Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

Understanding and Mitigating Security Risks and Vulnerabilities in 5G Network Infrastructures with Integration of AI and ML

[1] Mukesh Kumar Bansal, [2] Mukesh Kumar Gupta
[1] Department of CSE, Suresh Gyan Vihar University Jaipur
[2] Department of EE, Suresh Gyan Vihar University Jaipur

Abstract: The rapid deployment of 5G networks promises transformative advancements in connectivity, data throughput, and low-latency communication, supporting innovations like IoT, smart cities, and edge computing. However, these advancements are introduced significant security risks and vulnerabilities that addressed to ensure robust and reliable network infrastructure. This research paper employs Generative AI (GAI) to analyze the primary threats which are associated with 5G networks, including like increased attack surfaces due to Internet of Things (IoT) proliferation, network slicing vulnerabilities, supply chain risks, privacy concerns, and potential for advanced persistent threats (APTs) etc. Through simulations and comparative analysis, this study highlights that Denial-of-Service (DDoS) attacks, poor isolation in network slicing, and supply chain compromises which are among the most severe risks in 5G ecosystems. This paper also discusses several legacy issues that stemming from backward compatibility with 4G networks, and the regulatory challenges which are posed by inconsistent global standards. The findings underscore the need for comprehensive mitigation strategies, such as robust security standards, continuous network monitoring, vendor security audits, and advanced encryption techniques etc. Addressing these challenges is a crucial to securing 5G networks and enabling the wide array of applications as they are designed to support.

Keywords: 5G Security, Generative AI, Network Vulnerabilities, DDoS Attacks, Network Slicing

1. Introduction

The rapid adoption and deployment of 5G technology mark a significant advancement in mobile communications, promising faster data speeds, lower latency, and the ability to support a vast number of connected devices. These capabilities are also enabled the proliferation of smart cities, autonomous vehicles, augmented reality, the IoT, and other innovative technologies etc [1]. However, with any technological breakthrough, the implementation of 5G networks introduces a myriad of security threats and vulnerabilities that must be addressed to ensure robust, secure, and reliable communication infrastructure etc. The enhanced features of 5G are beneficial to expand the attack surface and present new challenges for security experts [2].

One of the major challenges in 5G is the increased attack surface due to the explosion of connected devices particularly IoT devices. These devices are often come with limited security features which makes them vulnerable to exploitation. The heterogeneous nature of 5G networks that integrating traditional IT systems with critical infrastructure and IoT devices creates a complex interdependencies, so that attackers can exploit [3]. 5G's support for network slicing creates multiple virtual networks on a shared infrastructure which poses risks, if isolation between slices is compromised, and potentially allowing lateral movement by malicious actors [4].

The reliance on global supply chains for 5G hardware and software introduces additional risks. Hardware components and software solutions are sourced from multiple vendors that can be compromised before deployment, and making supply chain security which are a crucial concern. Firmware updates the necessary for maintaining performance and security which are also become a vector for malicious actors to introduce vulnerabilities [5]. Moreover, APTs represent a significant concern. These sophisticated attackers can infiltrate networks for extended periods, collecting sensitive data and potentially disrupting critical services etc [6].

Another area of concern is user privacy. The high precision of 5G network location tracking can expose the detailed user location data, and raising significant privacy concerns.

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

The vast amount of data generated by 5G-enabled devices can be targeted for interception, and increasing the risk of unauthorized access, and data breaches. Physical security threats also expand in 5G [7]. The decentralized nature of edge computing nodes and the proliferation of base stations are also increasing the number of physical targets vulnerable to attack.

Furthermore, the 5G networks is also must maintained the compatibility with legacy networks (such as 4G and 3G), which can inherit vulnerabilities from older technologies. These older devices may lack the security measures that required to protect data in the 5G environment to create the potential weak points within the network [8]. The vulnerabilities in signalling and communication protocols are used for interoperability between different networks which can be exploited for attacks such as eavesdropping or message modification.

The deployment of the 5G network also raises regulatory and compliance challenges. Due to the global nature of 5G infrastructure, inconsistencies in regulations between different countries can complicate the efforts to enforce security standards [9]. Ensuring the compliances with evolving regulations also places a considerable burden on network operators and making it essential to develop the universal standards and best practices for 5G security [10].

To mitigate these threats, robust security measures such as strong encryption, rigorous access controls, continuous network monitoring, and international collaboration on threat intelligence are essential. This paper also explores the vulnerabilities in 5G networks and leverages generative AI to analyze and address these risks effectively. The integration of GAI techniques offers a potential solution for threat detection, mitigation, and overall network resilience. Through this research, we provide insights into securing 5G networks against emerging threats and ensuring they remain resilient as they support increasingly critical and innovative services.

2. Literature Review

The advent of the 5G technology has garnered the significant attention from researchers, policymakers, and industry stakeholders due to its transformative potential in communication systems. This literature review discusses the existing work of related 5G security threats, vulnerabilities, and the potential of GAI to address these challenges.

Substantial research has explored the security threats which are posed by the deployment of 5G networks. The increased attack surface in 5G is a major concern because vast number of IoT devices are connected to these networks. These devices often lack robust security measures and making them highly susceptible to exploitation. The integration of heterogeneous networks with combining traditional IT systems, IoT devices, and critical infrastructure which introduces complex interdependencies and can be exploited for lateral movement attacks [11].

Network slicing is another emerging vulnerability within the 5G network architecture. The network slicing allows multiple virtual networks to operate on shared physical infrastructure [12]. The isolation between slices is not always secure. If a malicious actor compromises with one slice, then there is a risk of lateral movement across slices that potentially affects other virtual networks. The dynamic nature of resource allocation in the network slicing always opens the door for the DoS attacks which can disrupt the overall network performance [13].

The issues of supply chain security have also been widely discussed. The 5G network infrastructure relies on components which are sourced from diverse global vendors, and introducing the risk of hardware or software being compromised during manufacturing or distribution. Frequent firmware updates further compound this risk as a malicious update could introduce vulnerabilities into the network [14]. Supply chain integrity must be verified through continuous auditing and stringent security protocols to mitigate these risks.

APTs are a significant concern in the 5G networks due to their stealthy and long-term nature [15]. APTs are capable of infiltrating networks and remaining undetected sensitive data during collection or sabotaging operations [16]. The sophisticated techniques, such as encryption and evasion methods, make detection and mitigation are extremely challenging. Real-time network monitoring and anomaly detection are crucial in combating APTs effectively.

Privacy concerns is related to 5G networks have also emerged as a focal point. The high-precision location tracking is enabled by 5G has the potential to expose detailed user location information, and posing significant privacy risks etc [17]. The vast amount of data generated by the 5G networks makes them an attractive target for data interception and unauthorized access [18]. Robust encryption methods and privacy-preserving technologies

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

such as differential privacy are essential to mitigate these risks and protect user data.

Physical infrastructure vulnerabilities in the 5G networks are another area of concern. The proliferation of 5G network base stations and edge computing nodes increases the number of physical targets for attacks [19]. Disruptions at these physical points can be compromised network availability and security. Furthermore, edge computing while enhancing performance and decentralizes computing power that creates new security challenges due to the distribution of data across multiple nodes [20].

Protocol vulnerabilities in the 5G networks are also present significant risks [21]. The Signalling protocols used in these networks are susceptible to attacks such as eavesdropping, impersonation, and message modification. Compatibility issues between different network protocols, including legacy systems can create security loopholes that attackers can exploit [22]. The development of secure signalling protocols is therefore essential to enhance the resilience of the 5G networks.

In recent years, GAI has emerged as a promising tool for identifying and mitigating security risks in the 5G networks. Generative adversarial networks (GANs) can simulate cyberattacks and identify potential vulnerabilities in 5G infrastructure. By generating synthetic attack scenarios, the security systems can be trained to detect and respond to previously unseen threats [23]. The GAI can be used for anomaly detection, where AI models learn to distinguish between normal network behavior and potentially malicious activities.

Generative AI can also enhance threat intelligence by predicting new forms of cyberattacks based on historical data [24]. This proactive approach also allows for the development of more resilient security mechanisms. Moreover, the use of GAI for data augmentation in the 5G networks can also help to improve the robustness of machine learning models that are used for threat detection, making security systems more capable of identifying evolving threats [25].

The literature underscores the multifaceted nature of security threats in 5G networks, ranging from increased attack surfaces, network slicing vulnerabilities, and supply chain risks to advanced persistent threats and privacy concerns. While traditional security measures are essential, the integration of GAI offers innovative solutions for threat detection, mitigation, and overall network resilience. The combination of real-time monitoring, encryption, secure protocols, and AI-driven threat intelligence is crucial for addressing the evolving challenges in 5G security. This research builds upon these findings by exploring the application of generative AI to analyze and mitigate security risks in 5G networks, offering a comprehensive approach to securing next-generation communication infrastructure.

3. 5G Infrastructure

5G infrastructure hardware primarily consists of four key components: the Radio Access Network (RAN), which connects end-user devices; the core network, which provides various services to customers interconnected via the access network; the backhaul, which links the backbone and edge networks; and transport infrastructure, which facilitates communication between the 5G RAN and the core network.

The rapid adoption of AI and machine learning (ML) in telecom infrastructure, particularly for enhancing network performance and customer experience, has led to a rise in malicious attacks. Adversarial AI attacks have surged in recent years, coinciding with the rapid rollout of 5G services. According to Deepsig:

- 55% of decision-makers believe AI enhances customer experience,
- 70% consider AI-driven network planning as the optimal method for transitioning to 5G, and
- 64% will focus their AI initiatives on improving network performance.

As AI and ML applications expand, so do the associated security risks in 5G networks as shown in figure 1. Malicious actors can compromise AI systems through:

- System bypassing by crafting deceptive files or injecting noise,
- Result manipulation by tampering with processed data or interacting maliciously with chatbots, and
- Data exfiltration by identifying, copying, and transferring sensitive information.

4. 5G Technology Overview

4.1 Application Areas

The International Telecommunication Union Radiocommunication Sector (ITU-R) defines three primary application areas for 5G capabilities:

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

Enhanced Mobile Broadband (eMBB)

- Function: eMBB is a progression from 4G LTE, offering faster connections, higher throughput, and increased capacity.
- Use Cases: Ideal for high-traffic environments such as stadiums, urban centers, and concert venues, enabling seamless streaming, downloads, and connectivity.

Ultra-Reliable Low-Latency Communications (URLLC):

- Function: Designed for mission-critical applications requiring extremely reliable and low-latency communication.
- Use Cases: Suitable for sectors like healthcare (remote surgeries), autonomous driving, and industrial automation, where even a slight delay can be critical.
- Technology: Utilizes short-packet data transmission to meet stringent latency and reliability standards.

Massive Machine-Type Communications (mMTC)

- Function: Facilitates connectivity for a vast number of IoT devices.
- Use Cases: IoT networks, smart cities, and large-scale sensor deployments. Drones and connected vehicles will also benefit, aiding in tasks like disaster recovery and tele-operations for autonomous systems.

4.2 Performance Metrics

Speed

- Peak Data Rates: 5G can deliver speeds up to 20 Gbps.
- Real-World Speeds: In the U.S., T-Mobile recorded average download speeds of 186.3 Mbps. South Korea leads globally with average speeds of 432 Mbps.
- Frequency Bands: Sub-6 GHz (Mid-band): Data rates between 10 Mbps to 1 Gbps. Low-Band (n5): Offers wider coverage but lower speeds (5–250 Mbps). mmWave (High-band): Can achieve speeds up to 5.9 Gbps (record as of 2023).

Latency

- Ideal Air Latency: Between 8 to 12 milliseconds (excluding retransmissions and handovers).
- Real-World Example: Verizon's early deployment reported latency of 30 ms.
- Edge Computing: Servers near towers can reduce latency to 10–15 milliseconds.
- Handovers: Latency during handovers ranges from 50 to 500 milliseconds.

Error Rate

- Adaptive Modulation: 5G uses an adaptive modulation and coding scheme (MCS) to maintain a low block error rate (BLER). When errors exceed a threshold, the transmitter reduces speed to improve accuracy.

Range

- Factors: Depends on frequency, power, and interference.
- Frequency Comparison: mmWave (e.g., n258): Shortest range. Mid-Band (e.g., n78): Moderate range. Low-Band (e.g., n5): Longest range.

4.3 Standards

IMT-2020

- Definition: The ITU's IMT-2020 standard requires peak download speeds of 20 Gbps and upload speeds of 10 Gbps.

5G NR (New Radio)

- Overview: Developed by 3GPP, 5G NR is the global air interface standard for 5G networks.
- Frequency Ranges: FR1 (Sub-6 GHz): For broader coverage. FR2 (Above 24 GHz): For high-speed, low-latency applications.
- Deployment: First commercial launches occurred in 2018, with widespread deployments starting in 2019.

5Gi (India-Specific Variant)

- Development: Created by IIT Madras, IIT Hyderabad, TSDSI, and CEWiT.
- Purpose: Enhances rural coverage with Low Mobility Large Cell (LMLC) technology.
- Status: Merged with 5G NR in 3GPP Release 17 (April 2022).

4.4 Fronthaul Network

- Architecture: Divides the connection between the Remote Radio Head (RRH) and the Base Band Unit (BBU) into two segments: NGFI-I (RU to DU): Next Generation Fronthaul Interface for Radio Units to Distributor Units. NGFI-II (DU to CU): Interface between Distributor Units and Central Units.
- Standards: Defined by IEEE 1914.1 and IEEE 1914.3 for efficient data transmission and network performance.

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

This structured breakdown covers 5G's application areas, performance characteristics, and standards comprehensively.

5.5 Security Attacks and Mitigation Approaches

The integration of AI and ML into 5G infrastructure significantly enhances network performance and resource management. However, it also introduces various security vulnerabilities. This section categorizes these security threats and presents systematic mitigation strategies to safeguard AI-driven 5G systems. The summary of attacks and its mitigations are illustrated in table1.

5.1 Poisoning Attacks

In a poisoning attack, intruders inject malicious or irrelevant data into the AI training repository to corrupt and weaken the model's functionalities. This can degrade network performance and lead to unreliable predictions.
Mitigation Approaches

- Data Quality Control: Perform thorough pre-processing in a controlled environment to ensure data integrity.
- Data Sanitization: Cleanse the data to remove potential threats and anomalies.
- Source Management: Block data ingestion from unmanaged or unverified sources.
- Ensemble Models: Use ensemble models to maintain accurate outputs despite compromised datasets.

In a 5G Open Radio Access Network (O-RAN) infrastructure, AI and ML models (e.g., Recurrent Neural Networks – Long Short-Term Memory, RNN-LSTM) are used for traffic prediction and radio resource optimization. These models require large volumes of historical data and periodic retraining. Attackers may exploit this process to inject irrelevant data and corrupt the model. Implementing robust management policies to restrict data ingestion to trusted sources can mitigate such attacks.

5.2 Backdoor Attacks

Backdoor attacks involve embedding malicious functionality within the AI model. Only attackers know the specific triggers that activate these malicious behaviors, typically by manipulating the model during training or incorporating hidden rules.
Mitigation Approaches

- Data Quality Enhancement: Improve data quality and integrity checks.
- Trigger Detection: Identify statistical anomalies between legitimate and malicious inputs.
- Regular Retraining: Periodically retrain models to deactivate discovered triggers.
- Data Pruning: Remove compromised data points from the training set.

In multi-supplier 5G environments, backdoors can infiltrate the supply chain. Identifying statistical differences between inputs and triggers and retraining the AI model at regular intervals can mitigate these threats.

5.3 Evasion Attacks

In evasion attacks, attackers subtly modify input data, causing the AI model to misclassify malicious inputs while maintaining its overall performance on regular data. The Mitigation approaches are given as:

- Data Compression: Compress data to reduce vulnerabilities.
- Null Libelling: Apply null labels to negatively impacted inputs.
- Attribute Preservation: Ensure essential attributes of inputs and outputs are preserved.
- Ensemble Models: Use ensemble models to maintain robust predictions.

Due to the open and broadcast nature of 5G wireless communications and the heterogeneity of IoT data, networks are vulnerable to evasion attacks. Attackers can observe spectrum patterns, predict transmission outputs using deep neural networks, and either jam transmissions or manipulate sensing phases. Preserving corrected inputs and outputs can mitigate such attacks.

5.4 Model Stealing Attacks

In model stealing attacks, adversaries create replica models by querying the live system or accessing APIs. These replicas can be used to generate adversarial samples or clone proprietary models. The Mitigation approaches are given as:

- Model Enhancement: Regularly update and refine models to prevent replication.
- Watermarking: Embed digital watermarks to protect model ownership.
- Query Control: Monitor and restrict API calls to prevent excessive or suspicious queries.
- Suspicious Activity Detection: Implement mechanisms to detect unusual query patterns.

Adversaries can clone proprietary 5G AI models (e.g., proactive maintenance or cost prediction models) by exploiting black-box access through API queries.

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

Restricting API usage, improving models with fresh data, and using watermarking techniques can mitigate this risk.

5.5 Data Extraction Attacks

Data extraction attacks aim to leak sensitive information, such as Personally Identifiable Information (PII), by analyzing input-output pairs and the associated confidence levels of AI models. The Mitigation approaches are given as:

- Privacy Controls: Embed privacy-preserving techniques into training datasets.
- Regular Privacy Audits: Quantitatively measure and evaluate privacy controls at regular intervals.
- Query Restriction: Limit and secure API calls to prevent unauthorized data extraction.
- Suspicious Query Detection: Monitor queries to detect potential data extraction attempts.

PII data is often used in 5G AI models. Implementing strict data privacy policies and securing API calls can help prevent PII data theft.

5.6 Some other 5G security risks include

Cyber-Attacks: 5G networks will be exposed to various cyber threats, including Distributed DDoS attacks, potential data breaches, and ransomware. The higher data speeds and lower latency provide cybercriminals with new opportunities to launch sophisticated attacks.

Supply Chain Vulnerabilities: With 5G infrastructure being built by multiple vendors across the globe, the supply chain becomes complex and potentially more vulnerable to security breaches. A compromised component within the supply chain could lead to widespread vulnerabilities. But at the same time, supply chain competition can drive innovation and enhancements.

Privacy Concerns: The massive influx of data generated by 5G-connected devices raises privacy issues. Unauthorised access to sensitive information can have negative consequences for individuals and organisations.
IoT Vulnerabilities: The proliferation of the IoT devices on 5G networks creates a challenge in securing these devices, as many IoT devices may not yet have robust security features.

The deployment of 5G technology offers immense advantages, such as ultra-fast connectivity and support for a vast number of devices. However, these benefits come with notable security threats and vulnerabilities.

Table 1: Summary of attacks and mitigations

Attack Type	Description	Mitigation Approaches
Poisoning	Injecting malicious data into the training set	Pre-processing, data sanitization, trusted sources, ensemble models
Backdoor	Implanting malicious triggers in the model	Data quality enhancement, trigger detection, regular retraining, data pruning
Evasion	Modifying inputs to evade detection	Data compression, null labeling, attribute preservation, ensemble models
Model Stealing	Creating replica models through queries or API access	Model enhancement, watermarking, query control, suspicious activity detection
Data Extraction	Extracting sensitive data from input-output pairs	Privacy controls, regular audits, query restriction, suspicious query detection

By understanding these attack vectors and implementing the corresponding mitigation strategies, telecom operators can enhance the resilience of AI-driven 5G networks against emerging security threats**.**

6. Prioritizing Mitigation Efforts

In securing AI-driven 5G networks, telecom organizations must prioritize mitigation strategies based on the prevalence, complexity, and potential impact of various attack types. A structured approach can help allocate resources effectively to minimize security risks.

6.1 Attack Prioritization Framework

Poisoning and Evasion Attacks
These are the most common types of attacks. They degrade the accuracy and reliability of AI models by injecting or modifying data inputs. The mitigation priorities will be as given below:

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

- Regular Data Sanitization
- Robust Data Quality Systems
- Continuous Data Validation

Backdoor Attacks

These are the most difficult attacks to detect due to hidden triggers and implanted malicious functionalities. They can compromise the integrity of the AI model, leading to unpredictable behavior. The mitigation priorities will be as given below:

- Statistical Anomaly Detection
- Regular Model Retraining
- Data Pruning

Model Stealing and Data Extraction Attacks

These attacks pose the greatest threat to data security, potentially leading to the theft of proprietary models and sensitive information. The mitigation priorities will be as given below:

- Watermarking and Digital Ownership Protection
- Restricted API Access
- Suspicious Query Detection

6.2 Best Practices for Risk Mitigation

- Content Sanitization: Ensure data is cleansed of potential threats before training AI models.
- Robust Data Quality Systems: Implement systems to maintain the integrity and accuracy of training data.
- Continuous Validation: Regularly validate incoming data to detect anomalies or malicious inputs.
- Model Retraining: Frequently retrain AI models with updated, verified data to mitigate emerging threats.

7. Results and Discussion

7.1 5G Network Security Threats Analysis

The deployment of 5G technology offers numerous benefits but also presents an array of security threats. Our analysis, augmented by generative AI, highlighted critical security vulnerabilities across multiple dimensions of the 5G infrastructure. These vulnerabilities were categorized into distinct areas, including increased attack surface, network slicing, supply chain risks, and privacy concerns as given in table 2.

Table 2: summarizes the identified threats along with their potential impacts and likelihood of occurrence.

Category	Threat Description	Potential Impact	Likelihood
Increased Attack Surface	IoT and heterogeneous devices increase entry points for attacks	High	Very Likely
Network Slicing Vulnerabilities	Poor isolation between slices leading to lateral movement of attackers	Severe	Likely
Supply Chain Risks	Hardware/software compromise before deployment	Severe	Likely
Advanced Persistent Threats (APTs)	Long-term infiltration and data theft	Critical	Moderate
Privacy Concerns	Location tracking and unauthorized data access	High	Likely
Physical Infrastructure Attacks	Disruption of base stations or edge computing nodes	High	Moderate
Protocol Vulnerabilities	Exploitable flaws in signalling and control protocols	Severe	Likely
Legacy Issues	Inherited vulnerabilities from older networks	Moderate	Likely
Cyberattacks	Amplified DDoS attacks and malware distribution	High	Very Likely
Regulatory Challenges	Inconsistent security regulations across regions	Moderate	Moderate

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

7.2 Simulation Results Using GAI Models

To quantify these threats, generative AI models were employed to simulate attack scenarios and predict potential vulnerabilities. The results showed in table 3 that increased attack surface and cyberattacks are the most prevalent threats, particularly due to the vast number of connected IoT devices in 5G networks. Our models indicated that the likelihood of Distributed DDoS attacks is significantly higher in 5G networks compared to 4G due to the expanded bandwidth and reduced latency.

Table 3**:** Comparative analysis of security threats in 4G and 5G networks based on their likelihood and severity.

Threat Category	4G Likelihood	4G Severity	5G Likelihood	5G Severity
DDoS Attacks	Moderate	High	Very Likely	Severe
Supply Chain Risks	Low	Moderate	Likely	Severe
Privacy Concerns	Moderate	Moderate	Likely	High
Network Slicing Vulnerabilities	N/A	N/A	Likely	Severe
Physical Infrastructure Attacks	Low	Moderate	Moderate	High

7.3 Discussion of Findings

The findings reveal that the heterogeneous nature of 5G networks and the massive proliferation of IoT devices drastically increase the attack surface, making 5G networks more susceptible to a variety of cyberattacks. Notably, the simulation results emphasize the potential for DDoS attacks to be far more severe in 5G due to its high data throughput and low latency.

Network slicing vulnerabilities were found to pose a significant risk, especially if the isolation between slices is not strictly maintained. Poor isolation could allow attackers to move laterally across slices, impacting critical services.

Supply chain risks remain a critical challenge, as 5G infrastructure components are sourced from multiple vendors. The threat of compromised hardware or software before deployment underscores the importance of strict vendor auditing and secure firmware updates.

Furthermore, privacy concerns are exacerbated by 5G's ability to provide granular location data. Generative AI simulations demonstrated that privacy breaches could occur more frequently if robust encryption and access controls are not implemented.

7.4 Mitigation Strategies

The results suggest several mitigation strategies to enhance 5G security:

- Robust Security Standards: Enforcing standardized security protocols across all components of the 5G infrastructure.
- Network Monitoring: Continuous real-time monitoring to detect anomalies and potential intrusions.
- Vendor Security Audits: Ensuring vendors comply with strict security measures to mitigate supply chain risks.
- Advanced Encryption Techniques: Implementing strong encryption to protect data during transmission and storage.

By addressing these challenges with targeted security measures, it is possible to mitigate the majority of identified risks and create a more secure 5G ecosystem.

This structure combines detailed analysis, tables for clarity, and a discussion of findings with proposed mitigation strategies. Let me know if you need further refinement!

Conclusion

The deployment of 5G networks presents both tremendous opportunities and significant security challenges. The integration of AI and machine learning into 5G infrastructure, while enhancing network performance and customer experience, also introduces new vulnerabilities. As 5G networks become more complex, with increased attack surfaces, network slicing, and the reliance on diverse vendors, the risks of malicious exploitation escalate. Advanced persistent threats, privacy concerns, physical infrastructure vulnerabilities, and protocol weaknesses further complicate the security landscape. However, the emerging role of generative AI offers promising avenues for proactive threat detection and mitigation, enabling more resilient and adaptive security measures. To address these challenges, a comprehensive approach involving robust security standards, continuous monitoring, supply chain integrity, and the adoption of privacy-preserving technologies is essential. Collaboration among stakeholders across industries and regions is crucial for sharing threat

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

intelligence and ensuring that 5G networks remain secure, efficient, and capable of supporting the next generation of digital services. As the adoption of 5G continues to expand, safeguarding the integrity of the infrastructure will be vital in ensuring its success and protecting users from emerging threats.

References

1. Marabissi, D.; L. Mucchi; R. Fantacci; et al.; "A Real Case of Implementation of the Future 5G City," Future Internet, vol. 11, iss. 1, 2 December 2018, https://doi.org/10.3390/fi11010004
2. Peterson, L.; O. Sunay; 5G Mobile Networks: A Systems Approach, Systems Approach LLC, USA, 2022, https://5g.systemsapproach.org/
3. Rodriguez, J.; Fundamentals of 5G Mobile Networks, John Wiley and Sons, Inc., USA, 2015
4. Akgun, B.; "Achieving Secure Communications in Dense Multiuser Mimo Systems for 5G and Beyond," The University of Arizona, Tucson, USA, 2019, https://repository.arizona.edu/handle/10150/636623
5. Du, Z.; B. Jiang; Q. Wu; Y. Xu; K. Xu; Towards User-Centric Intelligent Network Selection in 5G Heterogeneous Wireless Networks, Springer Singapore, Singapore, 2020
6. Dun and Bradstreet, "Wireless Telecommunications Equipment Manufacturing," First Research Industry Profiles, 27 May 2019, https://www.proquest.com/reports/wireless-telecommunications-equipment/docview/2234482578/se-2?accountid=44888
7. Mishra, A.; Fundamentals of Network Planning and Optimisation 2G/3G/4G: Evolution to 5G, 2nd Edition, John Wiley and Sons, Inc., USA, 2018
8. Liyanage, M.; I. Ahmad; A. Abro; A. Gurtov; M. Ylianttila; A Comprehensive Guide to 5G Security, John Wiley and Sons, Ltd., USA, 2018
9. Huawei, Securing the Future of 5G, AI Business eBook Series, China, 2022
10. Launay, F.; A. Perez; LTE Advanced Pro: Towards the 5G Mobile Network, John Wiley and Sons, Inc., USA, 2019
11. Penttinen, J.; 5G Explained: Security and Deployment of Advanced Mobile Communications, John Wiley and Sons, Inc., USA, 2019
12. Pujolle, G.; Software Networks: Virtualization, SDN, 5G and Security, 2nd Edition, John Wiley and Sons, Inc., USA, 2019
13. Latif, S.; J. Qadir; S. Farooq; M. Imran; "How 5G Wireless (and Concomitant Global 5G Infrastructure Market Revenues 2020-2030." Statista, August 11, 2022. https://www.statista.com/statistics/1256267/worldwide-5g-infrastructure-market-revenues.
14. Global 5G Security Market (2021 to 2026) - by Technology, Solution, Category, Software, Services, and Industry Vertical Support." GlobeNewswire News Room. Research and Markets, May 14, 2021.
15. R. Santos, D. Souza, W. Santo, A. Ribeiro, and E. Moreno, "Machine Learning Algorithms to detect DDoS Attacks in SDN," Concurrency and Computation: Practice and Experience, vol. 32, no. 16, p. e5402, 2020
16. M. Yao, M. Sohul, V. Marojevic, J.H. Reed, Artificial intelligence defined 5G radio access networks, IEEE Commun. Mag. 57 (3) (2019) 14–20.
17. S. Jayasinghe, Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Federated Learning based Anomaly Detection as an Enabler for Securing Network and Service Management Automation in Beyond 5G Networks," in 2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 2022, pp. 345–350
18. J. Kaur, M.A. Khan, M. Iftikhar, M. Imran, Q.E.U. Haq, Machine learning techniques for 5G and beyond, IEEE Access 9 (2021) 23472–23488.
19. M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Multi-stage Optimized Machine Learning Framework for Network Intrusion Detection," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1803–1816, 2020
20. 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.
21. 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.
22. 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]
23. 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

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.11 Issue 1 Page No 10-19

24. 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
25. 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

Correspondence to: Mukesh Kumar Bansal, Department of Computer Science and Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: mkbansal.edu@gmail.com