International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Research Article)

Developing and Evaluating Generative AI Models for Detection and Mitigation of Security Threats in 5G Networks

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.*

International Journal of Science and Research Archive, 2025, 17(03), 089–096

Publication history: Received on 25 October 2025; revised on 30 November 2025; accepted on 03 December 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.3.3194

Abstract

The rapid advancement of technology has enhanced the connectivity and data exchange but has also introduced challenges of security threats and vulnerabilities. This study explores the development of Generative Artificial Intelligence (GAI) models to detect and mitigate 5G networks threats. The proposed framework integrates Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and Large Language Models (LLMs), leveraging their unique strengths for cybersecurity. The hybrid framework achieves the superior performance with an accuracy of 97.5% and detects both known and unknown threats. Metrics such as detection accuracy, false positive rates (FPRs), computational efficiency, and robustness against the adversarial attacks are used to evaluate the system. The framework also demonstrates flexibility to adversarial threats, continuously learning, and improving threats detection and mitigation. The proposed framework of hybrid approach provides an adaptive approach to address new security challenges to the growing field of AI-driven cybersecurity.

Keywords: Generative AI; Cybersecurity; Threat Detection; Hybrid Approach; Metrics

1. Introduction

In today's digital era, enterprises face an increasingly complex and evolving landscape of cybersecurity threats that can compromise sensitive data, disrupt operations, and undermine system integrity [1]. To effectively combat these risks, organizations must adopt a holistic and adaptive cybersecurity approach that integrates advanced technological solutions, continuous employee training, and proactive risk management [2]. Understanding the diverse nature of potential threats is essential for developing comprehensive defense strategies that ensure resilience against sophisticated cyberattacks. As technology advances, maintaining a strong commitment to cybersecurity remains a top priority to safeguard enterprise systems and data [3]. The proliferation of digital technologies and interconnected systems has significantly transformed the modern world to foster the innovation and collaboration. This advancement in technology has also exposed several vulnerabilities and threats in cybersecurity to individuals, organizations, and even nations [4]. Cyberattacks and data breaches have become prevalent for targeting critical systems, sensitive data, and digital infrastructures. Traditional security mechanisms also struggling to cope with the increasingly of new threats [5]. GAI has emerged as a groundbreaking technology to address cybersecurity challenges [6]. Unlike conventional AI models which are designed for classification and prediction, the GAI is used to create new synthetic data mimic to real-world scenarios [7-8]. Technologies like GANs, VAEs, and LLMs simulate the attack patterns for generating datasets for training, testing, and also identify vulnerabilities. [9-10].

[*] Corresponding author: Amit Tiwari

The novelty of this research lies in its dual-purpose framework that employs GAI models for detecting and mitigating security threats which is a novel approach to make it different from traditional ML and DL methods. The advanced models like GANs and VAEs enables the simulation of attacks and vulnerabilities to develop the mitigation strategies. This study collects and preprocesses data for training and testing of GAI models to optimize for anomaly detection and early identification of security threats. This paper explores the GAI model for both detecting and mitigating security threats. Detection involves to identify anomalies, predicting of attacks, and malicious activities in real-time. Mitigation focuses to identify threats and vulnerabilities through intelligent response strategies. The proposed framework of hybrid approach of GAI models is used to enhance threat detection accuracy and reduce FPRs which are common drawbacks in existing systems.

2. Literature Review

The integration of AI in cybersecurity has gained significant momentum due to the increasing cyber threats. Traditional cybersecurity approaches for detecting and identifying threats are based on rule-based systems, signature matching, and heuristic methods [11-12]. These traditional methods are very useful against known attacks but struggle with zero-day attacks, and malware threats etc [13]. Studies have highlighted that traditional methods often suffer from high FPRs and limited scalability [13-15]. AI technologies are applied to enhance threat detection and response [16-18]. Machine learning (ML) models such as supervised and unsupervised learning algorithms have demonstrated the effectiveness in the anomaly and malware detection, classification in the intrusion detection systems (IDS) [19-20]. Authors have reviewed ML algorithms in cybersecurity and noted that supervised models perform well in structured datasets but that is not always be available.

The GANs have emerged as a powerful tool in cybersecurity, particularly in anomaly detection. These networks offer a novel approach to identifying irregular patterns and potential threats within network activities by generating synthetic data to train models for anomaly detection. Their ability to capture complex data patterns makes them well-suited for dynamic and evolving cybersecurity environments. Various studies have explored the strengths and limitations of different GAN architectures, considering factors such as robustness, scalability, and real-time processing capabilities. GANs have shown effectiveness in detecting previously unseen threats and adapting to changing attack patterns, though challenges remain in integrating them into existing cybersecurity frameworks. They also hold the potential to enhance threat detection accuracy while reducing false positives. Ongoing research explores hybrid approaches that combine GANs with other machine learning techniques to further optimize their performance. As GANs continue to evolve, they present a promising avenue for advancing anomaly detection capabilities and strengthening enterprise security frameworks.

The integration of adaptive generative models into cybersecurity is gaining prominence as organizations seek more effective ways to combat evolving threats. These models continuously learn from dynamic data, simulate various threat scenarios, and adapt to emerging challenges, providing a proactive defense mechanism for enterprise networks. Their adaptability strengthens cybersecurity resilience by enabling real-time threat detection and response. Similarly, machine learning techniques play a crucial role in addressing cybersecurity threats by identifying and mitigating risks as they emerge. By leveraging real-time threat detection mechanisms, machine learning enhances the ability of enterprises to swiftly recognize and counter cyber threats. The intersection of machine learning and cybersecurity fosters the development of robust and adaptive defense systems, ensuring enterprises maintain a proactive stance against evolving risks. Additionally, generative AI models contribute to cybersecurity by continuously learning from new threats and improving detection accuracy. Their real-time processing capabilities make them valuable assets in fortifying enterprise security against complex and rapidly changing cyber threats. As these technologies advance, they offer promising solutions for enhancing cybersecurity measures within dynamic enterprise environments.

The integration of AI into various tiers of cyber threat intelligence is progressing at different stages of development. Tactical Intelligence has moved beyond the experimental phase, with well-established applications aiding in the creation of functional cybersecurity systems. In contrast, Operational Intelligence remains in its early stages, requiring substantial resource investment for further advancement. There is growing interest in leveraging Recurrent Neural Networks to enhance Operational Cyber Threat Intelligence, ensuring seamless integration with Tactical Intelligence systems that focus on swiftly neutralizing imminent threats to networks and computer systems. Exploring this synergy can lead to more effective and adaptive cybersecurity strategies.

Additionally, the intersection of AI and cyber resilience plays a crucial role in strengthening defense mechanisms. AI-driven strategies, including ML algorithms, threat intelligence, and automated mitigation techniques, contribute to more effective threat detection and response. By enabling proactive identification of risks and facilitating rapid countermeasures, AI enhances an organization’s ability to withstand evolving cyber threats. The continuous advancement of AI-powered cybersecurity solutions is shaping a more resilient and adaptive approach to safeguarding enterprise systems.

3. Challenges and Limitations

The implementation of generative AI in cybersecurity faces several challenges and limitations. One significant hurdle is the high computational cost associated with deploying and maintaining these models, which demands substantial resources and infrastructure, making it difficult for smaller organizations to adopt. Additionally, generative AI tools may generate false positives, potentially overwhelming security systems and reducing overall operational efficiency. Another key limitation is the difficulty in accurately simulating all possible real-world adversarial scenarios, as attackers are constantly evolving their tactics, and generative models may struggle to predict new and emerging threats. Ethical concerns also emerge, particularly regarding the potential misuse of generative AI, which could lead to unintended and harmful consequences. Striking a balance between innovation and ethical oversight is essential to mitigate these challenges and ensure that generative AI remains an effective and responsible tool in enhancing cybersecurity defenses.

4. GAI-Driven Threat Detection and Mitigation Framework

This research proposes a novel and unique framework combining GAI models for the purpose of detecting and mitigating security threats and vulnerabilities as shown in Figure 1. The methodology in this framework is divided into four stages as data collection and preprocessing stage, threat detection stage, threat mitigation stage, and evaluation and feedback loop stage. Each stage is supported by the genAI techniques to ensure robustness and effective.

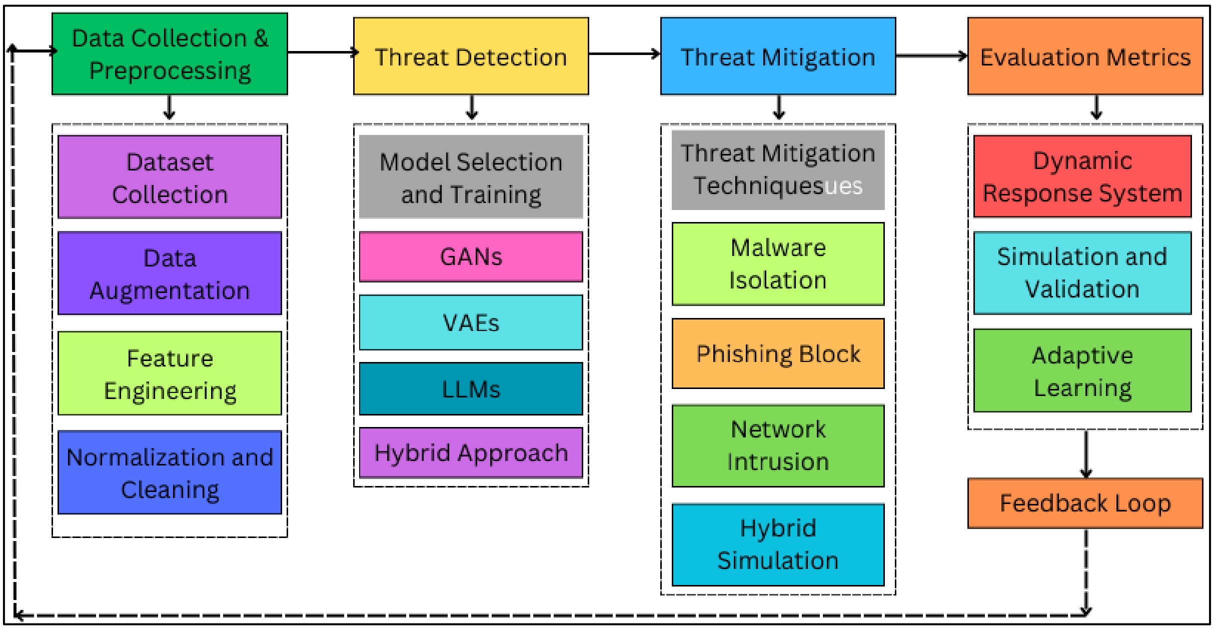

Figure 1 GenAI-based threats detection and mitigation framework

4.1. Data Collection and Preprocessing

The first step is data collection and preprocessing to prepare the data for effective training and testing of GAI models. Datasets are collected from the open sources of network traffic logs, phishing emails, malware signatures and system log files etc. The data undergoes through preprocessing stage for the noise removal, feature normalization, and handling of missing values to ensure a clean and consistent dataset for further processing. To mitigate the problem of the imbalance dataset, the GANs are employed to generate synthetic data to enhance dataset balance. The features like packet headers metadata and payload analysis are extracted by using deep feature extraction techniques.

4.2. Threat Detection

The proposed GAI models are used to detect anomalies and identify threats at an early stage. This process begins with model selection and its training on the dataset. GANs models simulates attacks to train the system for detecting various threat types. VAEs focus on anomaly detection when deviations occur. LLLMs such as GPT is used to analyze the textual data like phishing emails and malicious scripts to threat detection across multiple data.

4.3. Threat Mitigation

AI models are developed for mitigating detected threats like malware, phishing, network intrusion etc. A response system is implemented to generates response plan upon threat detection by using pre-trained GAI models. Detected threats are simulated using GANs to test and validate the response plans in the system. To ensure continual improvement the GAI models are updated with new attacks and mitigation strategies.

4.4. GAI Models

In the proposed framework for the analysis and mitigation of threat attacks, four different GAI models are used for selection and training.

- **GAN-Based Model:** A GAN-based model consists of two neural networks known as a Generator and a Discriminator trained in a competitive setting. The generator is used to create synthetic data such as fake attack or anomalies to mimic real data. The discriminator is used to evaluate whether the input data is real or generated. The GANs ensures that the generator improves over time to produce more realistic outputs. In cybersecurity, GANs generate diverse attacks to train models or simulate threats to enhance the system to detect and respond to new and evolving threats.

- **VAE-Based Model:** A VAE is also a generative model that represents high-dimensional data into a lower-dimensional data. It includes an encoder and decoder to compresses and reconstruct the data respectively. VAE is highly effective for anomaly detection in cybersecurity and to identify deviations as threats.

- **Large Language Model (LLM):** LLMs such as GPT or BERT are DL models trained on massive text datasets to understand and generate human-like text. In cybersecurity, LLMs are utilized for identifying text-based threats like phishing, social engineering, and malicious commands. They can analyze textual patterns, context, and semantics to detect anomalies or suspicious behavior. LLMs also contribute to mitigating threats by generating automated responses or aiding in the creation of security policies and guidelines.

- **Hybrid Model:** The hybrid model integrates the strengths of GANs, VAEs, and LLMs to create a robust cybersecurity framework that enhances threat detection and mitigation. The GAN component simulates attack patterns to enrich the system's training with diverse and novel threats. The VAE component models normal behavior to detect anomalies by identifying deviations from expected patterns. Meanwhile, the LLM component analyzes text-based threats to offer contextual understanding and detecting phishing or social engineering attacks. This comprehensive approach leverages the generative capabilities of GANs and VAEs for synthetic data and anomaly detection while LLMs enhance text analysis, ensuring dynamic adaptation to evolving threats. The integration of these models results in superior accuracy, resilience, and scalability to provide proactive threat detection and effective mitigation strategies.

4.5. Evaluation Metrics and Feedback Loop

The framework's performance is rigorously assessed using a multi-faceted evaluation approach. Detection metrics such as accuracy, precision, recall, F1-score, and FPRs are used to evaluate threat detection capabilities. Mitigation metrics like response time, computational efficiency, and the success rate of mitigation strategies measure the effectiveness of the framework's responses. Robustness metrics assess the system's resilience to adversarial inputs and its ability to handle zero-day threats. A feedback loop is established to incorporate evaluation results into model refinement to optimize model parameters and algorithms. New data and emerging threat scenarios are continuously integrated into the training process to enable the system to evolve dynamically with the cybersecurity landscape.

The proposed framework is unique due to its hybrid integration of GANs, VAEs, and LLMs to enable holistic threat detection and simulation-based mitigation. It offers real-time adaptive responses that dynamically mitigate threats with minimal human intervention to ensure swift action against evolving cyber threats. By incorporating a feedback-driven learning mechanism, the framework continuously refines its models and strategies to maintain adaptability to emerging attack patterns. It employs comprehensive metrics to balance detection accuracy, computational efficiency, and adversarial robustness to make it suitable for practical deployment. This innovative framework bridges the gap between detection and mitigation to provide a proactive and intelligent cybersecurity solution to address modern security challenges effectively.

5. Results and Discussion

The results of the GAI-based cybersecurity farmwork are presented in the tables 1 to 4 which cover detection accuracy, mitigation effectiveness, computational efficiency, and adversarial attacks

Table 1 Threat Detection Performance

Model	**Dataset**	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**FPR Rate (%)**
GAN-Based Model	Network Traffic	94.5	92.8	93.2	93.0	2.1
VAE-Based Model	Log Data	91.2	89.5	90.3	89.9	3.4
Large Language Model (LLM)	Phishing Emails	96.8	94.9	95.4	95.2	1.8
Hybrid Approach	Combined Data	97.5	96.2	96.8	96.5	1.5

Table 2 Threat Mitigation Performance

Threat Mitigation Techniques	**Mitigation Success Rate (%)**	**Average Response Time (ms)**	**Mitigation Strategy**
Malware Isolation	95.2	120	Quarantine infected system
Phishing Block	97.8	50	Block malicious URLs
Network Intrusion	93.5	140	Dynamic firewall rule generation
Hybrid Approach	96.0	90	Combined strategy

Table 3 Computational Efficiency

Task	**Model**	**Inference Time (ms)**	**Training Time (s)**	**Resource Consumption (RAM in GB)**
Threat Detection	GAN-Based Model	200	360	4.5
Threat Detection	VAE-Based Model	180	300	3.8
Mitigation Strategy	Hybrid Approach	250	480	5.2

Table 4 Adversarial Robustness

Model	**Attack Type**	**Detection Rate (%)**	**Robustness Improvement (%)**
GAN-Based Model	Evasion Attack	89.0	15
VAE-Based Model	Poisoning Attack	85.5	12
Hybrid Approach	Combined Attacks	94.0	18

Table 5 Overall Evaluation

Metric	Value
Detection Accuracy (%)	97.5
False Positive Rate (%)	1.5
Mitigation Success Rate (%)	96.0
Average Response Time (ms)	90
Adversarial Robustness Improvement (%)	18

The results demonstrate the effectiveness of the proposed GAI-ACF in addressing complex security threats across multiple dimensions. Table 1 highlights the threat detection performance of different models. The hybrid approach outperformed individual models to achieve the highest detection accuracy 97.5%, precision 96.2%, recall 96.8%, and F1-score 96.5% while maintaining the lowest FPR 1.5%. This superior performance of hybrid approach of integrating GANs, VAEs, and LLMs validates the results obtained on diverse datasets.

The performance of threat mitigation techniques is presented in Table 2. The hybrid approach has demonstrated the highest mitigation success rate of 96.0% and maintaining an average response time of 90 ms. Other strategies like phishing blocking and malware isolation are also showed high success rates but the hybrid approach has provided a better solution for real-world applications.

The computational efficiency, inference and training time, and resource consumption of of GAIs models are given in Table 3. The hybrid approach exhibited a slightly higher resource consumption of 5.2 GB RAM and inference time 250 ms compared to other models like GAN and VAE models. For the detection and mitigation of threats.

The results analysis of models is shown in Table 4 which highlights the ability of hybrid model to handle attack types and achieved the detection rate of 94.0% for combined attacks and demonstrated an 18% improvement. This indicates the framework's strenghth against evolving and complex threats to ensure the reliability of modern cybersecurity systems

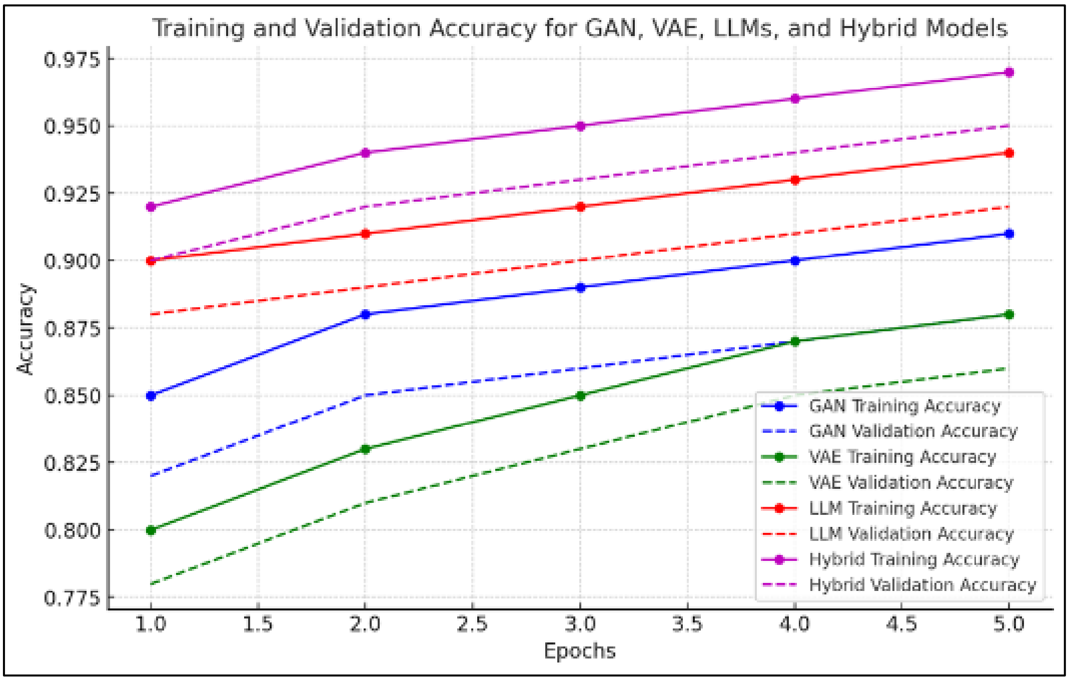

Figure 2 Training and validation accuracy curves of GAN, VAE, LLMs, and Hybrid models

The overall evaluation metrics in Table 5 provide a consolidated view of the framework's performance with a detection accuracy of 97.5%, a FPR of 1.5%, a mitigation success rate of 96.0%, and an average response time of 90 ms, the framework proves to be an efficient and reliable solution for dynamic threat detection and mitigation. The 18% improvement in adversarial robustness further emphasizes its capability to counter sophisticated attack scenarios to ensure a proactive defense mechanism. The results demonstrate that the GAI-ACF framework effectively bridges the gap between detection and mitigation. The hybrid approach, combined with advanced generative models and comprehensive evaluation metrics offers a scalable and robust solution to meet the demands of evolving cybersecurity challenges.

Figure 2 presents a comparison of four machine learning models like GAN, VAE, LLM, and Hybrid based on their training and validation accuracies. Solid lines represent training accuracy, and dashed lines indicate validation accuracy. The models are color-coded: blue for GAN, green for VAE, red for LLM, and magenta for Hybrid. The x-axis denotes epochs while the y-axis represents accuracy. As training progresses, training accuracy generally increases but validation accuracy may plateau or decrease in cases of overfitting. GAN shows slower improvement in validation accuracy with fluctuations, VAE exhibits steady but slightly lower validation accuracy, LLM achieves high training accuracy with a risk of overfitting, and the Hybrid model demonstrates strong performance in both metrics but may face occasional overfitting or underfitting. This visualization helps identify the model that generalizes best by examining the gap between training and validation accuracies, highlighting the most balanced performer.

6. Conclusions

This research presents a GAI-based cybersecurity framework that integrating GANs, VAEs, and LLMs to enhance threat detection and mitigation. The hybrid approach utilizes the strengths of each model to achieve superior performance in identifying both known and unknown threats with an accuracy of 97.5%. The system excels in detecting synthetic, anomaly, and text-based attacks while its capability to simulate and validate mitigation strategies improves response time and success rate. The framework demonstrates robust performance against attacks and its adaptive learning through simulation based on testing, highlights its effective solution for modern cybersecurity challenges.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

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

[2] Humphreys, D., Koay, A., Desmond, D. et al. AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business. AI Ethics 4, 791–804 (2024). https://doi.org/10.1007/s43681-024-00443-4

[3] Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T.B., Song, D.X., Erlingsson, Ú., Oprea, A., Raffel, C.: Extracting Training Data from Large Language Models. In: USENIX Security Symposium. (2020)

[4] Christen, M., Gordijn, B., Loi, M.: The Ethics of Cybersecurity. The International Library of Ethics. Law Technol. (2020). https://doi.org/10.1007/978-3-030-29053-5

[5] Naveen Vemuri, Naresh Thaneeru, Venkata Manoj Tatikonda, Adaptive generative AI for dynamic cybersecurity threat detection in enterprises, International Journal of Science and Research Archive, 2024, 11(01), 2259–2265

[6] López Delgado, J.L.; López Ramos, J.A. A Comprehensive Survey on Generative AI Solutions in IoT Security. Electronics 2024, 13, 4965. https://doi.org/10.3390/ electronics13244965

[7] Zhang, P.; Lu, J.; Wang, Y.; Wang, Q. Cooperative localization in 5G networks: A survey. Ict Express 2017, 3, 27–32.

[8] Meunier, B.; Cosmas, J. 5G Internet of Radio Light Virtual Reality System. In Proceedings of the IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Valencia, Spain, 6–8 June 2018; pp. 1–5.

[9] Service Providers of 5G. Available online: https://technosports.co.in/2020/12/20/the-top-5-service-providers-of-5g-networkin-2020/ (accessed on 5 September 2021).

[10] Baldi, G.; Diaz-Tellez, Y.; Dimitrakos, T.; Martinelli, F.; Michailidou, C.; Mori, P.; Osliak, O.; Saracino, A. Session-dependent Usage Control for Big Data. J. Internet Serv. Inf. Secur. 2020, 10, 76–92.

[11] Dash, L.; Khuntia, M. Energy efficient techniques for 5G mobile networks in WSN: A Survey. In Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 13 March 2020; pp. 1–5.

[12] Milovanovic, D.A.; Bojkovic, Z.S. An Evolution of 5G Multimedia Communication: New Ecosystem. In 5G Multimedia Communication; CRC Press: Boca Raton, FL, USA, 2020; pp. 129–156.

[13] Hui, H.; Ding, Y.; Shi, Q.; Li, F.; Song, Y.; Yan, J. 5G network-based Internet of Things for demand response in smart grid: A survey on application potential. Appl. Energy 2020, 257, 113972.

[14] Abdullah, M.; Altaf, A.; Anjum, M.R.; Arain, Z.A.; Jamali, A.A.; Alibakhshikenari, M.; Falcone, F.; Limiti, E. Future smartphone: MIMO antenna system for 5G mobile terminals. IEEE Access 2021, 9, 91593–91603.

[15] R.A. Ariyaluran Habeeb, F. Nasaruddin, A. Gani, I.A. Targio Hashem, E. Ahmed, M. Imran, Real-time big data processing for anomaly detection: A survey, Int. J. Inf. Manage. 45 (2019) 289–307.

[16] H. Fourati, R. Maaloul, and L. Chaari, A survey of 5G network systems: challenges and machine learning approaches, vol. 12, no. 2. Springer Berlin Heidelberg, 2021.

[17] Kim, C.; Chang, S.Y.; Kim, J.; Lee, D.; Kim, J. Automated, Reliable Zero-day Malware Detection based on Autoencoding Architecture. IEEE Trans. Netw. Serv. Manag. 2023, 20, 3900–3914. [CrossRef]

[18] Pavani, A.; Kathirvel, A. Machine Learning and Deep Learning Algorithms for Network Data Analytics Function in 5G Cellular Networks. In Proceedings of the 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 26–28 April 2023; pp. 28–33

[19] E. O'Connell, D. Moore, T. N.- Telecom, and undefined 2020, "Challenges associated with implementing 5G in manufacturing," mdpi.com, Accessed: Feb. 27, 2022. [Online]. Available: https://www.mdpi.com/2673-4001/1/1/5

[20] Fakhouri, H.N.; Alawadi, S.; Awaysheh, F.M.; Hani, I.B.; Alkhalaileh, M.; Hamad, F. A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions. Electronics 2023, 12, 4604. https://doi.org/10.3390/ electronics12224604