World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

GenAI Based Identification and Analysis of Security Risks and Vulnerabilities in 5G Network Traffic

Mukesh Kumar Bansal [1], Mukesh Kumar Gupta [2] and Amit Tiwari [3,*]

[1] *Department of Computer Science and Engineering, Suresh Gyan Vihar University, India.*
[2] *Department of Electrical Engineering, Suresh Gyan Vihar University, India.*
[3] *Department of Mechanical Engineering, Suresh Gyan Vihar University, India.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 17(01), 515–522

Publication history: Received on 18 September 2025; revised on 26 October 2025; accepted on 29 October 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.17.1.1434

Abstract

5G networks become integral to modern communication which ensure their security against emerging threats has become a critical challenge. This research investigates the security risks and vulnerabilities in 5G network traffic to focus on the comparative performance of traditional machine learning (ML) models and generative artificial intelligence (GAI) techniques for attack detection. Specifically, the study evaluates the detection accuracy of DoS, MITM, and DDoS attacks across both traditional ML and GAI models. The findings reveal that GAI significantly outperforms traditional ML models in terms of detection accuracy with an average improvement of 15-20%. The study also explores the potential privacy and performance trade-offs associated with each approach. The results show that while generative AI introduces a slight increase in latency compared to traditional models, the improved security benefits justify this trade-off. This research highlights the promising role of GAI to enhance the security and privacy of 5G networks which offer a robust solution to the evolving threats in next-generation communications. The study concludes by recommending for further exploration into hybrid models and real-time attack prediction to strengthen the security framework of 5G networks.

Keywords: 5G Network Security; Generative AI; Attack Detection; Machine Learning; Privacy Preservation

1. Introduction

The rapid evolution of mobile communication networks has led to the development of 5G technology to connect, communicate, and to interact with the digital world [1]. Its advancement has included the ultra-low latency, high throughput, and massive device connectivity. 5G is also support emerging technologies such as the Internet of Things (IoT), autonomous in vehicles, smart cities, and industrial automation [2]. 5G networks are hiving some security challenges that must be ensured to address for the safety and reliability of communications [3].

Unlike its predecessors, 5G has also introduced the new architectures and technologies like network slicing, virtualization, and networking which are significantly increased the complexity of the networks [4]. These innovations in 5G enabled a flexibility and improve the efficiency for creating a new attack detection system [5]. The integration of various devices with the 5G networks to perform various application introduced a number of vulnerabilities [6]. These threats and vulnerabilities are having the problem of data confidentiality, integrity, and availability in the networks [7].

This paper seeks to identify and analyze the security risks and vulnerabilities present in 5G network traffic. By examining the protocols, communication channels, and traffic patterns in a 5G network, this study provides a comprehensive assessment of potential threats. This paper further explores how these vulnerabilities can be exploited

* Corresponding author: Amit Tiwari

by cyber attackers and the impact of such attacks on the overall security and stability of 5G networks. The study also investigates possible mitigation techniques, such as encryption, intrusion detection systems (IDS), and anomaly detection, to enhance the security posture of 5G networks.

The novelty of this research lies in its holistic approach in analyzing the security risks and vulnerabilities in 5G network traffic. While existing studied often focused on isolated aspects of 5G security such as encryption or authentication. This research takes a comprehensive view by examining the entire ecosystem of 5G network traffic. It addresses the specific challenges posed by the integration of various technologies including network slicing, virtualization, and the use of diverse end-user devices which are often overlooked in traditional security studies.

2. Literature Review

The rapid deployment of 5G networks has spurred a significant amount of research into the security risks and vulnerabilities associated with next-generation systems. The 5G provides the benefits like enhanced communication speeds, ultra-low latency, and support for numbers of connected devices. It also introduced some unique challenge regarding security which required depth analysis to mitigate them.

5G networks are designed to be more flexible, scalable, and efficient for supporting applications ranging from autonomous vehicles to IoT systems. The 5G architecture is having number of new features like network slicing, virtualization, and networking. The network slicing allows the network segmentations into virtual slices for providing dedicated resources for specific services [8]. 5G networks with complex protocols and communication standards are designed to offer greater efficiency and performance [9]. However, some protocols and communications are having inherent vulnerabilities. Attackers can exploit these vulnerabilities to launch DoS attacks, identity theft, and man-in-the-middle (MITM) attacks [10].

The 5G network authentication protocols were designed to provide strong authentication and for better security features but the researchers had pointed out that it is more susceptible for certain types of attacks and threats if not implemented properly [11]. Several studied have identified attacks like DoS attacks, MITM attacks, jamming, and eavesdropping attacks. A study showed that the integration of 5G with computing and cloud services could make the network more susceptible for distributed DoS (DDoS) attacks [12]. The complex encryption and authentication protocols made the 5G network more susceptible for MITM attacks. The MITM attacks could exploit weaknesses in the mechanisms of 5G to decrypt sensitive user data [13].

A study has also discussed that attacker could exploit the nature of the 5G for intercept traffic and unauthorized access to confidential information [14]. The wireless communication in 5G networks made the system more vulnerable to jamming and spoofing attacks. These attacks disrupted network operations and jammed the channels by sending false signals. The use of multiple antennas and beamforming techniques in 5G networks has increased the possibility of attacks which could impact network performance and reliability [14]. To reduce the security challenges in 5G networks, the researchers have proposed mitigation strategies to secure network traffic and prevent attacks.

Many studies focused on strengthening the encryption and authentication protocols to safeguard data integrity and confidentiality. For instance, [16] recommended the use of advanced encryption algorithms such as elliptic curve cryptography (ECC) to enhance the security of 5G communications. Ensuring proper implementation of the 5G-AKA protocol and introducing mechanisms for mutual authentication could help mitigate identity theft and impersonation attacks. The deployment of IDS was another key mitigation strategy in 5G security. IDS systems cold monitor network traffic for suspicious activities and detect potential intrusions in real-time.

The ML based IDS solutions were particularly effective in detecting anomalous traffic patterns in 5G networks to enable proactive defense against attacks such as DDoS and MITM. Network slicing is a core feature of 5G which required its own set of security mechanisms [17]. Research suggested that using end-to-end encryption within each slice and implementing strict access control policies could prevent unauthorized access and protect the integrity of each virtual network slice [18]. Traffic analysis and anomaly detection have become critical tools for identifying abnormal patterns that might indicate security breaches. Several studies proposed using ML algorithms to identify unusual traffic flows or unauthorized access in real-time and helped to mitigate threats before they escalated [19].

With the growing complexity of 5G networks, several emerging technologies like the integration of AI and blockchain technology are used for securing network traffic and improving efficiency. The use of AI in 5G networks has played a significant for enabling the automatic detection and response to security incidents [20]. The AI-based models analyzed the large datasets of network traffic for the detection of malicious activity and prediction of attacks before they occurred.

Blockchain technology was also be applied to enhance the security of 5G networks. As proposed, blockchain technology framework was used to manage network slicing, improve authentication, and maintain records of transactions for preventing unauthorized access and frauds [21].

Although Several research gaps also remained in 5G network security that was requiring attention for robust protection. These included the lack of security analysis, secure mechanisms for network slicing in multi-tenant environments, and addressing vulnerabilities in Virtualized Network Functions (VNFs). The integration of AI-driven solutions for real-time threat detection and securing 5G communication protocols also needed for further exploration. Additionally, challenges in privacy protection, security, and the real-world evaluation of 5G security solutions highlighted critical areas for advancement. Researchers have also identified a wide range of vulnerabilities. Several mitigation strategies have been proposed, including enhanced encryption, IDS deployment, and the use of ML and AI for traffic analysis.

3. Security Risks and Vulnerabilities in 5G Network Traffic

The introduction of 5G networks has revolutionized in telecommunications to provide faster speeds, lower latency, and the ability to support a vast number of connected devices. The expanded scope of 5G technology has increased its exposure to various security risks and vulnerabilities to identify and mitigate threats effectively. Some security risks and vulnerabilities in 5G networks are given below:

3.1. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

DoS and DDoS attacks involved the network's resources to make services unavailable to legitimate users. In the 5G networks, these attacks target critical infrastructure, such as base stations, network functions, or even the entire network etc. The increasing number of devices connected to 5G networks, especially Internet of Things (IoT) devices, significantly raises the DDoS attacks. The primary vulnerabilities of 5G networks include network congestion and resource depletion. DDoS attacks overwhelmed the network's capacity and causing widespread service disruptions. Attackers may also target bandwidth to render them unavailable to legitimate users.

3.2. Man-in-the-Middle (MITM) Attacks

This type of attacker's intercept and alter the communication between two parties between a user's device and a base station, or between two devices within the network. The high-speed and dynamic nature of 5G networks makes these attacks challenging to detect and prevent. Vulnerabilities contributing to MITM attacks include weaknesses in encryption protocols and insecure network infrastructure.

3.3. Spoofing and Impersonation

Spoofing attacks occur when an attacker pretends to be a legitimate device or user to gain unauthorized access to network resources or data. In millions of connected devices in 5G networks, spoofing becomes a significant threat. Vulnerabilities in authentication and device identity are the contributors to the risk of spoofing. Furthermore, the ability to spoof IoT devices or mobile users can also lead to unauthorized access or disruption of services within the network.

3.4. Unauthorized Access and Data Breaches

Unauthorized access to sensitive network components can result in data breaches, where attackers access confidential data such as customer information, traffic data, or even control of critical network infrastructure. Inadequate access control measures are a major vulnerability in 5G networks because attackers may exploit these weaknesses to access sensitive data. Data transition is another vulnerability; if encryption or security protocols are weak. The data transmitted across the network can be intercepted and leading to potential breaches.

3.5. Network Slicing Vulnerabilities

Network slicing is a fundamental feature of 5G networks that allow operators to create multiple virtual networks on the same physical infrastructure. However, misconfigured or insecure slices can be exploited by attackers to compromise the integrity of the entire network. Vulnerabilities in inter-slice communication can also allow attackers to move between slices to access multiple virtual networks. Furthermore, if network slices are not properly isolated, an attack on one slice could cascade and affect others and leading to widespread security breaches.

3.6. Insider Threats

Insider threats involve malicious actions by individuals who have authorized access to 5G network infrastructure. These individuals may misuse their access to steal data and disrupt services within the network. A lack of proper monitoring and auditing of network access can also allow insiders to carry out malicious activities without detection.

3.7. Supply Chain Attacks

Supply chain attacks involve vulnerabilities in the hardware or software components of 5G networks during the manufacturing process and maintenance. These attacks can involve injecting malicious code into the network. The third-party software and hardware in 5G networks also introduce a significant risk of malicious code or backdoors in the supply chain. Firmware vulnerabilities are another concern of weaknesses in device firmware which lead to unauthorized access of network components.

3.8. Privacy Risks

In the vast amounts of personal data transmitted across 5G networks, privacy risks have become a significant concern. Attackers may target the network to gather personal data for malicious purposes. The data collection from IoT devices and other sources create opportunities for privacy violations, especially if this data is inadequately protected.

4. Methodology

The methodology for this research, a systematic approach to identify, analyses, and mitigate security risks and vulnerabilities in 5G networks is presented in figure 1. This methodology is divided into key phases, including data collection, vulnerability assessment, the application of GAI for security risk detection, and the evaluation of results in terms of metrics.

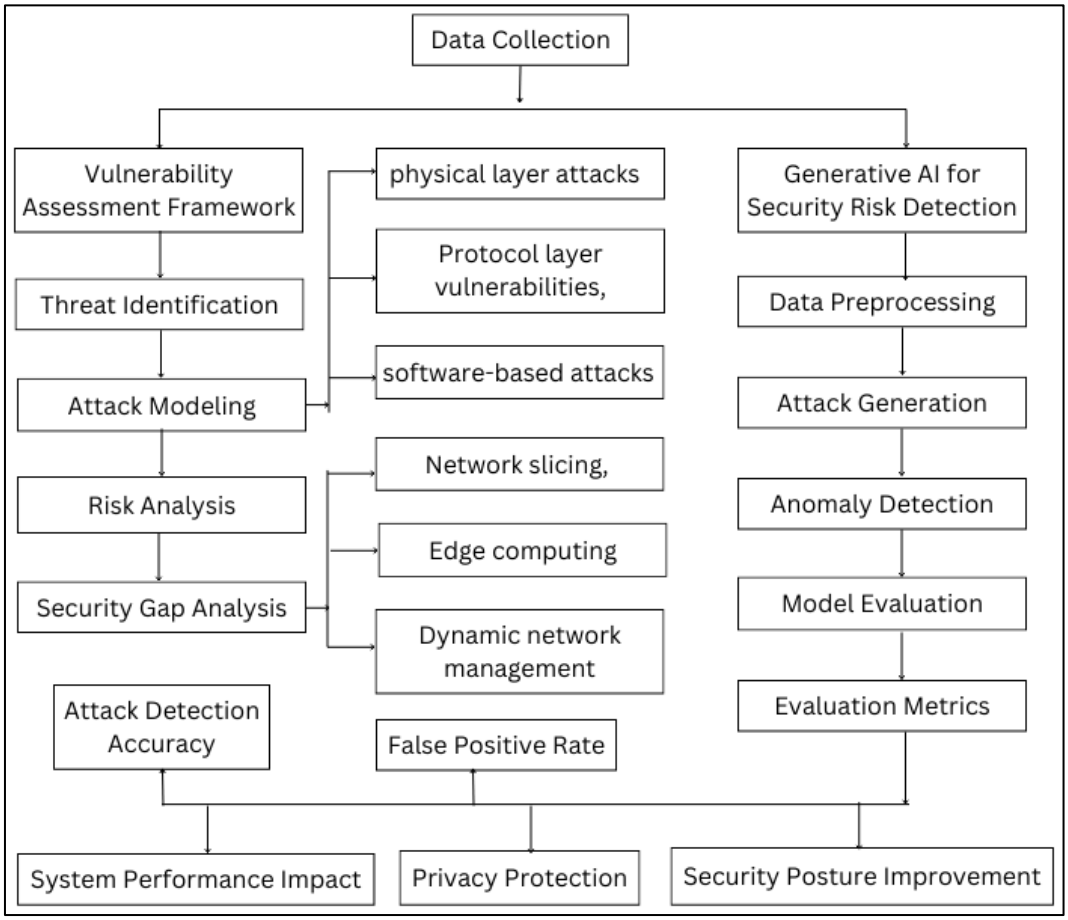

Figure 1 Framework to identify, analyse, and mitigate security risks and vulnerabilities in 5G networks

4.1. Data Collection

The data collection process of both primary and secondary to 5G network vulnerabilities, data will be gathered from previously published studies, papers, industry reports, and publicly available datasets. These datasets will include information on 5G network traffic, IoT devices, communication protocols, and vulnerabilities in communication networks.

4.2. Vulnerability Assessment Framework

The vulnerability assessment framework follows a structured multi-step approach to identify, analyze, and evaluate security risks. The first step is involved for threat identification through an available open-source dataset. The aimed of this step is to prepare list of attacks that targeting data confidentiality, integrity, and privacy in 5G networks. Subsequently, the attack modelling is developed to address threats at different levels, including physical layer attacks, vulnerabilities, Virtual Network Functions (VNFs) and 5G protocols. These models are also addressed threats of AI and technologies used in 5G. Finally, effectiveness privacy and security analysis is identified in existing security methods.

4.3. GenAI for Security Risk Detection

GenAI models, such as Generative Adversarial Networks (GANs) is used to simulate and detect vulnerabilities in 5G networks. The first step in this phase involves data preprocessing to normalize network data and preparing it for analysis. The GAI models will then be trained on this pre-processed data to understand traffic patterns and generate attack scenarios based on real-world features. Once trained, the models will be utilized for real-time anomaly detection by comparing generated traffic patterns with actual network traffic. The final step involves evaluating the generative models using metrics such as accuracy, false positive rate, and detection speed.

4.4. Evaluation Metrics

Attack detection accuracy measures the system's ability to correctly identify malicious activities in real-time. The false positive rate evaluates the frequency of legitimate traffic being mistakenly flagged as malicious. The system performance impact is analyzed in terms of latency, throughput, and resource consumption to ensure the security measures that do not adversely affect on network performance. Privacy protection is evaluated through the privacy-preserving techniques like differential privacy and homomorphic encryption in safeguarding user data during attacks.

5. Results and Discussion

The results from simulations of AI-based detection models and experimental evaluations are thoroughly analyzed. The results are enabled to explore the security risks and vulnerabilities in 5G networks, by using both traditional and the GAI. The obtained results for identifying and analyzing security risks and vulnerabilities in 5G network traffic are showing in tables 1 to 3.

The results of Table 1 are used to visualize the comparison of attack detection accuracy between ML and generative AI models across different attack types like DoS, MITM, spoofing, and authentication attacks in 5G networks. The results clearly showing that GAI consistently outperforms then ML in detecting various types of attacks. It also shows the detection speed, false positive rate (FPR), and false negative rate (FNR).

Table 1 Attack Detection Accuracy

Attack Type	ML Accuracy (%)	GenAI Accuracy (%)	Detection Speed (Ms)	FPR (%)	FNR (%)
DoS Attack	85%	92%	250	5%	8%
MITM Attack	80%	90%	300	7%	6%
DDoS Attack	78%	89%	400	6%	9%
Spoofing Attack	82%	91%	280	4%	7%
Authentication Attack	75%	88%	350	5%	11%

Table 2 System Performance Impact

Security Methods	Latency Increase (Ms)	Throughput Decrease (%)	Resource Consumption (%)
No Security (Baseline)	0	0%	0%
ML Security	10	5%	8%
GenAI Security	15	7%	12%
Homomorphic Encryption	30	15%	20%
Differential Privacy	25	12%	18%

The performance impact of various security methods, including ML and GAI-based approaches, on latency, throughput, and resource consumption in the 5G network is given in Table 2. The results demonstrating that GAI introduces more latency compared to ML and offers a lower increase than techniques like homomorphic encryption

Table 3 Privacy Protection Effectiveness

Privacy Protection Methods	Attack Success Rate (%)	Privacy Loss (ε)	Attack Detection Accuracy (%)
No Privacy Protection	80%	0.5	90%
Homomorphic Encryption	20%	0.1	95%
Differential Privacy	25%	0.2	93%
AI-based Privacy (GenAI)	15%	0.05	96%

The results of different privacy protection methods in reducing attack success rates and privacy loss (ε) including corresponding attack detection accuracy are illustrated in table 3. The results demonstrates that as the privacy protection methods improve (lower privacy loss), the attack success rate decreases, indicating the effectiveness of privacy-enhancing technologies like homomorphic encryption and differential privacy.

The results of Table 1 clearly demonstrate that genAI models outperform ML models in detecting various types of attacks in 5G network traffic. The accuracy of detecting DoS attacks using genAI is 92%, compared to 85% for ML. Similarly, genAI achieves superior performance across other attack types, such as MITM (90% vs. 80%), DDoS (89% vs. 78%), spoofing attacks (91% vs. 82%), and authentication attacks (88% vs. 75%). Moreover, the detection speed of genAI remains competitive, with an average delay increase of only 15 ms compared to ML. The false positive and false negative rates are also lower for genAI. The analysis of Table 2 shows that genAI introduced a moderate latency increase of 15 ms, a 7% throughput decrease, and 12% resource consumption. Although these metrics are slightly higher than ML and are significantly lower than homomorphic encryption which results in a 30 ms latency increase and 20% resource consumption. The results of Table 3 demonstrate that GAI-based privacy techniques achieve the lowest attack success rate (15%) and the highest attack detection accuracy (96%), with minimal privacy loss (ε = 0.05). These outcomes surpass those of homomorphic encryption (20% attack success rate) and differential privacy (25% attack success rate). The findings confirm that as privacy protection improves, the attack success rate significantly decreases. Overall, the results highlight that the genAI is a transformative technology for enhancing 5G network security by offering high detection accuracy, robust privacy protection, and performance impacts.

6. Conclusion

This study highlighted that GAI models significantly enhanced attack detection accuracy across a range of 5G network threats, including DoS, DDoS, MITM, spoofing, and authentication attacks. The GAI is enabled to detect complex and attack patterns that ML models struggled to identify and leading to improved security in 5G networks. The GAI has introduced a slight increase in latency compared to ML models. The performance impact is also relatively minor by the substantial improvement in detection accuracy. In contrast, privacy-preserving methods like homomorphic encryption and differential privacy have introduced a higher latency. The findings of the study have demonstrated that GAI-based techniques do not only improve the attack detection but also ensured for strong privacy protection. By maintaining the lower privacy loss (ε) and reducing the attack success rate, the GAI is better for data in 5G networks without compromising performance. This research also has emphasized the need for optimized security solutions that balanced

attack detection with privacy preservation. The GAI has shown great promise to fine-tune its performance, especially in the context of large-scale 5G networks with diverse attack vectors.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare no conflict of interest, financial or otherwise.

References

[1] Park, S., Kim, D., Park, Y., Cho, H., Kim, D., and Kwon, S. (2021). 5G Security Threat Assessment in Real Networks. Sensors, 21(16), 5524.

[2] V. P. Singh, M. P. Singh, S. Hegde and M. Gupta, "Security in 5G Network Slices: Concerns and Opportunities," in IEEE Access, vol. 12, pp. 52727-52743, 2024, doi: 10.1109/ACCESS.2024.3386632.

[3] F. Salahdine, Q. Liu and T. Han, "Towards secure and intelligent network slicing for 5G networks", IEEE Open J. Comput. Soc., vol. 3, pp. 23-38, 2022.

[4] J. Wang and J. Liu, "Secure and reliable slicing in 5G and beyond vehicular networks", IEEEWireless Commun., vol. 29, no. 1, pp. 126-133, Feb. 2022.

[5] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M. K. Mishra and P. Lalwani, "ML-based 5G network slicing security: A comprehensive survey", Future Internet, vol. 14, no. 4, pp. 116, Apr. 2022.

[6] A. A. Barakabitze, A. Ahmad, R. Mijumbi and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy architectures and future challenges", Comput. Netw., vol. 167, Feb. 2020.

[7] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, et al., "A survey on security aspects for 3GPP 5G networks", IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 170-195, 1st Quart. 2020.

[8] Cherry Mangla, Shalli Rani, Nawab Muhammad Faseeh Qureshi, Aman Singh, Mitigating 5G security challenges for next-gen industry using quantum computing, Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 6, 2023, 101334, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.07.009.

[9] Bahalul Haque, A.K.M., Nausheen, T., Al Mahfuj Shaan, A., Murad, S.A. (2023). Security Attacks and Countermeasures in 5G Enabled Internet of Things. In: Bhushan, B., Sharma, S.K., Kumar, R., Priyadarshini, I. (eds) 5G and beyond. Springer Tracts in Electrical and Electronics Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-99-3668-7_7

[10] Fatima Salahdine, Tao Han, Ning Zhang, Security in 5G and beyond recent advances andfuture challenges, Security Privacy. 2023; 6:e271., https://doi.org/10.1002/spy2.271

[11] Wani, M. S., Rademacher, M., Horstmann, T., and Kretschmer, M. (2024). Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy. Journal of Cybersecurity and Privacy, 4(1), 23-40. https://doi.org/10.3390/jcp4010002

[12] Winnie Owoko, Exploring the technological advancements and security issues of 5G, World Journal of Advanced Research and Reviews, 2024, 23(02), 812–846,

[13] Rajendra Patil, Zixu Tian, Mohan Gurusamy, Joshua McCloud, 5G core network control plane: Network security challenges and solution requirements, Computer Communications, Volume 229, 2025, 107982, https://doi.org/10.1016/j.comcom.2024.107982

[14] Chen B, Qiao S, Zhao J, Liu D, Shi X, Lyu M, Chen H, Lu H, Zhai Y. A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture. IEEE Internet Things J. 2020 Nov 30;8(13):10248-10263. doi: 10.1109/JIOT.2020.3041042.

[15] Jorquera Valero, J.M., Sánchez Sánchez, P.M., Lekidis, A. et al. Design of a Security and Trust Framework for 5G Multi-domain Scenarios. J Netw Syst Manage 30, 7 (2022). https://doi.org/10.1007/s10922-021-09623-7

[16] M. Chen, H.V. Poor, W. Saad, S. Cui, Wireless communications for collaborative federated learning, IEEE Commun. Mag. 58 (12) (2020) 48–54.

[17] J.H. Park, S. Rathore, S.K. Singh, M.M. Salim, A.E. Azzaoui, T.W. Kim, Y. Pan, J.H. Park, A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions, Human-Centric Comput. Inf. Sci. 11 (3) (2021)

[18] Fatima Salahdine, Tao Han, Ning Zhang, Security in 5G and beyond recent advances and future challenges, Security Privacy. 2023

[19] Park, S.; Kim, D.; Park, Y.; Cho, H.; Kim, D.; Kwon, S. 5G Security Threat Assessment in Real Networks. Sensors 2021, 21, 5524. Editor: Naoki Shibata, 2021.

[20] Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion,Volume 97, 2023, 101804, https://doi.org/10.1016/j.inffus.2023.101804

[21] Honghui Xu, Yingshu Li, Olusesi Balogun, Shaoen Wu, Yue Wang, Zhipeng Cai, Security Risks Concerns of Generative AI in the IoT, IEEE Internet Of Things Magazine, 2024