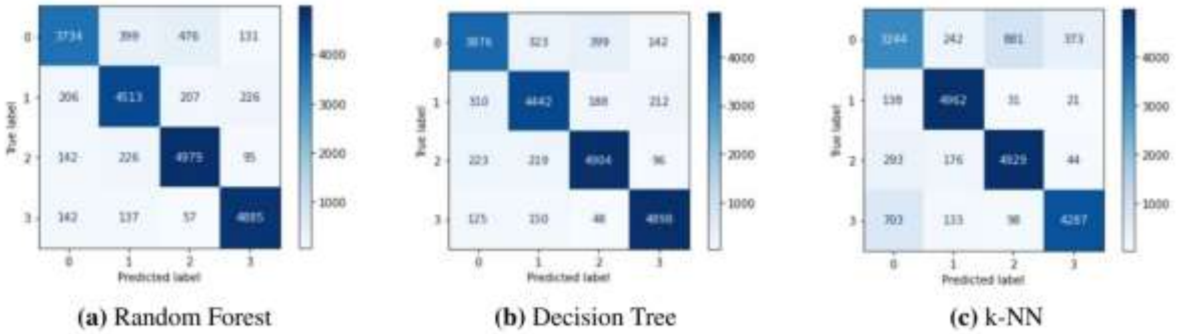


Figure 5. 6 device types and number of packets sent



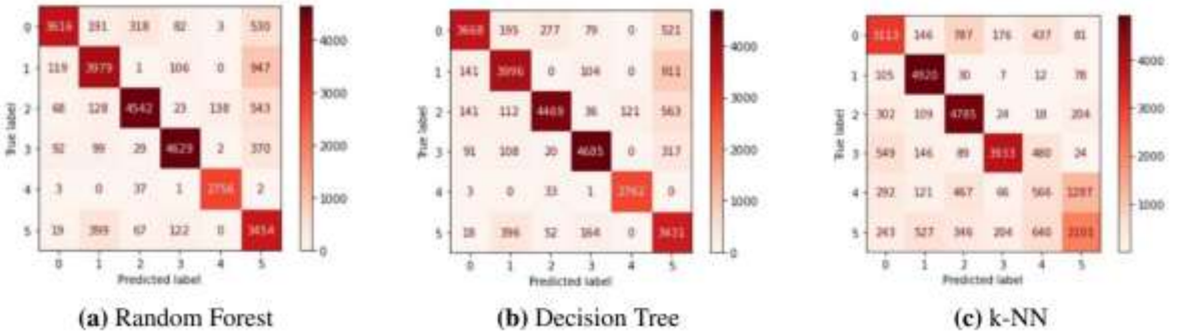
(a) Random Forest (b) Decision Tree (c) k-NN

Figure 6. Confusion Matrix for 2 device types



(a) Random Forest (b) Decision Tree (c) k-NN

Figure 7. Confusion Matrix for 4 device types



(a) Random Forest (b) Decision Tree (c) k-NN

Figure 8. Confusion Matrix for 6 device types

Table 1. Number of device types and accuracy rate of the algorithms

Number of device types	Random Forest	Decision Tree	k-NN
2 devices	98%	98%	95%
4 devices	88%	88%	85%
6 devices	84%	84%	71%

According to the findings obtained from the experiments, it has been observed that the Random Forest and Decision Tree algorithms are more effective than the k-NN algorithm. For all three machine learning algorithms, it has been observed that the accuracy rates increase as the number of device types decreases. In the experiment in which two device types were used, the highest accuracy rate was obtained as 98% with Random Forest and Decision Tree algorithms.

4. Discussion

The use of technological devices in all areas of our lives is increasing and provides convenience to human life. However, these devices bring some risks when communicating with each other. For this reason, it is essential to take security measures while adapting these devices to our lives. It is possible to obtain extremely confidential information from the communication traffic created by the devices. Even if the traffic is encrypted, inferences for the traffic and devices can be made from this data flow. An attacker who observes the traffic can classify these devices using attributes such as time and packet size using machine learning methods. The accuracy of this classification may vary depending on the selected machine learning method and data set. Likewise, this accuracy rate may vary depending on the number of devices in the data set. For attackers, high accuracy rate means self-confidence to classify a device and learn device type of victim uses. That may cause privacy issues for the victim side. As machine learning can be used in attacks, attacks on machine learning models are also discussed in this study. In this study, machine learning algorithms that are widely used to classify devices are explained and experiments are carried out. Padding method, which is widely used to reduce the attacker's accuracy rate and to provide security, is explained. In addition, attacks on machine learning models are mentioned. In the experiment in which six type of devices were used, it was observed that the Random Forest and Decision Tree algorithms, which achieved 84% accuracy, were more effective than the k-NN algorithm, which achieved 71% accuracy. In the experiment where the number of device types was four, it was observed that the Random Forest and Decision Tree algorithms, which achieved 88% accuracy, were more effective than the k-NN algorithm, which achieved 85% accuracy. The highest accuracy was found in experiments using two device types. An accuracy rate of 98% was obtained in the Random Forest and Decision Tree algorithms, and 95% in the k-NN algorithm. Especially for the k-NN algorithm, it was observed that the accuracy rate increased as the device type decreased. In future studies, it is aimed to develop an effective and optimal defense method for all kinds of machine learning methods used in attacks and to develop a secure framework against attacks on machine learning models.

Author Contributions

The percentage of the author(s) contributions is presented below. All authors reviewed and approved the final version of the manuscript.

	A.E.	Ö.C.
C	50	50
D	50	50
S	50	50
DCP	50	50
DAI	50	50
L	50	50
W	50	50
CR	50	50
SR	50	50
PM	50	50
FA	50	50

C=Concept, D= design, S= supervision, DCP= data collection and/or processing, DAI= data analysis and/or interpretation, L= literature search, W= writing, CR= critical review, SR= submission and revision.

Conflict of Interest

The authors declared that there is no conflict of interest.

Ethical Consideration

Ethics committee approval was not required for this study because of there was no study on animals or humans.

Acknowledgments

This study is supported by Ege University Scientific Research Projects Committee under the grant number FM-HZP-2023-29550.

References

Abdulkareem NM, Abdulazeez AM. 2021. Machine learning classification based on Random Forest Algorithm: A review. IJSB, 5(2): 128-142.

Aksoy A, Gunes MH. 2019. Automated IoT device identification using network traffic. In: ICC 2019 - IEEE International Conference on Communications, 20-24 May, Shanghai, China, pp: 1-7.

Alex C, Creado G, Almobaideen W, Alghanam OA, Saadeh M. 2023. A Comprehensive survey for IoT security datasets taxonomy classification and machine learning mechanisms. COSE, 134: 103283.

Alghuried A. 2017. A model for anomalies detection in internet of things (IoT): using inverse weight clustering and decision tree. MSc thesis, Dublin Institute of Technology, Dublin, Ireland, pp: 142.

Biggio B, Nelson B, Laskov P. 2012. poisoning attacks against support vector machines. arXiv, 1206.6389.

Biggio B, Corona I, Maiorca D, Nelson B, Šrndić N, Laskov P, Roli F. 2013. Evasion attacks against machine learning at test time. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases, 23-27 September 2013, Prague, Czech Republic, pp: 387-402.

Charbuty B, Abdulazeez A. 2021. Classification based on decision tree algorithm for machine learning. JASTT, 2(01): 20-28.

Dogru N, Subasi A. 2018. Traffic accident detection using random forest classifier. In: 15th Learning and Technology Conference (L&T), 25-27 February 2018, Jeddah, Saudi Arabia, pp: 40-45.

Ergün A, Can Ö. 2022a. Ensuring IoT Privacy using padding strategies against machine learning approaches. IJMSIT, 6(2): 193-197.

Ergün A, Can Ö. 2022b. Machine learning attacks against internet of things devices. IJMSIT, 6(1): 23-28.

Gawri B, Kasturi A, Neti LBM, Hota C. 2022. An efficient approach to kNN algorithm for IoT Devices. In: 2022 14th International Conference on Communication Systems & Networks (COMSNETS), 3-8 January 2022, Bengaluru, India, pp: 734-738.

Kröger J. 2018. Unexpected inferences from sensor data: a hidden privacy threat in the internet of things. In: IFIP International Internet of Things Conference, 5-8 November 2018, Valencia, Spain, pp: 147-159.

Kwon H, Kim Y, Park KW, Yoon H, Choi D. 2018. Multi-targeted adversarial example in evasion attack on deep neural network. IEEE Access, 6: 46084-46096.

Pinheiro AJ, de Araujo-Filho PF, Bezerra JDM, Campelo DR. 2020. Adaptive packet padding approach for smart home networks: a tradeoff between privacy and performance. IEEE IoT-J, 8(5): 3930-3938.

Sivanathan A, Gharakheili HH, Loi F, Radford A, Wijenayake C, Vishwanath A, Sivaraman V. 2018. Classifying IoT devices in smart environments using network traffic characteristics. IEEE TMC, 18(8): 1745-1759.

Tolpegin V, Truex S, Gursoy ME, Liu L. 2020. Data poisoning attacks against federated learning systems. In: European Symposium on Research in Computer Security, 14-18 September 2020, Guildford, United Kingdom, pp: 480-501.

Wang H, Xu P, Zhao J. 2021. Improved KNN algorithm based on preprocessing of center in smart cities. Complexity, 2021: 1-9.

Yerlikaya FA, Bahtiyar Ş. 2022. Data poisoning attacks against machine learning algorithms. Expert Syst Appl, 208: 118101.