Fortified-Edge 2.0: Machine Learning based Monitoring and Authentication of PUF-Integrated Secure Edge Data Center

Seema G. Aarella
Dept. of Computer Science and Engineering
University of North Texas, USA.
Email: seema.aarella@unt.edu

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas, USA.
Email: saraju.mohanty@unt.edu

Elias Kougianos
Dept. of Electrical Engineering
University of North Texas, USA.
Email: elias.kougianos@unt.edu

Deepak Puthal
Electrical Engineering and Computer Sciencee
Khalifa University, Abu Dhabi, UAE.
Email: deepak.puthal@ku.ac.ae

***Abstract*—A collaborative edge computing model involves multiple edge devices, such as Edge Data Centers (EDCs) and Edge Routers. Data can be stored and processed at the Edge in Collaborative Edge Computing (CEC). Edge security is very crucial as it is prone to external attacks at different layers of its architecture. In this work, a novel machine-learning-based approach is proposed to improve the security of EDCs using Security-by-Design (SbD) principle in CEC framework. This research aims to provide a security scheme for EDCs in a collaborative edge computing environment through machine-learning-based monitoring and authentication. Through this method, any drastic change in the device's behavior will be considered critical, and the device can be removed from the network, securing the network from further harm. This research proposes a support vector machine (SVM)-based algorithm to monitor the EDC authentication process and detect an intrusion or malicious authentication requests during load balancing.**

***Index Terms*—Security-by-Design (SbD), Collaborative Edge Computing, Edge Data Centers, Machine Learning, Secure Authentication, Device Monitoring**

I. Introduction

Collaborative edge computing (CEC) involving multiple IoT-Edge devices has tremendous potentials for low-cost and heavy duty computing in smart villages [1]. Edge computing provides Speed, reliability, security, scalability, and repeatability, with the ability to process data closer to the end layer of Internet-of-Things (IoT). Since the Edge Data Centers (EDC) are capable of limited processing only, a collaborative Edge Computing environment helps offload the processing tasks to other EDCs in the environment. The EDCs participating in the load balancing must be verified and authenticated to protect data and the system [2]. Heterogeneity of the edge computing environment makes security a challenge, strong monitoring and authentication protocols can boost security and prevent data breaches and device damage.

Edge Data Center monitoring is necessary for optimal and secure operation. It can be monitored for Physical features, Environmental features, and Operational statistics. Monitoring systems help to ensure security, and aid power analysis by monitoring power consumption, detecting and resolving network problems, providing end-to-end visibility, and maintaining data center performance [3], [4].

Decentralized computing process involves Server-aided computation and Verifiable computation. In server-aided computing, data processing is at risk of compromise if the IoT end devices are already compromised. In verifiable computing, the fog nodes are used to compute the data, it needs a secure mechanism to verify the nodes as well as the data coming from the nodes [5].

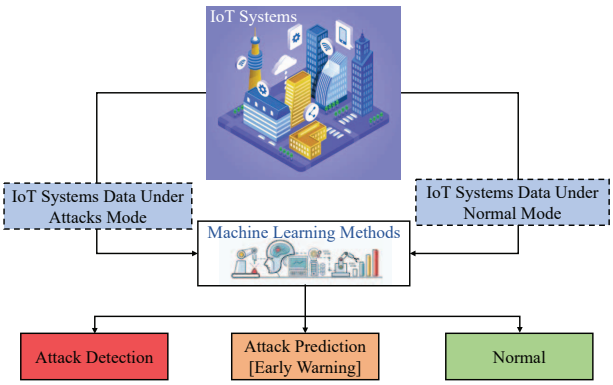

Fig. 1: Machine Learning for Security of IoT Systems.

Machine learning (ML) helps design effective protocols for cybersecurity through monitoring as it is data-driven, availability of big data enables ML algorithms for the same. ML algorithm like Deep learning is employed in providing big data security through malware detection and intrusion attack detection [6]. Data analysis near real-time processing nodes helps prevent security issues from arising due to data movement. The application of ML in securing the IoT systems is shown in Figure 1. In this research we explore the use of

ML in authenticating and monitoring EDCs in a collaborative edge computing environment, the purpose is to establish how ML can support integrated security to the edge.

The rest of the paper is organized in the following manner. Section II summarizes contributions of the current paper. Related prior works are discussed in Section III. The needs for ML in EDC is presented in Section IV. Section V discusses the proposed framework. Section VI has the details of the experimental results. The conclusions and future research are provided in Section VII.

II. Contributions of the Current Paper

Cyber-physical systems in a CEC environment like a smart village need a secure computing scheme for the EDCs communicating in the distributed network [1]. During load balancing most often, EDCs need to offload tasks to other available EDCSs, in this process authentication is required before offloading. Since the resource-constrained edges are considered, lightweight authentication protocols with low computation and energy requirements are appropriate.

A. Problems Addressed

Problems addressed in this research are as below:

- Enhancing secure authentication of EDCs in CEC
- ML methods with Low memory, smaller data requirement and low computing power
- Intrusion detection and identity protection of EDC
- ML model with high accuracy in prediction, low error rate, efficient classification functions
- Secure authentication through integrated hardware and software

B. Solution Proposed

Continuing from the previous research, Fortified Edge is an SRAM PUF-based Certificate Authority (CA) protocol for the trusted authentication of EDCs, where EDCs authenticate each other using a valid CA certificate issued by the authentication server after authenticating the EDCs by the CRPs. In this research, we implement an ML-based authentication model which utilizes PUF-based security and improves security for EDC.

Computing the ML algorithms at the edge utilizes less power compared to transmitting the data to a remote server for computation. Computing also depends on the type of data being processed. Large data like audio, image, and video needs more computing power and memory, however, to enable less computing power the data considered for ML at the edge is smaller.

- Improving the authentication model of Fortified-Edge
- Supervised ML method for authentication and authorization, using small data size
- SVM based ML method for classifictaion and prediction
- EDC data analysis and feature extraction
- ML for monitoring and authentication based on EDC features
- Suitable model for low computing requirements at the edge in CEC

C. Novelty of the current research

Fortified-Edge [7] is an initiation using Security-by-Design(SbD), intended towards making security an integral part of application design and development. Fortified-Edge proposes Hardware-Assisted Security (HAS) through its SRAM PUF-based CA authentication model for secure authentication of EDCs in CEC. Furthering the research Fortified-Edge 2.0 proposes an integrated security model by adding ML to monitor and authenticate the EDCs based on the features of EDC and authentication data.

In supervised learning classification or regression models are used to train the categorized data. classification model outputs data with defined labels, whereas the regression model outputs data with no defined labels (continuous) [8]. The goal of supervised ML is to accurately predict the known output variable based on the input variables, making it an ideal choice for this research.

Supervised learning methods are widely used for intrusion detection, and DDOS attacks in the IoT, "instance-based" Models like SVM are very efficient for smaller datasets and do not require a lot of memory for processing [9]. Considering the low data at the edge of a CEC in a smart village environment, SVM will be a suitable method to employ for authentication and authorization. The following are the Novel solutions presented in this work:

- EDC monitoring and authentication through supervised ML
- SVM as a ideal ML method to incorporate at Edge with its available resources
- Selection of a variety of features for training SVM to make it accurate
- Intrusion and malicious authentication detection
- SVM to validate authentication process and predict invalid authentication requests

III. Related prior research

Some of the research involving SVM method of ML for applications at the edge are listed in the Table I.

A lightweight ML model is proposed for Radio Frequency (RF) Enabled systems authentication process, using RF-PUF a deep neural network-based framework, where, process variations in RF properties are used as the PUFs of the wireless transmitters and the neural network is used to detect the variations at the receiver [15].

An ML-based Physical Layer Authentication for wireless industrial Cyber-Physical Systems (CPS) to improve the authentication process without any computational burden is proposed in [16]. A study of ML-based solutions for IoT security is presented in the research [17], which includes ML techniques like supervised learning, and unsupervised learning.

An ML-based security system for Edge computing devices in a smart grid is proposed in the research [18], this research proposes a Physical Layer authentication (PLA) scheme using K-Nearest Neighbor (KNN) method to authenticate the edge devices, a Radio Frequency Fingerprinting (RFF) method to

TABLE I: Comparative Table for State-of-the-Art Literature.

Research	Year	ML Model	Applications	Performance Metrics
Yufei et al. [10]	2021	OC-SVM and SVDD	HTTP Anomaly Detection for Edge	Precision, Recall, Accuracy, F1-score
Hou et al. [11]	2019	SVM	Network Security of Edge Computing	Accuracy
Oshana et al. [12]	2022	SVM	Attack Detection System	Precision, Recall, F1-score
Imtiyaz et al. [13]	2020	SVM	Transformer Monitoring at the Edge	Accuracy, Precision, Recall
Khosroshahi et al. [14]	2019	3D SVM	DDoS Attack Source Detection	Accuracy, Precision, Error Rate
Fortified-Edge 2.0 (Current Paper)	2023	SVM	EDC Authentication and Monitoring in CEC	Accuracy, Precision, Recall, ROC-AUC

verify the data packets being sent, to protect device and data authentication.

Some of the ML methods used for device authentication are DT, NB, and LR, which can use the data related to the device behavior and device information, which is a combination of the static and dynamic information of the device [19]. ML algorithms like deep neural network (DNN), convolutional neural network (CNN), and modified CNN are used to optimize the traditional encryption methods and create data models for privacy preservation [20].

IV. Need for Machine Learning for Edge-Server Authentication and Monitoring

ML and AI can provide the new and powerful capabilities for security optimization in the IoT based services and infrastructure. In this research we explore the ML methods to suitably improve security of the EDC and define an integrated-security model which satisfies the principles of Security-by-Design (SbD) [21], [22]. SbD is based on 7 different principles such as [21]: 1) Cybersecurity features should be proactive not reactive, 2) Cybersecurity should be default, 3) Cybersecurity should be integrated into design, 4) Cybersecurity should be incorporated as a full-functionality with positivesum without trade-offs, 5) Cybersecurity-Solution should provide end-to-end Security for the lifecycle protection, (6) Cybersecurity-Solutions should have transparency, and 7) Cybersecurity-Solutions should have respect for the users.

The decentralized edge computing (EC) still faces challenges like task scheduling, resource allocation, optimization of energy, response time, security, and privacy. A combination of edge computing and ML will help address the issues with more stability and reliability. Because of distributed nature of edge, attacks like Distributed-Denial -of-Service (DDoS), jamming attacks, man-in-the-middle, spoofing attacks, malware injection attacks, and authentication and authorization attacks, are a threat to its security and privacy. ML methods like Hypergraph Clustering, Deep reinforcement learning (DRL), federated learning, and post-decision state learning (PDS) are employed in optimizing resource allocation, data privacy, edge security, offloading decision making, and energy consumption [23].

EC has become a target of cyber-attacks, which are classified into broad categories like identification attacks, binding down attacks, and battery-draining attacks. Security and privacy issues at the edge include access control, authentication, confidentiality and data integrity, privacy, trust, and policy enforcement. The current heterogeneous architecture of the edge demands a robust security system to address the issues involved [24].

An emerging paradigm in EC is Edge-Intelligence Edge, a combination of edge infrastructure and AI employed to resolve the challenges of edge computing. ML methods provide the ability and intelligence for an edge, by learning about attack vectors and patterns without being explicitly programmed, provided the processing needs, availability of labeled or unlabeled data, and need for real-time processing are determined [25]. In this current research, we focus on the security of edge considering the CEC infrastructure and employing ML methods to implement a secure authentication and monitoring system.

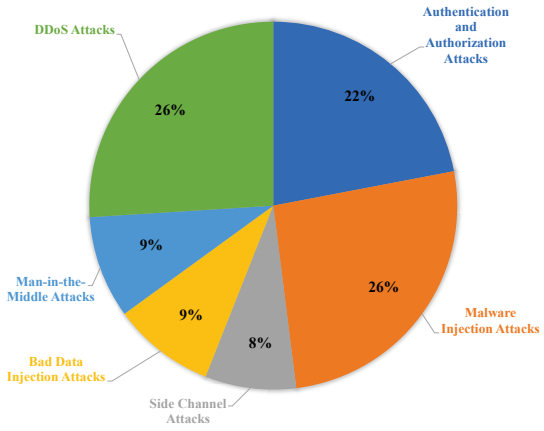

Fig. 2: Security Threats to Edge [26].

CEC enables developing applications for the smart village, where the resource-constrained nature of its infrastructure makes way for resource utilization methods like task offloading through a scheme called load balancing [1]. Authentication and Authorization are important features of the distributed-

edge in CEC which needs to be optimized for secure operation. Some of the authentication and authorization attacks on edge computing systems are dictionary attacks, authentication protocol attacks, authorization protocol attacks, and over privilege attacks [27]. It is seen that Authentication and Authorization attacks estimate for 26% of security threats to the edge (see Fig. 2) [26]. Hence, this research is based on ML-driven authentication and monitoring scheme development.

V. The Proposed Framework: Fortified-Edge 2.0

The architecture for the fortified edge 2.0 with ML is shown in the Fig. 3. It considers various attributed like the following:

- Geographical location
- Authentication time
- CA certificate validity status
- EDC ID
- EDC location's site ID

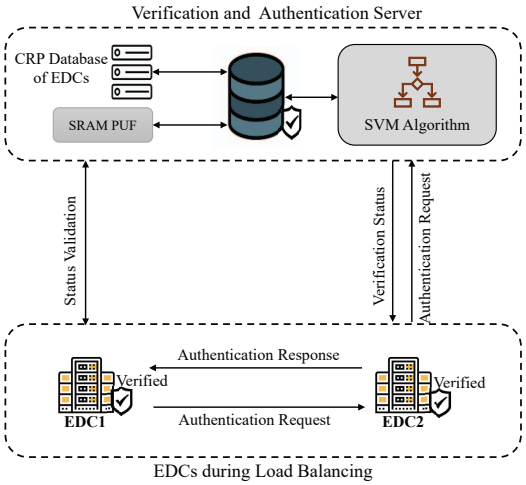

Fig. 3: Architecture of Fortified Edge 2.0 using Machine Learning.

SVM method based on statistical learning theory is considered for classification and prediction, since the labeled data for EDCs are crucial for authentication validation.The algorithm is effective is predicting accurate results based on the sample provided to it. SVM not only improves the performance but also reduces the need for complex hardware. The basic idea of SVM algorithm for authentication is shown in Fig. 4.

Training dataset is created by combining the EDC authentication data such as, EDC ID, CA validity and authentication time, with the EDC physical data like geographical location, site ID and state. The data is logically filtered to get a set of labeled data for each EDC at a given site with a unique site ID. From the dataset 3 features are selected for training the data, distance of the EDC, authentication time and CA validity, target of the prediction is the status of the authentication request. distance d_r is the estimated distance of requesting EDC from the authenticating EDC using the Haversine formula, t_r is the average response time taken for authenticating under normal conditions, maximum time

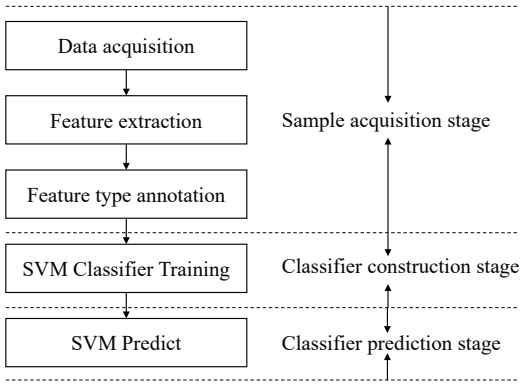

Fig. 4: Basic function of the SVM algorithm.

is set to 2s, based on the tests done for server reponses for 1000 requests which resulted in response time of 1.5ms. Linear kernel is selected for the Support Vector Classification (SVC), to classify the linearly inseperable data. SVC creates a decision boundary between the instances of data having various class values [28]. SVM creates a hyper-plane that differentiates the classes. The advantages of uisng SVM are it works well with clear margin of data separation, it is effective in high dimensional spaces, the use of support vectors makes it efficient in training set creation that is memory efficient.

Algorithm 1: Algorithm for EDC data acquisition and SVM training.

Input: Load EDC Site Dataset
Input: Load EDC Authentication Dataset
Output: Train the SVM Model to predict the authentic EDC
get Authentication Metadata ;
get Location S_{id} ;
get CA Validity data c_r;
get Authentication Time t_r;
calculate the distance d_r;
set target as status=0 or 1;
split data into Train set and Test set;
create Confusion Matrix;
use SVC Classifier for Classification and prediction;
if *status=1* **then**
    Request is authentic;
else
    Malicious Request;
/* The SVM is trained to predict genuine and malicious authentication requests */

Algorithm 1, shows the process used for training the ML model to identify the malicious requests from the genuine request. Any intrusion will be detected by verifying the geographical location, and data related to the authentication, any variation of data from normal data will be flagged as malicious and the authentication process will abort, thus preventing attacks on the distributed edge. The features considered for creating the dataset are shown in the Table II. A 2k dataset with the columns listed is used for training, and testing.

TABLE II: Features Considered for SVM Training.

Features	Variables
Site_ID	S_{id}
EDC_ID	E_{id}
EDC_ID_Requestor	E_{idr}
Latitude_EDC	L_a
Longitude_EDC	L_o
Latitude_EDC_Requestor	L_{ar}
Longitude_EDC_Requestor	L_{or}
Distance	d_r
Certificate_Validity	c_r
Authntication_Time	t_r

VI. Experimental Results

EDCs for distributed computing are implemented on Raspberry Pi4 boards, the SRAM PUFs are extracted from an development board for CA certificate generation. SVM is developed using Python, the local computer is the acting server for running the ML algorithm for authentication. The metrics used for performance evaluation of the proposed framework are accuracy, precision and recall, and Area Under the Curve (AUC). Receiver Operator Characteristic (ROC) is a probability curve that plots True Positive Rate (TPR) against the False Positive Rate (FPR) at various threshold values. AUC shows the ability of the classifier to distinguish between classes. Fig. 5 shows the ROC curve obtained for the SVM model classifier, if the AUC value is 1, the classifier is able to distinguish between all positives and negatives accurately. For the current model the AUC value obtained is 0.99, and that the classifier is 99% accurate in predicting.

Accuracy is the ration of the number of correct predictions and the total number of predictions. Accuracy is calculated using the True Positive (TP), True Negative (TN), False Positive (FP) and False Negative(FN) values as [29]:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

From the Fig. 5, it is seen that we obtained an accuracy of 100%. Precision shows how correctly the predicted cases turned out to be positive. Precision is calculated using:

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

We obtained 100% precsion results for the SVM model. Recall(Sensitivity) shows how many actual positive cases the model was able to predict effectively. Recall score of 100% was obtained for the SVM model. Recall is calculated using the following:

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

$F1$ Score is the harmonic mean of precision and recall, it is calculated from:

$$F1\_Score = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{4}$$

Confusion matrix is created to verify if any misclassification has happened, if there is none, the correct values are seen in the diagonal area. Fig. 6 shows the confusion matrix generated.

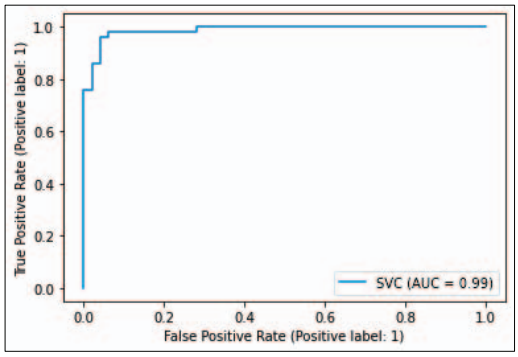

Fig. 5: SVM Model Characteristics.

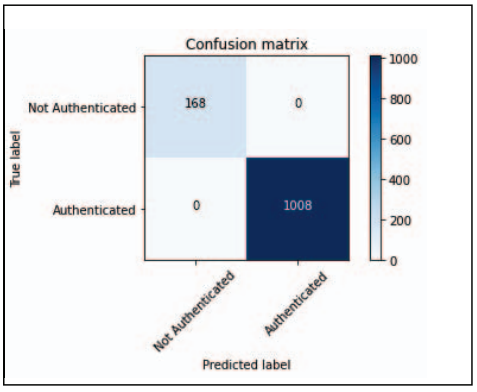

Fig. 6: Confusion Matrix.

The dataset with updated information about location, site, and authentication times makes the algorithm more efficient in predicting attacks and anomalies during authentication. To further evaluate the current research, we compare the results with state-of-the-art literature from Table I, which lists the research based SVM for different applications at the IoT Edge. It is evident that SVM algorithm does not need large computing infrastructure like cloud as it can perform effectively at the edge with limited computing power. Table III shows the performance evaluation results of the current research Fortified-Edge 2.0 against the peers.

VII. Conclusions

Fortified-Edge 2.0 aims at designing a security application that follows the principles of Security-by-Design (SbD). The research is an integrated security solution that combines the Hardware-Assisted Security (HAS) feature of the PUFs in the SRAM PUF based CA model for authenticating the Edge Data Centers with the software power of Machine Learning to improve the secure authentication process at the edge. As shown in this research the SVM model with linear classifier is 100% effective in predicting the valid authentication requests. The prediction accuracy is greatly improved as the number of features included is more. This increases the security at the edge by eliminating malicious requests. As a pointer for the future research, SVM can be used for detecting communication

TABLE III: Comparison of Results for State-of-the-Art-Literature.

Research	ML Model	Accuracy	Precision	Recall	AUC	F1-Score
Yufei, et al. [10]	OC-SVM and SVDD	0.983	0.952	0.97	NA	0.961
Hou, et al. [11]	SVM	0.99	NA	NA	NA	NA
Oshana, et al. [12]	SVM	NA	1.0	1.0	NA	1.0
Imtiyaz, et al. [13]	SVM	0.983	0.886	0.995	NA	NA
Khosroshahi, et al. [14]	3D SVM	0.985	0.971	NA	NA	NA
Fortified-Edge 2.0 (Current Paper)	SVM	1.0	1.0	1.0	0.99	1.0

related anomalies at the edge, by including the related features, to prevent network and communication attacks like bad data injection attacks and malware injection attacks.

REFERENCES

[1] D. Puthal, S. P. Mohanty, S. Wilson, and U. Choppali, "Collaborative Edge Computing for Smart Villages," *IEEE Consumer Electronics Magazine*, vol. 10, no. 3, pp. 68–71, 2021.

[2] D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, "Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 60–65, 2018.

[3] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64–71, May 2016.

[4] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog Computing Security Challenges and Future Directions," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 92–96, May 2019.

[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[6] D. B. Rawat, R. Doku, and M. Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security," *IEEE Transactions on Services Computing*, vol. 14, no. 6, pp. 2055–2072, 2021.

[7] S. G. Aarella, S. P. Mohanty, K. Elias, and D. Puthal, "Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing," in *Proceedings of ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, p. In Press, dOI: https://doi.org/10.1145/3583781.3590249.

[8] V. Gupta, Mishra, V. Kumar, Singhal, Priyank, and A. Kumar, "An Overview of Supervised Machine Learning Algorithm," in *11th International Conference on System Modeling and Advancement in Research Trends (SMART)*, 2022, pp. 87–92.

[9] K. Istiaque Ahmed, M. Tahir, M. Hadi Habaebi, S. Lun Lau, and A. Ahad, "Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction," *Sensors*, vol. 21, no. 15, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/15/5122

[10] Y. An, F. R. Yu, J. Li, J. Chen, and V. C. M. Leung, "Edge Intelligence (EI)-Enabled HTTP Anomaly Detection Framework for the Internet of Things (IoT)," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3554–3566, 2021.

[11] S. Hou and X. Huang, "Use of Machine Learning in Detecting Network Security of Edge Computing System," in *IEEE 4th International Conference on Big Data Analytics (ICBDA)*, 2019, pp. 252–256.

[12] R. Oshana, M. A. Thornton, and M. Caraman, "A Side Channel Attack Detection System Using Processor Core Events and a Support Vector Machine," in *Proc. 11th Mediterranean Conference on Embedded Computing (MECO)*, 2022, pp. 1–8.

[13] I. Ahmad, Y. Singh, and J. Ahamad, "Machine Learning Based Transformer Health Monitoring Using IoT Edge Computing," in *Proc. 5th International Conference on Computing, Communication and Security (ICCCS)*, 2020, pp. 1–5.

[14] Y. Khosroshahi and E. Ozdemir, "Detection of Sources Being Used in DDoS Attacks," in *Proc. 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2019, pp. 163–168.

[15] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2019.

[16] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, and J. Chen, "Threshold-Free Physical Layer Authentication Based on Machine Learning for Industrial Wireless CPS," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6481–6491, 2019.

[17] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?" *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.

[18] A. Xu, Y. Jiang, J. Wu, Y. Zhang, W. Hou, H. Wen, and Y. Zheng, "Efficiency and Security for Edge Computing Assisted Smart Grids," in *2019 IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–5.

[19] H. Wu, H. Han, X. Wang, and S. Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access*, vol. 8, pp. 153 826–153 848, 2020.

[20] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey," *Security and Communication Networks*, vol. 2020, p. 8872586, Sep 2020. [Online]. Available: https://doi.org/10.1155/2020/8872586

[21] S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4–5, March 2020.

[22] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 320–333, April-June 2021.

[23] H. Hua, Y. Li, T. Wang, N. Dong, W. Li, and J. Cao, "Edge Computing with Artificial Intelligence: A Machine Learning Perspective," *ACM Comput. Surv.*, vol. 55, no. 9, jan 2023. [Online]. Available: https://doi.org/10.1145/3555802

[24] L. A. Ajao and S. T. Apeh, "Secure edge computing vulnerabilities in smart cities sustainability using petri net and genetic algorithm-based reinforcement learning," *Intelligent Systems with Applications*, vol. 18, p. 200216, 2023.

[25] S. Singh, R. Sulthana, T. Shewale, V. Chamola, A. Benslimane, and B. Sikdar, "Machine-Learning-Assisted Security and Privacy Provisioning for Edge Computing: A Survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 236–260, 2022.

[26] [Online]. Available: https://www.whiteboxsolution.com/blog/edge-computing-security-you-better-know-these-risks-and-guidelines/#Edge_computing_security_risks

[27] A. Alnoman, S. K. Sharma, W. Ejaz, and A. Anpalagan, "Emerging Edge Computing Technologies for Distributed IoT Systems," *IEEE Network*, vol. 33, no. 6, pp. 140–147, 2019.

[28] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35 365–35 381, 2018.

[29] L. Rachakonda, S. P. Mohanty, and E. Kougianos, "iLog: An Intelligent Device for Automatic Food Intake Monitoring and Stress Detection in the IoMT," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 2, pp. 115–124, March 2020.