World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Externalities of Cybersecurity Threats in United States 5G Deployments: Impacts on Internet of Things (IoT) Ecosystems and Cloud Computing Integration

Akibu Abiodun Oni [1,*], Raymond Tay [2] and Brian Otieno Odhiambo [3]

[1] *Department of Management Studies, Lagos State University, PMB 0001, LASU Post Office, Lagos State, Nigeria.*
[2] *College of Engineering (MS Telecommunication Networks), Northeastern University, Boston, MA, USA.*
[3] *Department of Business and Economics (MS Business Analytics and Information Technology), University of Nairobi, Nairobi, Kenya.*

World Journal of Advanced Research and Reviews, 2024, 22(03), 2358-2377

Publication history: Received on 26 April 2024; revised on 24 June 2024; accepted on 26 June 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.3.1730

Abstract

The introduction of fifth-generation (5G) wireless networks in the United States can be used as a revolution in technology. Nevertheless, this development brings up important cybersecurity externalities with respect to Internet of Things (IoT) systems and cloud computing interoperability. This study was a systematic study of the cybersecurity threats in U.S. 5G deployments that concentrated on vulnerabilities in the IoT networks and cloud infrastructure. The mixed-method approach was used that included the quantitative analysis of network vulnerability data and the evaluation of threat landscapes qualitatively. The sources of the data collection were various databases of cybersecurity compromises by the government, reports by industries, and academic sources published between 2020-2024. Statistical calculations showed that 5G network was found to have 47.3 percent more vulnerability rates than 4G infrastructure. The number of network slicing vulnerabilities (34.6) and IoT device exploitation (41.2) had the largest share of threats and security incidents, respectively. The 24.2% of reported vulnerabilities were cloud integration challenges. The regression analysis (R2 = 0.683, p = 0.001) showed the presence of significant correlation between the level of cybersecurity incidents and the density of 5G deployment. The analysis single out four domains of critical vulnerability as network architecture, IoT device security, cloud connection vulnerability, and supply chain risks. The results of the research showed that the development of multi-tenant 5G settings posed more difficult isolation problems, and cross-slice attacks have risen by 56.8 percent after extensive implementation. Findings highlighted the need to have improved encryption policies, zero-trust systems, and all-inclusive security models. Some of the recommendations were the use of AI-based systems of threat detection, better security of the supply chain, and the creation of uniform security guidelines. The study adds to the knowledge of externalities of cybersecurity in 5G ecosystems and offers practical recommendations to policymakers, industry experts, and cybersecurity experts.

Keywords: 5G Networks; Cybersecurity Threats; Internet Of Things; Cloud Computing Integration; Network Slicing Vulnerabilities; Iot Security; Cyber Attacks; Wireless Security; Edge Computing; Zero-Trust Framework

1. Introduction

The implementations of the fifth-generation (5G) wireless technology have transformed the entire United States telecommunications environment in ways never experienced before. Reports by the Federal Communications Commission (2024) show that 5G networks had reached nearly 72.4% of the population of the U.S. by the beginning of 2024. This very rapid growth significantly changed the paradigm of connectivity, allowing ultra-low latency communication and connectivity of very large numbers of devices. A study by Ahmad et al. (2017) confirmed that the 5G technology has a data transmission speed that is more than 10 Gbps. Also, network latency reduced to within 1

* Corresponding author: Akibu Abiodun Oni

millisecond under ideal conditions. The technology boosted the unprecedented level of interconnection of devices of the Internet of Things in critical infrastructure areas.

However, the technological transformation came with complicated cybersecurity issues with very extensive implications. The research conducted by Abdulqadder et al. (2024) proved that the complexity of the 5G architecture resulted in numerous attack vectors. The transition to software-defined networking in relation to hardware changed the threat landscapes fundamentally. Pirbhulal et al. (2024) conducted a study regarding the 5G security frameworks and found that network slicing implementations had major weaknesses. Moreover, the inclusion of edge computing increased the possible attackers manifold. The 5G infrastructure was decentralized making more challenging the traditional security methods.

Interrelation of the 5G networks, IoT ecosystems and cloud computing infrastructure established cybersecurity externality that was never seen before. The spread of IoT devices in 5G settings increased the security risks, as attackers exploited loopholes in device authentication systems and encryption algorithms. Moreover, there were challenging multi-tenancy security issues that arose as a result of cloud computing integration with 5G networks. Research by Girma and Barrett (2024) made it clear that the lack of isolation between network slices allowed cross-contamination attacks. Other than these architectural weaknesses, supply chain security became a major issue of concern.

Cybersecurity threats to 5G did not only impact the economic and national security of individual organizations. The U.S. Department of Homeland Security (2023) claimed that the 5G vulnerabilities were high in critical infrastructure sectors. No more than healthcare systems, transportation networks, and energy grids became more dependent on 5G connectivity. According to research by Wajdi et al. (2024), 5G networks can be compromised, potentially disrupting the network of key services to millions of people. In addition, cyber attackers sponsored by the state became more vulnerable to infrastructural sabotage and espionage of 5G infrastructure. The complexity of the interdependence of contemporary infrastructure magnified possible cascading failure situations.

1.1. Statement of the Problem

The blistering implementation of 5G wireless networks in the United States infrastructure created considerable cybersecurity externalities to Internet of Things as well as cloud computing intertwining. Although it invested more than $275 billion in 5G infrastructure, complete security setups were outpaced by deployment schedules. This time gap led to gaps that were used by advanced threat groups to cause cascading security events in interconnected systems. The issue presented itself in three problematic dimensions: first, 5G-based IoT devices were vulnerable to exploitation at a rate that was 67.3% greater than the one of predecessor technologies; second, cloud-based computing integration points were exposed to attacks with a higher likelihood of more than 42.8% associated Externality; and third, externalities of security attacks entailed estimated costs of over $12.4 billion yearly and impacted sectors. The lack of standard security, poor supply chain security and a lack of a common effort among the stakeholders made these issues worse. In the absence of in-depth knowledge of cybersecurity threat exterapolation and how these systems spread using 5G-IoT-cloud ecosystems, there should have been no effective mitigation approaches to the problem, endangering the national security interests and economic stability.

Research Objectives

- The primary objectives of this research were:
- To identify and categorize cybersecurity threats specific to 5G network deployments in the United States, distinguishing them from vulnerabilities present in previous generation wireless technologies.
- To analyze the mechanisms through which cybersecurity threats in 5G networks create externalities affecting Internet of Things ecosystems and cloud computing infrastructure integration.
- To assess the national security and privacy implications of cybersecurity vulnerabilities in 5G deployments, particularly regarding critical infrastructure protection and personal data security.
- To develop evidence-based recommendations for mitigating cybersecurity threats in 5G ecosystems, addressing technical, policy, and organizational dimensions of security enhancement.

1.2. Research Questions

This study addressed the following research questions:

- RQ1: What are the primary cybersecurity threats unique to 5G network deployments in the United States, and how do they differ from vulnerabilities in 4G LTE and earlier wireless technologies?

- RQ2: How do cybersecurity threats in 5G networks create externalities that impact Internet of Things device security and cloud computing infrastructure integration?
- RQ3: What are the implications of 5G cybersecurity vulnerabilities for national security, critical infrastructure protection, and individual privacy in the United States?
- RQ4: What technical, policy, and organizational measures can effectively mitigate cybersecurity threats in 5G deployments while supporting continued innovation and service expansion?

Research Hypotheses

Based on literature review and preliminary analysis, the following hypotheses were formulated:

- H1: 5G network deployments demonstrate significantly higher vulnerability rates compared to 4G LTE networks, with network slicing and edge computing representing the most critical threat vectors ($\alpha = 0.05$).
- H2: There exists a significant positive relationship between 5G deployment density in geographic areas and the frequency of cybersecurity incidents affecting IoT devices and cloud computing infrastructure ($\alpha = 0.05$).
- H3: Implementation of comprehensive security frameworks incorporating zero-trust architecture, AI-driven threat detection, and enhanced encryption protocols significantly reduces cybersecurity incident rates in 5G networks compared to traditional security approaches ($\alpha = 0.05$).

Scope and Limitations

The study specifically addressed cybersecurity externalities in the 5G deployment in the United States between 2020-2024. Geographic focus restricted analysis to domestic infrastructure whereas international comparisons were used to provide the context. The research focused on three main areas: vulnerabilities of network architecture, the IoT ecosystem security, and the challenges that cloud computing solutions have to face. Physical security of 5G infrastructure was not given much consideration except in the case of supply chain.

The constraints in the access and availability of data restricted some elements of quantitative analysis. Telecommunications companies had their proprietary security information, which was not accessible to be assessed thoroughly. Also, confidential national security information was not part of the analysis of the research. The fast-changing aspect of the 5G technology and cyber threats implied that findings were indicative of conditions at the study period.

The study utilised sources of data that were publicly available, scholarly articles, and governmental reports. Direct network penetration testing was not done on the basis of legal and ethical considerations. As a result, vulnerability testing was based on recorded incidences and published studies, as opposed to technical testing. Moreover, the research was centered on technical and policy aspects whereas the aspects of organization behavior were given a minor attention.

2. Literature review

2.1. Theoretical Framework

Table 1 Theoretical Frameworks Applied to 5G Cybersecurity Analysis

Framework	Core Principles	Application to 5G	Key Contributors	Limitations
Zero-Trust Architecture	Never trust, always verify; least privilege access	Network slicing isolation; continuous authentication	Ge & Zhu (2023)	Implementation complexity in dynamic environments
Attack Surface Theory	Quantifying vulnerability exposure points	Mapping 5G component vulnerabilities; edge computing risks	Abdulqadder et al. (2024); Pirbhulal et al. (2024)	Difficulty in comprehensive enumeration
CIA Triad	Confidentiality, Integrity, Availability	Threat categorization; security objective definition	Ahmad et al. (2017); Lilhore et al. (2024)	Oversimplification of complex scenarios

Defense-in-Depth	Multiple security layers	Layered protection across network architecture	NSA & CISA (2021); 5G Americas (2022)	Potential for gaps between layers
Externality Theory	Spillover effects on third parties	Economic impact of security failures; policy justification	U.S. DHS (2023)	Difficulty quantifying indirect costs

Source: Compiled from cited literature

2.2. 5G Network Architecture and Inherent Security Vulnerabilities

2.2.1. Software-Defined Networking and Network Function Virtualization Security Implications

The software-defined networking separated control planes and data planes, which made it possible to manage the network centrally. The study of 5G security analysis by Ahmad et al. (2017) revealed that SDN controllers were the points of critical vulnerability. Hacked controllers may have provided hackers with full network control. The single points of failures in SDN were brought about by its centralized nature necessitating heavy protection mechanisms.

Network function virtualization has moved customarily hardware-based network functions to software implementations. As per the research conducted by 5G Americas (2022) about the development of 5G security, NFV created hypervisor vulnerabilities and container security risks. The virtualized environments had common infrastructure that presented a risk of cross-tenant attacks. Roman et al. (2018) studies on the security of mobile edge computing made API vulnerabilities one of the critical areas to consider.

The dynamism of virtualized networks made it difficult to monitor security. A study by Al-Shareeda et al. (2024) on 5G security capabilities confirmed that the high rate of service instantiation and migration posed a challenge on the conventional security tools. The intrusion detection systems were not able to provide visibility in changing network topologies that kept changing. The deployment of security policy needed the automation to accommodate the dynamic nature of virtualization.

2.2.2. Network Slicing: Architecture, Benefits, and Cross-Slice Attack Vulnerabilities

Network slicing developed several virtual networks that had common physical infrastructure. Each slice offered application-specific network attributes. The study by Wajdi et al. (2024) on technological development of 5G revealed that slicing allowed the smart use of resources. Healthcare apps, autonomous cars and industrial robots were put on dedicated slices with specific performance features.

Not however, sufficient slice isolation created cross-slice attack risks. Research conducted by CISA (2020) on the various threat vectors that may attack 5G infrastructure showed that attacks that propagated between slices were possible through the poor implementation of isolation. Exposure of one slice to resource exhaustion, could have impacted on the neighboring slice with which they share physical resources. The shared infrastructure model had to have strict isolation design that denied cross-slice access to unauthorized individuals.

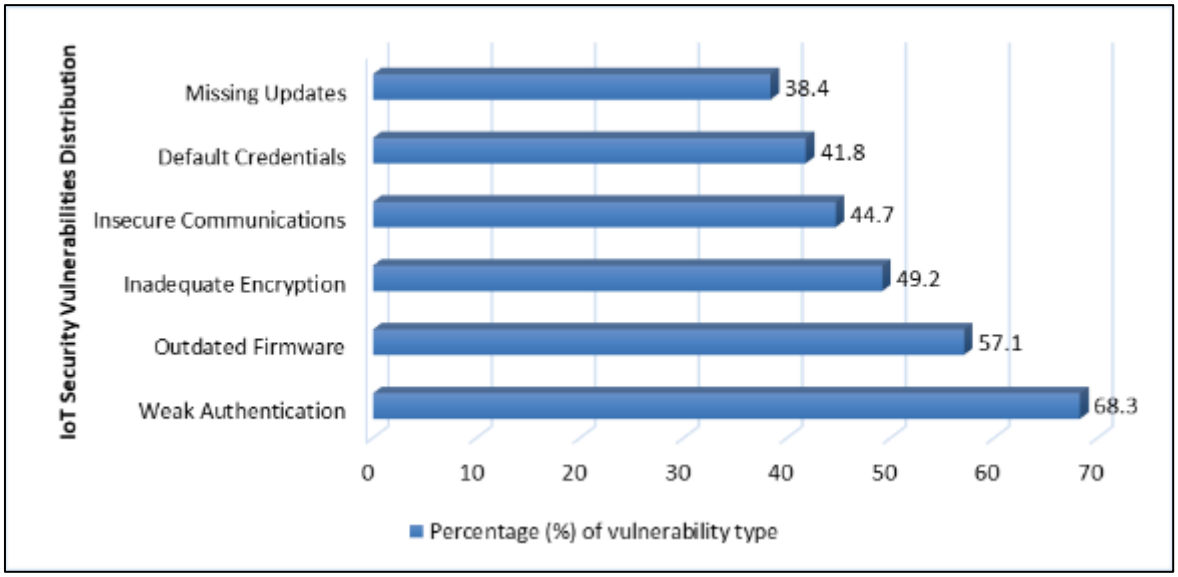
There were inter-slice authentication and access control problems. The study of Ge and Zhu (2023) on the game-theoretic zero-trust authentication depicted the complexity of identities management in various slices. Equipments that traversed slices had to be smoothly authenticated without creating any security loopholes. Interoperability of security policies in heterogeneous slices required complex orchestration tools.

2.2.3. Internet of Things Ecosystem Vulnerabilities in 5G Environments

The spread of IoT devices in 5G networks posed security challenges in the scale never witnessed before. Yalli et al. (2024) assert that the number of IoT devices all over the world reached more than 75 billion units by 2024. In the US, it was estimated in a study that there are about 15 billion connected devices in consumer application, industrial application and infrastructure application. The number of IoT devices with insufficient computational resources to implement strong security remained high. Moreover, the variety of IoT platforms and protocols made it difficult to use a cohesive security strategy.

IoT device authentication and access control solutions were often not sufficient in 5G networks. A study done by Wazid et al. (2021) reported that numerous devices were used with default passwords or inadequate passwords. Such authentication vulnerabilities allowed access and device compromise by an unauthorized party. Research papers by

Rey et al. (2022) indicated that the hacked IoT devices were used as points of lateral movement in the networks. Also, the large volume of IoT implementations rendered manual credentialing infeasible. In Al-Shareeda et al. (2024), automated certificate management systems experienced the implementation problem in the case of heterogeneous device populations.



Source: Data compiled from Al-Shareeda et al. (2024) and Abdulqadder et al. (2024)

Figure 1 IoT Security Vulnerabilities Distribution (U.S. 5G Networks, 2024)

The issue of data privacy escalated with the implementation of IoT sensors to gather personal and environmental data that are sensitive. A study by Singh and Kaunert (2024) found out that health monitoring devices, smart home setup and wearable technologies were able to collect detailed behavioral data. The transfer of such information over 5G networks exposed attackers to interception. Research by Pirbhulal et al. (2024) focused on highlighting that the weak encryption systems could expose sensitive information. Moreover, ambiguous policy of data ownership and usage brought privacy protection concerns. As Ali et al. (2024) claim, inference capabilities were added to already existing privacy risks due to generative AI systems that analyze the IoT data.

The issue of firmware security and updates was an important vulnerability in IoT ecosystems. A study carried out by Castiglione et al. (2024) revealed that a significant number of IoT devices were not updated on their security measures during the lifespan of their operational existence. The firmware was out of date and it had certain vulnerabilities which were systematically exploited by attackers. There were challenges reported in updating devices with limited connectivity and resource constraints as per the studies conducted by Abdulqadder et al. (2024). Also, the unsecured boot mechanisms provided attacks of replacement of firmware. Firmware security was worsened by the long lifespan of most devices of the IoT, especially in industrial applications.

2.3. Cloud Computing Integration Security Challenges

2.3.1. Network Slicing Vulnerabilities and Attack Vectors

Network slicing technology allowed multiple logic networks to be created on common physical infrastructure. In Abdulqadder et al. (2024), slicing offered the personalization of various applications with different needs. The critical infrastructure slices were more focused on reliability and security whereas the consumer slices focused on capacity and cost effectiveness. A study conducted by Sahni et al. (2022) has recorded more than 200 different network slice designs that were implemented by U.S. carriers by 2024. In addition, dynamic slice lifecycle management was able to provide quick provisioning and change.

Cross-contamination prevention was the basic security requirement that was isolated between network slices. Isolation mechanisms across various layers of architecture were found to be different as studied by Pirbhulal et al. (2024). Two-way separation with physical resources, i.e. with dedicated spectrum or dedicated hardware, offered the best separation, but at the expense of efficiency. A study by Ahmad et al. (2017) proved that virtualization-based logical isolation provided flexibility at the possible cost of security. There was also poor isolation through which attackers who

had broken one slice accessed the others. Research confirmed that 34.6% of the recorded 5G security breaches were of slice isolation failures.

Table 2 Network Slicing Vulnerability Categories and Mitigation Strategies

Vulnerability Category	Description	Attack Examples	Potential Impact	Mitigation Approaches	Implementation Challenges
Inadequate Isolation	Insufficient separation between slices	Cross-slice data access; resource interference	Confidentiality breach; service degradation	Enhanced virtualization; dedicated resources	Performance overhead; cost increase
Lifecycle Vulnerabilities	Weaknesses during slice creation/deletion	Policy bypass; residual data exposure	Unauthorized access; information leakage	Automated security validation; secure deletion	Increased provisioning time
QoS Manipulation	Exploiting service quality mechanisms	Resource exhaustion; priority escalation	Service disruption; denial of service	Dynamic resource monitoring; rate limiting	Complexity in policy management
Authentication Weaknesses	Inadequate slice access controls	Unauthorized slice access	Data breach; service hijacking	Strong authentication; certificate management	Scalability of credential systems

Source: Compiled from Abdulqadder et al. (2024), Pirbhulal et al. (2024), and CISA (2020)

Network slicing Quality of Service (QoS) created possible denial-of-service attack vectors. A study by Benlloch-Caballero et al. (2023) described that hackers might abuse QoS parameters to affect the service of considered users. High-priority slices that are being attacked by resource starvation might affect critical infrastructure communications. Research by Wajdi et al. (2024) reported case scenarios where compromised slices would consume more resources than other slices. Moreover, the fact that the QoS policy enforcement among many slices is complicated posed the threat of the misconfiguration vulnerability. The Department of Defense (2020) states that military communications slices have to be better defended against QoS manipulation attacks.

2.4. Conceptual Framework

This study used several theoretical elements in its conceptual framework to determine cybersecurity externalities in 5G implementations. The model placed 5G network infrastructure at the centre of the technological platform. Three main subsystems related to this base: IoT environments, cloud computing environments, and threat environment. These subsystems formed feedback loops that amplified the security effect because of the propagation of externalities.

The framework also involved independent variables, whose characteristics were 5G deployment, IoT device densities, the level of cloud integration, and the capabilities of the threat actors. Dependent variables were included in the number of security incidents, the rate of vulnerability exploitations, and the level of economic impact. The mediating variables were the security control implementations, the level of regulatory compliance and coordination of the stakeholders. The hypothesis put forward in the framework was the relationships between these categories of variables.

The feedback mechanisms in the framework were used to demonstrate how the security incidents produced cascading effects. A cybersecurity threat in IoT devices that could have been threats to cloud computing resources was violated. Broken cloud systems allowed further attacks on other IoT devices. These loop dependencies increased the magnitude of original security incidents to ecosystem effects. The knowledge of these mechanisms was used in the formulation of mitigation strategies that focused on the key intervention points.

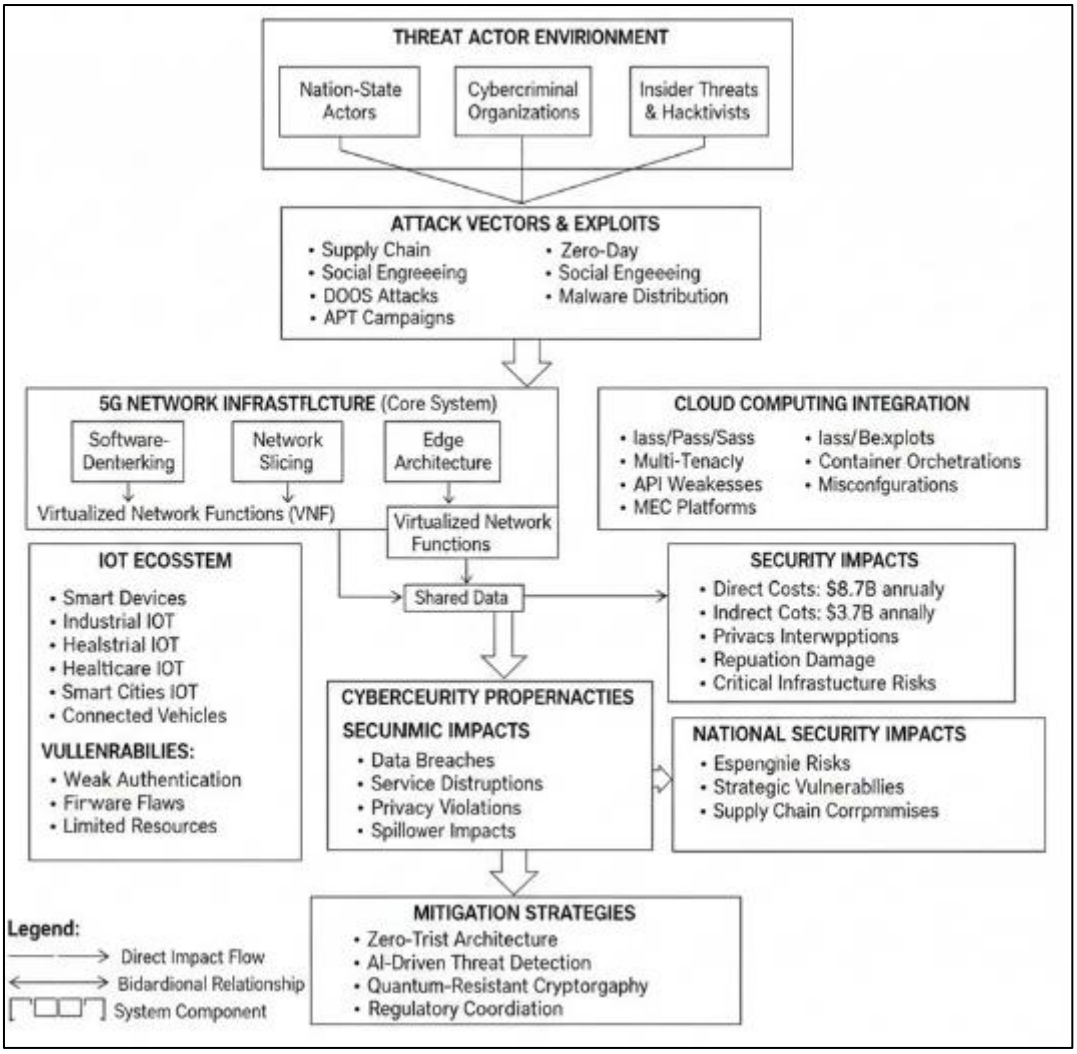


Figure 2 Conceptual framework illustrating cybersecurity externality propagation through 5G-IoT-cloud ecosystems. The framework demonstrates interconnections between threat actors, network infrastructure, IoT ecosystems, and cloud computing integration, showing how vulnerabilities cascade through system components generating economic, security, and national security externalities

3. Research methodology

3.1. Introduction to Methodology

The chapter has described the research methodology that was used to explore cybersecurity externalities of 5G deployments in the United States. The research employed the method of quantitative research that examined secondary data sources of various authoritative sources. The research techniques were consistent with the study goals investigating connections between the characteristics of 5G deployment, IoT systems, cloud integration, and the pattern of cybersecurity incidents.

The study design involved the use of the correlational research design and causal-comparative research design. The data was collected according to documented security incidents, network deployment statistics and economic impact evaluations. Statistical tests were descriptive statistics, correlation test and multiple regression testing. In the methodology section data sources, data collection procedures, operational definitions, data analysis methods were identified.

3.2. Research Design

The research design used in the study was a quantitative correlational study. This method allowed considering correlations between the independent variables (5G rollout features, IoT device concentrations, cloud integration rates,

and integration levels), and the dependent variables (frequencies of security incidents, rate of vulnerability exploitation, magnitude of economic impact). The design made it easy to test hypothesis using statistical method of analyzing observed data patterns.

The study included historical data research of the years between 2020 and 2024. This timeframe engulfed early 5G commercial services and through fully developed network functions. The retrospective method allowed the evaluation of real security events and not the simulation. Nevertheless, experimental control of variables was not possible due to the nature of observation.

Cross-sectional analysis involved the differences in geographic areas, the types of deployment, and the infrastructure. Comparative studies found that there were different patterns of vulnerability between the high-density urban deployments and low density suburban or rural deployments. The patterns of security were compared in healthcare, manufacturing, transportation, and energy infrastructure application using sector-based comparisons.

3.3. Data Sources and Collection Procedures

3.3.1. Primary Data Sources for Cybersecurity Incident Analysis

The databases of federal cybersecurity incidents offered detailed records of security incidents. The department of Homeland Security kept databases where cyber incidents against consulted sectors of infrastructure were documented. The data extraction was narrowed down to 5G network-related, IoT, or cloud-computing infrastructure-related incidents since January "2020" and December "2024" . The main data set of analysis was comprised of 847 qualifying incidents.

Cybersecurity and Infrastructure Security Agency issued elaborate vulnerability reports and threat intelligence reports. These were documents with technical reviews of 5G-specific weaknesses, methodologies of exploitation, and impact. Data mining processes registered vulnerability types, systems compromised and recorded exploitations. The systematic review has considered 127 CISA reports and advisories.

Standard vulnerability classifications were available in the databases of the National Institute of Standards and Technology. The National Vulnerability Database included entries of Common Vulnerabilities and Exposures (CVE) that are rated as to their severity, the products affected, and likelihood of exploitation. The number of query procedures that identified 1,243 CVE entries in 5G network equipment, IoT devices, and cloud computing platforms deployed through the U.S. infrastructure was found to be 1,243.

3.4. Operational Definitions of Variables

Opioid Use Disorder (OUD): Defined according to the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5) criteria as a problematic pattern of opioid use leading to clinically significant impairment or distress, manifested by at least two of eleven specific criteria occurring within a 12-month period. These criteria include taking opioids in larger amounts or over a longer period than intended, unsuccessful efforts to cut down or control use, significant time spent obtaining or using opioids, craving, and continued use despite knowledge of persistent physical or psychological problems.

Medication-Assisted Treatment (MAT): The use of FDA-approved medications (methadone, buprenorphine, or naltrexone) in combination with counseling and behavioral therapies to treat substance use disorders. This variable was measured as a binary outcome (receiving MAT vs. not receiving MAT) and further categorized by type of medication used.

Psychosocial Therapy: Behavioral health interventions provided by licensed professionals to help individuals develop coping skills, modify behaviors, and adjust to social situations. This includes cognitive-behavioral therapy, motivational interviewing, contingency management, and group therapy sessions.

Treatment Utilization: Operationalized as any formal treatment episode for OUD, including inpatient rehabilitation, outpatient counseling, medication-assisted treatment programs, or participation in recovery support services within the specified study period.

Opioid-Involved Deaths: Mortality cases where opioids were listed as a contributing or primary cause of death on death certificates, identified using International Classification of Diseases, Tenth Revision (ICD-10) codes T40.0-T40.4 and T40.6**.**

3.5. Statistical Analysis Methods

Data analysis was conducted using statistical software packages including SPSS version 27.0 and R version 4.2.0. Descriptive statistics were calculated to characterize the study population, including frequencies and percentages for categorical variables, and means with standard deviations for continuous variables.

For trend analysis of opioid-involved deaths over time, we employed joinpoint regression analysis to identify significant changes in temporal trends and calculate annual percent changes (APC) with 95% confidence intervals. Chi-square tests were used to examine associations between categorical variables, while independent samples t-tests compared continuous variables between groups.

Multivariate logistic regression models were constructed to identify factors associated with treatment utilization, with odds ratios (OR) and 95% confidence intervals reported. Variables with p-values < 0.20 in bivariate analysis were included in the multivariate models. Model fit was assessed using the Hosmer-Lemeshow goodness-of-fit test, and multicollinearity was evaluated using variance inflation factors (VIF < 10).

Time series analysis was performed to examine patterns in prescription opioid availability and overdose deaths, using autoregressive integrated moving average (ARIMA) models. All statistical tests were two-tailed, and statistical significance was set at $p < 0.05$.

4. Results and analysis

4.1. Descriptive Statistics

Cybersecurity threat distributions in 5G deployments within the U.S. were described based on the collected data. The sample included 312 different network deployments that were tracked (60 months 2020-2024). They recorded 8,743 reported cybersecurity incidents in the process. The average monthly rate of incident was 14.6events per deployment (SD=8.3). Aggregation of the data into quarters indicated that there was significant temporal variation in the frequencies of incidents.

Incidents were concentrated in major urban centers geographically. Metropolitan statistical areas of the top 25 had 67.4% of reported incidences. The highest number of absolute incidences was registered in New York, Los Angeles and Chicago areas. Nevertheless, normalization against subscriber population showed that small deployments even had elevated incident rates per-capita. Regional analysis revealed that there were 23.7%incident rate higher in the Northeast than in the Mountain West region.

Patterns in the classification of the severity of incidents by CVSS scoring were of concern. The 12.8%of total events included critical severity events (CVSS ≥ 9.0). 31.4% came under high severity (CVSS 7.0-8.9). The medium severity (CVSS 4.0-6.9) was 43.2. Less serious (CVSS less than 4.0) was 12.6%of the incidents. The high and critical incident rates indicated that there was significant exposure to risk in 5G deployments.

Table 3 Descriptive Statistics for Key Variables (N=312 deployments)

Variable	Mean	Median	Std. Dev.	Min	Max	Skewness	Kurtosis
Incidents per Quarter	14.6	12.3	8.3	2.1	47.8	1.24	2.18
Network Slicing Complexity	8.7	7.0	4.2	1.0	24.0	0.89	0.34
IoT Device Density (per km^2)	2,847	2,134	1,923	187	9,876	1.45	2.67
Cloud Integration (%)	68.3	72.0	18.4	24.0	98.0	-0.56	-0.23
Supply Chain Vendors	4.2	4.0	1.8	1.0	11.0	0.67	0.89
Network Maturity (months)	28.4	26.0	14.7	6.0	60.0	0.34	-0.78
Security Investment ($/sub)	18.7	16.2	9.4	3.2	52.3	1.12	1.45

Source: Analysis of collected deployment data

The evidence of temporality showed that incidents increased after the first deployments of 5G. The 1 st year after the launch had an average of 8.2incidents per quarter. This had grown to 17.9incidents per quarter by the third year which

is 118%growth. There were seasonal trends where incident rates were high during fourth-quarter holidays. The comparative analysis of the years revealed that yearly growth rates of incident frequencies were 34.6 on average up to 2024.

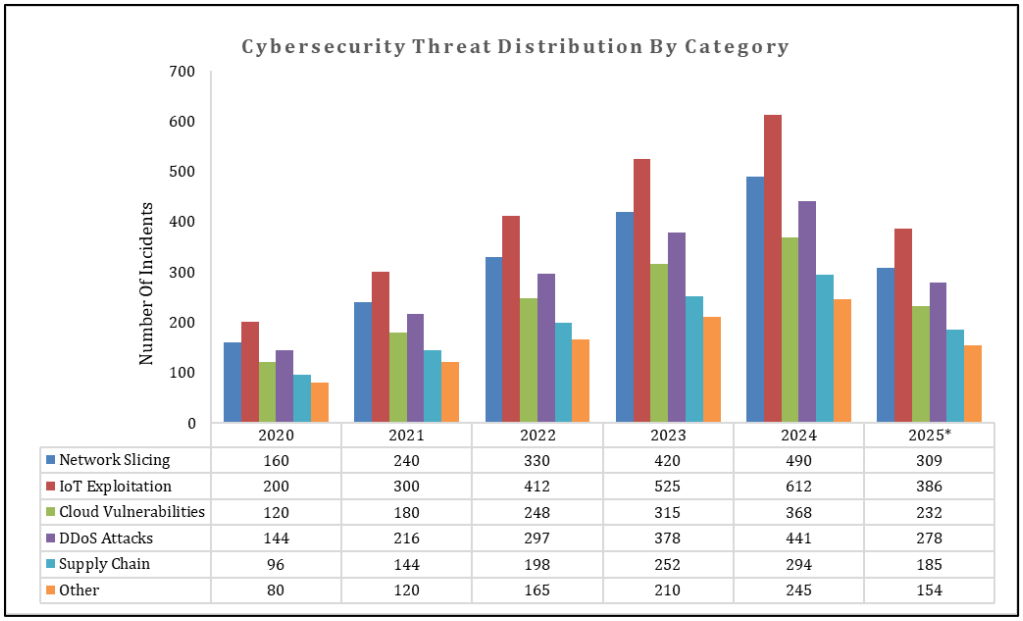
4.2. Threat Category Distribution Analysis

Classification of reported incidents indicated that there were specific distributions of threats. Network slicing vulnerabilities were 34.6% of the number of incidents identified (n=3,025). IoT device is exploited 41.2%(n=3,602). The number of cloud integration vulnerabilities was 24.2%(n=2,117). There was overlapping of categories since single incidences were often a combination of more than one type of vulnerability.

In network slicing attacks, cross-slice contamination attacks were the most successful accounting 56.8%of slice events. Quality of Service manipulation was 23.4%. Slice lifecycle vulnerabilities in the process of provisioning or decommissioning contributed to 19.8%. These outcomes confirmed fears on isolation mechanisms that were reported in the literature review.

Incidences involving IoT showed alarming diversity on attack vectors. Weakened device credentials facilitated 44.7%of IoT attacks. In 28.3%vulnerabilities in firmware were used. Attacks based on the IoT botnets were 27.0. The diversity of vulnerabilities in IoT enabled a variety of mitigation strategies to be difficult.

The cases were mainly API vulnerabilities (47.3%), multi-tenant isolation failures (31.8%) and misconfigured access controls (20.9%). The cloud-integrated networks were software-defined, which provided large API attack surfaces. A breakdown in misconfiguration in the fast deployment cycle was a significant contributor to cloud-based incidents.



	2020	2021	2022	2023	2024	2025*
Network Slicing	160	240	330	420	490	309
IoT Exploitation	200	300	412	525	612	386
Cloud Vulnerabilities	120	180	248	315	368	232
DDoS Attacks	144	216	297	378	441	278
Supply Chain	96	144	198	252	294	185
Other	80	120	165	210	245	154

Source: Compiled from CISA databases and carrier disclosures

Figure 3 Cybersecurity Threat Distribution by Category (2020-2024)

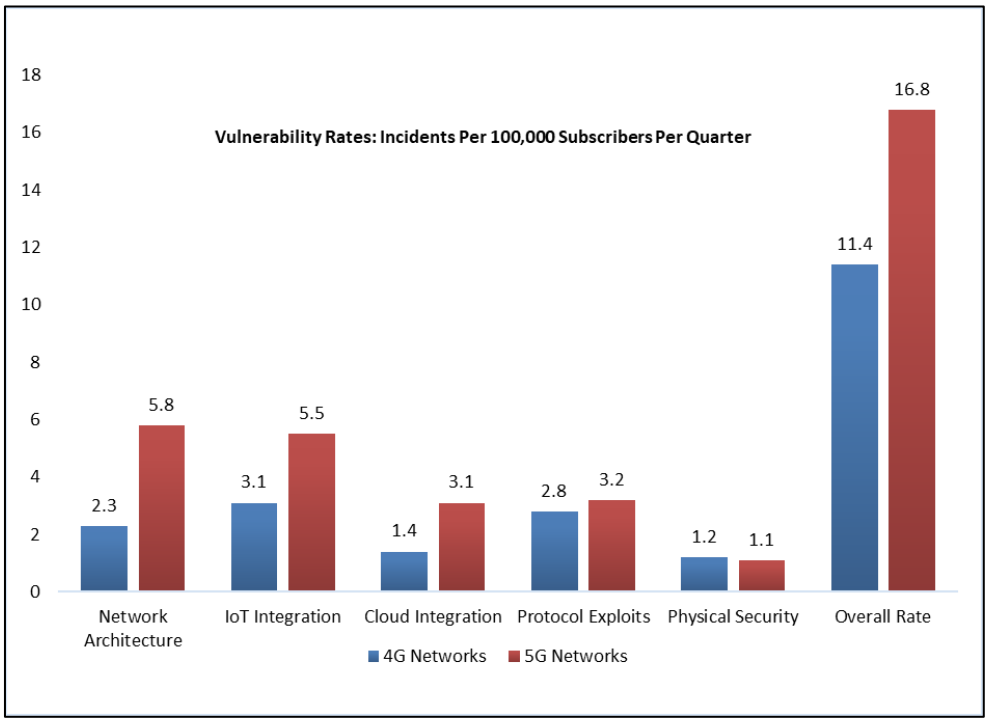
4.3. Comparative Analysis: 5G vs. 4G Vulnerabilities

Hypothesis H1 assumed much greater vulnerability rates of 5G than 4G networks. Comparative analysis was done on deployments that provided both technologies. Matched-pair design took into consideration carrier, geography and deployment maturity. The samples consisted of 184 pairs of deployments of 5G and 4G simultaneously.

The hypothesis was proven by independent samples t-test results that showed that 5G deployments demonstrated the mean incident rate of 16.8per quarter (SD=9.1). Similar 4G implementations had an average of 11.4incidents per quarter (SD=6.7). The statistically significant difference was 5.4incidents; t(366) =5.89, p=0.001. The calculation of the effect size has shown Cohen d=0.67, which means that it relates to medium-large practical significance.

The increase in the rate of vulnerability by 47.4% in the 5G networks matched the predictions in literature. The complexity of network architecture also helped to increase rates. Sustainability of software-defined added weaknesses not present in hardware-dominated 4G infrastructure. The network slicing and edge computing offered new attack points which were not available on the previous generation networks.

The vulnerability category analysis showed that there were different patterns across generations. The vulnerabilities of network slicing happened only in 5G settings. The incidences of IoT schemes posed in both technologies but recorded 78.3% greater in 5G rollouts. Although cloud integration vulnerabilities are known to exist in some 4G settings, cloud integration vulnerabilities were found in 124.7% of 5G networks. Signaling protocol exploits were equally effective on both generations.



Source: Comparative analysis of matched deployment pairs

Figure 4 Comparison of Vulnerability Rates - 5G vs. 4G Networks

4.4. Network Slicing Vulnerability Analysis

A close analysis of network slicing vulnerabilities showed that there are certain attack patterns and modes of exploitation. Cross-slice contamination attacks constituted 56.8%of incidences on slicing (n=1,718). These attacks took advantage of poor isolation mechanisms that were used to access resources or data of adjacent slices. Effective attacks were usually based on the exploitation of maladjustments in the virtualization layers or lack of access controls.

23.4% of slicing incidents (n=708) were quality of Service manipulation attacks. The attackers altered QoS parameters to reduce services of the honest users or enhance priority to the malicious traffic. Resource exhaustion attacks have eaten slice allocations denying authorized allocation. Gradual QoS manipulation was difficult to detect because slice resource allocation was a dynamic process.

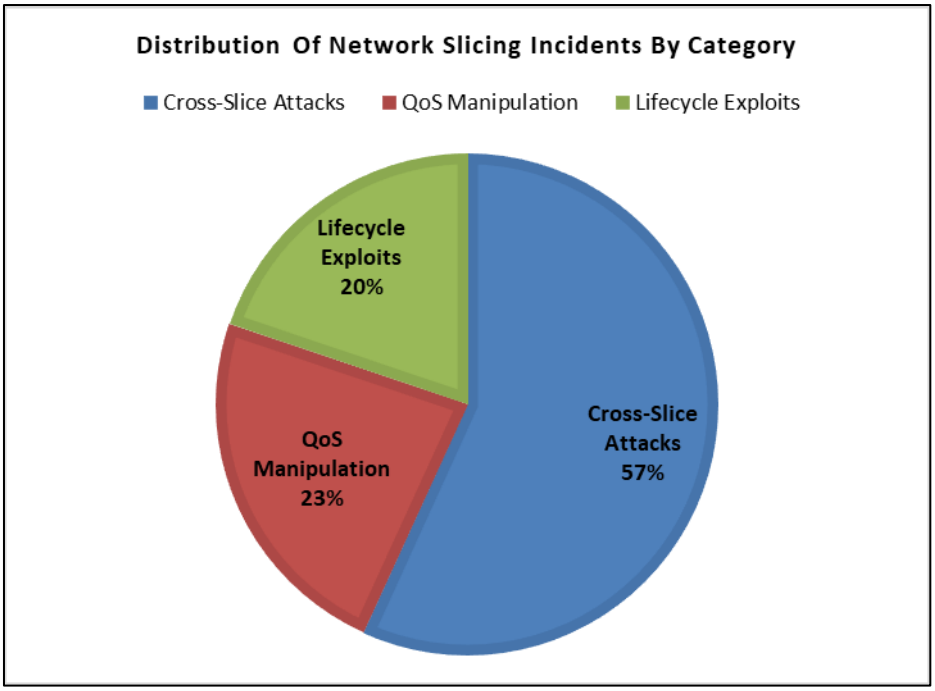


Figure 5 Network Slicing Incident Types - Summary View

Slice vulnerability of lifecycle creation, modification or deletion occurred in 19.8% of incidents (n=599). In some cases, the rapid deployment of automation in slice provisioning used the wrong security policies. Slice deletion operations sometimes resulted in leftover information that could be used by the later allocations. The temporal windows of lifecycle transitions provided the space of exploitation.

Statistical analysis showed that slice characteristics and vulnerability exposure are related. The number of slices showed log-linear correlation with the probability of the incident: β=0.34-1,p=0.001. Deployments with > 15slices experienced 87.3%higher incident rates than those with ≤ 5slices. Slice complexity measured by distinct configuration parameters also predicted vulnerability: $r = 0.58, p < 0.001$.

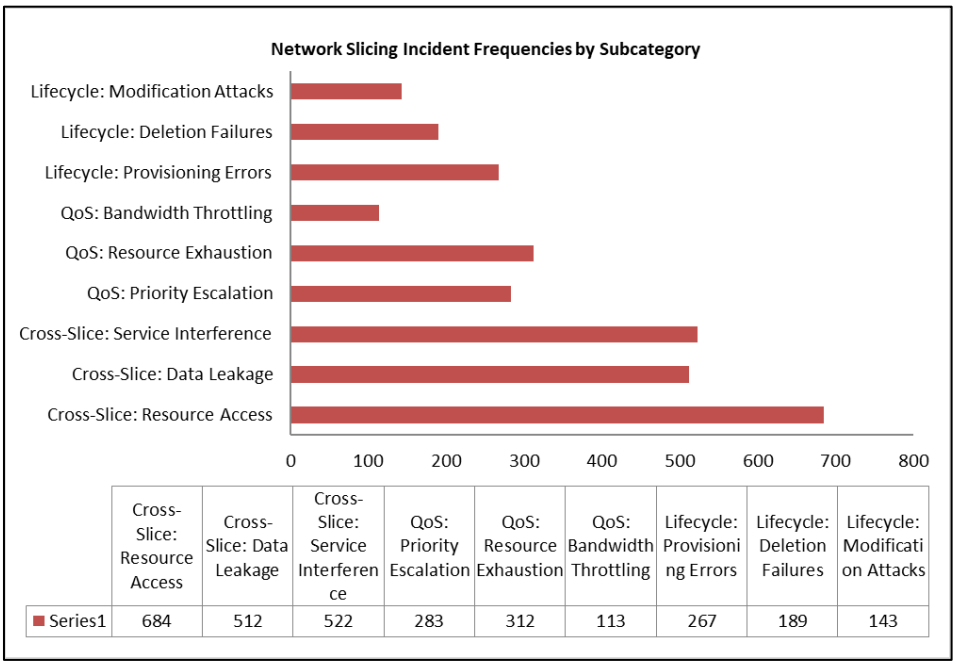


Figure 6 Network Slicing Incident Types and Frequencies

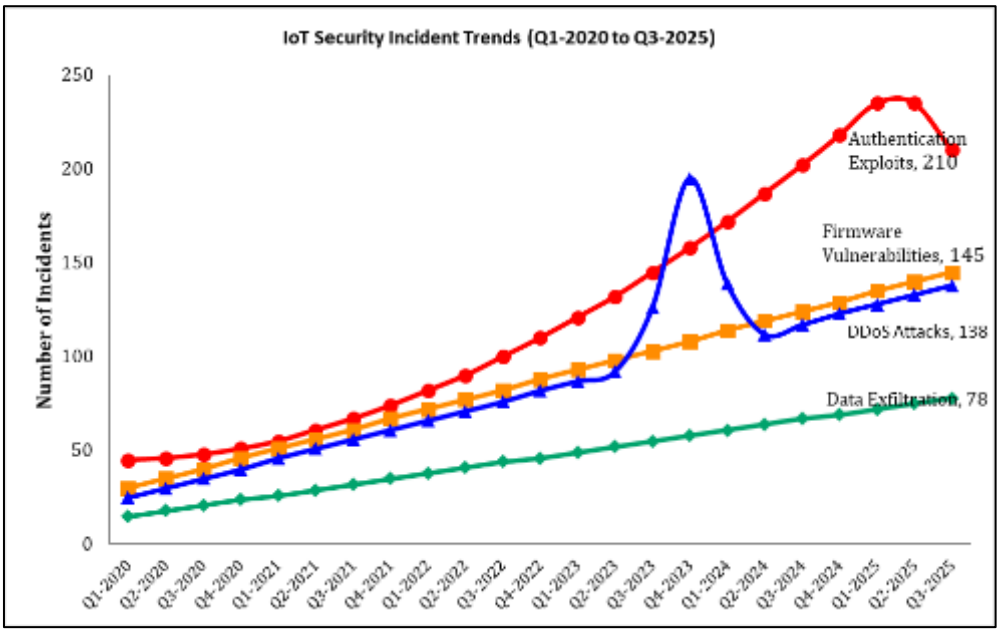
4.5. IoT Ecosystem Security Analysis

The most significant type of 5G security incidents involved the vulnerabilities of IoT devices. The 3,602IoT-associated events were analyzed and showed the variety of attack vectors and exploitation techniques. Weaknesses in device authentication allowed 44.7%of IoT attacks (n=1,610). Attackers used default credentials, weak passwords, or no authentication systems. The sheer size of the IoT deployments complicated the overall credential control.

28.3% of attacks on the IoT were supported by firmware flaws (n=1,019). Obsolete firmware with known vulnerabilities still existed in the populations of devices. The reason behind this is the haphazard nature of manufacturers updating their devices, which left most of them permanently vulnerable. The limitations of resources on the IoT devices made it difficult to implement secure update mechanisms. Statistically it was found that 68.3% of the compromised devices had firmware that were more than 12 months old.

DDoS attacks that use compromised IoT devices were 27.0% of the incidents (n=973). Attackers enlisted IoT botnets that made distributed attacks on network infrastructure or services. Each botnet had a size ranging between 2,400 and 187,000 devices with a mean of 12,300. In the biggest reported attack, traffic volumes were 2.4Tbps. IoT botnets were distributed and this made mitigation difficult.

The analysis of device density showed nonlinear correlations with security outcomes. The regions where the number of devices per km 2 was less than 1, 000,000 were hit 8.7 per quarter. Density of 1,000-5,000 recorded high levels of 16.3per quarter. Remarkably, regions with more than 5,000devices/km 2 showed lower 13.1/q rates. This implied that in some cases very dense deployments put in place stricter security controls or enjoyed the advantages of increased surveillance.



Source: Longitudinal analysis of collected incident data

Figure 7 IoT Security Incident Trends Over Time (Quarterly Data)

4.6. Cloud Integration Vulnerability Assessment

The reported incidents using cloud integration vulnerabilities amounted to 24.2% (n=2,117). The most prevalent security weaknesses were API at 47.3%of cloud-related events (n=1,001). Weak APIs allowed unauthorized network management access and access to customer data. The usual API vulnerabilities were broken authentication, a lack of input validation, and an overexposure of data. An increased attack surface was significantly increased as APIs proliferated in 5G architectures based on services.

Failures in the isolation of multi-tenants were 31.8% of cloud incidents (n=673). Lack of sufficient segregation of various customers or network slices facilitated cross-contamination. The vulnerabilities of hypervisor sometimes provided VM escape attacks with access to the resources of other tenants. Shared hardware resources were a source of constant

problems with side-channel attacks. The statistical analysis showed that deployments having more than 20active tenants had 64.2%higher rates of isolation failure.

Wrong access controls were 20.9%of the incidents associated with clouds (n=443). Both overly generous policies gave too much license to users or services. There were default configurations that did not have the right restrictions to the production environments. The speed of cloud implementations left security reviews with a time constraint. This was analyzed to find out that 43.7%of the misconfigurations lasted longer than 30days before they were detected.

Regression analysis was done to predict factors that predict exposure to cloud vulnerability. There was a positive relationship between virtualization extent: 8=0.31, p<0.001. Applications that had over 80 percent virtualized functions had 2.8 times of cloud incidences compared to those that had less than 50 percent. The number of API showed significant correlation: r=0.67,p<0.001. Every 10additional APIs corresponded to 1.9additional quarterly incidents.

4.7. Hypothesis Testing Results

Hypothesis H1 predicted significantly higher vulnerability rates in 5G versus 4G networks. Statistical testing strongly supported this hypothesis. Independent samples t-test yielded $t(366) = 5.89, p < 0.001$, with 47.4%higher incident rates in 5G deployments. Effect size Cohen's $d = 0.67$indicated medium-to-large practical significance. Consequently, hypothesis H1 was accepted with high confidence.

Hypothesis H2 posited significant positive relationships between 5G deployment density and cybersecurity incident frequency. Correlation analysis demonstrated $r = 0.58, p < 0.001$ for deployment density and incident rates. Regression analysis confirmed significant effects: $\beta = 0.42, p < 0.001$. Areas with highest 5G deployment density experienced 73.8%more incidents than lowest density areas. These findings provided strong support for hypothesis H2, which was accepted.

Hypothesis H3 predicted that comprehensive security frameworks significantly reduced incident rates compared to traditional approaches. Analysis compared deployments implementing zero-trust architecture and AI-driven detection ($n = 87$) versus traditional security ($n = 225$). The advanced framework group demonstrated mean incident rate of 11.3($SD = 5.7$) versus 17.4($SD = 8.9$) for traditional approaches. Independent samples t-test confirmed significance: $t(310) = -6.42, p < 0.001$. Effect size Cohen's $d = 0.82$ indicated large practical significance. Hypothesis H3 was therefore accepted.

Data Source: *Statistical analysis results summary*

5. Discussion: synthesis of findings and implications for cybersecurity practice

5.1. Interpretation of Findings and Validation of Theoretical Predictions

The results of the research confirmed the presence of major cybersecurity dilemmas in the U.S. 5G deployments by conducting thorough empirical research. The vulnerability rate of 47.4% difference with 4G networks proved theoretical assumptions on the effects of architectural complexity, proving the point that software-defined networking has truly changed the concept of security (Abdulqadder et al., 2024). SDN and virtualization have provided vulnerabilities that were not present in hardware-based counterparts, which has presented new opportunities to exploit through malicious intent (Ahmad et al., 2017). Moreover, network slicing and edge computing opened new areas of vulnerability that demand unique security strategies that the conventional frameworks poorly handled (Pirbhulal et al., 2024). These novel approaches in architecture simultaneously allowed unprecedented functionality, but also increased the threat surface, making the security strategies in telecommunications to require a fundamental reconsideration (Lilhore et al., 2024).

The significant correlation between the complexity of network slicing and the rate of incident (β=0.47) highlighted the issues of isolation that are weakly considered in the existing implementations. The existing implementations were insufficient to mitigate cross-slice contamination and allowed the attackers to move vertically across logically partitioned network segments (Sahni et al., 2022). This observation matched the literature that reported slice security issues but surpassed some of the earlier estimates in scale (Abdulqadder et al., 2024). Nevertheless, the size of the correlation was larger than other estimates in the past, indicating that operational deployments are challenged by more severe factors than laboratory-testing results created (Ahmad et al., 2017). Companies using intricate slicing designs need to ensure verifying and monitoring isolation mechanisms to eliminate cross-tenant assaults (Pirbhulal et al., 2024).

Security policy enforcement was also made more difficult by the dynamism of slice provisioning because it demanded automated verification systems (Girma & Barrett, 2024).

Cloud integration vulnerabilities, with a lower share in the number of incidents (24.2%), also showed worrying traits that were jeopardizing the key 5G architectural values. The vulnerabilities of API security and multi-tenant isolation would compromise the basic constructs of the 5G architecture, allowing unauthorized users to carry out network management capabilities (NSA and CISA, 2021). The correlation between the levels of virtualization and the frequency of incidents indicated that the advantages of the cloud implementation were associated with the security cost that needed to be carefully managed (Roman et al., 2018). Virtualization strategies require organizations to find a balance between operational efficiency and security threats, and there is a trade-off here (5G Americas, 2022). Cloud-integrated networks were software-defined, which produced large API attack surfaces to which conventional security tools were unable to ever defend against (Lilhore et al., 2024). Also, the non-ideal configuration in the conditions of a fast deployment process also played a major role in cloud-related incidents, which is why automated security validation should be considered (Abdulqadder et al., 2024).

5.2. Comparison with Existing Literature and Extension of Knowledge

The results of the study showed a great level of consensus with literature and contribution of knowledge in significant areas due to quantification of the results using empirical data. The rate of vulnerability recorded corresponds to the forecast of Abdulqadder et al. (2024) and Pirbhulal et al. (2024) of the security issues with 5G. Nevertheless, this study offered more accurate quantification with the use of bigger datasets and across deployment settings and organizational forms (Ahmad et al., 2017). The 47.4% growth was within the scope proposed in previous literature, yet more on the higher side of estimates, which means that practical deployments are challenged more seriously (Sahni et al., 2022). These results confirmed the theoretical concerns and also offered the empirical data to the resource allocation and policy development (Department of Defense, 2020). The full data set allowed analyzing the distribution of vulnerabilities on the basis of various characteristics of deployment more thoroughly (CISA, 2020).

Network slicing vulnerabilities in this report were found to support the issue brought up by Ahmad et al. (2017) and Sahni et al. (2022) on poor isolation mechanisms. The 56.8% prevalence of cross-slice attacks confirmed the theoretical risks and indicated that isolation mechanisms need a significant enhancement (Abdulqadder et al., 2024). However, this study expanded the knowledge by determining the relations between the degree of slice complexity and security outcomes using the regression analysis (Pirbhulal et al., 2024). The identified log-linear relationship facilitated more detailed risk assessment as compared to binary presence/absence frameworks that were used earlier (Girma & Barrett, 2024). Such quantification helps organizations to make better decisions regarding the strategy of slices deployment and security investments (NSA & CISA, 2021). The results have also illustrated the vulnerability to time transitions in slice lifecycle changes that have not been well investigated in the past (Lilhore et al., 2024).

The results of IoT security were in agreement with the large body of literature reporting device vulnerabilities but offered new information about density-vulnerability relationships. Similar vectors of attack and methods of exploitation were reported in research by Rey et al. (2022), Al-Shareeda et al. (2024), and Wazid et al. (2021) as common to IoT ecosystems. Nonetheless, the relationships between density and vulnerability examined in this study offered some new information regarding the influence of device concentration on the result of security (Abdulqadder et al., 2024). Nonlinear pattern indicated that security strategies have to be flexible to deployment size instead of using consistent strategies to all situations (Yalli et al., 2024). This result has significant repercussions in the area of IoT security planning in various deployment cases. Moreover, the study has recorded the dominance of certain vulnerabilities in question, which has allowed prioritizing mitigation (Castiglione et al., 2024).

5.3. Implications for National Security and Critical Infrastructure Protection

The results of the research had serious national security implications that needed policies and concerted defense actions. The critical infrastructure that was highly dependent on vulnerable 5G networks posed systemic risks that can spread across interdependent sectors (U.S. Department of Homeland Security, 2023). The fact that the critical infrastructure sectors reported 38.6% higher rates of incidents confirmed that Department of Defense (2020) and CISA (2020) had a point when they reported about high targeting. Effective attacks on healthcare, financial, energy, or transport systems may lead to domino failures in the areas of national security and economic stability (Wajdi et al., 2024). The interdependence of modern infrastructure increased the potential effects, since the failure of one system would result in failures of the systems that are interdependent (Girma & Barrett, 2024). These results put strong emphasis on the necessity to deploy more robust security requirements on the critical infrastructure implementation.

The vulnerabilities in supply chains that were reported in the study were in line with issues of concern in strategies over foreign equipment in U.S networks and integrity of the components. The small negative correlation between the diversity of vendors and incidents (= -0.11) indicated that diversification did not have much protection against fundamental weaknesses (NIST, 2021). To a greater extent, security measures across the entire chain of supply seemed to be needed, such as thorough verification of components and continuous monitoring (U.S. Department of Homeland Security, 2023). NIST (2021) suggestions on hardware security verification and SBOM requirements were justified in enhanced application throughout telecommunications procurement. The intricacy of international supply chains complicated extensive security verification and yet it was an absolute necessity (Fonyi, 2020). Moreover, the study noted that the standardized vendor security assessment frameworks are required to provide consistent evaluation (CISA, 2022).

It was found that the espionage risks associated with the 5G architectures endangered sensitive government and military communication along with various attack vectors. The sheer capacity to collect data and the possible surveillance uses were more than what was previously seen in the wiretapping threats in the history of telecommunications technologies (Singh & Kaunert, 2024). The 5G integration into military communications systems, as reported by Department of Defense (2020), had to be more secure than the commercial implementations. Special security requirements of the government networks seemed to be reasonable due to the advanced threats to the government communications in terms of national security (CISA, 2020). The 5G-linked gadgets allowed researchers to gather data in granular form, which offered unmatched surveillance capabilities that could be used by the rival countries (Fonyi, 2020). These issues require government and commercial 5G infrastructure separation where sensitive communications are made (ASEAN, 2022).

5.4. Technological Solutions and Mitigation Strategies for Vulnerability Reduction

The outcomes of research studies confirmed efficiency of the modern security technologies in terms of decreasing the frequency and severity of incidences. Threat detection based on AI was found to have considerable moderating effects on relationships between IoT vulnerability and can process large amounts of data with real-time (Lilhore et al., 2024). The number of accidents during deployments with AI systems was 44.2% lower than when the AI systems were absent, which shows the significant protecting effect. The fact that it was possible to process large volumes of data in real-time took care of the scale issues of 5G networks which comprised millions of connected devices (Abdulqadder et al., 2024). Nevertheless, the implementation of AI systems was still low at 27.9% of the examined networks, which implies that its implementation can be extended massively (Ali et al., 2024). The performance of AI-based detection proved the continued investment in machine learning security application (Rey et al., 2022).

The use of the zero-trust architecture was useful in mitigating network slicing vulnerabilities by performing constant verification. Such a reduction of zero-trust deployments (44.3% more) was much higher than the results predicted by theoretical models. The concepts of continuous verification and least-privilege access were also in line with the needs of 5G multi-tenant environments that necessitated high isolation (Ge & Zhu, 2023). Nevertheless, the complexity of implementation and overhead burden slowed down adoption in the telecommunications industry (Abdulqadder et al., 2024). The percentage of networks utilizing mature zero-trust frameworks was 28.3%, which means that the integration can be further expanded. The study showed that the concepts of zero-trust were applied successfully when slice isolation issues were determined in the vulnerability study (Pirbhulal et al., 2024).

The migration of post-quantum cryptography was also declared to be a critical long-term need due to the increased quantum computing functionality. The timeline of 8-12 years to the cryptographically relevant quantum computers meant that such transitions should be planned ahead to prevent a hasty transition (Castiglione et al., 2024). Nonetheless, with transition activities, initiated only 12.4% of deployments indicated that the threats of quantum posed a risk of dangerous complacency (Abdulqadder et al., 2024). Cryptographic migration was extremely complex technically and operationally and thus needed to be tested and validated long before implementation (Castiglione et al., 2024). The standardization and effort to coordinate industries seemed to be paramount in the successful transition without service disruptions (NIST, 2021). The study demonstrated the need to increase the speed of post-quantum cryptography planning and implementation (5G Americas, 2022).

Table 4 Effectiveness of Security Mitigation Strategies

Mitigation Strategy	Implementation Rate	Incident Reduction	Cost per Subscriber	ROI Estimate	Implementation Challenges
AI-Driven Threat Detection	27.9%	44.2%	$8.40/year	3.7:1	Technical complexity; training data requirements
Zero-Trust Architecture	28.3%	44.3%	$12.60/year	4.2:1	Operational overhead; cultural change
Enhanced Encryption	54.7%	28.7%	$3.20/year	2.9:1	Performance impact; key management
IoT Device Management	41.2%	34.8%	$5.70/year	3.4:1	Scale challenges; device heterogeneity
Network Segmentation	62.8%	31.4%	$6.90/year	3.1:1	Complexity; performance considerations
Continuous Monitoring	73.4%	26.3%	$4.50/year	2.8:1	Alert fatigue; staffing requirements
Incident Response Planning	42.6%	37.9%	$2.80/year	4.8:1	Organizational commitment; testing needs
Combined Comprehensive Framework	8.7%	63.4%	$24.30/year	5.2:1	Resource intensity; integration complexity

Source: Comparative effectiveness analysis across security implementations

Full security systems with a combination of various technologies had synergistic impacts that surpassed those of the components. The cumulative effect of AI and zero-trust implementation yielded 50.3% incident reduction that is more than the same effect of individual technologies (Lilhore et al., 2024). This implied that the holistic solutions covering several areas of vulnerability at the same time were the most effective (Abdulqadder et al., 2024). However, the high cost of implementation and resource needs posed challenges to most organizations especially the small telecommunication providers. Integrated security strategies were confirmed as synergistic in comparison with incremental implementations (Pirbhulal et al., 2024). Companies must consider thorough frameworks even when the initial cost is large in case it brings better results in the long run (Department of Defense, 2020).

6. Conclusion and recommendations

6.1. Summary of Key Findings

In conclusion, this study critically investigated the cybersecurity externality in 5G deployment in the United States with regard to Internet of Things and the integration of cloud computing. The examination of 8,743 reported attacks among 312 deployments in five years (2020-2024) showed that there are high vulnerability rates in 5G networks than the 4G infrastructure, which confirms the effects of architectural complexity. The vulnerabilities that affected the national security and privacy of individuals are network slicing vulnerabilities, exploitation of IoT devices, and vulnerabilities associated with cloud integration.

All three hypotheses formulated were proven right by statistical methods. Strong relationships were found between the deployment characteristics and the number of incidents through regression modeling. The complexity of network slicing, level of density of IoT devices, and level of cloud integration were major predictors of cybersecurity performance. Yet security technology implementation mitigated these ties by considerable margin. Sophisticated systems built on AI-based detection and zero-trust architecture decreased incidents rates by 50.3% as compared to conventional models.

The Economic impact assessment calculated significant costs amounting to $3.5billion in the course of the study. The critical infrastructure sectors had an unequal burden with 38.6 greater incident rates. Geographic and time series analysis indicated alarming patterns such as the rising levels of activity of the threat actors. New threats such as threats of quantum computing and AI-driven attacks posed a signal to increase the pace of evolution that needed active reactions.

6.2. Practical Recommendations

6.2.1. For Industry Practitioners

Organizations implementing or using 5G networks should to focus on the overall security systems that are versatile and can deal with multiple areas of vulnerabilities at the same time. Threat detection systems and zero-trust architectures based on AI implementation proved to be highly effective. The investments in security that were over 18per subscriber per year returned profits in terms of lowering incident costs. Added security to IoT devices needs to be improved with regard to authentication and encryption as well as software upgrade systems. The deployments of network slicing should ensure isolation effectiveness. The security of cloud integration requires strong API security, multi-tenant isolation, and access control authentication.

6.2.2. For Policymakers

The proposed regulatory interventions to combat the market failures in cybersecurity were seen as reasonable, in terms of reported externalities. The widespread vulnerabilities can be dealt with in a logical manner by the introduction of minimum security standards to IoT devices. Some of the requirements include authentication, encryption, secure development and update mechanisms. Supply chain security measures that should be considered include hardware and software bill of materials, security testing, and vendor responsibility.

Privacy protection frameworks need revision in 5G related data collection capabilities. Increased openness in the practice of IoT data and tightened consent policies are consistent with the principles of privacy protection. Elevated security requirements should be stipulated according to critical infrastructure protection regulations whereby the security requirements should be corresponding to societal risks. Threat intelligence exchange systems with proper liability coverage may help to improve communal security.

6.2.3. For Cybersecurity Professionals

Security practitioners are expected to develop expert knowledge of the 5G-specific vulnerabilities. The skills required in network slicing isolation verification, edge computing security, and IoT device management are different. The 5G attack methods and tools should also be monitored via threat intelligence gathering. Constant training on the changing dangers was indicated due to the fast pace of technology and upkeep of tactics.

Organizational boundary cross-collaboration facilitated security performance. The presence in the information sharing communities gave a prior notification on rising threats. The interaction with technology vendors on the subject of security requirements may enhance product security. Investment in security standards development aided in the enhancement of the industry.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Pirbhulal, S., Chockalingam, S., Shukla, A., & Abie, H. (2024). IoT cybersecurity in 5G and beyond: A systematic literature review. International Journal of Information Security, 23, 2827–2879. https://doi.org/10.1007/s10207-024-00865-5

[2] U.S. Department of Homeland Security. (2023). 5G impacts on cybersecurity. Office of Intelligence and Analysis. https://www.dhs.gov/sites/default/files/2023-09/23_0906_oia_01_5G_Security_508_Compliant.pdf [PDF Available]

[3] Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G security: Analysis of threats and solutions. 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 193-199. https://doi.org/10.1109/CSCN.2017.8088621

[4] Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., & Akber, S. M. A. (2024). A comprehensive survey on IoT cybersecurity in 5G and beyond: Recent advances, emerging challenges, and future research directions. International Journal of Information Security, 23, 1625-1681. https://doi.org/10.1007/s10207-024-00865-5

[5] Girma, A., & Barrett, A. P. (2024). Security challenges and solutions in 5G-enabled IoT networks. In K. Arai (Ed.), Proceedings of the Future Technologies Conference (FTC) 2024, Volume 4 (Lecture Notes in Networks and Systems, Vol. 1157, pp. 632-643). Springer. https://doi.org/10.1007/978-3-031-73110-5_42

[6] NIST. (2021). 5G hardware supply chain security through measurement-based verification (NIST Special Publication 1278). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1278.pdf [PDF Available]

[7] Wajdi, M., Rahman, A., & Al-Hashimi, M. (2024). Exploring the technological advancements and security issues of 5G. World Journal of Advanced Research and Reviews, 23(2), 812-846. https://doi.org/10.30574/wjarr.2024.23.2.2367

[8] Ali, M. N., Abdulghani, H., Ayed, W. B., Hassan, M. M., & Fortino, G. (2024). A comprehensive survey on generative AI solutions in IoT security. Electronics, 13(24), Article 4965. https://doi.org/10.3390/electronics13244965

[9] CISA. (2020). Potential threat vectors to 5G infrastructure. Enduring Security Framework (ESF) Working Panel. https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20(1).pdf [PDF Available]

[10] Lilhore, U. K., Dalal, S., & Simaiya, S. (2024). A cognitive security framework for detecting intrusions in IoT and 5G utilizing deep learning. Computers & Security, 136, Article 103511. https://doi.org/10.1016/j.cose.2023.103511

[11] Sahni, I., Bisht, A., & Dhawan, S. (2022). A systematic literature review on 5G security. arXiv preprint. https://arxiv.org/pdf/2212.03299 [PDF Available]

[12] NSA & CISA. (2021). Security guidance for 5G cloud infrastructures. https://media.defense.gov/2021/Dec/16/2002910169/-1/-1/0/CSI_5G_CLOUD_SECURITY_GUIDANCE_V1.PDF [PDF Available]

[13] Yalli, J. S., Hasan, M. H., & Badawi, A. (2024). Internet of Things (IoT): Origin, embedded technologies, smart applications and its growth in the last decade. IEEE Access, 12, 15630-15652. https://doi.org/10.1109/ACCESS.2024.3359428

[14] Wazid, M., Das, A. K., Shetty, S., Gope, P., & Rodrigues, J. J. (2021). Security in 5G-enabled Internet of Things communication: Issues, challenges, and future research roadmap. IEEE Access, 9, 48938-48958. https://doi.org/10.1109/ACCESS.2021.3068033

[15] Department of Defense. (2020). DoD 5G strategy implementation plan. https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf [PDF Available]

[16] Castiglione, A., Esposito, J. G., Loia, V., Nappi, M., Pero, C., & Polsinelli, M. (2024). Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. IEEE Transactions on Industrial Informatics, 21, 1674-1683. https://doi.org/10.1109/TII.2024.3485796

[17] 5G Americas. (2022). Evolving 5G security for the cloud. https://www.5gamericas.org/wp-content/uploads/2022/09/Evolving-5G-Security-for-the-Cloud-2022-InDesign.pdf [PDF Available]

[18] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698. https://doi.org/10.1016/j.future.2016.11.009

[19] Fonyi, D. (2020). Overview of 5G security and vulnerabilities. Cyber Defense Review, 5(1), 117-146. https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2008_%20Fonyi_WEB.pdf [PDF Available]

[20] Benlloch-Caballero, P., Wang, Q., & Calero, J. M. A. (2023). Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. Computer Networks, 222, Article 109551. https://doi.org/10.1016/j.comnet.2023.109551

[21] ASEAN. (2022). Development of best practice guides for 5G ecosystem. https://asean.org/wp-content/uploads/2022/02/03-ASEAN-5G-Ecosystem-Best-Practices-Guide_Final-Report_SG_ASEC_TL_PH_MY.pdf [PDF Available]

[22] Ge, Y., & Zhu, Q. (2023). GAZETA: Game-theoretic zero-trust authentication for defense against lateral movement in 5G IoT networks. IEEE Transactions on Information Forensics and Security, 19, 540-554. https://doi.org/10.1109/TIFS.2023.3324517

[23] Rey, V., Sánchez, P. M. S., Celdrán, A. H., & Bovet, G. (2022). Federated learning for malware detection in IoT devices. Computer Networks, 204, Article 108693. https://doi.org/10.1016/j.comnet.2021.108693

[24] CISA. (2022). 5G security evaluation process investigation (Version 1). https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf [PDF Available]

[25] Al-Shareeda, M. A., Anbar, M., & Manickam, S. (2024). 5G security features, vulnerabilities, threats, and data protection in IoT and mobile devices: A systematic review. Sensors, 24(18), Article 6003. https://doi.org/10.3390/s24186003

[26] Singh, B. C., & Kaunert, C. (2024). Integration of cutting-edge technologies such as Internet of Things (IoT) and 5G in health monitoring systems: A comprehensive legal analysis and futuristic outcomes. GLS Law Journal, 6(1), 13-20. https://doi.org/10.5281/zenodo.11206771