



Heriot-Watt University  
Research Gateway

# Digital Twin-Empowered Smart Attack Detection System for 6G Edge of Things Networks

## Citation for published version:

Yigit, Y, Chrysoulas, C, Yurdakul, G, Maglaras, LA & Canberk, B 2023 'Digital Twin-Empowered Smart Attack Detection System for 6G Edge of Things Networks' arXiv. <https://doi.org/10.48550/arXiv.2310.03554>

## Digital Object Identifier (DOI):

[10.48550/arXiv.2310.03554](https://doi.org/10.48550/arXiv.2310.03554)

## Link:

[Link to publication record in Heriot-Watt Research Portal](#)

## Document Version:

Other version

## General rights

Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

## Take down policy

Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact [open.access@hw.ac.uk](mailto:open.access@hw.ac.uk) providing details, and we will remove access to the work immediately and investigate your claim.

# Digital Twin-Empowered Smart Attack Detection System for 6G Edge of Things Networks

Yagmur Yigit <sup>\*†</sup>, Christos Chrysoulas <sup>\*</sup>, Gokhan Yurdakul <sup>‡</sup>, Leandros Maglaras <sup>\*</sup>, and Berk Canberk <sup>\*</sup>

<sup>\*</sup> School of Computing, Engineering and The Build Environment, Edinburgh Napier University, United Kingdom

<sup>†</sup> Department of Computer Engineering, Istanbul Technical University, Turkey

<sup>‡</sup> BTS Group, Turkey

Email: {Y.Yigit, C.Chrysoulas, L.Maglaras, B.Canberk}@napier.ac.uk,

yigity20@itu.edu.tr, yurdakulg@btsgrup.com

**Abstract**—As global Internet of Things (IoT) devices connectivity surges, a significant portion gravitates towards the Edge of Things (EoT) network. This shift prompts businesses to deploy infrastructure closer to end-users, enhancing accessibility. However, the growing EoT network expands the attack surface, necessitating robust and proactive security measures. Traditional solutions fall short against dynamic EoT threats, highlighting the need for proactive and intelligent systems. We introduce a digital twin-empowered smart attack detection system for 6G EoT networks. Leveraging digital twin and edge computing, it monitors and simulates physical assets in real time, enhancing security. An online learning module in the proposed system optimizes the network performance. Our system excels in proactive threat detection, ensuring 6G EoT network security. The performance evaluations demonstrate its effectiveness, robustness, and adaptability using real datasets.

**Index Terms**—Internet of Things (IoT), Edge of Things (EoT), 6G, Digital Twins (DT), Cybersecurity.

## I. INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) is reshaping the global technological landscape. By 2030, the number of IoT devices is predicted to nearly double, reaching over 29.4 billion [1]. A significant portion of these devices will be interconnected at the edge, forming what is known as the Edge of Things (EoT) network. In this new era, businesses are transitioning to edge deployments, moving closer to end-users and away from traditional data centres. The EoT network encompasses a distributed computing paradigm, where data processing, storage, and analysis occur closer to the data sources, reducing latency and enhancing real-time responsiveness. This meteoric rise is mirrored by the rapid proliferation of devices connected to the edge, significantly increasing the edge network's workload. As more devices and systems connect to the EoT network, the attack surface for hackers expands, providing them with increased opportunities to exploit vulnerabilities and gain unauthorized access to critical systems.

Edge computing is a rapidly growing market, projected to reach USD 3,605.58 billion by 2032 [2]. The global cost of cybercrime is expected to rise by 69.94 per cent by 2028, reaching an alarming figure of USD 13.82 trillion [3]. These figures underscore the importance of edge-based detection. Cyber threats to EoT networks can lead to data breaches,

service disruptions, and even physical harm. Traditional security solutions may be insufficient, emphasizing the need for intelligent and adaptive systems capable of proactive threat detection.

Digital Twin (DT) technology is promising for bolstering security in 6G EoT networks. It enables real-time monitoring and simulation of physical assets, predicting potential security issues or vulnerabilities [4]. Deploying DT processing at the edge allows timely insights into security threats and informed decision-making to bolster network security and ensure optimized performance [5]. Additionally, 6G applications demand more edge servers and introduce new attack vectors targeting local infrastructure and users [6]. This highlights the need for comprehensive defence strategies in 6G edge networks. Employing multiple detection models can provide a comprehensive solution to address the dynamic nature of network traffic [7]. To address these challenges, we present a digital twin-empowered smart attack detection system for 6G edge-of-things networks. Leveraging the capabilities of DT and edge computing, our system aims to establish a robust and resilient defence mechanism against cyber threats from IoT devices and edge connection expansion. In our evaluation, we choose the Long Short-Term Memory Autoencoder (LSTM-AE) model for comparison due to its capacity to capture temporal dynamics. We fine-tuned LSTM-AE hyperparameters through rigorous testing to ensure a robust evaluation of the proposed solution.

The key contributions of this article are as follows:

- We propose a sophisticated smart attack detection system that integrates DT technology into the edge network, enhancing security and enabling proactive threat detection and response for 6G EoT networks.
- Our system utilizes a dynamic and adaptive approach to update feature selection (FS) and classification methods consistently. This approach ensures optimal performance in identifying and mitigating various 6G EoT network attack types.

The paper proceeds with a literature review in Section II, followed by the proposed solution Section III and performance evaluation Section IV. We conclude this paper in Section V.

## II. RELATED WORK

The prominence of IoT and edge technologies has brought about a heightened emphasis on cybersecurity [8]. In this section, we review some relevant works that address similar challenges. Mao *et al.* gave a thorough survey of security threats and countermeasures concerning edge computing, caching, and intelligence regarding 6G network edge [6]. Yao *et al.* explored existing research on intrusion detection systems and proposed innovative detection methods and hybrid system architecture for edge-based industrial-IoT (IIoT) [9]. An anomaly detection framework based on software-defined networking (SDN) is proposed to address the challenge of DDoS attacks on edge devices in distributed and complex environments, utilizing flow information extracted by the edge controller and the GA-XGBoost algorithm for flow classification [10]. Singh *et al.* suggested an edge-based hybrid intrusion detection framework (EHIDF) using machine learning (ML) approaches to detect both known and unknown attacks in the mobile edge computing (MEC) environment [11]. Their EHIDF outperformed previous works with improved accuracy and reduced false alarm rate.

Lee *et al.* presented a lightweight machine learning-based intrusion detection system called IMPACT, designed specifically for resource-constrained IoT devices, utilizing deep auto-encoder and feature abstraction with linear support vector machine (SVM) [12]. Another work introduces a novel privacy-preserving and collusion-resilient identification system called FLACI for EoT, utilizing federated learning to share models instead of raw data among edge nodes [13]. It uses a community detection technique to find collusive groups of attackers and a rating-based mechanism to evaluate the trustworthiness of nodes. Zhang *et al.* addressed the challenge of model poisoning attacks on DT model training and proposed an algorithm called MASTER, which utilizes multi-timescale deep Q-learning networks to optimize the scheduling of local training epochs and devices for accurate forecasting in smart parks [14]. This algorithm achieved endogenous security awareness and significantly improved DT model training accuracy and delay in a smart park integrated with DT and 6G edge intelligence. Moreover, the ADRIoT framework, an innovative anomaly detection framework for IoT networks utilizing edge computing to uncover potential threats swiftly, is presented [15]. It employs an edge-assisted architecture, enabling the detection module to run locally on the edge, facilitating prompt detection of IoT-based attacks. A multi-edge collaborative mechanism is designed to pool resources in a local network to address resource limitations.

Although the mentioned studies significantly contribute to cybersecurity in IoT and edge networks, our proposed system presents a distinctive and innovative approach. It creates a dynamic and adaptive security mechanism by integrating DT technology with edge networks. Through real-time analysis and synchronized virtual representations, our system excels in proactive threat detection and mitigation exhibiting a robust and resilient security posture of 6G EoT networks.

## III. PROPOSED 6G EoT SYSTEM MODEL

Fig. 1 depicts the proposed 6G EoT system architecture. It combines two networks. The first network, the EoT network, consists of the things, edge, and cloud layers. *The things layer* forms the foundation of the EoT network, encompassing a myriad of interconnected smart devices and sensors that collect data from the physical world. *The edge layer* is an intermediary tier between the device and the cloud. It consists of edge computing nodes strategically positioned to the devices they serve. The nodes have relatively higher computational capabilities and perform localized data processing and preliminary analysis. The requirement for constant data transfer to the central cloud is lessened by this layer, which also reduces latency and network congestion. Real-time decision-making, rapid response to emergencies, and low-latency services are all made feasible by edge computing nodes. *The cloud layer* represents the traditional centralized cloud infrastructure. Large-scale data centres boast significant computational capabilities and extensive storage capacity in this layer. Additionally, this layer manages resource-intensive operations, complicated data analytics, long-term storage, and other duties that may not be appropriate for the edge layer. The edge layer relieves the strain of delivering all data to the cloud, while the cloud layer assures scalability and thorough analysis, resulting in optimum performance.

The second network is the DT network. In our proposed system, the digital twin of the edge layer is built. We have meticulously constructed a digital twin representation of the edge layer, wherein the entities present within the edge layer mirror the physical elements of our digital twin network. This alignment ensures the edge layer remains closely intertwined with its virtual counterpart. The second layer is *the twin layer*, which is digital replicas of the edge layer entities. This layer enables real-time synchronization and analysis by establishing a smooth connection between the physical and digital worlds. The smart attack detection mechanism is strategically positioned in our third layer of the DT network. As a result, the architecture's overall resilience and dependability are strengthened. This placement allows the system to identify and respond to possible threats and security breaches proactively.

### A. Smart Attack Detection

The functioning of our proposed detection system is delineated through the following sequential steps:

- Data generated by the edge node is initially passed through YANG models to facilitate standardized representation and seamless integration with the system.
- The data is then transmitted to the detection module, where it undergoes further analysis and evaluation.
- Within the detection module, a meticulous assessment is conducted using the system's FS and classification methods to identify potential attacks at the edge node.
- In the event of an attack being detected, the mitigation module is promptly activated to neutralize the threat while simultaneously alerting the system administrator regarding the security breach.

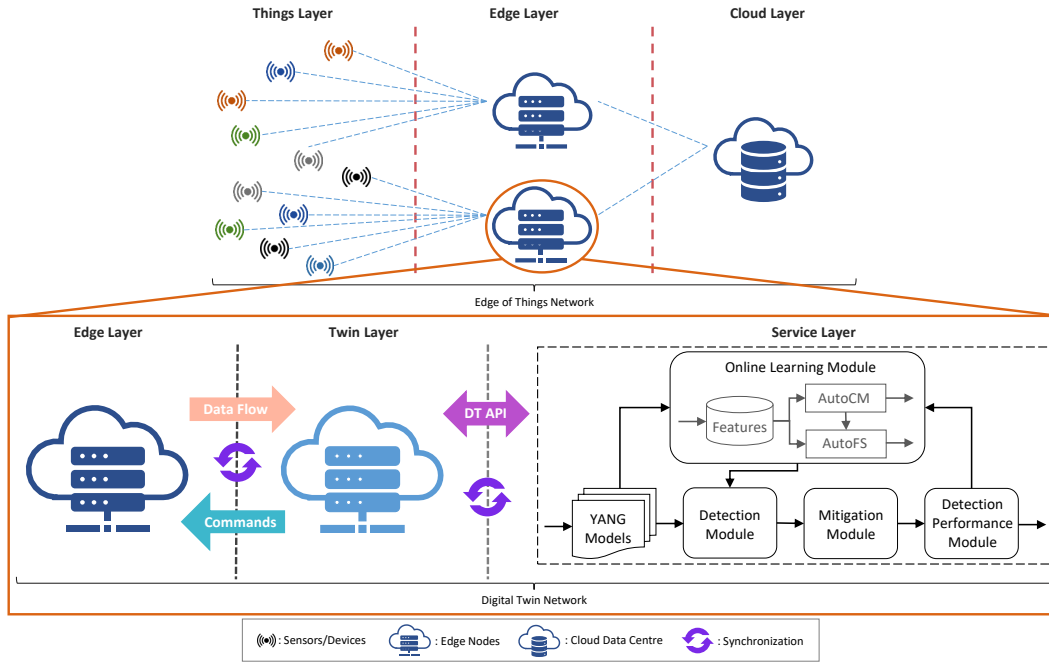


Fig. 1. The digital twin-empowered 6G EoT smart attack detection system architecture.

- In cases where no attack is identified, the detection performance module comes into play. It comprehensively investigates the reliability of the system’s classification technique.
- The system maintains its current model if the classification method’s reliability surpasses a predefined threshold, ensuring continuous operation based on the existing setup.
- However, if the classification technique’s reliability falls below the predetermined threshold, the detection performance module promptly communicates with the online learning module. This module updates the system’s FS and classification methods in near real-time, bolstering its adaptive capabilities and ensuring it remains proficient in identifying and mitigating potential attacks effectively.

This approach in the proposed detection system enables proactive threat detection, swift mitigation, and continuous improvement, making it a robust and adaptive solution for safeguarding the edge network against potential security breaches.

1) *Online Learning Module:* We used our AutoFS [16] and AutoCM [17] approaches from our previous works in this module. AutoFS includes five feature selection approaches, while AutoCM contains ten classification algorithms. The general workflow of this module is as follows: After taking a notification from the detection performance module, the online learning module imports one thousand records from the YANG models. Since the obtained data is unlabeled, we employed the labelling method to assign labels to the data and a baseline dataset that contains 65% of attack samples since attacks are uncommon from our previous work [17]. Unlabeled data undergoes labelling through the application of the labelling

algorithm. This process involves augmenting the dataset with one thousand samples from the baseline dataset. Subsequently, ten classification algorithms are employed to train and test their models using two thousand labelled data samples. Finally, the AutoCM selects the most suitable classification method using the final classification method algorithm.

Once the most appropriate classification method is determined, AutoCM transmits this method to AutoFS. AutoFS is responsible for identifying the optimal FS method for the system among five available techniques. The labelled one thousand random data samples are utilized as input for the five FS methods. Each FS method selects the ten most relevant features based on their algorithms. The data, refined by the FS techniques, is employed for training and testing the classification method received from AutoCM. Subsequently, the performance metrics obtained from the five techniques are forwarded to the final FS algorithm. This algorithm, in turn, determines the best FS method by optimizing the performance metrics for each technique. Once the best FS method is identified, it is the basis for updating the system’s FS method and the classification model. This iterative process ensures the system continually adapts to the most effective and efficient FS and classification approach, enhancing its overall performance and accuracy.

The ultimate objective of both the final classification method and FS algorithms is to maximize  $\sigma_i$  while simultaneously optimizing  $\vartheta_i$  as performance metrics.  $\sigma_i$  represents a weighted sum of precision and recall for the  $i_{th}$  classification or FS method, whereas  $\vartheta_i$  pertains to the detection time associated with the same  $i_{th}$  classification or FS method.

TABLE I  
THE NUMBER OF SAMPLES USED IN DATASETS

Datasets		Number of Records Used
Edge-IIoT	Backdoor Attack	1000
	DDoS HTTP Attack	500
	DDoS UDP Attack	500
	Fingerprinting Attack	1000
	MITM Attack	1000
	Password Attack	1000
	Port Scanning Attack	1000
	Ransomware Attack	1000
	SQL Injection Attack	1000
	XSS Attack	1000
	Normal	18000
ToN-IoT	Password Attack	1000
	Scanning Attack	1000
	XSS Attack	1000
	DDoS Attack	1000
	Ransomware Attack	1000
	Injection Attack	1000
	Backdoor Attack	1000
	Normal	14000

$$\arg \max (\alpha_i \sigma_i + \beta_i \vartheta_i), \quad i \in [1, 10] \vee [1, 5]$$

$$\sigma_i = (0.6) \frac{TP}{TP + FN} + (0.4) \frac{TP}{TP + FP}, \quad i \in [1, 10] \vee [1, 5]$$

$$\vartheta_i = t_i^{end} - t_i^{start}, \quad i \in [1, 10] \vee [1, 5] \quad (1)$$

In Equation 1,  $TP$  refers to the true positive,  $FN$  represents the false negative, and  $FP$  stands for false positive. Additionally,  $t_{end}$  denotes the finishing time, while  $t_{start}$  represents the starting time.

2) *Attack Mitigation Module*: Upon successful detection of an attack by the smart attack detection mechanism, this module swiftly comes into action to neutralize the identified threat. This module deploys proactive measures to safeguard the edge nodes and the broader system by leveraging the insights the detection process provides. Through real-time analysis of the attack's characteristics, it formulates targeted countermeasures to mitigate its impact effectively. The malicious traffic is blocked, and the related IP address is added to the suspended IP address list. If the attack is classified as high risk, the system is isolated to the affected edge node. If the attack is classified as mid-high risk, the affected edge node is isolated after taking system admin approval. By integrating such swift and adaptive mitigation strategies, the system can swiftly respond to emerging threats, preserving the integrity and uninterrupted functionality of the 6G edge-of-things network.

3) *Detection Performance Module*: This module is vital in assessing the classification method's efficacy within the digital twin-empowered 6G EoT smart attack detection system. Essential metrics like TP and FN are used to evaluate the detection performance. The determination of FN and TP in real-world scenarios where ground truth is often unavailable or challenging to establish is difficult. We address this concern

TABLE II  
THE DETECTION RATE PERFORMANCE

Train Dataset	Test Dataset	Detection Rate (%)		
		LSTM-AE	PS	
ToN-IoT	Edge-IIoT	Password Attack	91.94	99.46
		Port Scanning Attack	81.79	96.89
		DDoS UDP Attack	92.64	99.24
		XSS Attack	93.27	99.82
		MITM Attack	91.08	99.36
		Backdoor Attack	90.39	99.18
		Fingerprinting Attack	87.38	97.02
		SQL Injection Attack	91.86	97.34
		Ransomware Attack	87.26	98.62
		DDoS HTTP Attack	94.15	99.36
		Edge-IIoT	ToN-IoT	DDoS Attack
Injection Attack	88.92			98.92
Ransomware Attack	79.82			98.25
XSS Attack	89.79			98.04
Backdoor Attack	82.96			97.86
Scanning Attack	85.24			97.35
Password Attack	92.58			96.80

by leveraging our labelling method in the online learning module, which combines labelled and unlabeled data to estimate these values. The following equation is used to measure the reliability of the classification method:

$$\varphi = 1 - \frac{FN}{TP + FN} \quad (2)$$

In Equation 2,  $\varphi$  denotes the reliability of the classification method, with a specific focus on the FN metric due to its significance in the data division. In cases where no attack is identified, the detection performance module thoroughly investigates the reliability of the system's classification technique. The verification of classification techniques primarily focuses on assessing the system's ability to maintain a low rate of FP. While TP and FN may not change, our system continuously monitors network traffic and evaluates the alerts generated.

The module's decision-making process involves comparing the classification method's reliability against a predefined threshold. The reliability threshold for our detection scheme was determined using an adaptive thresholding technique, considering critical factors such as the observed rates of FP and FN over time. When the system shows an elevated FP rate, the threshold is dynamically adjusted to be more stringent, effectively mitigating false alarms. Conversely, if FN rates are a concern, the threshold is appropriately relaxed to enhance detection sensitivity. This approach allows us to maintain an optimal balance between FP and FN, ensuring the reliability and effectiveness of the detection scheme. The system continues to run using its present model if reliability exceeds the specified threshold, ensuring ongoing and consistent performance based on the current configuration. However, when the classification technique's reliability falls below the predetermined threshold, signalling potential limitations or changes in the system's operational environment, the detection performance module promptly initiates communication with the online learning module. This facilitates near real-time updates to the system's FS and classification methods, em-

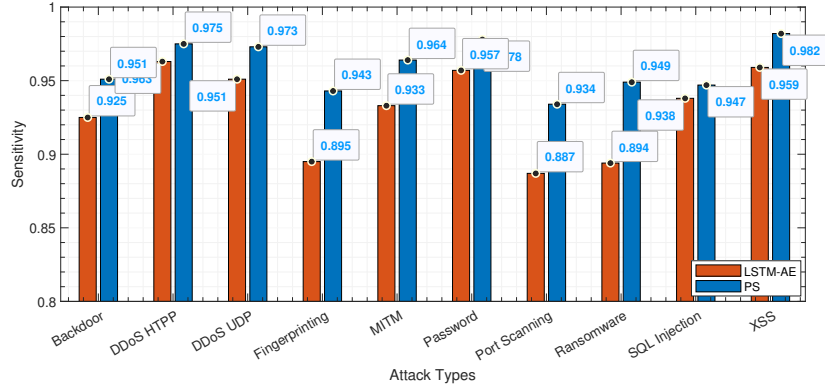


Fig. 2. The performance comparison of the Edge-IIoT dataset.

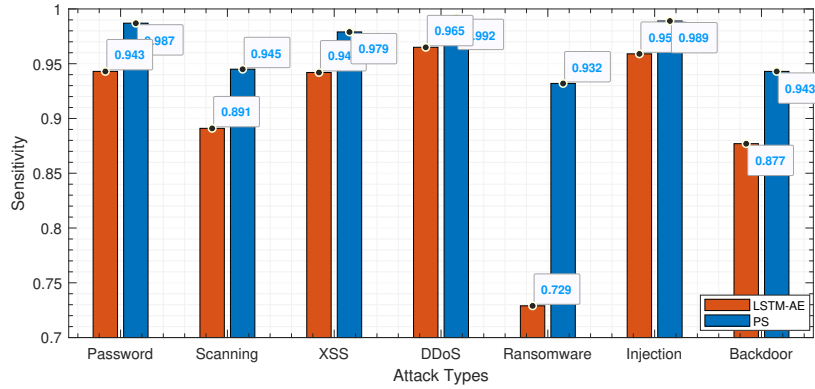


Fig. 3. The performance comparison of the ToN-IIoT dataset.

powering the system with adaptive capabilities to identify and mitigate potential attacks effectively. The system improves its overall security and resilience in the constantly changing EoT environment by dynamically altering its defence measures, which keeps it adept in responding to new threats.

#### IV. PERFORMANCE EVALUATION

We built a simple edge network architecture using the NS-3 [18]. This network has twelve edge devices in the things layer and two edge nodes in the edge layer. We used the Microsoft Azure DT (ADT) platform to build twin graphs of edge nodes [19]. We investigated the performance of our system using Edge-IIoTset [20], [21] and ToN-IIoT [22], [23] datasets. The Edge-IIoTset dataset is specifically designed for evaluating IoT and IIoT applications and consists of fourteen attacks targeting connectivity protocols. On the other hand, the ToN-IIoT dataset was created to assess the effectiveness and efficiency of AI-based cybersecurity applications tailored for next-generation IoTs and industrial IoTs. We randomly selected the specific number of samples from these datasets, as seen in Table I. LSTM networks are well-suited for capturing temporal dynamics; therefore, we choose an LSTM network to compare our intrusion detection work. We conducted a comparison between our proposed solution (PS) and the

LSTM-AE utilized in [15]. To this end, we employed an autoencoder with two encoder layers and two decoder layers. In both the encoder and decoder components, the Dense layer was succeeded by batch normalization and the LeakyReLU activation function. Subsequently, the decoder output features were passed to the LSTM model for further processing. The selection of parameters for our LSTM-based model was a result of systematic experimentation and optimization. We conducted tests, cross-validation, and performance evaluations to arrive at the configurations that provided the best trade-off between model complexity and predictive accuracy. We ensured that the LSTM approach is also effective and efficient in comparing our PS.

We employed sensitivity as a performance metric, which represents the ratio of correctly identified attack samples to the total number of samples that should have been identified as attacks. Initially, we conducted a separate evaluation of the performance results for each dataset. As illustrated in Fig. 2 and Fig. 3, our solution demonstrates superior performance compared to the other approach. After that, we investigated the detection performance. We trained the initial model with the whole dataset and then tested them with the other dataset. We send the different attacks in order, which is given in Table II, to test our solution AutoCM and AutoFS performance.

Table II clearly indicates that our solution exhibits enhanced robustness and adaptability to different attack types. Moreover, it outperforms LSTM-AE regarding attack detection rate, indicating its heightened effectiveness and accuracy in identifying potential threats. These achievements underscore our system's heightened effectiveness and accuracy in swiftly identifying and neutralizing potential threats, bolstering the overall security posture of the 6G Edge of Things Networks. Furthermore, the observed superiority of our solution in handling diverse attack scenarios signifies its potential for real-world IoT and IIoT environments, where dynamic security challenges are commonplace. These positive outcomes strongly validate the efficacy of our digital twin-empowered smart attack detection system as a proactive and efficient cybersecurity solution, offering a path towards enhanced security and resilience in 6G EoT networks. Furthermore, we assessed the impact of DT on network security by quantifying the reduction in successful attacks and the improvement in incident response times resulting from its implementation. We also scrutinized its resource utilization to ensure it operates efficiently within network constraints while delivering significant security enhancements. These findings underscore the DT's effectiveness as a potent tool for fortifying network security in 6G EoT environments.

## V. CONCLUSION

In this paper, we introduced a digital twin-empowered smart attack detection system for 6G Edge of Things networks. Integrating digital twin technology and edge computing enables real-time monitoring and proactive threat detection, bolstering the security of IoT environments. Our system's online learning module ensures continuous improvement by updating feature selection and classification methods, making it adaptable to dynamic attack landscapes. Performance evaluations using real datasets indicate the system's superior performance. The results highlight the system's effectiveness, robustness, and adaptability in detecting diverse attack types, making it a promising solution for securing 6G edge-of-things networks.

## ACKNOWLEDGMENT

Yagmur Yigit would like to thank the Google DeepMind Scholarship Programme for their support.

## REFERENCES

- [1] Statista. Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2023, with Forecasts from 2022 to 2030. [Online]. Available: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide>, Accessed June 22, 2023.
- [2] P. Research. Edge Computing Market Size, 2022 to 2032 (USD BILLION). [Online]. Available: <https://www.precedenceresearch.com/edge-computing-market/>, Accessed June 23, 2023.
- [3] Statista. Estimated Cost of Cybercrime Worldwide 2017-2028. [Online]. Available: <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>, Accessed July 20, 2023.
- [4] Y. Yigit, L. D. Nguyen, M. Ozdem, O. K. Kinaci, T. Hoang, B. Canberk, and T. Q. Duong, "TwinPort: 5G Drone-assisted Data Collection with Digital Twin for Smart Seaports," *Scientific Reports*, vol. 13, p. 12310, 2023.
- [5] J. Hong, Y.-G. Hong, X. de Foy, M. Kovatsch, E. Schooler, and D. Kutscher. IoT Edge Challenges and Functions, Work in Progress, Internet Engineering Task Force. [Online]. Available: <https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-edge/09/>, Accessed June 15, 2023.
- [6] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and Privacy on 6G Network Edge: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1095–1127, 2023.
- [7] E. Horsanali, Y. Yigit, G. Secinti, A. Karameseoglu, and B. Canberk, "Network-Aware AutoML Framework for Software-Defined Sensor Networks," in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2021, pp. 451–457.
- [8] C. S. Kalutharage, X. Liu, and C. Chrysoulas, "Explainable AI and Deep Autoencoders Based Security Framework for IoT Network Attack Certainty (Extended Abstract)," in *Attacks and Defenses for the Internet-of-Things*, W. Li, S. Furnell, and W. Meng, Eds. Cham: Springer Nature Switzerland, 2022, pp. 41–50.
- [9] H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang, and L. Lu, "Hybrid Intrusion Detection System for Edge-Based IIoT Relying on Machine-Learning-Aided Detection," *IEEE Network*, vol. 33, no. 5, pp. 75–81, 2019.
- [10] G. Ren, Y. Zhang, S. Zhang, and H. Long, "Edge DDoS Attack Detection Method Based on Software Defined Networks," in *Algorithms and Architectures for Parallel Processing*. Cham: Springer International Publishing, 2022, pp. 597–611.
- [11] A. Singh, K. Chatterjee, and S. C. Satapathy, "An edge-based hybrid intrusion detection framework for mobile edge computing," *Complex & Intelligent Systems*, vol. 8, pp. 3719 – 3746, 2022. [Online]. Available: <https://doi.org/10.1007/s40747-021-00498-4>
- [12] S. J. Lee, P. D. Yoo, A. T. Asyhari, Y. Jhi, L. Chermak, C. Y. Yeun, and K. Taha, "IMPACT: Impersonation Attack Detection via Edge Computing Using Deep Autoencoder and Feature Abstraction," *IEEE Access*, vol. 8, pp. 65 520–65 529, 2020.
- [13] W. Lalouani and M. Younis, "A Robust Distributed Intrusion Detection System for Collusive Attacks on Edge of Things," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, 2022, pp. 1004–1009.
- [14] S. Zhang, Z. Yao, H. Liao, Z. Zhou, Y. Chen, and Z. You, "Endogenous security-aware resource management for digital twin and 6G edge intelligence integrated smart park," *China Communications*, vol. 20, no. 2, pp. 46–60, 2023.
- [15] R. Li, Q. Li, J. Zhou, and Y. Jiang, "ADRIoT: An Edge-Assisted Anomaly Detection Framework Against IoT-Based Network Attacks," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10 576–10 587, 2022.
- [16] Y. Yigit, B. Bal, A. Karameseoglu, T. Q. Duong, and B. Canberk, "Digital Twin-Enabled Intelligent DDoS Detection Mechanism for Autonomous Core Networks," *IEEE Communications Standards Magazine*, vol. 6, no. 3, pp. 38–44, 2022.
- [17] Y. Yigit, O. K. Kinaci, T. Q. Duong, and B. Canberk, "TwinPot: Digital Twin-assisted HoneyPot for Cyber-Secure Smart Seaports," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023, pp. 740–745.
- [18] NSNAM. The ns-3 Network Simulator. [Online]. Available: <https://www.nsnam.org/>, Accessed Apr. 27, 2023.
- [19] Microsoft. Azure Digital Twins Documentation. [Online]. Available: <https://docs.microsoft.com/en-us/azure/digital-twins>, Accessed Apr. 12, 2023.
- [20] I. Dataport. (2022) Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications: Centralized and Federated Learning. [Online]. Available: <https://iee-dataport.org/documents/edge-iiotset-new-comprehensive-realistic-cyber-security-dataset-iot-and-iiot-application>, Accessed May 10, 2023.
- [21] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40 281–40 306, 2022.
- [22] N. Moustafa. ToN IoT datasets. [Online]. Available: <https://iee-dataport.org/documents/toniot-datasets>, Accessed May 3, 2023.
- [23] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "Ton-iiot telemetry dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165 130–165 150, 2020.