Anomaly Detection system for an 5G Enabled Industrial Internet of Things

Asterios Mpatziakas*†, Alexandros Emvoliadis*, Anastasios Drosou*, Nestor D. Chatzidiamantis†, Dimitrios Tzovaras*
* *Information Technologies Institute*,
Centre for Research and Technology (CERTH),
Thessaloniki, Greece
{ampatziakas, alemvoliadis, drosou, Dimitrios.Tzovaras}@iti.gr
† *Dept. of Electrical and Computer Engineering Aristotle University of Thessaloniki Thessaloniki, Greece*,
Thessaloniki, Greece
{nestoras}@ece.auth.gr

***Abstract*—Industry 4.0 (I4.0) integrates Information and Operational Technologies (IT and OT) to enhance industrial efficiency, sustainability, and cost-effectiveness. This paradigm includes 5th generation (5G) networks, Internet of Things (IoT), Digital Twins, and Artificial Intelligence (AI), but also introduces new security risks. We present a novel anomaly detection system for 5G-enabled Industrial IoT (IIoT) using deep learning techniques and multi-stage detection to address these challenges.**

***Index Terms*—Artificial Intelligence, Beyond-Fifth Generation, cybersecurity, Industry 4.0, Industrial Internet of Things**

I. Introduction

Traditionally, Industrial and Operational Technology (OT) environments operated independently from Information Technology (IT). However, OT systems are now increasingly integrated with IT to enhance efficiency and productivity. This convergence is rapidly advancing, integrating diverse technologies. This integration exposes production and manufacturing infrastructures, along with their processes, to the broader IT and Internet ecosystem, which significantly increases their vulnerability to a wide range of cyber-threats and risks.

To address these threats, anomaly and intrusion detection mechanisms are critical for safeguarding industrial systems, especially those using 5G, Beyond-5G (B5G), Cyber-Physical Systems (CPS), and IIoT. As industrial environments become more connected and face increasingly sophisticated threats, the need for robust defense mechanisms is more urgent than ever, as these systems provide a crucial first line of defense, ensuring the security, resilience, and reliability of critical industrial infrastructures.

Modern anomaly detection solutions use advanced algorithms to monitor network traffic, system behavior, and data patterns continuously. These solutions are designed to identify any unusual or suspicious activities that may indicate a potential intrusion [1]. Once an anomaly is detected, prompt mitigation measures are deployed, which can include isolating compromised systems, updating security protocols, or even shutting down critical components to prevent further damage or data breaches [2].

The remainder of the paper is structured as follows: Section II presents an extensive review of the relevant literature while section III contains and explains the model proposed. Then Section IV presents the performance evaluation assumption and results. Finally, section V contains the conclusions of this paper along with future research directions and aims.

II. Related Work

This section reviews recent literature on industrial cybersecurity anomaly detection. I4.0 promises real-time, secure, and autonomous manufacturing environments. The Industrial Internet of Things plays a pivotal role in turning this potential into reality by facilitating advanced wireless connectivity (5G/b5G) for seamless data collection and processing across interconnected industrial facilities and Cyber-Physical Systems. However, implementing IIoT systems involves the integration of diverse technologies, resulting in the collection of data that may be incomplete, unstructured, redundant, or noisy. This situation gives rise to security vulnerabilities and challenges related to the quality of data within these systems.

Deploying anomaly detection systems is an effective approach to ensuring data integrity. These systems provide specific insights to determine whether a device is malfunctioning, if a critical event is unfolding, or if there is a breach in the system's security. By employing early anomaly detection mechanisms, the IIoT system can avoid being influenced by anomalous data when making decisions.

A. Cybersecurity Attacks in IIoT and 5G

This subsection presents a listing of known cybersecurity attacks against systems utilizing IIoT and 5G net-

This work has received funding from the European Union Horizon Europe research and innovation programme under grant agreement No. 101057083 – Zero-SWARM.

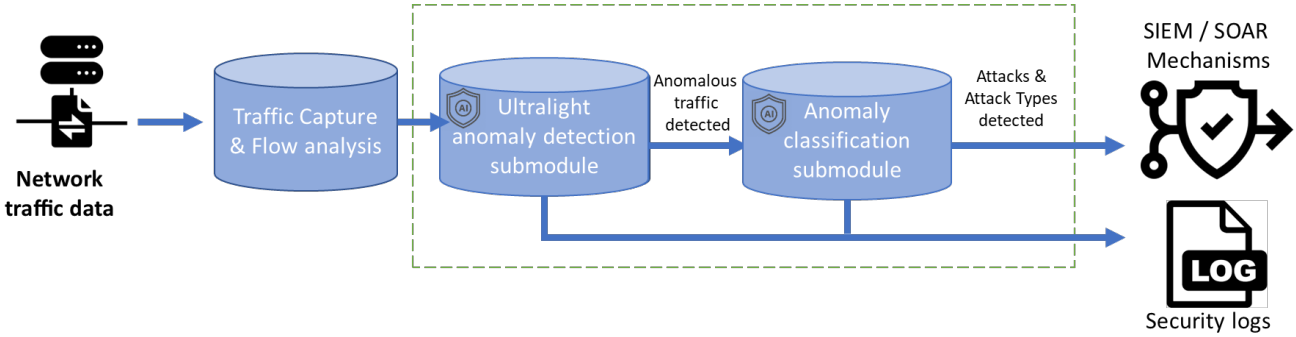

Fig. 1. High level architecture of the proposed approach.

TABLE I
CYBERSECURITY ATTACKS FACED BY IIOT/5G NETWORKS MAPPED TO OSI LAYER

Type	Layer	Attacks
Network Attacks	Network Layer	Traffic Analysis, Wormhole, Sybil, RFID Spoofing and Unauthorized Access, WLAN spoofing, Routing Information, Man in the Middle/ Eavesdropping, Selective Forwarding, Replay, Sinkhole, DoS/ DDoS, Threats to Neighbour Discovery Protocol, Impersonation
	Session Layer	Denial/ DDoS
	Transport Layer	Desynchronization, SYN flood
Software Attacks	Application Presentation Layer	Virus, Worms, Trojan Horses, Spyware, Ransomware, Cryptojacking
	All Layers	Misuse of audit tools
Data Attacks	Presentation Layer	Data Inconsistency
	Session Layer	Unauthorized Access (Remote to Local , User to Root)
	Network Layer	Data Inconsistency, Data Breach, Network virtualisation bypassing:
	Data Link Layer	Data Transit attack

works, based on [3]–[9]. These attacks are summarized in Table I. Cybersecurity attacks can be classified into Network, Software, and Data Attacks, and can be mapped to the seven layers of the OSI reference model [10].

Network attacks involve the manipulation of the functionalities of the network to gain access to sensitive or private or cause problems to the normal network operations. Software attacks, as the name implies are attacks that utilize software, many times self-propagating to exploit and introduce vulnerabilities into a system or interrupt its' normal operations. Finally, data attacks are the types of attacks that affect data integrity or ownership in the system examined.

B. Anomaly Detection and Classification in 5G/B5G Networks

The ongoing development of 5G (and beyond) networks is geared towards accommodating increased data capacity, increased number of connected devices, more densely populated networks, all while delivering reduced latency and lower power consumption compared to existing network generations. 5G upon fully realized deployment, will enable a wide array of vertical markets and industries to introduce a variety of new, diverse services along with new or not realized diverse threats against them.

Network anomaly detection in older generation networks is a well-studied subject and the approaches utilized can fall into three different categories [11]: a) manual detection of the anomalies based on expert opinion, b) measuring of network related metrics and based on predefined thresholds define benign and anomalous traffic and c) utilization of Machine Learning algorithms that are trained to recognize normal and abnormal traffic. The first two options are considered outdated [12] as they cannot keep up with the complexity and the scales of modern networks. However experimental studies [12] show that even ML based methods may not be able to keep up with the traffic density and throughput required by 5G/B5G networks.

Literature [11] suggests that Deep Learning (DL) is the ideal approach to address the problem of anomaly detection in 5G/B5G networks: DL-based methods achieve SotA results in the task. Additionally, classic ML classification algorithms typically rely upon feature engineering methods to reduce the dimensionality of their input while DL algorithms can automatically extract high-level features from large amounts of raw data, preventing overfitting based on regularization techniques. There are numerous applications of DL algorithms to detect anomalies in 5G networks: e.g. in [11] the authors utilize a stack of self-attention based networks. In [11], the authors suggest a two-phase scheme: A Long Short-Term Memory Recurrent Network (LSTM) is used to detect the anomaly, while a DNN composed by a Deep Belief Networks (DBN) and Stacked AutoEncoders (SAE) is utilized to classify the anomaly into a specific category. In [13], the network flow data is treated as an image, inputted to a Residual U-

Net Architecture, in an attempt to better model time dependent features without delays. In [14], a Variational Autoencoder (VAE) using Convolutional Neural Networks (CNN) is used to detect and classify the anomalies.

C. Anomaly Detection and Classification in IIoT Networks and CPS

Early detection of anomalies in an industrial process is essential to implement decisions based on real-time information, thus reducing maintenance costs, minimizing machine downtime, increasing safety, and improving product quality [1].

A recent literature review of approximately 100 papers published after 2018 about IIOT anomaly detection [15], showed that DL methods make up 56.5% of the proposed approach. Approximately, 22% of the remaining papers proposes statistics-based methods (e.g., Kalman Filters, Fourier Transformations, Markov Chains) and finally 21% utilizes ML based methods (e.g., Decision Trees, SVM, Density-Based Spatial Clustering of Applications with Noise (DBSCAN)). Concerning the DL based methods [15] , shows that Transformers are most common type of NN utilized, followed by Variational Autoencoders and LSTM Long-Short Term Memory) networks.

Authors in [16] propose the use of Graph DNN for network anomaly detection and presents examples for three industrial use cases: smart transportation, smart ener-gy, and smart factory. In [17] it is proposed to use a two-stage distributed approach that combines Autoencoder DNNs for traffic compression and the AdaBoost ML algorithm for the classification of the traffic to anomalous and benign. In [2] an approach is presented that utilizes Fully Connected DNN to detect anomalies in two Cyber-Physical Systems and showcases that generating synthetic adversarial data and retraining the DNN utilizing them, results to improved performance. In [3], the authors present a multi-stage, low latency module for a) the detection, b) the classification and c) the response against attacks against mission-critical Smart Factory Networks. The same paper shows that Multi-Layer Perceptron Models (MLP) perform better from RNN, LSTM and CNN networks for anomaly detection, while CNN networks outperform the same networks for attack classification models. Finally, an Intrusion Response System (IRS) uses a predefined rule set where each type of attack is linked to a specific single countermeasure. The topic of proactive anomaly detection to secure the 5G enabled IIoT ecosystem is a hot topic of research and innovation in the Information and Communications Technology (ICT) industry [18] . There is a race to introduce proactive anomaly detection solutions that can automatically and adaptively introduce security measures for unforeseen future attacks and enforce appropriate security measures to protect the IIoT network against them. The following section contains our proposed model.

III. Proposed Model

This section contains a presentation of the architecture functionalities of the three sub-modules of the Anomaly Detection (AD) module: First the Ultralight Anomaly Detection (UAD) sub-module which detects anomalies by monitoring network traffic. Then the Anomaly Classification (AC) submodule which discerns if the pattern of a detected anomaly corresponds to known attacks. Finally, the Deep Packet Inspection (DPI) submodule tools allows the system operator to further gain knowledge about unknown anomalous traffic detected. Our approach, is based on the combination of multiple methods that result in a SotA approach:

- The multi-stage approach of [3], [14], to ensure rapid anomaly detection and robust anomaly classification.
- The training approach proposed by [2], and [14] i.e., the utilization of synthetic training data creation to enhance model performance. However we propose the use of SotA Autoencoder models, i.e. Conditional Variational Autoencoder (CVAE) presented in section III-A instead of the Fast Gradient Signed Method.
- We build on the findings of [13] which showed successful application of 1D CNN in anomaly detection on 5G data. We apply a similar 1D CNN presented in III-A, to IIoT related data.
- We build on the findings of [14] who combined autoencoders with 2D CNN also for attach type classification in 5G data. We advance this approach by using more modern variant CNN, called Dilated Causal CNN (DCCNN) [19] , presented in section III-B, to IIoT related data.

A. Ultralight Anomaly Detection submodule

Swift anomaly detection in network traffic is essential for securing systems, enabling faster mitigation against malicious activity. Anomalous traffic may indicate attacks, malfunctions, or hardware errors. Network traffic anomaly detection has been extensively researched: The available literature suggests that artificial intelligence extends better to large-scale intrusion data with higher dimension compared to 'traditional' ML methods. The submodule receives raw traffic data as input, captured in real time. A high level overview of the functionality and I/O of the submodule is shown in Figure 1. The following traffic related features are then calculated and taken into consideration, as proposed by [20]: Basic Flow Features e.g. Destination Port, Protocol, Flow Duration, Total Forward Packets, along with inter-Arrival Time (IAT) Statistical Metadata e.g. Flow IAT Mean, Standard Deviation etc. Let $X \in \mathbb{R}$ be the input data containing Basic flow data and IAT Statistical metadata described earlier, and $C \in \{\text{Benign}, \text{Anomalous}\}$ the class labels associated with it. Let $Q_\phi(Z|X,C)$ and $P_\Theta(X|Z,C)$ be the Encoder and Decoder networks, and ϕ, θ be learnable parameters.

The purpose of the encoder is to use X, C to create a latent variable $Z \sim Q_\phi(Z|X,C)$. In the decoding phase,

the latent variable Z and $c \in C$ are utilized as inputs to generate new samples for label c, $\hat{X} \sim P_\Theta(X|Z,C)$.

The Log-Cosh CVAE utilizes the following objective function:

$$L_{\text{log-cosh}}(X,\hat{X}) = \frac{1}{a}\sum_i \log\left(\cosh\left(a(X_i - \hat{X}_i)\right)\right) \quad (1)$$

where $a \in \mathbb{R}$ is a hyper-parameter, $X_i \in X$, and $\hat{X}_i \in \hat{X}$ are the i-th elements of X and $\hat{X}$, respectively.

Finally, the comprehensive loss function for the model is:

$$\begin{aligned} L(\phi,\theta;X,C,a) = {} & L_{\text{log-cosh}}(X,\hat{X}) \\ & - D_{\text{KL}}\left[Q_\phi(Z|X,C) \parallel P_\Theta(X|Z,C)\right] \end{aligned} \quad (2)$$

where D_{KL} denotes the Kullback–Leibler divergence. Collecting benign traffic data for a network is a trivial process. By generating $\hat{X}$ for anomalous traffic data we can create a labelled dataset S that is balanced for all $c \in C$, created by merging, $\hat{X}$, X, C . This is utilized to train a lightweight 1D Convolutional CNN that performs binary classification. This classifier is then used to discern between anomalous and benign traffic. This the same approach proposed in [21], which to our knowledge has not been tested in IIoT and 5G network traffic.

B. Anomaly Classification submodule

After an anomaly is detected by the UAD, the next step is to try and discern a) the type of anomaly and b) in the case of a cyber-threat, its' type. Correct recognition concerning the types of attacks faced by the system is essential to select the appropriate countermeasures to mitigate them. Moreover, this tool helps to monitor cases of false positives: Benign traffic identified as anomalous might indicate that the UAD submodule needs retraining. The submodule receives the segments of traffic recognized as anomalous by the UAD and uses the same features as it to try and classify the anomalous traffic to three classes: 1. Attack when the pattern of the traffic corresponds to a known attack type, 2. Benign when the pattern of the traffic corresponds to normal traffic i.e., a false positive. 3. Unknown, which warrants more inspection by the system operator.

CNNs segment the input data using so called filters, which allows them to learn specific patterns. Contrary to other types of DNN e.g., LSTM, CNN are by design not fully connected. This meaning that the not all nodes of the network relate to one another thus less calculations are required and CNN are less computationally expensive. Simple CNN have been shown to effectively model multi-dimension patterns and capture the high temporal correlation of traffic data. A special case is the DCNN: In this variant of the CNN, the filters are applied by skipping certain elements in the input, allow the receptive field of the network to grow exponentially [19]. This property

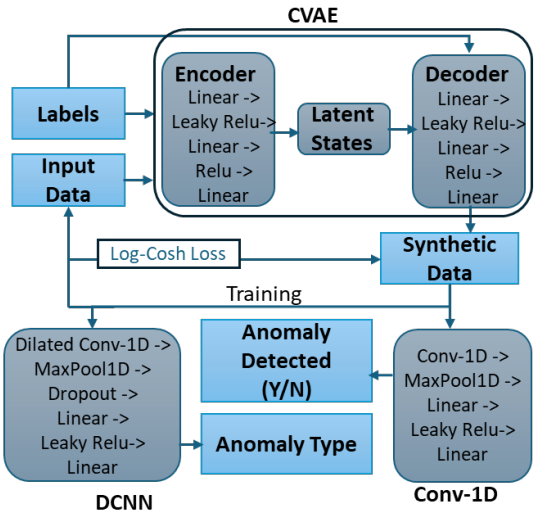

Fig. 2. High level architecture of the Neural Networks.

allows them to model even sparse data along with both long-term and short sequence relationships present.

Let $X = \{X_{t-(k-1)}, X_{t-(k-2)}, X_{t-1}, X_{t-(k-1)}\}$ be the input data, i.e., a time series of consecutive observations of anomalous traffic data, with $k \in \mathbb{N}$ being the kernel size, $t \in \mathbb{N}$ being the time window size (i.e., the number of observations in the time series), and O_t the output obtained using the values from X. The dilated causal convolution operations over the network layers are described by the following equation :

$$x_l^t = g\left(\sum_{k=0}^{K-1} w_l^k x_{l-1}^{(t-(k\cdot d))} + b_l\right) \quad (3)$$

where x_l^t is the output of the neuron at position t in the lth layer, K is the width of the convolutional kernel, w_l^k represents the weight at position k, d is the dilation factor of the convolution, and b_l is the bias term.

IV. Performance Evaluation

The following subsection presents the lab evaluation results concerning the modules discussed in section III, i.e. the UAD and the AC modules.

A. Experimental Setup

The proposed algorithms were evaluated in multiple, modern, publicly available datasets. In all cases, the algorithms were written in python, while the Deep Neural networks used utilize the Pytorch Deep learning framework. To optimize the hyper-parameters of the algorithms used, the number of layers and the window size of the input data for the DCCN, a SotA Bayesian hyper-parameter optimization algorithm, the Tree-structured Parzen Estimator was utilized [22]. In all cases the datasets where split into two parts: 70% percent of data was used for training while the remaining part was used for testing the algorithm. The split was done in a stratified manner

TABLE II
Low Footprint Dataset Results

	Algorithm	Accuracy	F1-score	Inference Time
Anomaly Detection	CONV-1D + CVAE (proposed)	0.925	0.9441	0.0428
	CONV-1D	0.922	0.9447	0.0421
	Random Forest	0.6516	0.6636	0.2935
	SGD	0.6353	0.6351	0.0640
	MLP	0.6259	0.6231	0.2958
Anomaly Classification	DCNN + CVAE (proposed)	0.72121	0.756	0.11095
	DCCN	0.71888	0.695755	0.1276
	Random Forest	0.667003	0.360698	0.44075
	SGD	0.577754	0.194291	0.09494
	MLP	0.399633	0.115552	0.29222

ensuring that all classes were represented in both the training and the testing phases. The following ML and DL algorithms were used to compare and evaluate the results of our proposed algorithms: Random Forest, MLP NN and Stochastic Gradient Descent (SGD). The proposed high level architectur of the NNs is shown in Figure 2

B. Experimental Results

The following results demonstrate that, in all cases, the proposed algorithms either outperform or match the performance of other commonly used algorithms for the same tasks, with metric differences such as accuracy being less than 0.01. Additionally, the proposed algorithms are relatively fast, performing the classification task in less than 0.5 seconds. Moreover, we see that using synthetic data for training, produced by the CVAE enhances the algorithms performance.

1) Low Footprint attacks: UNSW-15 is a publicly available dataset that commonly used to train and evaluate AD systems in the IIoT context [23] .This dataset contains normal traffic as well as nine different attack types i.e. network Analysis, Backdoor utilization, DoS attack, Exploit based attacks, Generic against Hash Functions, network Reconnaissance, Fuzzers for anomalous activity, Shellcode attacks, and Worm attacks. Most of these attacks have a low footprint, meaning that their network presence is sparse or that they change their traffic pattern over time to behave in a manner like benign traffic. This characteristic makes the attacks described here harder to detect and classify. Table II contains the results.

2) Traffic over 5G network: The 5G-NIDD is an open dataset that describes real network data collected from 5G base stations [24], including Next Generation Node B (gNB), Evolved Node B (eNB), a Multi-access Edge Computing (MEC) station and an 5G Core. It contains both normal (benign) traffic along with 8 attack types that can be categorized either as DoS/DDoS attack types, or Port Scan attack types. Table III contains the results.

3) Attacks against a 5G Core: The 5GAD-2022 is a dataset that captures network traffic data [25], in the context of a third-party attacking a 5G Core (free5GC): In addition to normal traffic it contains 6 attack types

TABLE III
Traffic over 5G Results

	Algorithm	Accuracy	F1-score	Inference Time
Anomaly Detection	CONV-1D + CVAE (proposed)	0.9999	0.9999	0.0416
	CONV-1D	0.9984	0.9987	0.043893
	Random Forest	0.9962	0.9962	0.129
	SGD	0.9925	0.9925	0.07945
	MLP	0.9954	0.9953	0.06883
Anomaly Classification	DCNN + CVAE (proposed)	0.9805	0.9815	0.1421
	DCCN	0.09976	0.9530	0.1392
	Random Forest	0.9797	0.9065	0.2193
	SGD	0.9774	0.9661	0.1188
	MLP	0.9345	0.496	0.1413

TABLE IV
Attacks against a 5G Core Results

	Algorithm	Accuracy	F1-score	Inference Time
Anomaly Detection	CONV-1D + CVAE (proposed)	0.9993	0.9994	0.1517
	CONV-1D	0.9961	0.996	0.1529
	Random Forest	0.9993	0.9994	0.1413
	SGD	0.8819	0.9073	0.0068
	MLP	0.9791	0.9828	0.0378
Anomaly Classification	DCNN + CVAE (proposed)	0.9855	0.9877	0.1421
	DCCN	0.9812	0.9917	0.1392
	Random Forest	0.9797	0.9065	0.2193
	SGD	0.9774	0.9661	0.1188
	MLP	0.9345	0.4960	0.1234

that can be categorized in the following categories: Reconnaissance Attacks, Network Reconfiguration Attacks, and DOS attacks. The attacks target the various network functions that comprise the 5G Core such as the Access and mobility management function (AMF) and the network repository function (NRF). Table IV contains the results.

4) Attacks in OPC-UA M2M communication: This dataset describes traffic in an IIoT environment, and more specifically traffic captured during Machine-to-Machine (M2M) communications that utilize the OPC-UA protocol [26] which is considered one of the most important communication protocols for Industry 4.0 and IIoT. Apart from the normal traffic, it contains traffic produced during the execution of three different attack types i.e., DoS, Man-in-the-middle and Spoofing/impersonation attacks. Table V contains the results.

V. Conclusions and Further Challenges

We propose an anomaly detection system specifically tailored for the cybersecurity needs of 5G-enabled IIoT networks. Our approach, combining deep learning techniques such as two different variants of CNN and CVAE, shows superior performance in identifying and classifying anomalous traffic patterns across multiple datasets related to the I4.0 context. Experimental results show that our

TABLE V
Attacks in OPC-UA M2M communication Results

	Algorithm	Accuracy	F1-score	Inference Time
Anomaly Detection	CONV-1D + CVAE (proposed)	0.9999	0.9999	0.0504
	CONV-1D	0.9999	0.9999	0.0514
	Random Forest	0.9999	0.9999	0.009
	SGD	0.9999	0.9999	0.0015
	MLP	0.9998	0.9998	0.0048
Anomaly Classification	DCNN + CVAE (proposed)	1	0.9999	0.05
	DCCN	1	0.9999	0.0504
	Random Forest	1	0.9999	0.0089
	SGD	1	0.9999	0.0015
	MLP	0.9998	0.9999	0.0048

approach achieves high accuracy in anomaly detection and classification with sub-second inference times, making it suitable for real-time applications in critical infrastructures..

Future research will aim to extend the capabilities of the proposed system by testing the method in advanced attack simulations within real industrial environments and refining the deep learning models to handle emerging security threats more effectively. There we aim to extensively test the scalability of the proposed solution, using an agent based approach for the deployment of our mechanisms. Additionally, we aim to integrate automated anomaly mitigation methods to further enhance system resilience against evolving cyber-attacks in complex industrial ecosystems.

Acknowledgment

This work is supported by the European Unions Horizon 2020 Research and Innovation Program through the ZeroSWARM project under Grant Agreement No. 101057083. The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the European Commission.

References

[1] B. Weinger, J. Kim, A. Sim, M. Nakashima, N. Moustafa, and K. J. Wu, "Enhancing iot anomaly detection performance for federated learning," *Digital Communications and Networks*, vol. 8, no. 3, p. 2022, 2022.

[2] Z. Jadidi *et al.*, "Security of machine learning-based anomaly detection in cyber physical systems," in *2022 International Conference on Computer Communications and Networks (ICCCN)*, 2022.

[3] P. Illy and G. Kaddoum, "A collaborative dnn-based low-latency idps for mission-critical smart factory networks," *IEEE Access*, vol. 11, pp. 96 317–96 329, 2023.

[4] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.

[5] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial iot: A survey on attacks and countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, March 2021.

[6] J. P. Mohan, N. Sugunaraj, and P. Ranganathan, "Cyber security threats for 5g networks," in *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022.

[7] M. Hasan *et al.*, "A review on security threats, vulnerabilities, and counter measures of 5g enabled internet-of-medical-things," *IET Communications*, vol. 16, pp. 421–432, 2022.

[8] C. Silpa, G. Niranjana, and K. Ramani, "Securing data from active attacks in iot: An extensive study," in *Proceedings of International Conference on Deep Learning, Computing, and Intelligence*, ser. Advances in Intelligent Systems and Computing, G. Manogaran, A. Shanthini, and G. Vadivu, Eds. Springer, 2022, vol. 1396.

[9] European union agency for cybersecurity, "Enisa threat landscape for 5g networks," 2022.

[10] J. D. Day and H. Zimmermann, "The osi reference model," *Proceedings of the IEEE*, vol. 71, no. 12, pp. 1334–1340, December 1983.

[11] L. Fernández Maimó, Á. L. Perales Gómez, F. J. García Clemente, M. Gil Pérez, and G. Martínez Pérez, "A self-adaptive deep learning-based system for anomaly detection in 5g networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018.

[12] L. Lei, L. Kou, X. Zhan, J. Zhang, and Y. Ren, "An anomaly detection algorithm based on ensemble learning for 5g environment," *Sensors*, vol. 22, no. 19, p. 7436, Sep. 2022.

[13] M. Doan and Z. Zhang, "Deep learning in 5g wireless networks - anomaly detections," in *2020 29th Wireless and Optical Communications Conference (WOCC)*, 2020.

[14] Y. Yuan, J. Yang, R. Duan, I. Chih-Lin, and J. Huang, "Anomaly detection and root cause analysis enabled by artificial intelligence," in *2020 IEEE Globecom Workshops (GC Wkshps)*, 2020.

[15] M. Rodríguez, D. P. Tobón, and D. Múnera, "Anomaly classification in industrial internet of things: A review," *Intelligent Systems with Applications*, vol. 18, 2023.

[16] Y. Wu, H.-N. Dai, and H. Tang, "Graph neural networks for anomaly detection in industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9214–9231, Jun. 15 2022.

[17] M. Zolanvari, A. Ghubaish, and R. Jain, "Addai: Anomaly detection using distributed ai," in *2021 IEEE International Conference on Networking, Sensing and Control (ICNSC)*, 2021.

[18] H. Alameddine, T. Madi, and A. Boukhtouta, "How proactive anomaly detection secures 5g networks," 2021. [Online]. Available: https://www.ericsson.com/en/blog/2021/8/proactive-anomaly-detection

[19] Y. He and J. Zhao, "Temporal convolutional networks for anomaly detection in time series," in *Journal of Physics: Conference Series*, vol. 1213, no. 4. IOP Publishing, 2019, p. 042050.

[20] R.-H. Hwang, M.-C. Peng, C.-W. Huang, P.-C. Lin, and V.-L. Nguyen, "An unsupervised deep learning model for early network traffic anomaly detection," *IEEE Access*, vol. 8, pp. 30 387–30 399, 2020.

[21] X. Xu, J. Li, Y. Yang, and F. Shen, "Toward effective intrusion detection using log-cosh conditional variational autoencoder," *IEEE Internet of Things Journal*, vol. 8, no. 8, 2021.

[22] S. Watanabe, "Tree-structured parzen estimator: Understanding its algorithm components and their roles for better empirical performance," *arXiv preprint arXiv:2304.11127*, 2023.

[23] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6.

[24] S. Samarakoon, Y. Siriwardhana, P. Porambage, M. Liyanage, S.-Y. Chang, J. Kim, J. Kim, and M. Ylianttila, "5g-nidd: A comprehensive network intrusion detection dataset generated over 5g wireless network," 2022. [Online]. Available: https://dx.doi.org/10.21227/xtep-hv36

[25] C. Coldwell, D. Conger, E. Goodell, B. Jacobson, B. Petersen, D. Spencer, M. Anderson, and M. Sgambati, "Machine learning 5g attack detection in programmable logic," in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 1365–1370.

[26] R. Pinto, "M2M using OPC UA," March 24 2020, iEEE Dataport. [Online]. Available: https://dx.doi.org/10.21227/ychv-6c68