Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Securing IoT Devices with Zero-Trust Architecture and Machine Learning Techniques: Analysing Defence and Attack Strategies

M. Bheemalingaiah[1], Basavaraj Chunchure[2], L. Venkateswa Reddy[3], G. Sreenivasulu[1], P. Srinivasa Rao[1], M. Pranathi[1]

[1]Département of CSE, J.B. Institute of Engineering and Technology, Hyderabad, India
[2]Department of CSE-DS, CVR College of Engineering, Hyderabad, India
[3]Department of CSE, Joginapally B.R. Engineering College, Hyderabad, India
Email: bheemasiva2024@gmail.com

With the proliferation of Internet of Things (IoT) devices, the frequency and sophistication of attacks targeting these devices have escalated. This study explores methods to secure IoT devices, emphasizing the significance of zero-trust architecture in enhancing IoT security. It also assesses the efficacy of various defence strategies against machine learning-based attacks. Specifically, this research investigates the impact of machine learning techniques in classifying IoT devices within encrypted traffic and examines the effectiveness of Random Forest and Decision Tree algorithms. Experimental analysis of IoT device traffic revealed an 85% accuracy rate for device classification using unaltered data, which dropped to 18% when employing a random fill method designed to obscure accurate information from attackers. The study's novelty lies in its detailed examination of the efficacy of these classification algorithms and the impact of data obfuscation methods on classification accuracy. This research is particularly relevant given the rapid expansion of IoT deployments and the increasing sophistication of cyberattacks. By highlighting the importance of zero-trust architecture and advanced machine learning techniques, the study provides timely and actionable insights to enhance the protection of IoT systems in the current technological landscape.

Keywords: IoT security, Zero-Trust Architecture, Machine Learning, Random Forest, Decision Tree, Encrypted Traffic.

1. Introduction

The Internet of Things (IoT) describes a network of physical objects embedded with sensors, software, and other technologies designed to exchange data by connecting to other devices and systems via the Internet. With the increasing popularity and demand for IoT devices, it is estimated that the total number of connected IoT devices will reach approximately 80 billion by 2030 [1]. This rapid expansion is driven by technological advancements and the growing necessity for IoT devices in various sectors. However, this proliferation also introduces significant security challenges, as these devices become attractive targets for cyberattacks that threaten the confidentiality, integrity, and availability of data.

The importance of implementing robust security measures to safeguard IoT devices cannot be overstated. Effective security measures are crucial to prevent attacks that target these critical aspects of data. Machine learning (ML) techniques have emerged as powerful tools in enhancing IoT security, offering sophisticated methods to detect and mitigate threats. Notably, ML methods are employed not only to strengthen security defences but also by attackers to devise more complex and effective attacks.

Recent developments in the field have highlighted the multifaceted nature of IoT security challenges and the potential of innovative solutions. Hennebelle et al. (2023) [2] proposed an end-to-end integrated system that combines IoT devices, edge computing, and blockchain technology for secure and privacy-preserving automated machine learning operations in diabetes mellitus prediction. This approach demonstrates the potential of combining multiple technologies to address security and privacy concerns in healthcare IoT applications.

The integration of federated learning models in spatial-temporal mobility applications has been explored by Belal et al. (2024) [3]. Their survey of existing federated learning models provides insights into the challenges and opportunities in deploying these models in dynamic environments, such as mobility prediction and traffic management systems.

In the context of IoT security threats, Gelgi et al. (2023) [4] conducted a systematic literature review of detection techniques for IoT botnet DDoS attacks. Their work categorizes various approaches and proposes a framework for future research, highlighting the ongoing need for effective detection and mitigation strategies in IoT environments.

The expanding scope of IoT applications is evident in the emergence of new paradigms such as the metaverse. Huynh-The et al. (2023) [5] reviewed the current state of blockchain applications in the metaverse, addressing questions of scalability, security, and interoperability among various platforms and applications within this virtual environment.

In the healthcare sector, Rejeb et al. (2023) [6] reviewed the current landscape of IoT applications, assessing various use cases such as remote monitoring systems and smart medical devices. Their work identifies key challenges that hinder adoption and proposes strategies for overcoming these barriers through enhanced interoperability and data security measures.

The Internet of Vehicles (IoV) represents another frontier in IoT applications, with its own set of security challenges. Mollah et al. (2021) [7] surveyed various blockchain solutions tailored for IoV applications, proposing a framework that integrates blockchain with existing transportation systems to enhance data integrity and trust among vehicles.

Network slicing in IoT within the context of 5G networks presents significant challenges related to resource allocation and quality of service guarantees. Wijethilaka et al. (2021) [8] examined existing network slicing techniques applicable to IoT environments, proposing best practices to optimize resource utilization across diverse IoT applications.

This study evaluates measures to ensure the security of IoT devices and examines the various attacks that exploit IoT vulnerabilities. It highlights the dual role of machine learning in both securing and attacking IoT systems. Specifically, the study aims to determine which machine learning techniques are most effective for different security measures and which are most potent in specific types of attacks.

The research begins by outlining commonly used security measures against IoT attacks. It then delves into security measures based on machine learning, followed by a discussion on machine learning-driven attacks targeting IoT devices and the types of violations they aim to exploit. Finally, the study assesses the effectiveness of machine learning algorithms, such as Random Forest and Decision Tree, in both defensive and offensive contexts.

The organization of this study is as follows: the second part explains zero-trust architecture, padding and shaping methods, machine learning methods used to ensure security, and machine learning-based IoT attacks. The third part evaluates the accuracy performances of Random Forest and Decision Tree classifier algorithms with filled and unfilled data. The fourth part presents the discussion and conclusions.

By synthesizing insights from recent research and addressing the multifaceted challenges of IoT security, this study aims to contribute to the ongoing efforts to enhance the resilience and reliability of IoT systems across various domains.

2. LITERATURE REVIEW

2.1 COMMON SECURITY MEASURES

To enhance the security of IoT devices, various strategies can be employed, including zero-trust architecture and fill and shape methods. These measures aim to increase the resilience of IoT systems against attacks, particularly those leveraging machine learning models.

Zero-Trust Architecture, Ensuring IoT security requires integrated solutions that provide visibility, segmentation, and comprehensive protection across the network infrastructure. The zero-trust model, based on the principle of "verify at all times and never trust," ensures that no data from internal or external networks is trusted by default. This model has gained importance with the rise of remote access to networks, making it crucial for protecting IoT devices [9].

In a zero-trust architecture, Role-Based Access Control (RBAC) uses the zero-trust access policy to grant users the minimum level of network access necessary for their tasks. This approach aligns with the principle of least privilege, preventing users from accessing or seeing other parts of the network they do not need. Additionally, zero-trust architecture enables the authentication of interconnected smart devices, maintaining comprehensive management control and visibility of all network components. This continuous verification process is essential for mitigating risks and ensuring the integrity and security of IoT ecosystems [10].

Padding, even when IoT traffic is encrypted, passive traffic monitors can still spy on the network and compromise privacy using machine learning techniques. To counter this, padding can be employed to adjust bandwidth in a way that misleads attackers attempting to classify IoT device traffic. The goal is to strike a balance between maintaining network performance and protecting privacy. By adding extra dimensions to packet sizes, padding disrupts the patterns that attackers rely on for traffic analysis.

For instance, a study using the Random Forest (RF) machine learning technique showed that the accuracy rate of identifying an IoT device by analysing the average and total sizes of encrypted traffic was 96% before padding, which decreased to 4.96% after applying a level-900 fill. This significant reduction demonstrates how padding can effectively mislead an attacker's machine learning model by altering packet sizes and adding noise to the traffic [11][12].

Shaping, traffic shaping is another effective method to protect IoT traffic from analytics attacks. By adding fake packets to traffic, shaping helps obscure user activity from attackers. A study proposed a traffic shaping method based on the Stochastic Traffic Padding (STP) algorithm, which fills traffic periods with regular intervals of fake packets, even when there is no actual user activity. This approach prevents attackers from detecting real traffic patterns.

The STP method allows for an adjustable balance between traffic bandwidth load and attacker confidence. By increasing the bandwidth load, the accuracy rate of an attacker's IoT device detection was reduced from 50% to 10%. This demonstrates the effectiveness of shaping in deceiving attackers and protecting IoT traffic from inference attacks [13].

2.2 SECURITY METHODS BASED ON MACHINE LEARNING

Technological advancements have significantly expanded the role of machine learning (ML) in enhancing the security of IoT devices. These advancements enable IoT devices to better protect themselves from common cyber threats through a variety of learning-based methods. As machine learning techniques become more sophisticated, they offer new avenues for improving IoT security. This section explores several key machine learning-based security methods and their applications in safeguarding IoT environments.

Learning-Based Authentication, Learning-based authentication methods leverage machine learning algorithms to improve the security of IoT devices against attacks such as spoofing and eavesdropping. One notable technique is Q-learning-based authentication, which allows IoT devices to enhance authentication processes by learning from interactions with their environment in the cloud, without needing a pre-existing training dataset. This approach adapts to evolving threats by continuously learning and updating its authentication strategies, making it a robust solution for verifying the identities of devices and users in real time [14][15].

Learning-Based Secure Offloading, secure offloading is a technique used to transfer data from IoT devices to alternative platforms, such as other devices or cloud services, to mitigate threats like Denial of Service (DoS) attacks and jamming. Q-learning-based secure offloading methods dynamically select data transfer options to counteract attacks like scrambling and spoofing. By leveraging machine learning algorithms to make informed decisions about where and how to offload data, these methods can enhance the security and efficiency of data handling processes, ensuring that critical information is protected against various forms of

cyber threats [16][17].

Learning-Based Malware Detection, Machine learning techniques are highly effective in detecting and preventing malware attacks, including viruses and Trojans. Algorithms such as K-nearest neighbours (K-NN) and Random Forest have been evaluated for their ability to detect both known and emerging malware threats. These algorithms analyse patterns in network traffic or system behaviour to identify malicious activities. Studies have demonstrated that these classifiers can achieve high detection rates for the latest malware variants, thereby providing a vital line of defense against malicious software targeting IoT devices [18].

Learning-Based Access Control, Machine learning can also be employed for access control to defend against attacks like DoS, privacy leakage, and malware infections. Techniques such as Support Vector Machines (SVM) and K-NN are used to detect unauthorized access attempts and manage permissions. By analyzing patterns in user behavior and access requests, these methods can identify potential intrusions and enforce access policies to protect sensitive data and system resources [19].

Adversarial Training Gradient, Adversarial training is a defensive strategy designed to make machine learning models more resilient to black-box attacks, where attackers manipulate inputs to deceive the model. This approach involves adding misleading or adversarial examples to the training data to strengthen the model's ability to resist such attacks. However, this method has limitations and may not fully address the complexities of adversarial machine learning scenarios [20].

Blocking the Transferability, it is a technique aimed at preventing attackers from using misleading data to manipulate machine learning models. This strategy involves introducing a "NULL" tag class into the training dataset to reduce the effectiveness of adversarial examples. By doing so, the model becomes less confident in potentially misleading inputs and classifies them as "NULL," thereby thwarting attempts to exploit the model's weaknesses [21].

Defence-Producer Adversarial Network (Defence-GAN), The Defence-Producer Adversarial Network (Defence-GAN) is a sophisticated mechanism designed to protect deep neural networks from adversarial attacks in both black-box and white-box scenarios. This method employs a producer adversarial network to generate and counteract misleading samples, enhancing the model's robustness against attempts to corrupt its training process. By using adversarial networks to improve model defenses, this approach helps ensure the integrity and reliability of machine learning models used in IoT security [16].

In summary, machine learning-based security methods offer a diverse range of tools and techniques for defending IoT devices from various types of cyber threats. These methods not only enhance traditional security measures but also introduce innovative approaches to deal with emerging threats in the IoT landscape. As IoT environments continue to evolve, these machine learning techniques will play a critical role in advancing IoT security and protecting against sophisticated attacks.

2.3 ATTACKS ON IOT WITH MACHINE LEARNING

Machine learning techniques can be employed by attackers to manipulate traffic on IoT devices, capture encrypted traffic information, and exploit it to violate privacy, disrupt systems, or mislead IoT environments. The widespread use of machine learning in IoT attacks

is driven by the goal of breaching confidentiality, integrity, and availability. As shown in the Table 1. Machine learning algorithms used in these attacks can be categorized into three types: supervised learning, unsupervised learning, and reinforcement learning [16].

1. K-Nearest Neighbour (K-NN):

o Type: Supervised Learning

o Function: K-NN is a data classification algorithm that estimates the probability of a data point belonging to a particular group based on the groups of the closest data points.

2. K-Means:

o Type: Unsupervised Learning

o Function: K-Means is a clustering algorithm that aims to minimize the sum of distances between observations and their corresponding cluster centres.

3. Q-Learning:

o Type: Reinforcement Learning

o Function: Q-Learning is an algorithm that seeks to find the best action to take in a given situation by learning from the consequences of actions in different states.

2.4 PRIVACY INVASION

Privacy invasion through machine learning techniques can lead to severe consequences, such as misuse of users' sensitive information. Encrypted packet sizes in IoT traffic can be analysed to infer details about IoT devices and their activities. Despite using padding and shaping methods, attackers can still classify encrypted data and identify devices on a network. For example, a study showed that an attacker could distinguish IoT devices with 81% accuracy using the K-NN algorithm on padded and shaped traffic at one-second intervals [22].

Table 1: Examples of attacks by machine learning categories.

Learning Type	Violations	Attacks
Unsupervised Learning	Integrity Breach	Evasion, Causative Discovery, Exploratory, Spurious Injection, Code
Supervised Learning	Confidentiality and Privacy Breach	Traffic Analysis, Cryptanalysis, Side Channel, Social Networking
Reinforcement Learning	Availability Violation	Spoofing, Jamming, Black Hole

2.5 BREACH OF INTEGRITY AND AVAILABILITY

As IoT devices become more prevalent, new security risks emerge. Attackers can use machine learning to imitate devices, manipulate traffic flow, and disrupt network operations, thus breaching integrity and availability. Machine learning, coupled with social engineering, reconnaissance attacks, Denial of Service (DoS), and Man-in-the-Middle attacks, enables attackers to impersonate users or systems, spoof devices, and capture sensitive information [23,24-27].

A study on adversarial machine learning-based partial-model attacks demonstrated how an attacker could influence decision-making in data fusion by controlling only a small subset of

IoT devices. Adversarial machine learning techniques were applied to jamming, spectrum poisoning, and priority violation attacks [28]. In these scenarios, attackers used exploratory attacks to extract channel access algorithms from

IoT data transmitters using deep neural network classifiers and evasion attacks to mislead transmitters during testing. While IoT relays trained channel access algorithms for relearning, attackers employed causative attacks to manipulate data sent to the relay.

3. RESULTS AND ANALYSIS

This section examines the efficacy of using random padding as a countermeasure against machine learning-based privacy violations in IoT environments. The focus is on an attacker using machine learning methods to breach privacy and a defender employing random padding to thwart these efforts. The effectiveness of the random padding method was evaluated against the Random Forest and Decision Tree algorithms using the dataset described in [12].

The performance of these classifiers, both with and without the random padding method, is presented in Table 3.

The random padding method involves assigning a random value between the original packet length and 1600 bytes to the length of each packet in the test data. This method aims to reduce the accuracy of the attacker's machine learning models by introducing noise into the data.

In this study, the dataset created in [12] was used, and traffic analysis was performed on five devices. The numerical distribution of devices in the training and test files is illustrated in Figures 1 and 2. The confusion matrices for the Random Forest and Decision Tree algorithms, both with and without random padding, are shown in Figures 3 through 6.

Table 2: Accuracy rates based on device numbers.

Number of Devices	Accuracy Rate (%)
5	80
10	76
14	74

3.1 ANALYSIS OF RANDOM FOREST ALGORITHM

The Random Forest classifier achieved an accuracy rate of 82.3% on unfilled data, indicating a high ability to correctly classify the IoT devices (Table 2.). However, when random padding was applied, the accuracy dropped significantly to 22.0%. This dramatic reduction highlights the effectiveness of random padding in misleading the Random Forest classifier, thereby protecting the privacy of IoT devices.

TABLE 3. Accuracy rates according to algorithms.

Algorthm	Random Filled	Unfilled
Random Forest	82.3%	22%
Decision Tree	83.9%	19.7%

3.2 ANALYSIS OF DECISION TREE ALGORITHM

Similarly, the Decision Tree classifier achieved an accuracy rate of 83.9% on unfilled data. With random padding, the accuracy dropped to 19.7%. Although the accuracy decrease is substantial, it is slightly less effective than the Random Forest in terms of reduction percentage. Nevertheless, the random padding method still proves to be a significant obstacle for the Decision Tree classifier.

3.3 COMPARATIVE ANALYSIS

Comparing the two algorithms, it was observed that the Random Forest classifier's accuracy was reduced more significantly than that of the Decision Tree classifier. The accuracy of the Random Forest dropped from 82.3% to 22.0%, while the Decision Tree's accuracy decreased from 83.9% to 19.7%. This indicates that the random padding method is slightly more effective against the Random Forest algorithm. The confusion matrices further illustrate the reduction in classification accuracy, emphasizing the efficacy of random padding as a defensive measure.

The experiments demonstrate that random padding is an effective method to protect IoT devices from privacy breaches caused by machine learning attacks. By significantly reducing the accuracy of the attacker's classifiers, random padding helps in maintaining the confidentiality of IoT traffic. The results indicate that while both the Random Forest and Decision Tree classifiers are adversely affected by random padding, the Random Forest algorithm is slightly more vulnerable. This finding suggests that defenders should consider implementing random padding as a robust method to enhance the security of IoT devices against machine learning-based attacks.

This section discusses the attacker who violates privacy using machine learning methods and the victim who tries to prevent this violation with the filling method. Accordingly, the effectiveness of random fill, which is one of the filling methods, was demonstrated against the Random Forest and Decision Tree algorithms by using the data set in the study [28]. The performance of the Random Forest and Decision Tree classifier algorithms without backfill and the accuracy rates after random padding are given in Table 4. The accuracy rates against the random padding method, in which the length of each packet of the test data is assigned to a random value between its own length and 1600 bytes, and the accuracy rates against the unfilled method in which the train-test data are not filled are shown [29].

In the experiments carried out in this study, the dataset created in the study [12] was used and traffic analysis of five devices was performed from these data sets. The numerical distribution of devices in the training and test files is shown in the graphs in Figure 1 and Figure 2.

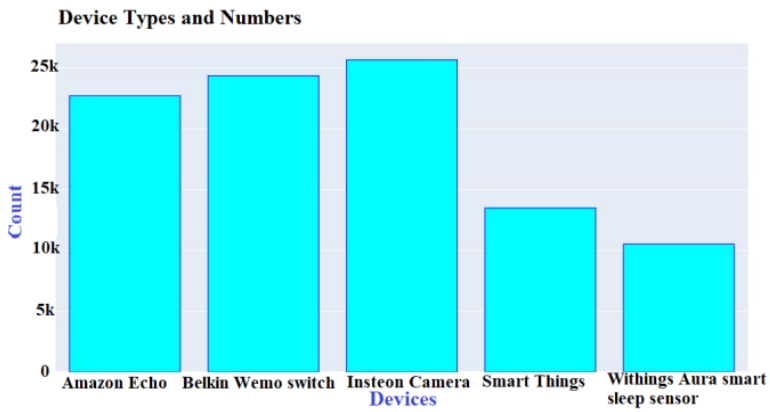

Figure 1. Train Devices and Numbers.

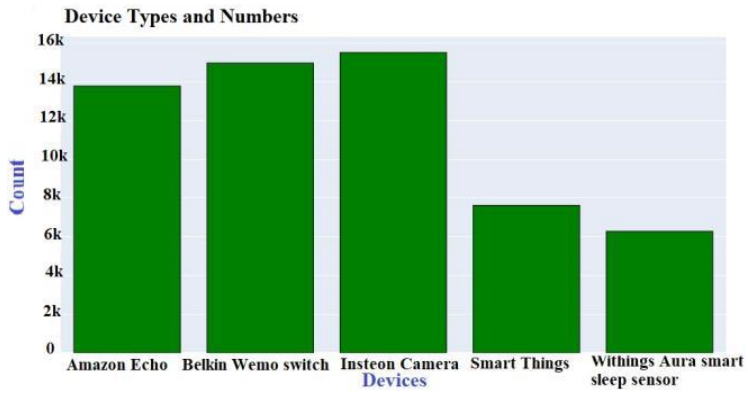

Figure 2. Test Devices and Numbers.

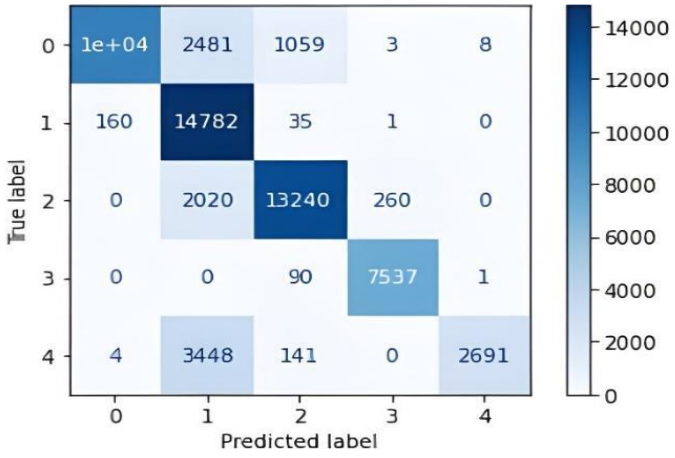

Figure 3: Confusion Matrix for Random Forest (Unfilled)

The confusion matrix in the analysis with the Random Forest algorithm is shown in Figure 3

and Figure 4. The confusion matrices in the analysis with the Decision Tree algorithm are shown in Figure 5 and Figure 6.

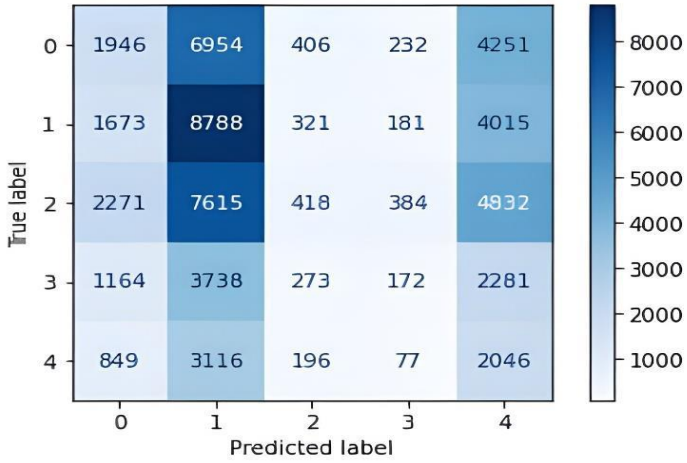

Figure 4: Confusion Matrix for Random Forest (Random Filled).

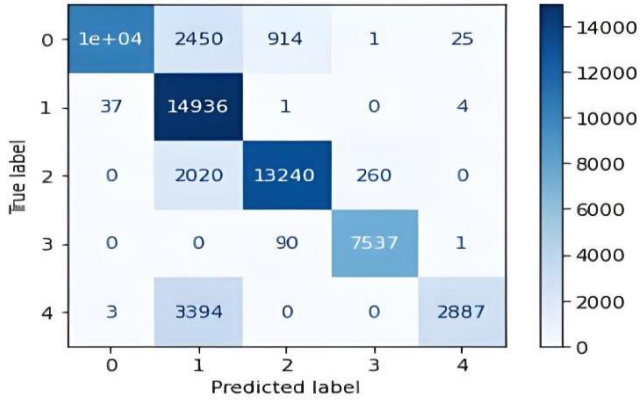

Figure 5: Confusion Matrix for Decision Tree (Unfilled).

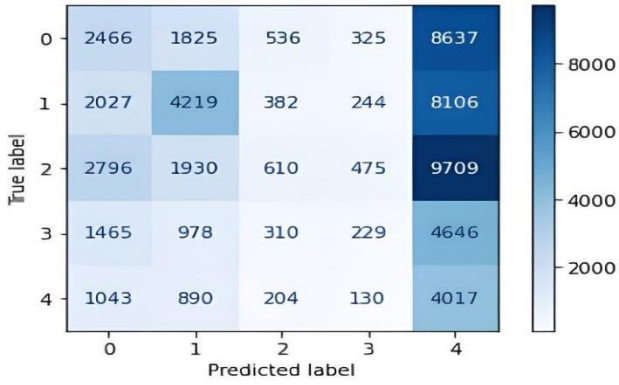

Figure 6: Confusion Matrix for Decision Tree (Random Filled).

It has been observed that the accuracy rate of the attacker decreases for both classifiers with random filling. The Decision Tree classification algorithm has an accuracy rate of 84.2%, while the Random Forest classification algorithm has an accuracy rate of 83.3%. The random fill of the Random Forest algorithm was found to be more effective than the Decision Tree's 19.8% accuracy rate with a 23% accuracy rate.

4. CONCLUSION

This study has explored the growing threat of machine learning-based attacks on IoT devices and the effectiveness of countermeasures, specifically random padding, to mitigate these threats. The rapid proliferation of IoT devices, coupled with their increasing integration into various aspects of daily life and critical infrastructure, underscores the necessity for robust security measures. Key findings from this study include: 1. Effectiveness of Random Padding: The experiments demonstrated that random padding significantly reduces the accuracy of machine learning classifiers used by attackers. The Random Forest classifier's accuracy dropped from 82.3% to 22.0%, and the Decision Tree classifier's accuracy decreased from 83.9% to 19.7% when random padding was applied. This substantial reduction highlights the potential of random padding to effectively obfuscate IoT traffic and protect device privacy. 2. Comparison of Classifiers: While both Random Forest and Decision Tree classifiers experienced significant accuracy reductions due to random padding, the Random Forest classifier showed a slightly higher susceptibility. This indicates that random padding may be more effective against more complex ensemble methods, though it remains a strong defence against decision tree-based classifiers as well. 3. Importance of Continuous Adaptation: The study emphasizes the importance of continuously adapting security measures to stay ahead of evolving threats. As attackers increasingly leverage advanced machine learning techniques, defenders must also employ sophisticated countermeasures such as random padding to maintain the confidentiality, integrity, and availability of IoT systems. 4. Broader Implications for IoT Security: The findings of this study have broader implications for the development of security strategies in IoT environments. Implementing techniques like random padding can be part of a comprehensive security approach, including zero-trust architecture and other machine learning-based security methods, to create multi-layered defences against sophisticated attacks.

References

1. R. O. Ogundokun, J. B. Awotunde, E. A. Adeniyi, and S. Misra, "Application of the internet of things (IoT) to fight the COVID-19 Pandemic," in Intelligent Internet of Things for Healthcare and Industry, Springer, Cham, pp. 83–103, 2022.
2. A. Hennebelle, L. Ismail, et al., "Secure and privacy-preserving automated machine learning operations into end-to-end integrated IoT-edge-artificial intelligence-blockchain monitoring system for diabetes mellitus prediction," Computational and Structural Biotechnology Journal, vol. 23, pp. 123-135, 2023. DOI: 10.1016/j.csbj.2023.11.038.
3. Y. Belal, S. Ben, M. H. Haddadi et al., "Survey of Federated Learning Models for Spatial-Temporal Mobility Applications," ACM Transactions on Spatial Algorithms and Systems, vol. 10, no. 1, pp. 1-25, 2024. DOI: 10.1145/3666089.
4. M. Gelgi, Y. Guan, et al., "Systematic Literature Review of IoT Botnet DDoS Attacks and

Evaluation of Detection Techniques," Sensors, vol. 24, no. 11, pp. 3571-3590, 2023. DOI: 10.3390/s24113571.
5. T. Huynh-The, T.R. Gadekallu et al., "Blockchain for the metaverse: A Review," Future Generation Computer Systems, vol. 139, pp. 1-16, 2023. DOI: 10.1016/j.future.2023.02.008.
6. A.Rejeb, K.Rejeb et al., "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," Internet of Things, vol. 20, pp. 100721-100732, 2023 DOI: 10.1016/j.iot.2023.100721.
7. M.Baqer Mollah, J.Zhao,D.Niyato et al., "Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey," IEEE Internet of Things Journal, vol .8 , no .11 , pp .8895-8910 , Nov .2021 DOI: 10 .1109/jiot .2020 .3028368.
8. S.Wijethilaka,M.Liyanage et al., "Survey on Network Slicing for Internet of Things Realization in 5G Networks," Communications Surveys & Tutorials, vol .23 , no .2 , pp .1100-1132 , Second quarter 2021 DOI: 10 .1109/comst .2021 .3067807.
9. N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, and Z. Baig, "Zero Trust Architecture (ZTA): A Comprehensive Survey," IEEE Access, vol. 10, pp. 3174679, 2022.
10. H. Babbar, S. Rani, D. K. Sah, S. A. AlQahtani, and A. K. Bashir, "Detection of Android Malware in the Internet of Things through the K-Nearest Neighbor Algorithm", Sensors, vol. 23, no. 16, p. 7256, 2023.
11. P. Dhiman, V. Kukreja, P. Manoharan, A. Kaur, M. M. Kamruzzaman, I. Dhaou, and C. Iwendi, "A novel deep learning model for detection of severity level of the disease in citrus fruits," Electronics, vol. 11, p. 495, 2022.
12. A. Sivanathan, H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Classifying IoT devices in smart environments using network traffic characteristics," IEEE Transactions on Mobile Computing, vol. 18, no. 8, pp. 1745-1759, 2018.
13. G. Bovenzi, F. Cerasuolo, A. Montieri, A. Nascita, V. Persico, and A. Pescapé, "A Comparison of Machine and Deep Learning Models for Detection and Classification of Android Malware Traffic," in Proceedings of the 2022 IEEE Symposium on Computers and Communications (ISCC), Rhodes, Greece, pp. 1–6, 2022.
14. X. Zhang, Y. Jiang, S. Li, et al., "A Survey on Security and Privacy Issues in Internet of Things," Journal of Network and Computer Applications, vol. 62, pp. 113-126, 2016.
15. G. Zhang, J. Li, X. Han, et al., "Machine Learning for Security in the Internet of Things: A Survey," Computers & Security, vol. 88, p. 101634, 2020.
16. E. Bout, V. Loscri, and A. Gallais, "How Machine Learning changes the nature of cyberattacks on IoT networks: A survey," IEEE Communications Surveys & Tutorials, 2021.
17. D. Yang and M. Xu, "Q-Learning Based Authentication Mechanism for IoT Networks," International Journal of Information Management, vol. 50, pp. 111-119, 2020.
18. L. Xiao, C. Xie, T. Chen, H. Dai, and H. V. Poor, "A mobile offloading game against smart attacks," IEEE Access, vol. 4, pp. 2281-2291, 2016.
19. M. Wu and X. Liu, "Secure Offloading Strategies for IoT Devices Based on Q-Learning", IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 345-358, 2020.
20. J. Zhang and Q. Li, "A Comprehensive Study on Malware Detection Algorithms for IoT Devices", IEEE Access, vol. 8, pp. 13720-13730, 2020.
21. Y. Xu and X. Wang, "Machine Learning Techniques for Access Control and Intrusion Detection in IoT," Computer Networks, vol. 162, pp. 132-143, 2019.
22. A. Engelberg and A. Wool, "Classification of Encrypted IoT Traffic Despite Padding and Shaping," arXiv preprint arXiv:2110.11188, 2021.
23. R. Roman, J. Lopez, M. Mambo, "Mobile Edge Computing: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, vol. 78, pp. 680-698, 2018.
24. S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146-164, 2015.
25. Y. Meidan, M. Bohadana, A. Shabtai, et al., "ProfilIoT: A Machine Learning Approach for IoT

Device Identification Based on Network Traffic Analysis," Proceedings of the Symposium on Applied Computing, 2017.
26. G. Baldini and L. Steri, "Adversarial Machine Learning in the Internet of Things: A Systematic Survey," Sensors, vol. 20, no. 19, p. 5791, 2020.
27. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities", Future Generation Computer Systems, vol. 78, pp. 544-546, 2018.
28. P. Kumar and H. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," Sensors, vol. 12, no. 1, pp. 55-91, 2012.
29. Z. Luo, S. Zhao, Z. Lu, Y. E. Sagduyu, and J. Xu, "Adversarial machine learning based partial-model attack in IoT," in Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, pp. 13-18, 2020.