ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5G Specific Threats Evaluation using Dataset-Driven Approach in IIoT

Rohan Rajoriya[1*], Megha Kamble[2]
[1]*Research Scholar, School of CST, LNCT University, Bhopal, India*
[2]*Professor, School of CST, LNCT University, Bhopal, India*
* **Corresponding Author:** rohanrajoriya@gmail.com

ARTICLE INFO

Received: 24 Dec 2024

Revised: 19 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

The advancement of fifth-generation (5G) technology is facilitating the expansion of the Internet of Things (IoT), which is becoming complicated when blended with industrial operations in terms of secured communication over 5G networks or imminent technologies. Industrial IoT (IIoT) applications in the 5G era provide massive connectivity with ultra-low latency and enhanced mobile broadband, leading to the inception and awareness of numerous 5G security challenges apart from various traditional security concerns. This work highlights the significance of using a dataset-driven methodology to study, discuss and evaluate various 5G network performance metrics of the derived augmented dataset in 5G-enabled IIoT network scenarios, which is achieved by integrating distinct 7 new features/labels and simulating various 5G-specific security attacks such as jamming attacks, network slicing exploits and service-based architecture (SBA) vulnerabilities, primarily on and over the ML-Edge-IIoTset dataset.

Keywords: 5G-IIoT, Dataset, 5G-specific attack: Jamming, Slicing exploit, SBA exploit.

INTRODUCTION

Background

5G-Enabled IIoT & Industry 4.0: The next phase of industrial change is being driven by the combination of 5G technology with Industrial IoT (IIoT) revolutionized Industry 4.0.(Ahmed et al., 2023). Significant connectivity enhancements that 5G offers are Ultra-Reliable and Low-Latency Communications (URLLC), Enhanced-Mobile Broadband(eMBB), Massive Machine-Type Communications(mMTC). (Shafi et al., 2017). These characteristics make it possible for billions of IIoT devices including sensors, actuators, robotics, and cloud systems to communicate with one another seamlessly. (Zhukabayeva et al., 2025) in smart factories, healthcare, grids to automate supply chains systems. (Chalapathi G. S. S.and Chamola, 2021).

5G-Enabled IIoT (Figure 1) offers Real-time industrial automation, autonomous vehicles and robotics systems depend on low latency and high bandwidth that facilitates data-intensive applications like forecasting repairs and continuous surveillance, network slicing by which it's possible to build virtual networks for particular industries, improve resource utilisation, and assure traffic split. (Mahmood et al., 2022)

5G-enabled IIoT is the foundation of Industry 4.0, facilitating sophisticated automation, predictive maintenance and intelligent decision-making that improves operational efficiency, decreases downtime and stimulates productivity. (Chandra Shekhar Rao et al., 2021).

Our study reveals vulnerabilities caused by 5G-specific attacks on IIoT dataset with the motivation, objective and significance of the study. Further, section discusses previous research and studies and identifies gaps for our problem. Lastly, propose a methodology and based on that, discuss the results outcome with limitations and finally conclude the work.

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

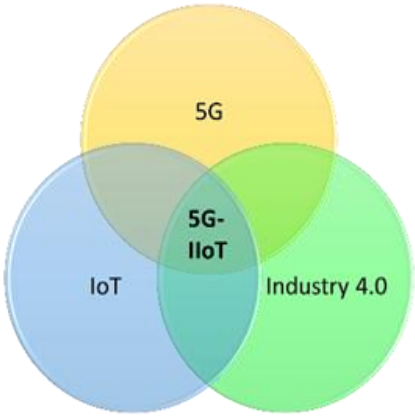

Figure 1. 5G-IIoT

Security threat caused from 5G network vulnerabilities: Although there are many advantages while adopting 5G-enabled IIoT, but there are also a number of security risks that might compromise industrial operations. 5G networks' openness and complexity introduce new weaknesses that malicious actors could take advantage of.

a. Jamming Attacks: 5G networks are wireless due to which they are vulnerable to jamming attacks, hackers overload the network with noise to obstruct transmission which can lead to high latency, packet loss and communication breakdowns in IIoT contexts, which can lead to negatively impact vital systems like automated manufacturing and robotics. (Gallenmüller et al., 2020)
b. Service-Based Architecture (SBA) Exploits: Using APIs, the 5G SBA enables dynamic network service management. Weak API security, on the other hand, can result in unauthorised API calls which can allow attackers to take control of devices, service interrupt, or retrieve secret data (Wehbe et al., 2023)
c. Network Slicing Exploits: Specialised virtual networks made possible by 5G network slicing could be vulnerable to illicit access or inter-slice attacks. By using inadequate isolation strategies between slices, attackers can get access to essential infrastructure and thereby cause resource depletion or service disruptions. (De Alwis et al., 2024)
d. Insider Threats: 5G network management is more complicated can lead to insider threats (attacks by someone inside the company) with access to insightful key infrastructure are more likely to occur. (Azad et al., 2024).

To safeguard industrial processes, data privacy, and service availability, it is imperative that these environments be secured against cyber attacks as IIoT devices are increasingly connected to 5G networks.

Motivation and Problem Statement

5G-Specific Attack Scenarios in Existing IIoT Datasets: The security environment for these systems has become more complicated as 5G networks and Industrial IoT (IIoT) continue to recast industries. Although a number of IIoT security datasets including WUSTL-IIOT-2021(Zolanvari et al., 2019), X-IIoTID(Al-Hawawreh et al., 2022), and Edge-IIoTset(Ferrag et al., 2022) has been created for threat detection mainly focus on traditional threats(DoS, Botnet, network flood etc.) and model training, the majority of current datasets are not well enough to explore the unique security issues that emerge in IIoT environments enabled by 5G and its features. In order to comprehend the distinct dangers faced by the next generation of connectivity, these datasets frequently lack 5G-specific attack scenarios related with jammer attacks, network slicing exploits and SBA vulnerabilities to develop next gen security framework intrusion detection system(IDS).

Evaluating vulnerabilities by dataset driven approach: With the commencement of 5G, assessing and preventing new attack vectors requires a dataset-driven approach for security analysis. Specifically, jamming, network slicing exploits, and SBA vulnerabilities are attack vectors that can significantly disrupt 5G-enabled IIoT

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

systems. However, evaluating these specific threats requires specific datasets enriched with real-world attack patterns that reflect the operational characteristics of 5G networks.

The 5G network faces threats from jamming attacks, network slicing exploits, and Service-Based Architecture (SBA) vulnerabilities where Jamming attacks can impact URLLC, affecting network latency, throughput, and packet loss. Network slicing exposes critical services to DoS attacks or resource exhaustion. SBA vulnerabilities can lead to utilizing APIs, exploited by attackers to disrupt critical services. A dataset-driven evaluation of API anomalies and unauthorized access attempts is crucial for assessing network resilience. Augmentation of (Edge-IIoTset) information with these 5G-specific attack scenarios helps one evaluate 5G network vulnerabilities comprehensively and grasp the influence of these hazards on industrial systems. This method will enable the creation of more efficient IDS, security policies and mitigating techniques catered for 5G enabled IIoT.

Objectives

Simulated 5G-specific attacks by Extending Edge-IIoTset dataset: The main goal of this work is to introduce reasonable 5G-specific attack scenarios hence extending the current Edge-IIoTset dataset. Inspecting security concerns in IIoT contexts starts with an existing Edge-IIoTset. However, It does not include the specific weaknesses of 5G-enabled IIoT networks such SBA vulnerabilities, network slicing exploits, and jamming attacks.

Attack Scenarios: This effort consists of simulating 5G-specific attacks to expand the dataset and increase its relevance to 5G-IIoT security. Among these simulated attacks are:

- Jamming Attacks: generating high latency and packet loss so as to affect communication.
- SBA Exploits: Targeting API flaws to disturb service-based communication
- Network Slicing Exploit: Weak isolation between virtual network slices allows one to create resource depletion or DoS attacks

These attack forms will help the augmented dataset to reflect the security issues experienced by 5G enabled IIoT networks more precisely.

5G-Specific Attacks impact measurement: Measure impact of the 5G-specific attack scenarios on network performance and dependability comes next once they have been replicated and fed into the augmented dataset. That is- extending Edge IIoTset. Understanding the risks these assaults create to real-world 5G-IIoT installations depends on knowing how they influence important performance criteria. Below are benchmark for review:

- Latency: Particularly in URLLC in important IIoT applications, jamming attack affect the latency of communication.
- Packet Loss: The degree of packet loss resulting from network slicing attacks and jamming will determine the dependability and stability of data flow.
- System Service Response: Especially for dynamic service management in 5G networks, SBA vulnerabilities affect service availability and API integrity.

This aim will enable a thorough investigation of the performance degradation brought about by these attacks and give understanding of the flexibility of 5G-enabled IIoT systems under reasonable threat conditions. The results will help to pinpoint network weak points, thereby facilitating the creation of more strong security solutions for 5G enabled IIoT scenarios.These goals seek to augment the Edge-IIoTset dataset with 5G-specific attack by means of quantitative analysis of their effects on network performance, therefore opening the path for the creation of better security frameworks and models for 5G-enabled IIoT systems.

Contributions

a. 5G specific attack scenario development: Designed and simulate attack scenarios specific to 5G-enabled IIoT networks, including SBA vulnerabilities, network slicing exploits, and jammer assaults.
b. Real-World IIoT Security Testing Dataset Augmentation: Improve the Edge-IIoTset by including 5G-specific attack patterns, therefore so as to be better suited for testing security models in 5G-IIoT real world scenario.
c. Impact analysis of packet loss and latency: Examined how 5G-specific attacks affected important performance indicators including latency, packet loss and network dependability and performance in practical environments.

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

LITERATURE REVIEW

IIoT Security Risks from 5G : Due to its advanced features and network design, 5G enabled IIoT technology poses security risks. The primary vulnerabilities in the following lead to network slicing exploits, jamming and packet loss, SBA exploits and insider attacks. Henceforth, 5G-enabled IIoT networks need better security and mitigation. Table 1 states a few studies related to 5G-specific attacks under IIoT environments

SNo.	Resource	5G Specific Attack Category			Industrial IoT Context	Conclusion
		Network Slicing	Jamming	SBA Vulnerabilities		
1	(Porambage & Liyanage, 2020)	Y	N	N	N	Discuss unwanted access, Data breaches, DoS and DDoS attack on slices
2	(De Alwis et al., 2024)	Y	N	N	N	Discuss NS security challenges and issues such as NS life-cycle security and inter- and Intra slice security, slice broker security and ZSM security
3	(Wu et al., 2022)*	Y	N	N	Y	Presented architecture for intelligent NS management for IIoT : smart transportation, smart energy, smart factory.
4	(Savadatti et al., 2024)	N	Y	N	N	Case Study validating 6 dimension taxonomy for 5G Jamming attacks.
5	(Ma et al., 2023)*	N	Y	N	Y	Proposed resilience control method-based event-triggered control (ETC) to minimise jamming attack's effect on the IIoT-based VCTS.
6	(Rehman et al., 2024)	N	Y	N	Y	Proposed FFL-IDS based on CNN for jamming and spoofing attack in IIoT.
7	(Liu et al., 2024)*	N	P	Y	Y	Constrained IIoT devices uses 5G federated LSTM autoencoder for anomaly detection and envision 5G

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

						Edge- IIoT architecture.
8	(Wehbe et al., 2023)	N	N	Y	N	Securing 5G SBA using HTTP/2 signalling protocol along with other web-based technologies (JSON, RESTful API) and security mechanisms.
9	(Li et al., 2022)	P	N	Y	P	Malicious attacks, data breaches and system compromises can result from IIoT supply chain vulnerabilities and privileged insiders
10	**Our Work***	Y	Y	Y	Y	Analyse 5G specific attack in Edge IIoT environment based on dataset driven approach
Notation – Y: Yes, N: No, P: Partial, *: Research						

Table 1. Available study for 5G-enable IIoT specific Attack

Identified gaps in 5G-specific attack simulation: Absence of realistic scenarios for 5G-specific threats, current IIoT security datasets and attack simulations mostly concentrate on typical IoT risks such as botnet attacks and network flooding. A few noted weaknesses include:

a. Absence of realistic 5G Attack Scenarios: Current datasets are not simulating 5G-specific vulnerabilities as SBA flaws, network slicing exploits or jamming attacks particular to the advanced architecture of 5G.
b. Limited Focus on 5G's New Features: Important features of 5G technology, like network slicing and URLLC are not adequately reflected in current attack simulations, therefore creating a major discrepancy in assessing the actual impact of these weaknesses.
c. Absence of Augmented Dataset: Comprehensive testing of security models for 5G-enabled IIoT networks is hampered by an absence of augmented datasets combining conventional IIoT attacks with 5G-specific attack types.

Attack Modeling in Network Security Research

Methods of Synthetic Attack Simulation: Synthetic attack simulations model network vulnerabilities. These tools help researchers replicate DoS attacks, ransomware, and jamming without running actual deployments at risk. attack models are widely used in many simulation models to assess the responses of network security systems to different attack situations, giving important data for security defenses and intrusion detection systems.

Requirement of Realistic Augmented Dataset to Study 5G-IIoT Threats: Realistic dataset augmentation is required to properly evaluate 5G-specific hazards in IIoT networks. Current datasets overlook 5G-specific attacks, including network slicing and SBA vulnerabilities. Creating more realistic attack models for 5G-enabled IIoT systems helps researchers improve security testing and develop IDS.

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

METHODOLOGY

Dataset Selection and Preprocessing

Edge-IIoTset Dataset Structure Overview: Comprising data from many network traffic sources, the Edge-IIoTset dataset is intended for IIoT security research. It covers 63 features, including attack types related to network protocol (TCP, UDP, HTTP, DNS, etc.), packet characteristics, and attack label-associated properties. Comprising 1,57,800 records, the ML dataset is designed to reflect both regular traffic and several attack forms, offering a complete basis for assessing security risks in IIoT systems.

Network Performance Metrics Features Selection: Network performance criteria are found important for thorough investigation:

- Latency: Essential for URLLC applications in 5G-IIoT, latency is the time delay in communication
- Packet Loss: Affecting network dependability, packet loss frequency during transmission.
- System Response Time: Using API Anomaly Score, the impact of System Response Time over several attack forms.

5G-Specific Attack Simulation

Jamming Attack Simulation: High latency and packet loss are modeled in this simulation to imitate jamming attacks. Especially impacting real-time IIoT applications like robotics and automated systems, these attacks overwhelm the 5G network with interference signals, therefore affecting communication.

Network Slicing Exploit Simulation: Targeting network slicing vulnerabilities, including prohibited access to various network slices, this simulation seeks to prevent resource depletion or inter-slice attacks. These attacks might cause DoS or disturbance of crucial services inside isolated network slices, therefore influencing service dependability and security.

SBA Exploit Simulation: Unauthorized API calls in the SBA exploit simulation let attackers control services or access private data. It also covers signaling abnormalities that interrupt service communication, hence causing service outages and failures in IIoT systems depending on 5G service layers for adaptive resource management.

Dataset Augmentation

Injection of Simulated Attacks into ML-Edge-IIoTset: The ML-Edge-IIoTset dataset is fed with simulated 5G-specific attacks, including SBA flaws, network slicing exploits, and jamming. This approach generates a more realistic depiction of 5G-enabled IIoT environments by adding 5G attack labels and matching network performance indicators (e.g., latency, packet loss), hence raising the dataset.

Ensuring Data Integrity and Class Balance: The implanted attack scenarios are meticulously crafted to mirror real-world circumstances in order to protect data integrity. Furthermore, by varying the assault frequency to prevent class imbalances, one guarantees that every attack type example: jamming, SBA exploit is sufficiently represented for efficient security model training.

Attack Impact Analysis by Performance Metric Evaluation

Latency and reliability evaluation due to attacks: The impact of 5G-specific attacks on network performance is evaluated by measuring latency (delay due to jamming) and reliability (due to packet loss and communication failure) metrics.

API Integrity and Performance Optimization: API lets you access sensitive data and services. Any unusual activity may indicate a cyberattack, data breach, or unauthorised access. Security and data confidentiality are protected via anomaly detection. Comparatively evaluating performance attack injection helps to evaluate network performance deterioration. Through this study, the impact of attacks on IIoT System Response using API anomaly is determined. Figure 2 proposed methodology for the work.

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

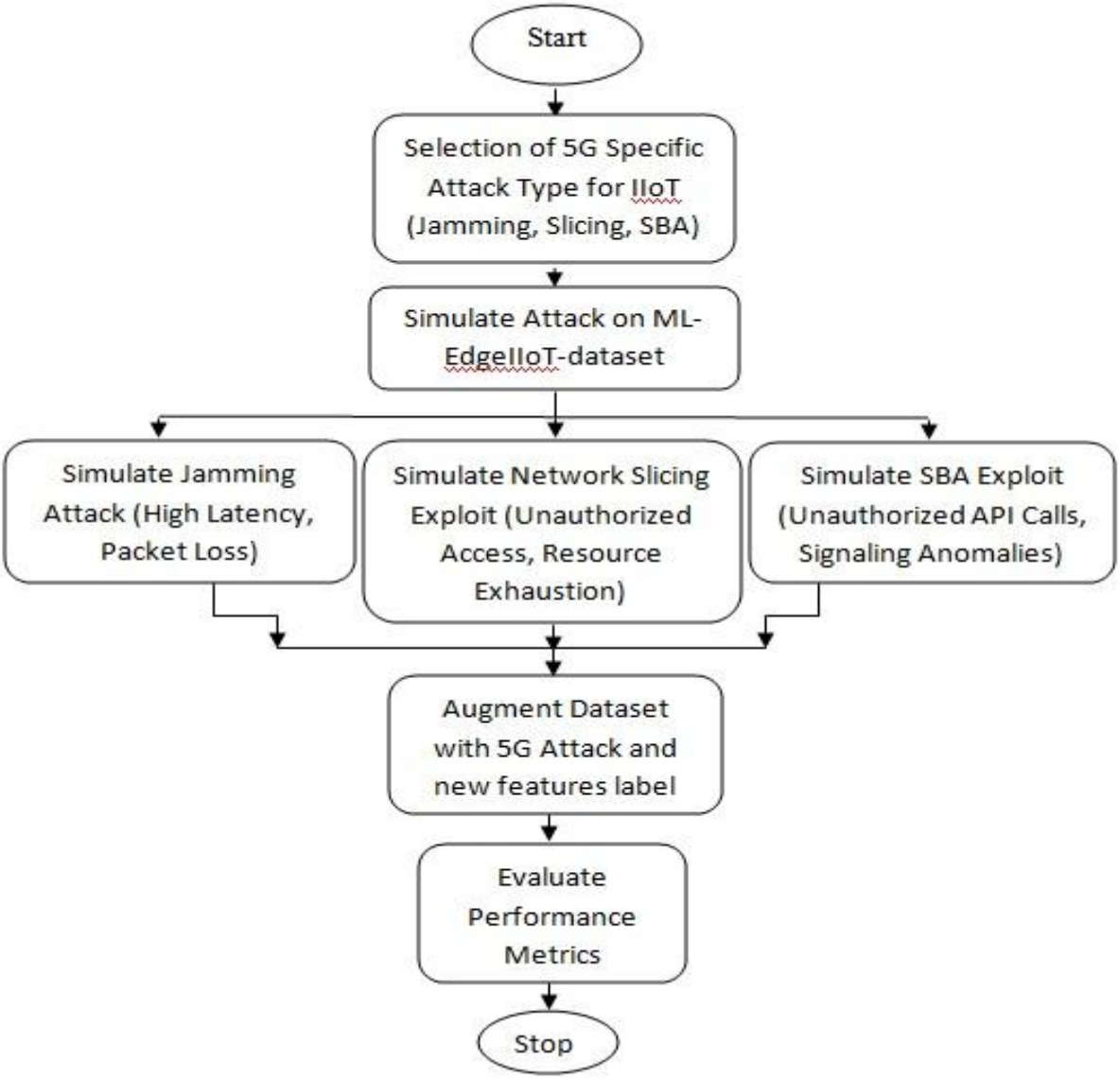

Figure 2. Proposed Methodology

RESULTS AND DISCUSSION

Dataset Validation and Characteristics Comparison

The original ML-Edge-IIoTset dataset is compared with the augmented dataset with attack scenarios tailored for 5G based on:

a. Distribution of feature: Evaluating how the insertion of additional features (latency, packet loss and 5G attack labels) affects the overall dataset.
b. Attack representation: To guarantee reasonable attack coverage in the augmented dataset, compare the frequency and variety of attack types e.g., jamming, network slicing exploits, SBA vulnerabilities.

Edge-IIoTset dataset contains Normal Traffic, Attack traffic and selected dataset for ML and DL.We have used ML-EdgeIIoT-Dataset.csv for our study. We have created Augmented-ML-EdgeIIoT-dataset.csv by adding 5G-specific attack features to the ML-EdgeIIoT-dataset.csv, it will be relevant for our study of 5G-specific threats (Jamming Attack, SBA Exploit and Slicing Exploit) at Edge IIoT networks. 5G-specific attack patterns can be successfully simulated without disrupting the integrity of the original data.

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

ML-EdgeIIoT-dataset.csv original features(63) provide critical information for modeling and simulating the impact of 5G-specific attacks on Edge IIoT networks, since they are injected into the same rows. The additional 7 new features in the augmented dataset(simulated_latency, packet_loss_rate, slice_id, traffic_conflict, api_anomaly_score, unauthorized_api_calls, 5GAttack_Type) as shown in Table 2 are prejudiced by the original dataset's columns like packet timestamps, TCP flags, HTTP request methods, mqtt.msg, sequence numbers, source/destination IP addresses and protocol information. However, augmented features don't directly come from the original data (as they are simulated); they are added on top of the existing records from ML-EdgeIIoT-dataset, and their values are based on the context and structure of the original dataset. Hence, the augmented dataset is a modified version of the original ML-EdgeIIoT-dataset, designed to reflect the effects of specific attacks in a 5G-enabled IIoT environment. The facts and figures were created using the Python code and visually represent different performance metrics.

Dataset	Total Records	Total Features	New 5G Attack-Specific Features
Original	157,800	63	-
Augmented	157,800	70	simulated_latency, packet_loss_rate, slice_id, traffic_conflict,api_anomaly_score, unauthorized_api_calls, 5GAttack_Type

Table 2. Overview and Comparison between Datasets.

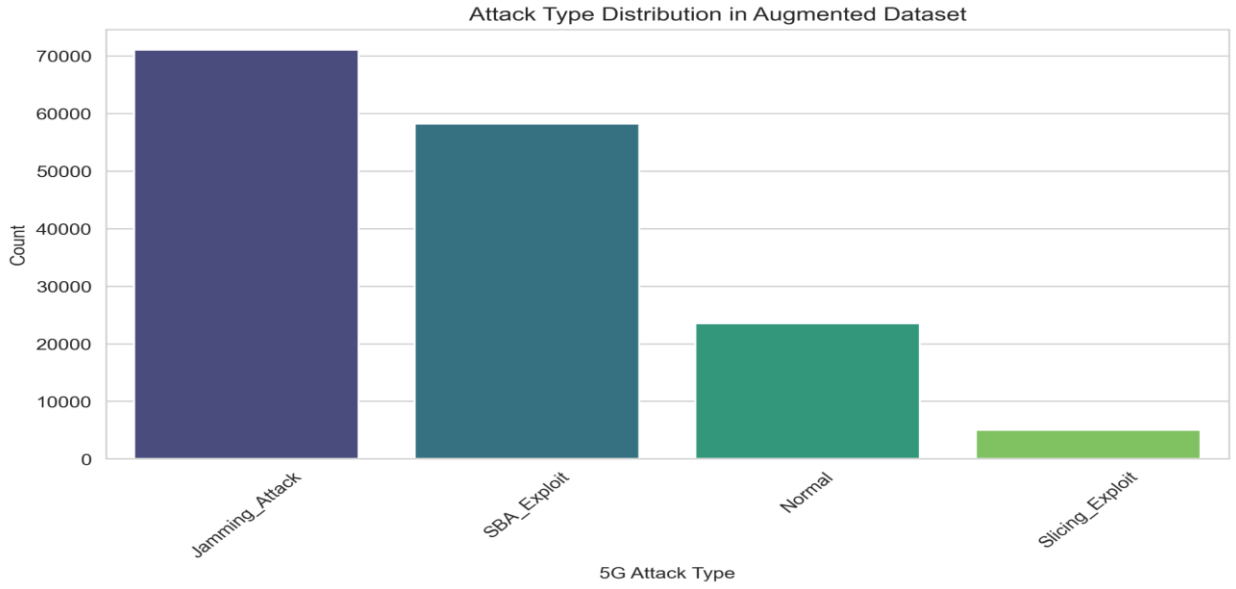

Figure 3. 5G-Specific Attack type distribution in Augmented Dataset

Table 3. 5G Specific Attack Type Count in Augmented Dataset

Attack Type	Record Count	Percentage (%)
Jamming Attack	71,026	45.01
SBA Exploit	58,229	36.90
Normal Traffic	23,523	14.91
Slicing Exploit	5,022	3.18
Total	**157,800**	**100**

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 3 and Figure 3 illustrate that jamming attacks are 45% of the dataset and are affecting network performance. 37% of SBA Exploits marked API security vulnerabilities. Slicing exploits are at least 3%, could have severe inference on network resource allocation.

Attack Simulation Analysis & Result

This section evaluates the realism of the simulated 5G-specific attacks in reflecting actual 5G network vulnerabilities. The assessment basically focused on:

a. Attack accuracy: How faithfully the simulated jamming, slicing attacks, and SBA vulnerabilities reflect real 5G security problems.
b. Realism: The degree to which these attacks produce packet loss and increase in latency of the network.
c. Effect on Key Metrics: Contrasting the consequences on packet loss and latency with actual attack conditions.

Packet Loss Study:

Attack Type	Avg. Packet Loss (%)	Max Packet Loss(%)	Min Packet Loss(%)
Jamming Attack	33.32%	49.99%	10.00%
SBA Exploit	30.00%	49.99%	10.00%
Slicing Exploit	30.26%	49.98%	10.01%
Normal Traffic	20.03%	29.99%	10.00%

Table 4. Packet loss per 5G-specific attack types

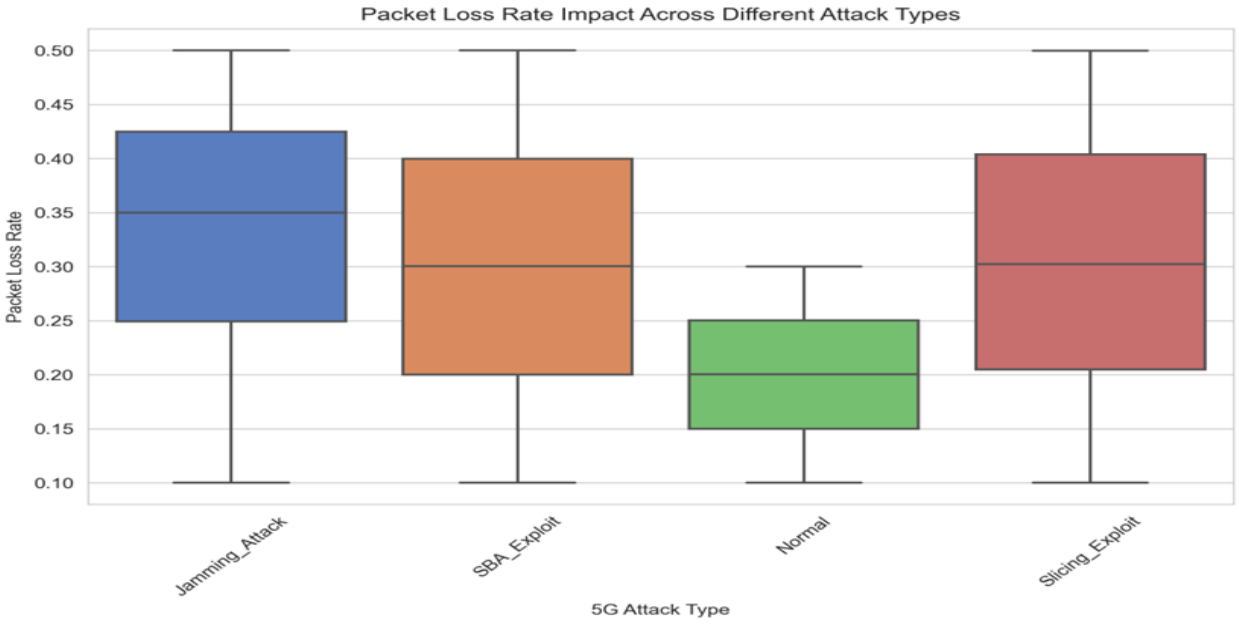

Figure 4. Box Plot: Packet Loss Rate for 5G-Specific Attack Types

Jamming attacks have the highest average packet loss, 33.32%, thus seriously compromising real-time communications in 5G-IIoT. SBA exploits and slicing attacks are compromising network service quality by causing somewhat moderate packet loss, approx. 30%. Normal traffic displays the lowest 20% packet loss among all attacks, therefore confirming the influence of the attack on network behaviour as illustrated in Table 4 and Figure 4.

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Simulated Latency Impact across Attacks:

5G Attack Type	Mean Latency (ms)	Std (ms)	Min Latency (ms)	Max Latency (ms)
Jamming_Attack	333.34	110.08	100	499.99
Normal	199.4	57.8	100.01	299.99
SBA_Exploit	300.33	115.71	100	499.99
Slicing_Exploit	297.6	115.32	100.07	499.94

Table 5. Simulated latency metrics across 5G-specific attacks.

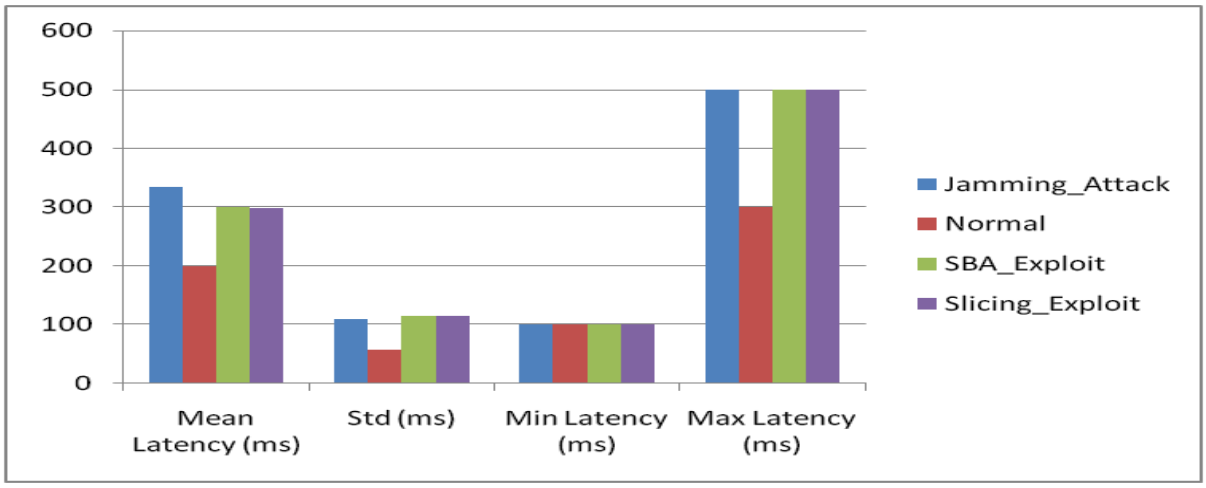

Figure 5. Line Chart: Latency Distribution Across 5G-Specific Attack

The highest latency resulted from the jamming attack, with an average of 333.34 ms, within a broad latency range from 100 ms to over 500 ms. Normal traffic exhibits the lowest mean delay, while significant variance persists, ranging from 100 ms to 300 ms. However, SBA exploits and slicing exploits have comparable latencies, averaging approximately 300 ms, accompanied by a substantial standard deviation, signifying considerable variability in response times as illustrated in Table 5 and Figure 5.

System Response Time Impact Across Different Attack Types (Using API Anomaly Score):

5G Attack Type	Mean System Response Time (ms)	Std (ms)	Min Response Time (ms)	Max Response Time (ms)
Jamming_Attack	35.09	20.15	0.0005	69.99
Normal	34.91	20.24	0.0107	69.99
SBA_Exploit	75.57	22.86	0.0192	99.99
Slicing_Exploit	35.25	20.09	0.0278	69.99

Table 6. System Response Time Impact Across Different Attack Types

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

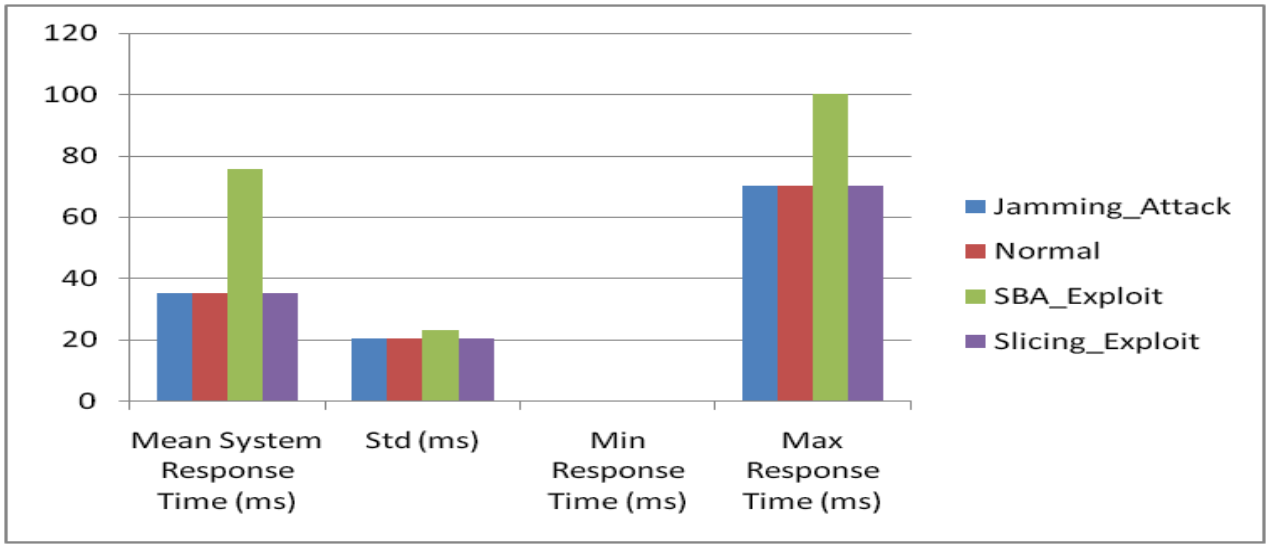

Figure 6. System Response Time Impact across Different Attack Types (using API Anomaly Score)

- System response times using the API anomaly score for normal traffic and jamming attacks are almost identical, measuring 34.9 ms and 35 ms, respectively. The fact that both have a standard deviation of around 20 ms suggests that the response times in the data are not consistently the same.
- System response times are substantially increased, on average, by 75.57 ms due to SBA exploits. This proves beyond a reasonable doubt that SBA exploits cause significant delays, most likely as a result of exploiting API vulnerabilities. Also, compared to other forms of attacks, response times for SBA exploits are more varied, as seen by a standard deviation of 22.86 ms.
- Slicing exploits, like jamming and normal traffic, have an average reaction time of 35.25 ms. With a standard deviation of 20.09 ms, response times for this sort of attack show some slight variance, as shown in Figure 6 and Table 6.

Unauthorized API Calls per Attack Type:

5G Attack Type	Avg. Unauthorized API Calls	Max Unauthorized API Calls	Min Unauthorized API Calls
Jamming_Attack	0	0	0
Normal	0	0	0
SBA_Exploit	0.273712	1	0
Slicing_Exploit	0	0	0

Table 7. Unauthorized API Calls Summary

ournal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

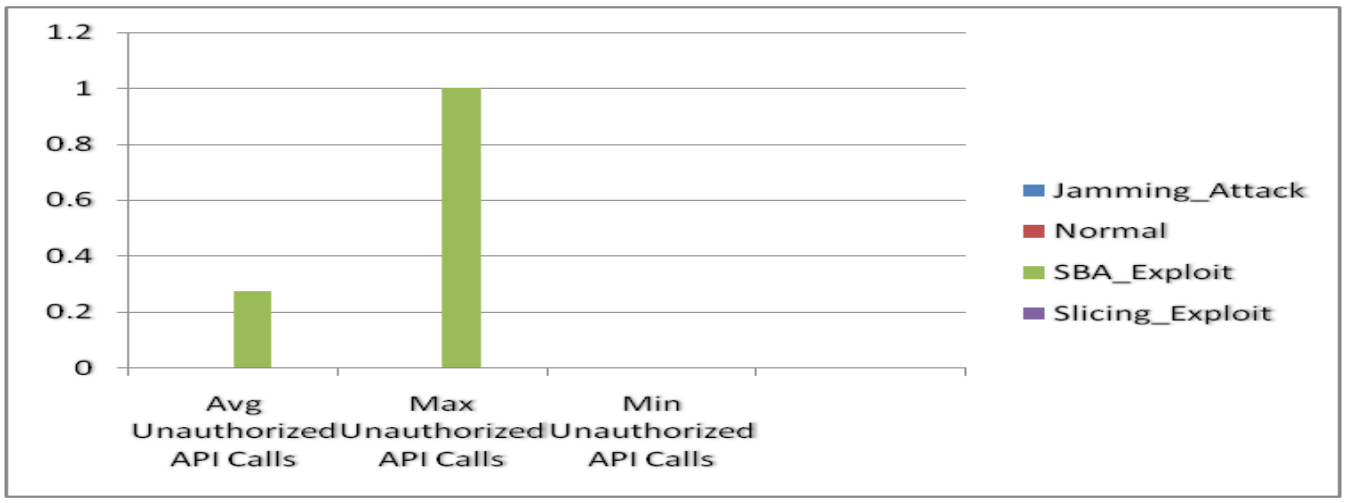

Figure 7. Unauthorized API Calls per Attack Type

Normal traffic and jamming attacks neither have any illegal API calls; this is expected, as they do not involve unauthorised service access at the API level. Even slicing exploits do not directly target API vulnerabilities; they also exhibit no unauthorised API calls. SBA exploits have an average of 0.27 unauthorised API calls and a maximum of 1 unauthorised API call. Although the frequency is somewhat low, this suggests that SBA exploit vulnerabilities allow for sporadic illegal API access in the system, as illustrated by Table 7 and Figure 7.

Network Slicing Conflict Analysis:

Slice ID	Total Traffic Conflicts	Total Records	Conflict Rate (%)
Slice_A	2635	52645	5.005224
Slice_B	2650	52641	5.034099
Slice_C	2668	52514	5.080550

Table 8. Traffic conflict summary

Among the slices, Slice C has the greatest traffic conflict rate—5.08%; Slice B (5.03%) and Slice A (5.00%) follow. Slice C suffers somewhat more conflicts, although having roughly identical total records (around 52,000 each slice), implying that its resource management or network slicing technique may be more prone to congestion or conflicts as shown in Table 8.

Limitations

Accuracy Challenges Attack Conditions in Replicating Real-World: Although the 5G-specific attack simulations are meant to reflect real-world threats, it is still difficult to replicate genuine attack settings in a controlled environment. Analysing the complexity and diversity of real-world attacks is challenging for 5G networks because of their dynamic character, changing network configurations, varying interference and eccentric real-time network conditions. However, the simulations offer useful approximations, but more precision requires future improvement and real-world validation.

Scalability Issues for Attacks Simulation on big IIoT Deployment:5G-specific attacks simulation on larger IIoT systems presents scalability challenges. The computational resources required to simulate realistic attacks on a large scale also rise with the proliferation of IoT devices and network slices. Performance constraints arising from this can complicate the assessment of threats across extensive, diverse IIoT systems. These scaling challenges

necessitate the development of optimal simulation models and the utilisation of distributed computing or cloud-based solutions to handle larger datasets and more complex attack simulations.

CONCLUSION AND FUTURE WORK

This work assimilated 5G-specific attack simulations with IIoT security datasets to represent a dataset-driven strategy to understand the effect of jamming, slicing exploits, and SBA vulnerabilities. By extending our research in implementing real-time testbeds to validate the simulated attacks and other performance metric parameters, introducing more complex attack scenarios investigating federated learning for distributed threat detection and pledge privacy and scalability in 5G-IIoT security systems, the augmented dataset will allow for further research into intrusion detection models and aid in the design of more resilient 5G-IIoT networks. This will help us create more robust security measures and mitigation strategies that are tailored for the unique challenges of 5G-enabled industrial environments.

REFRENCES

[1] Ahmed, S. F., Alam, M. S. B., Hoque, M., Lameesa, A., Afrin, S., Farah, T., Kabir, M., Shafiullah, G. M., & Muyeen, S. M. (2023). Industrial Internet of Things enabled technologies, challenges, and future directions. *Computers and Electrical Engineering*, *110*, 108847. https://doi.org/10.1016/j.compeleceng.2023.108847

[2] Al-Hawawreh, M., Sitnikova, E., & Aboutorab, N. (2022). X-IIoTID: A Connectivity-Agnostic and Device-Agnostic Intrusion Data Set for Industrial Internet of Things. *IEEE Internet of Things Journal*, *9*(5), 3962–3977. https://doi.org/10.1109/JIOT.2021.3102056

[3] Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, *27*, 101227. https://doi.org/10.1016/j.iot.2024.101227

[4] Chalapathi G. S. S.and Chamola, V. and V. A. and B. R. (2021). Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions. In J. Chang Weiand Wu (Ed.), *Fog/Edge Computing For Security, Privacy, and Applications* (pp. 293–325). Springer International Publishing. https://doi.org/10.1007/978-3-030-57328-7_12

[5] Chandra Shekhar Rao, V., Kumarswamy, P., Phridviraj, M. S. B., Venkatramulu, S., & Subba Rao, V. (2021). 5G Enabled Industrial Internet of Things (IIoT) Architecture for Smart Manufacturing. In K. A. Reddy, B. R. Devi, B. George, & K. S. Raju (Eds.), *Data Engineering and Communication Technology* (pp. 193–201). Springer Singapore.

[6] De Alwis, C., Porambage, P., Dev, K., Gadekallu, T. R., & Liyanage, M. (2024). A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions. *IEEE Communications Surveys & Tutorials*, *26*(1), 534–570. https://doi.org/10.1109/COMST.2023.3312349

[7] Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access*, *10*, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809

[8] Gallenmüller, S., Naab, J., Adam, I., & Carle, G. (2020). 5G URLLC: A Case Study on Low-Latency Intrusion Prevention. *IEEE Communications Magazine*, *58*(10), 35–41. https://doi.org/10.1109/MCOM.001.2000467

[9] Li, S., Iqbal, M., & Saxena, N. (2022). Future Industry Internet of Things with Zero-trust Security. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-021-10199-5

[10] Liu, X., Su, X., Del Campo, G., Cao, J., Fan, B., Saavedra, E., Santamaria, A., Roning, J., Hui, P., & Tarkoma, S. (2024). Federated Learning on 5G Edge for Industrial Internet of Things. *IEEE Network*. https://doi.org/10.1109/MNET.2024.3469988

[11] Ma, S., Wang, H., Zhu, L., & Zhang, Q. (2023). Joint Security and Resilience Control in IIoT-Based Virtual Control Train Sets Under Jamming Attacks. *IEEE Transactions on Vehicular Technology*, *72*(9), 11196–11212. https://doi.org/10.1109/TVT.2023.3266561

[12] Mahmood, A., Beltramelli, L., Fakhrul Abedin, S., Zeb, S., Mowla, N. I., Hassan, S. A., Sisinni, E., & Gidlund, M. (2022). Industrial IoT in 5G-and-Beyond Networks: Vision, Architecture, and Design Trends. *IEEE Transactions on Industrial Informatics*, *18*(6), 4122–4137. https://doi.org/10.1109/TII.2021.3115697

[13] Porambage, P., & Liyanage, M. (2020). *Security in Network Slicing* (pp. 1–12).

https://doi.org/10.1002/9781119471509.w5gref166
[14] Rehman, T., Tariq, N., Khan, F. A., & Rehman, S. U. (2024). FFL-IDS: A Fog-Enabled Federated Learning-Based Intrusion Detection System to Counter Jamming and Spoofing Attacks for the Industrial Internet of Things. *Sensors*, *25*(1), 10. https://doi.org/10.3390/s25010010
[15] Savadatti, S., Kuldeep Dhariwal, S., Krishnamoorthy, S., & Delhibabu, R. (2024). An Extensive Classification of 5G Network Jamming Attacks. *Security and Communication Networks*, *2024*(1), 2883082. https://doi.org/10.1155/2024/2883082
[16] Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., De Silva, P., Tufvesson, F., Benjebbour, A., & Wunder, G. (2017). 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. *IEEE Journal on Selected Areas in Communications*, *35*(6), 1201–1221. https://doi.org/10.1109/JSAC.2017.2692307
[17] Wehbe, N., Alameddine, H. A., Pourzandi, M., Bou-Harb, E., & Assi, C. (2023). A Security Assessment of HTTP/2 Usage in 5G Service-Based Architecture. *IEEE Communications Magazine*, *61*(1), 48–54. https://doi.org/10.1109/MCOM.001.2200183
[18] Wu, Y., Dai, H.-N., Wang, H., Xiong, Z., & Guo, S. (2022). A Survey of Intelligent Network Slicing Management for Industrial IoT: Integrated Approaches for Smart Transportation, Smart Energy, and Smart Factory. *IEEE Communications Surveys & Tutorials*, *24*, 1–1. https://doi.org/10.1109/COMST.2022.3158270
[19] Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors*, *25*(1), 213. https://doi.org/10.3390/s25010213
[20] Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., & Jain, R. (2019). Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), 6822–6834. https://doi.org/10.1109/JIOT.2019.2912022.