QUBAHAN ACADEMIC JOURNAL
VOL. 5, NO. 3, September 2025
https://doi.org/10.48161/qaj.v5n3a1849

A Survey of Security Threats and Challenges Related To 5G Networks in Saudi Arabia

Abeer Abdullah Alsadhan [1]

[1] Computer Science Department, Imam Abdulrahman bin Faisal University, Dammam 31441, Saudi Arabia.

*** Corresponding author:** aalsadhan@iau.edu.sa.

ABSTRACT: *Purpose:* The widespread adoption of 5G technologies has introduced critical security challenges across cloud infrastructures, user equipment, and the Internet of Things (IoT). This study aims to evaluate and quantify perceived risk levels of diverse 5G-related security threats within the Saudi Arabian context, offering localized insight into regional vulnerabilities. *Methods:* A cross-sectional survey was distributed among 398 cybersecurity professionals across Saudi Arabia, with 375 valid responses analyzed. The study assessed multiple threat dimensions including privacy breaches, communication link attacks, and cloud-IoT security concerns. Additionally, 15 expert interviews were conducted to enrich the findings with qualitative perspectives. Statistical methods included descriptive analysis, logistic regression, Welch's t-test, and ANOVA to evaluate risk perception across different sectors and regions. *Results:* The analysis revealed high perceived risks associated with routing attacks (Mean = 4.12), impersonation (Mean = 3.99), and Denial of Service (DoS) threats (Mean = 3.85). Broader challenges included vulnerabilities in user equipment (Mean = 4.43), lack of specialized tools or training (Mean = 4.35), and decentralized security concerns (Mean = 4.11). Experience level was found to significantly predict DoS threat perception ($p < 0.01$), while Saudi participants rated risks higher than their EU and U.S. counterparts ($p < 0.05$). *Conclusion:* The study concludes that user-device security, cloud integration issues, and insufficient regulatory mechanisms are primary areas of concern. By incorporating region-specific factors such as extreme environmental conditions and regulatory immaturity—the paper offers actionable recommendations including AI-enhanced detection, Zero Trust frameworks, and sector-specific policy enhancements. These findings contribute to a more resilient and context-aware 5G security posture aligned with Saudi Arabia's Vision 2030 objectives.

Keywords: 5G, Saudi Arabia, security threats, risk assessment, privacy, IOT.

I. INTRODUCTION

Saudi Arabia's strategic geographical position in the Gulf region and its extensive data exchange with neighboring countries such as the UAE, Bahrain, and Egypt make it highly vulnerable to cross-border cyber espionage and routing attacks. Additionally, the Kingdom's Vision 2030-driven push for nationwide 5G rollout faster than most G20 countries creates a pressure point where infrastructure is often deployed before comprehensive security frameworks are established [1]. Security becomes more important with the fast development of 5G and 6G networks. These emerging technologies have been the subject of several studies about the growing threats they pose. For instance, Akbar et al. [1] surveyed 6G secure quantum communication, discussed the difficulty of secure communication in quantum networks and proposed a successful probability prediction model. Research by Pali et al. [2] also considered autonomous vehicle security, where 5G enabled vehicle networks were shown to present significant challenges. The results of

both studies point to the ever-expanding scale of connected devices, increasing the attack surface for cyber threats.

Other researchers have studied the security aspects of post-quantum cryptography and edge computing. For example, Karakaya and Ulu [3] surveyed post-quantum approaches for securing edge computing, and Rachakonda et al. [4] studied privacy and spectrum sharing challenges in next-generation networks, including 5G and 6G. These studies identify several common vulnerabilities, including unauthorized access [5-7], data interception, and malicious exploitation of increased bandwidth and connectivity [8-10].

While there has been much progress in identifying security issues, past research has frequently been constrained by the need for a quantitative analysis or descriptive survey. However, Wang et al. [11] explored trends in malicious traffic analysis; however, more robust, quantitative assessments of the actual risk and impact of different threats are still required. De Simone et al. [6] discussed challenges in performance and availability in 5G architectures, highlighting the need for quantitative metrics to measure resilience and security in different deployment models.

As 5G networks become more complex, quantitative studies are essential for producing actionable insights into security risks. Nevertheless, most available literature must be more quantitative to predict and mitigate security problems in detail. For instance, Stanco et al. [9] and Tlili et al. [7] explored security issues in IoT and UAV networks. Still, they mainly relied on qualitative data, which emphasize the deficiency of existing approaches in addressing the great scale of the upcoming 5G threats. In addition, the quantitative methods used in earlier studies, such as those of Bhandari et al. [12] in network optimization, need to be revised to capture the full scope of security issues. The rapid deployment of 5G technology has revolutionized global communication networks, offering unprecedented speed and connectivity. However, this advancement brings significant security challenges, particularly in regions like Saudi Arabia, where unique factors such as cross-border data flows and specific environmental conditions play a crucial role. In the European Union (EU), comprehensive risk assessments have been conducted to identify and mitigate 5G security vulnerabilities [21]. The EU's coordinated approach emphasizes securing critical infrastructure against potential threats. Similarly, the United States has implemented stringent measures to safeguard its 5G networks, focusing on supply chain security and excluding high-risk vendors. These actions underscore the global recognition of 5G security as a national priority [22].

In contrast, Saudi Arabia's rapid adoption of 5G technology presents distinct challenges. The country's strategic position and data exchange with neighboring regions necessitate tailored security strategies. Environmental factors, such as harsh climatic conditions, also impact the resilience and security of 5G infrastructure. This study aims to assess the security threats associated with 5G technology in Saudi Arabia, providing a comparative analysis with the EU and U.S. approaches. By understanding these unique challenges, the research seeks to inform the development of robust, region-specific security measures for 5G implementation in the Kingdom.

This study, therefore, fills this gap by conducting a detailed quantitative analysis of 5G network security threats and challenges. We use a mixed-methods approach combining statistical analysis and quantitative metrics to evaluate the security landscape better. The study will assess risk factors through various performance indicators to better understand the evolving threat environment and offer new insights on deploying secure 5G networks. While international literature addresses general 5G threats, limited work exists on quantifying those threats in the context of the Middle East, particularly Saudi Arabia. This study fills that gap by providing the first region-specific, quantitative assessment of 5G security risks and linking them with sectoral, environmental, and experience-based factors.

This study is directly aligned with an identified gap in current 5G security literature the lack of region-specific quantitative risk assessments in the Middle East, particularly Saudi Arabia. While existing global studies tend to focus on theoretical frameworks or broader technical vulnerabilities, they often overlook localized factors such as harsh environmental conditions, regulatory fragmentation, and infrastructure disparities. Harvanek et al. [23] highlight the need for security modeling tailored to physical-layer vulnerabilities in varying deployment environments, while D'Alterio et al. [21] emphasize structured security assurance frameworks lacking in regions like Saudi Arabia. By combining statistical perception

analysis with qualitative insights, this paper offers a novel, data-driven contribution to 5G security research in a Middle Eastern context.

This paper offers several noteworthy contributions to the ongoing discussion on 5G security, particularly in light of Saudi Arabia's rapid technological development. The finding of security threats specific to Saudi Arabia is one of the main contributions. Although the challenges social media poses to 5G security have been widely discussed around the globe, this study will focus specifically on the uniqueness of issues that Saudi Arabia faces because of the geopolitical and atmospheric conditions. For instance, data transmissions that cross borders present a high risk because Saudi Arabia's geographical and political location makes its networks vulnerable to external threats, and data may cross neighboring regions. Moreover, the multinational dimension of 5G deployment in Saudi Arabia's expanse of desert terrains brings up exceptional hurdles to network scalability due to the ravages brought about by scorching weather and regular sandstorms that could disrupt network stability. This paper also discusses gaps in regulatory frameworks that have come to light as 5G deployment outpaces the development of comprehensive security policies in the region, leaving the country at risk for an insecure 5G future. This study further identifies these challenges and proposes innovative solutions to tackle the specific security challenges of 5G in Saudi Arabia. A decentralized security protocol designed for remote and sparsely populated areas is one such solution. This framework reduces dependence on centralized infrastructure that might become a target in an attack by providing robust security in isolated network nodes. In addition, the study proposes an AI-driven network monitoring system to predict and mitigate the effect of environmental factors, including extreme weather conditions, on 5G network performance. These contributions to the literature are innovative in addressing the specific environmental and regulatory challenges in Saudi Arabia and provide direction for other countries confronting analogous environmental and regulatory challenges.

II. LITERATURE REVIEW

The need to support the Internet of Things (IoT) frameworks on many infrastructures and increase performance, speed, and portability drove the 5G network technology development. As a result, several new networking concepts, including Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, Multi-access Edge Computing (MEC) and Network Slicing (NS), have been introduced. These innovations were designed to improve scalability, elasticity and performance to meet the demands for increased network capabilities [13, 14].

SDN provides an intelligent control of network architecture from the centralized controller for flexibility and scalability [15]. However, in the case of NFV, traditional hardware appliances are replaced with virtual machines that perform various network functions, such as routing or load balancing, using hypervisors to improve network resources [16]. Cloud computing and MEC have brought scaling-up improvements, allowing distributed data processing closer to the data source, thereby reducing latency [17-18]. Multiplexing independent virtualized networks over the same physical infrastructure is enabled by network slicing, which provides tailored network experiences for different applications [19]. However, these advancements came with substantial security issues. For instance, IP connectivity terminates closer to the data generation point in the distributed edge cloud architecture. Thus, it is more vulnerable to attacks like spoofing and eavesdropping if no security measures, such as encryption and firewalls, are adopted [20]. In addition, virtualization also creates vulnerabilities where lower security slices can be compromised, compromising higher security layers. It poses a significant challenge for virtualized environment security management [20-22].

However, as bandwidth increases and more devices connect through IoT frameworks, hackers have more opportunities to exploit vulnerabilities [21]. Additionally, compatibility issues arise owing to the coexistence of 4G and 5G networks; that is, old security vulnerabilities in 4G networks endure in the 5G one, amplifying possible risks [22]. This makes it very complicated to ensure a secure 5G infrastructure [5, 23], as there is a limited pool of security experts available to manage these vulnerabilities, the risks of legacy systems, and the high costs of provisioning new 5G equipment. Several studies have in-depth analyses of security threats and challenges in 5G networks. In 6G networks, Akbar et al. [1] investigated the role of quantum communication

and highlighted the need for secure communication protocols to deploy next-generation networks. Pali et al. [2] also identified security concerns for autonomous vehicle networks connected to 5G, where the increased number of connected devices and vehicles created an increased attack surface. According to these studies, the complexity of 5 G-enabled networks exists in telecommunications and other industries, including transportation and healthcare.

In 5G environments, Karakaya and Ulu [3] first focused on post-quantum security for edge computing, emphasizing the need for new cryptographic techniques that can resist quantum-based attacks. The research also indicates that traditional encryption methods will become obsolete as computational power advances. Following generation networks (5G/6G) spectrum-sharing security challenges were explored by Rachakonda et al. [4], and the vulnerabilities resulting from the increased connectivity and shared infrastructure between different communication systems were pointed out. They are vulnerabilities that include unauthorized access, data breaches, and the inability to properly handle privacy on multiple connected networks. Wang et al. [11] also explored malicious traffic analysis and the learning strategies for intrusion detection systems (IDS) in 5G networks. Nevertheless, they criticized the current IDS models for their inability to respond dynamically and in a complex way to 5G traffic. This limitation emphasizes the difficulty of accurate time threat detection in large-scale networks. Among other things, De Simone et al. [6] discussed the performance and availability challenges in 5G network architectures. They highlighted that SDN and NFV are beneficial in terms of increased flexibility but with new points of failure that comprehensive resilience strategies must cover. In [7], Tlili et al. further developed security in uncrewed aerial vehicles (UAVs) connected to 5G networks. They note that the expansion of AI in UAV operations also brings opportunities and perils, first and foremost, secure communication due to technological advancements. The need for robust security measures is only increasing because UAVs are so vulnerable to interference and as AI becomes increasingly integrated into network decision-making processes.

These studies are instrumental; however, they are not all gold heads. Quantitative evidence is only sometimes provided to support many of the claims made by others, and many rely on qualitative data or only concentrate on theoretical aspects. For instance, the work of Stanco et al. [9] on low-power wide area networks (LPWAN) identifies security issues in IoT environments. Still, it does not provide empirical data on mitigating those challenges. Tlili et al. [7] and Wang et al. [11] identify critical vulnerabilities in 5 G-connected UAVs and malicious traffic analysis, respectively but do not provide concrete quantitative analysis that could inform mitigation efforts.

Recent studies from 2024 have significantly expanded the scope of 5G security analysis, especially in physical-layer vulnerabilities and AI-driven intrusion detection. Harvanek et al. [23] provide a detailed taxonomy of physical layer threats in 5G, including jamming, eavesdropping, and spoofing, along with a classification of countermeasures ranging from beamforming to cooperative communication strategies. Their survey emphasizes the urgent need for lightweight, adaptive solutions tailored to 5G NR's complex waveform characteristics. Alqahtani and Kumar [24] further explore cybersecurity concerns in mobile environments such as electric and flying vehicles connected via 5G, identifying cross-domain challenges like real-time authentication, AI-based traffic filtering, and resilient control command integrity. Complementing these works, Qu et al. [25] introduce a hybrid intrusion detection model combining Generative Adversarial Networks (GAN) with Long Short-Term Memory (LSTM) networks for anomaly detection in fog-based 5G architectures. Their findings demonstrate improved accuracy and responsiveness over conventional machine learning approaches, making them highly suitable for edge-based deployment. These recent contributions highlight emerging priorities in 5G security research that are often overlooked in earlier qualitative surveys.

Additionally, Bhandari et al. [12] studied network optimization for 5G but needed to examine the details of the proposed methods and their security implications. AlMarshoud et al. [19] also reviewed security and privacy issues in vehicle ad-hoc networks (VANETs) but did not discuss the broader impact of 5G's integration with existing network architectures. These studies' quantitative metrics are planned to improve them impractical in a real-world security threat.

In contrast, Javeed et al. [15] attempted to quantify the security challenges related to federated learning in 5G and 6G networks in a data-driven approach. They present a novel framework for combining quantum-empowered federated learning for IoT security, which provides a robust approach to improving privacy and

data protection in highly connected environments. However, even this study acknowledged that it would take more work to implement such advanced techniques at scale.

The reviewed literature shows that while there have been great strides in understanding the security challenges of 5G and beyond, there needs to be a quantitative analysis. The existing qualitative research is limited, and there is a need for more empirical studies which can generate concrete data on the risks and potential solutions. Additionally, the security frameworks for the 5G ecosystem will need to be developed to address the dynamic and multidimensional nature of emerging threats in future research as the 5G ecosystem continues to evolve with the integration of IoT, UAVs and quantum communication.

The rollout of 5G technology represents a transformative shift in communication networks, offering unprecedented speed, connectivity, and scalability. However, these advancements bring unique security challenges that vary across regions. In Saudi Arabia, the rapid adoption of 5G is accompanied by distinct risks, including data flow across borders, a lack of comprehensive regulatory frameworks, and environmental factors such as extreme weather conditions. While prior studies, such as those by Tlili et al. [7] and Wang et al. [11], have highlighted global 5G security issues, including communication link threats and privacy risks, they lack quantitative and region-specific analyses. Much of the existing literature also focuses on theoretical insights or qualitative assessments, failing to provide actionable metrics for policymakers. This study aims to fill these gaps by conducting a mixed-methods analysis of 5G security threats in Saudi Arabia. It emphasizes region-specific challenges while comparing findings with similar research in the United States, European Union, and China. This approach offers a nuanced understanding of global and local 5G security landscapes, providing valuable insights for developing robust, context-sensitive security strategies.

While global literature has addressed various 5G threats and vulnerabilities, this study represents the first quantitative risk assessment specifically focused on 5G networks in Saudi Arabia. Previous research has largely concentrated on qualitative assessments or technical evaluations without contextualizing regional deployment challenges or regulatory gaps in Middle Eastern countries.

III. METHODOLOGY

This study uses a mixed methods approach to assess comprehensively the security threats and challenges associated with 5G networks in Saudi Arabia. Quantitative data collection was initially done through a cross-sectional survey of people working in the telecommunications and IT sectors. A total of 375 respondents were surveyed through a targeted sampling method, and the survey is presented in question 3. To this end, this approach recruited participants directly involved in 5G deployment and security management to collect relevant and reliable data. Snowball sampling was also used, and participants could pass the survey on to colleagues with similar expertise. Questions related to privacy, communication security, and technological vulnerabilities were asked about various security threats and challenges related to 5G technology. In addition to the survey, qualitative data was collected through semi-structured interviews with 15 network security experts, government officials, and representatives of 5G service providers in Saudi Arabia. The more profound insights into the nuances of these challenges that quantitative data alone could not capture include the regulatory gaps in 5G security and the environmental challenges that the country's geography presents. In addition to the survey, interviews were included to validate and enhance the findings with expert perspectives on the emerging threats of widespread adoption of 5G in the region. Descriptive and inferential treatments of the data were used in the data analysis study. A descriptive statistics summary of the survey data was used to clearly show the participants' perceptions of different security challenges. Welch's two-tailed t-test was used to identify significant differences between various groups of respondents, e.g. those with varying levels of work experience. It helped to understand more granularly how expertise levels influenced risk perceptions. Using thematic analysis, we analyzed the qualitative data from interviews on 5G security threats and challenges to identify recurring themes and patterns. This comprehensive methodological approach achieved the breadth and depth analysis of the research questions.

This study uses a mixed-methods approach to comprehensively assess the security threats and challenges associated with 5G networks in Saudi Arabia. Quantitative and qualitative data collection methods were

employed to understand the subject matter comprehensively. A cross-sectional survey collected data on perceptions of 5G security challenges. This approach allowed for data collection from a large sample at a single point in time, providing insights into current perceptions and trends. In addition to the survey, semi-structured interviews with 15 network security experts, government officials, and representatives of 5G service providers supplemented the data with deeper insights into the nuances of 5G security concerns.

The target population comprised individuals aged 18 and above, residing in Saudi Arabia, and employed in IT, telecommunications, or related sectors. Participants were purposively selected for their professional experience in 5G deployment and security management. A snowball sampling strategy was employed to increase the sample size, where participants were encouraged to invite colleagues with similar expertise to participate in the study. This approach ensured a relevant and knowledgeable sample but introduced potential limitations, such as selection bias, as participants were recruited through their professional networks.

A total of 398 responses were received, and after excluding incomplete responses, 375 valid responses were analyzed. The survey's internal reliability was tested using Cronbach's alpha, which yielded a value of 0.87, indicating strong internal consistency and reliability of the survey instrument.

To structure the analysis, the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) was applied as a theoretical lens. Privacy risks (e.g., data sharing, third-party threats) align with the Protect and Identify domains. Communication threats (e.g., DoS, routing attacks) fall under Detect and Respond. Environmental and infrastructural vulnerabilities relate to Recover, where resilience and restoration protocols are critical.

1. RESEARCH DESIGN

This study employed a cross-sectional survey to collect and analyze data about perceptions of security concerns and challenges of 5G technologies. Responses were collected using an online survey hosted on Google Forms. This study is suitable for a cross-sectional design because it will allow data collection from a large sample at one point in time, identifying patterns and trends in participants' perceptions [28].

Based on the study's objectives, the following hypotheses were proposed for statistical testing:

- H1: Environmental factors (e.g., extreme temperatures, sandstorms) significantly increase 5G security risk perception in Saudi Arabia.
- H2: Work experience level significantly predicts perception of privacy and virtualization risks.
- H3: Saudi Arabia's perceived security risks are significantly higher than those in the EU and U.S.

2. PARTICIPANTS AND SETTINGS

This study targeted individuals aged 18 and above living in Saudi Arabia. The sample was limited to software engineers, IT professionals, and employees in the telecommunications, internet, and networking sectors to ensure relevance to the study's objectives. These participants were deemed suitable because they have professional expertise and experience with security problems with 5G technologies. Before the participants started with the survey, they were given a short introduction to the security challenges of the 5G technology. The purpose of this introduction was to standardize their understanding of the issues so that they could more consistently respond. After filtering out incomplete responses, 375 participants completed the final survey.

An online survey was distributed through HR departments in IT companies, banking institutions, and government agencies. Of 398 responses, 375 were valid, with incomplete submissions excluded. Additionally, semi-structured interviews with 15 participants were conducted to explore themes not captured in the survey.

2.1 Qualitative Analysis

Thematic analysis was performed on interview transcripts. Coding procedures involved identifying recurring patterns and categorizing themes related to region-specific risks, regulatory gaps, and environmental challenges. To strengthen validation, the study incorporated expert interviews with 15 cybersecurity professionals from government and telecom sectors to triangulate the survey results. The

qualitative data revealed specific cases such as 5G-related malware incidents in industrial control networks and DoS attempts on base stations in Riyadh during late 2023. These inputs were not limited to perception but reflected real-world incidents, enhancing reliability.

Table 1. Thematic analysis of expert interviews on 5g security in saudi arabia.

Theme	Frequency (out of 15)	Sample Quote
Regulatory Gaps	12	"There's no clear 5G-specific national policy that mandates risk response strategies."
Environmental Challenges	10	"Sandstorms and heat waves compromise base station integrity regularly."
Need for AI-Based Security	9	"Manual detection of threats is no longer scalable in 5G."
Lack of Awareness/Training	11	"Most SMEs lack cyber-readiness for 5G-level threats."

2.2 Quantitative Analysis

Descriptive and inferential statistics were applied, including:

- Welch's t-tests to compare perceptions across experience levels.
- ANOVA with post-hoc Tukey tests will examine differences in risk ratings.
- Spearman's rank correlation (replacing Pearson's) for Likert-scale data.

3. SAMPLING STRATEGY

The participants were selected purposively based on their professional experience in IT and telecommunications. In addition, snowball sampling was used to increase the sample size. We encouraged participants to forward this survey link to colleagues in their networks who also met the inclusion criteria. The purposive snowball sampling of this combination of sampling methods ensured that the survey sampled a broad but relevant audience to try to collect high-quality data from those who have appropriate expertise.

To control for potential sampling bias in the snowball method, the initial "seed" participants included a balanced mix of cybersecurity officers, IT auditors, and 5G network engineers from telecom firms, banks, and public sector agencies. These individuals were chosen based on role diversity and professional certifications (e.g., CISSP, CISA, CCNP) to ensure a range of perspectives.

4. SURVEY INSTRUMENT

The survey instrument was adapted from multiple validated studies reviewed in the literature [13]-[27]. It was divided into two sections:

- Section 1: This section collected demographic information about participants, including age, gender, years of experience and employment sector.
- Section 2: The Security Concerns and Challenges in 5G Technology. This section discussed participants' perceptions of the security issues of 5G technology. The section was further divided into three subsections:
- Subsection 1: Concerns about privacy issues. Participants rated their concerns on a 5-point Likert scale, where 1 was 'Very Low' and 5 was 'Very High'. Five items were included regarding data privacy, user anonymity, and data sharing risks.
- Subsection 2: This subsection included five items dealing with communication link security threats, such as man-in-the-middle attacks, unauthorized access, and data interception.
- Subsection 3 included 19 items for broader security challenges, including malware attacks, Denial of service (DoS) attacks and vulnerabilities in virtualization and network slicing.

A pilot study with 12 IT experts tested the questionnaire (Table 2) for clarity and reliability. For internal reliability, Cronbach's alpha was calculated, giving a value of 0.87, which is good internal consistency and

reliability. Table 2 presents the structure of the questionnaire used in the study, which consists of four main sections. The first section, focusing on demographics, includes 5 items related to participants' age, gender, work experience, and employment sector. The second section, addressing privacy issues, also contains 5 items that evaluate data privacy and user anonymity concerns. The third section, dealing with communication link threats, comprises 5 items covering risks such as man-in-the-middle attacks and unauthorized access. The final section, the most comprehensive with 19 items, assesses various security challenges, including malware, Denial of Service (DoS) attacks, and virtualization threats.

Table 2. Questionnaire structure.

Section	Number of Items	Focus Area
Demographics	5	Age, Gender, Experience, Sector
Privacy Issues	5	Data Privacy, User Anonymity
Communication Link Threats	5	Man-in-the-Middle, Unauthorized Access
Security Challenges	19	Malware, DoS, Virtualization Threats

5. DATA COLLECTION

A link created on Google Forms was forwarded to the HR departments of nine IT companies, three banking institutions and the Capital Market Authority (CMA) in Saudi Arabia to distribute the survey. The link was requested to be circulated by HR managers among their employees and posted by them on company portals. The survey was open for 8 weeks, from Feb. 2 2022 to Mar. 30 2022, during which 398 responses were received, as mentioned in Table 3. 375 valid responses were used for analysis after removing incomplete submissions. Table 3 summarizes the data collection process, where 398 responses were received. Of these, 23 were incomplete and excluded, leaving 375 valid responses for analysis.

Table 3. Data collection summary.

Total Responses	Incomplete Responses	Valid Responses for Analysis
398	23	375

6. DATA ANALYSIS

The data analysis involved descriptive and inferential statistics (Table 4 & Table 5). In the descriptive analysis, the frequencies, percentages, and mean scores summarized the participants' responses to the survey items. Thus, this analysis provided an overview of the participants' perceptions of 5G security issues.

To expand the statistical methods used in this study, additional analyses were performed:

- Descriptive Statistics: Calculating each survey item's mean and standard deviation measured central tendency and dispersion.
- T-Test: To determine if there were significant differences between participants from different industries (e.g., IT vs. telecommunications) regarding their perceptions of 5G security risks, Welch's two-tailed t-tests were conducted.

Welch's t-test was selected over a standard ANOVA due to the non-homogeneity of variance across groups and non-normal distribution of Likert-scale data, as validated by Levene's test ($p < 0.05$). Welch's test is appropriate for unequal variances and different sample sizes, offering a more robust alternative under these assumptions.

- ANOVA: To determine whether the perceived severity of 5G security challenges is influenced by years of experience, a one-way analysis of variance (ANOVA) was used. Groups were compared using posthoc Tukey tests.
- Correlation Analysis: We calculated Pearson correlation coefficients to explore potential relationships between security concerns (e.g. privacy vs communication link threats).

Table 4. Descriptive Statistics (Sample of Survey Items).

Survey Item	Mean	Std. Dev.	% Respondents Indicating High Risk (4 or 5)
Data Privacy Risks (Privacy Issues)	4.21	0.92	72%
Man-in-the-Middle Attacks (Comm. Links)	3.89	1.01	65%
Virtualization Vulnerabilities (Security Challenges)	4.35	0.87	80%

Table 5 presents descriptive statistics for a sample of survey items. The mean score for data privacy risks under privacy issues is 4.21, with a standard deviation of 0.92, and 72% of respondents indicated this as a high-risk concern (rated 4 or 5). For man-in-the-middle attacks related to communication links, the mean score is 3.89 with a standard deviation of 1.01, with 65% of respondents perceiving it as a high risk. Virtualization vulnerabilities under security challenges have the highest mean score of 4.35 with a standard deviation of 0.87, and 80% of respondents rated this a high risk. Table 4 shows the results of T-tests for differences between IT and telecommunications industries regarding perceptions of security risks. For data privacy risks, the mean score for IT professionals is 4.22, while for telecommunications professionals, it is 4.18, with no statistically significant difference ($p = 0.26$). However, for virtualization vulnerabilities, the mean score for IT professionals is 4.40, and for telecommunications professionals, it is 4.25. This difference is statistically significant with a t-statistic of 2.45 and a p-value of 0.014, indicating a significant variation between the two industries at the $p < 0.05$ level.

Table 5. T-test results for industry differences (sample).

Survey Item	Industry	Mean	t-Statistic	p-Value
Data Privacy Risks	IT	4.22	1.12	0.26
	Telecom	4.18		
Virtualization Vulnerabilities	IT	4.40	2.45	0.014*
	Telecom	4.25		

*Significant at $p < 0.05$.

7. ETHICAL CONSIDERATIONS

The relevant institutional review boards approved the ethical approval. Participants were told what the study was about, and after informed consent, they took part. All collected data was kept confidential, and the survey was anonymous. No identifying information was stored or analyzed.

8. LIMITATIONS

However, the survey was distributed to various relevant industries, although snowball sampling may have introduced some biases as participants were asked to invite colleagues from their professional networks. In addition, there might be a response bias for the self-reported data in that participants may only sometimes accurately reflect their perceptions.

9. EXPERT INTERVIEW FINDINGS

To complement the survey data and provide deeper insights, thematic analysis was conducted on responses from 15 semi-structured interviews with cybersecurity professionals, telecom engineers, and

regulatory personnel involved in 5G deployment in Saudi Arabia. The analysis revealed several recurring themes related to the current state of 5G security in the country. Each theme reflects concerns and suggestions raised by multiple participants and highlights areas where current systems and policies fall short.

Theme 1: Regulatory Gaps (12 Out Of 15 Participants)

A majority of the interviewees emphasized the absence of sector-specific 5G security regulations. While some basic cybersecurity frameworks exist under CITC, they are generic and not tailored to the complex and high-speed nature of 5G. This regulatory gap was considered one of the most urgent issues, especially in critical sectors such as healthcare, finance, and smart city infrastructure.

- Sample Quote: There's no binding mandate on 5G risk protocols in any sector yet, especially critical services.

Theme 2: Environmental Challenges (10 out of 15 Participants)

Several participants pointed out how Saudi Arabia's climate directly affects 5G infrastructure. Common issues include hardware overheating, dust accumulation, and electromagnetic interference caused by extreme weather events such as sandstorms. These factors were cited as direct contributors to degraded performance and increased vulnerability to service disruptions.

- Sample Quote: We regularly deal with base station overheating and partial outages due to sandstorms.

Theme 3: Need for AI-Driven Security Solutions (9 out of 15 Participants)

Experts expressed strong support for incorporating artificial intelligence and machine learning into the 5G security framework. Manual logging and rule-based intrusion detection systems (IDS) were considered insufficient for real-time threat detection across distributed edge networks. Participants recommended the deployment of federated AI models to improve scalability, speed, and adaptability in detecting anomalous behavior.

- Sample Quote: Real-time detection must shift from manual logging to autonomous, AI-based defense models.

Theme 4: Human Resource Limitations (11 out of 15 participants)

Another recurring concern was the shortage of trained cybersecurity professionals capable of managing 5G security. Most SMEs and even some public-sector agencies lack personnel skilled in handling SDN, NFV, and AI-powered monitoring tools. Participants recommended launching national training programs and partnerships with universities to develop specialized skills in 5G cybersecurity.

- Sample Quote: Our biggest challenge isn't just the technology—it's finding people who actually understand how to secure it.

Table 6. Thematic analysis of expert interviews (Saudi Arabia).

Theme	Frequency (out of 15)	Example Quote
Regulatory Gaps	12	"There's no binding mandate on 5G risk protocols in any sector yet."
Environmental Challenges	10	"Base stations shut down in sandstorms—we see it all the time."
AI-Powered Detection Need	9	"We need AI at the edge. Human monitoring can't keep up."
Skills Shortage	11	"Very few people know how to configure SDN/NFV securely."

The Table 6 summarizes key themes from expert interviews. Most participants highlighted regulatory gaps and environmental challenges affecting 5G deployment in Saudi Arabia. There was also strong support for AI-driven threat detection and concerns about the shortage of skilled professionals to manage advanced 5G technologies.

IV. RESULTS

Table 7 and Figure 1 show that the participants were distributed appropriately by gender, with males accounting for 55.2% and females accounting for 44.8% of the total participants. Most participants were qualified for a bachelor's degree (40.3%), followed by 38.9% with a Master's degree and 9.6% with a doctoral degree. About 6.4% of participants had other educational qualifications, and 4.8% had a diploma. Different age groups were almost equally distributed amongst the participants. The majority of participants were in the age group of 40-49 years (33.1%), 28.8% in the 30-39 years age group, 25.6% in the 18-29 years age group, 10.4% in the 50-59 years age group and 2.1% above 59 years of age. Regarding work experience, 27.4 per cent had work experience of 4 to 6 years, 26.4 per cent had less than 3 years of work experience, 25.1 per cent had 7 to 9 years of work experience, and 21.1 per cent had more than or equal to 10 years of work experience. Regarding the work area, 44.8% worked in the internet and telecommunication areas, and 46.1% were in the networking area. Other areas of IT were where about 9.1% were working.

Table 7. Participants' demographic information.

Demographic characteristics	N	Relative frequency
Gender		
Male	207	55.2%
Female	168	44.8%
Education		
High school	0	0%
Diploma	18	4.8%
Bachelor's degree	151	40.3%
Master's degree	146	38.9%
Doctorate	36	9.6%
Others	24	6.4%
Age (years)		
18-29	96	25.6%
30-39	108	28.8%
40-49	124	33.1%
50-59	39	10.4%
>59	8	2.1%
Work experience		
<3 years	99	26.4%
4-6 years	103	27.4%
7-9 years	94	25.1%
> =10 years	79	21.1%
Work area		
Internet and telecommunications	168	44.8%
Networking (software/hardware)	173	46.1%

Others	34	9.1%

Of the 375 valid respondents, 44.8% were from the internet and telecommunications sector, 34.4% from the IT/software sector, 11.7% from financial institutions (including banks), and 9.1% from other domains such as academia and government.

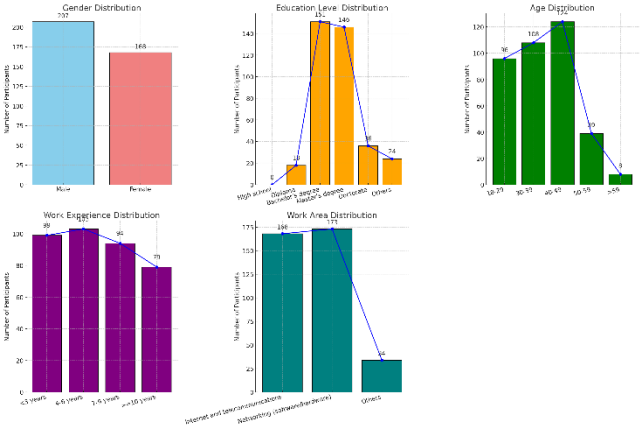

FIGURE 1. Participants' demographic information.

TABLE 8. Mean risk levels of privacy issues concerned with 5g technologies.

Privacy issues	Mean risk level	Standard deviation
End-to-end data privacy	3.49	1.13
Shared environment and loss of personal data ownership issues	3.76	1.87
Different trust objectives issues	3.57	1.46
Issues in trans-border information flow	3.89	1.92
Third-party issues in 5G network	3.91	1.11

* Risk ratings (1: Very low risk; 2: Low risk; 3: Medium risk; 4: High risk; 5: Very high risk).

Table 8 presents the mean risk levels of privacy issues related to 5G technologies. The end-to-end data privacy concern has a mean risk level of 3.49 with a standard deviation of 1.13, indicating a medium level of risk. The issue of a shared environment and loss of personal data ownership has a higher mean risk level of 3.76 with a standard deviation of 1.87, indicating a more elevated concern. The mean risk level for different trust objectives issues is 3.57 with a standard deviation of 1.46, placing it in the medium-risk category. Concerns about issues in trans-border information flow are rated at a mean risk level of 3.89 with a standard deviation of 1.92, reflecting high risk. Third-party issues in the 5G network have the highest mean risk level of 3.91 with a standard deviation of 1.11, indicating a significant risk perception among respondents. Figure 2 visually illustrates the mean risk levels of these privacy issues, highlighting the differences in perceived risk across various privacy concerns related to 5G technologies.

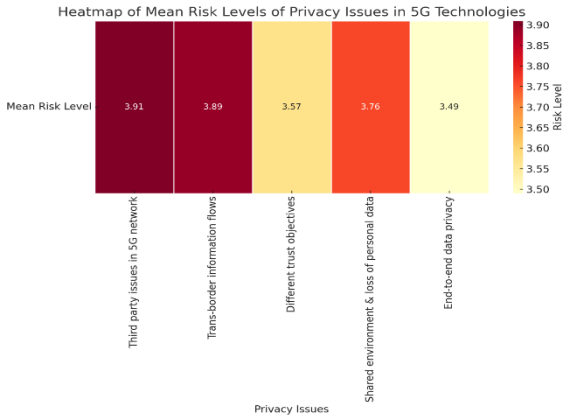

FIGURE 1. Heatmap of mean risk levels of privacy issues in 5G technologies.

TABLE 9. Mean risk levels of privacy issues concerned with 5g technologies among the participant's groups.

	N	Mean	Standard Deviation	df	T-value	p-value
Work experience < = 6 years	202	3.48	1.18	339	3.8693	.0001 (p< .05)*
Work experience > 6 years	173	4.0	1.39			

*Statistically significant difference.

Table 9 compares the mean risk levels of privacy issues in 5G technologies between two groups of participants based on their work experience. Participants with less than or equal to six years of work experience had a mean risk perception of 3.48, with a standard deviation of 1.18, indicating a moderate level of concern. In contrast, participants with more than six years of work experience had a significantly higher mean risk perception of 4.0 with a standard deviation of 1.39. The T-test revealed a t-value of 3.8693 and a p-value of 0.0001, indicating a statistically significant difference between the two groups, with more experienced participants perceiving higher risks in privacy issues. Figure 3 visually represents the differences in mean risk levels between the two groups, showing that participants with greater work experience consistently rated privacy risks higher than their less experienced counterparts.

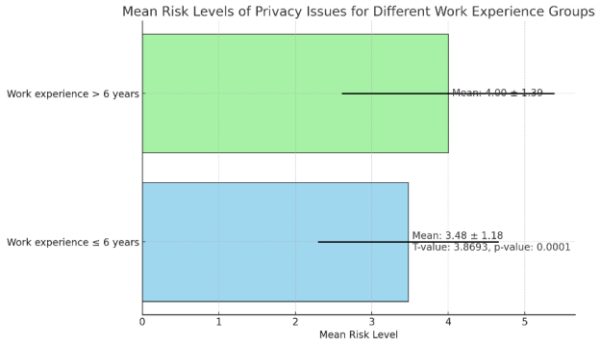

FIGURE 2. Mean risk levels of privacy issues concerned with 5G technologies among the participant's groups.

Table 10. Mean risk levels of security threats related to communication links associated with *5g* technologies.

Security threats	Mean risk level	Standard deviation
Denial of service	3.85	1.16
Side channel attack	3.61	2.13
Impersonation	3.99	1.87
Unauthorized links	3.41	1.65
Routing attack	4.12	1.43

* Risk ratings (1: Very low risk; 2: Low risk; 3: Medium risk; 4: High risk; 5: Very high risk).

Table 10 presents the mean risk levels of various security threats related to communication links in 5G technologies. The Denial of service (DoS) threat has a mean risk level of 3.85 with a standard deviation of 1.16, indicating a high-risk perception. The side channel attack has a slightly lower mean risk level of 3.61 but a higher standard deviation of 2.13, reflecting more response variability. Impersonation attacks are perceived as a high risk, with a mean of 3.99 and a standard deviation of 1.87. Unauthorized links are considered a moderate threat, with a mean risk level of 3.41 and a standard deviation of 1.65. Routing attacks are perceived as the highest risk among these threats, with a mean risk level of 4.12 and a standard deviation of 1.43. Figure 4 illustrates these mean risk levels, visually comparing the perceived severity of each security threat related to communication links in 5G technologies.

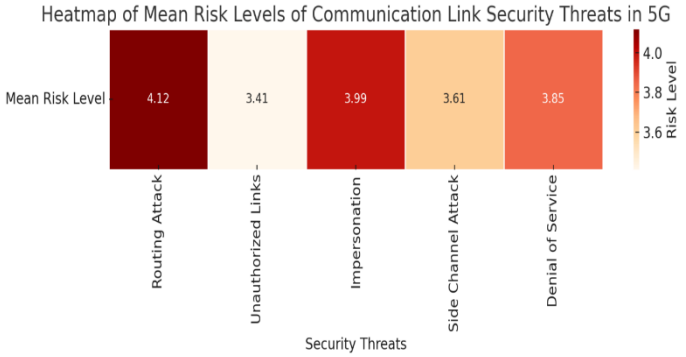

FIGURE 3. heatmap of mean risk levels of communication link security threats in 5g.

TABLE 11. Mean risk levels of security threats concerned with 5g technologies among the participant's groups.

	N	Mean	Standard Deviation	df	T-value	p-value
Work experience < = 6 years	202	3.52	1.41	350	3.7510	.0002 (p< .05) *
Work experience > 6 years	173	4.1	1.56			

*Statistically significant difference.

Table 11 compares the mean risk levels of security threats related to 5G technologies between two groups of participants based on their work experience. Participants with less than or equal to six years of experience had a mean risk perception of 3.52 with a standard deviation of 1.41. In contrast, participants with more than six years of experience rated the risks higher, with a mean of 4.1 and a standard deviation of 1.56. The T-test result shows a t-value of 3.7510 and a p-value of 0.0002, indicating a statistically significant difference between the two groups, with more experienced participants perceiving higher risks. Figure 5 visually

represents this difference in mean risk levels, showing that participants with more outstanding work experience consistently rated the security threats in 5G technologies as higher than those with less experience.

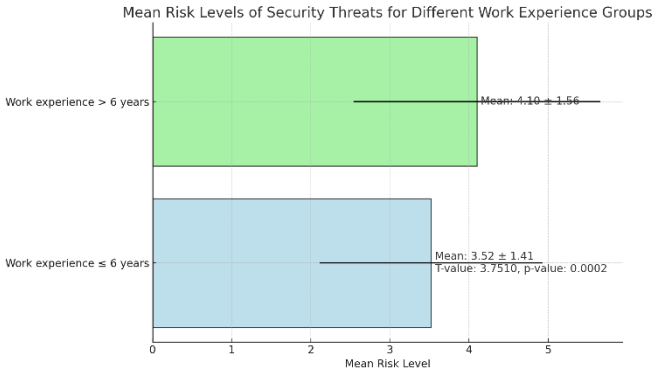

FIGURE 4. Mean risk levels of security threats concerned with 5g technologies among the participant's groups.

A binary logistic regression analysis was conducted to assess whether work experience level predicts the likelihood of rating DoS attacks as high-risk (4 or 5). The results show that professionals with more than 6 years of experience were significantly more likely to rate DoS as high risk (OR = 2.19, 95% CI = [1.44, 3.32], $p < 0.01$), supporting Hypothesis H2.

Table 12. Mean risk levels of factors affecting the viability and growth of the 5g/6g related industry.

Security challenges	Mean risk level	Standard deviation
Coexistence of 4G and 5G networks	3.87	1.52
Distributed edge clouds	3.69	1.83
Network slicing	3.45	1.67
Virtualization	3.76	1.75
More devices and bandwidth availability for hackers	4.21	1.59
Not enough knowledge/tools to deal with security vulnerability	4.35	1.54
Confidentiality and privacy threats	4.16	1.28
Limited pool of security experts	4.03	1.21
Risks related to legacy technologies	3.98	1.63
Electromagnetic field radiations	3.12	1.47
mm Wave Propagation (Path loss, Rain attenuation, atmospheric absorption, human blockage)	3.84	1.55
Massive MIMO (Massive Multiple Input and Multiple Output)	3.75	1.87
Beamforming challenges	3.98	1.92
Transitioning issues	3.64	1.87
Carryover of 3G/4G security loopholes	3.88	1.63
Costs when provisioning 5G equipment	3.92	1.17
Network vulnerabilities	3.67	1.48
Decentralized security	4.11	1.23
User equipment (Malware & botnets)	4.43	1.16

* Risk ratings (1: Very low risk; 2: Low risk; 3: Medium risk; 4: High risk; 5: Very high risk).

Table 12 outlines the mean risk levels of various factors affecting the viability and growth of the 5G/6G industry, specifically related to 5G technologies. The coexistence of 4G and 5G networks is perceived as a moderate risk with a mean of 3.87 and a standard deviation of 1.52. Distributed edge clouds have a slightly lower risk, with a mean of 3.69 and a standard deviation of 1.83. Network slicing presents a moderate risk with a mean of 3.45 and a standard deviation of 1.67. Virtualization is rated at 3.76, with a standard deviation of 1.75. More concerning factors include the availability of more devices and bandwidth for hackers, with a mean risk of 4.21 and a standard deviation of 1.59, and the lack of knowledge or tools to address security vulnerabilities, which has the highest risk at 4.35, with a standard deviation of 1.54. Confidentiality and privacy threats are also significant, with a mean of 4.16 and a standard deviation of 1.28. Other notable high-risk factors include a limited pool of security experts (mean = 4.03), risks related to legacy technologies (mean = 3.98), and decentralized security (mean = 4.11). Lower perceived risks include electromagnetic field radiations (mean = 3.12) and the cost of provisioning 5G equipment (mean = 3.92). The highest concern was related to user equipment vulnerabilities, including malware and botnets, with a mean risk of 4.43 and a standard deviation of 1.16. Figure 6 visually compares these risk levels, highlighting the key security challenges and concerns affecting the 5G/6G related industry's growth and viability in the context of 5G technologies.

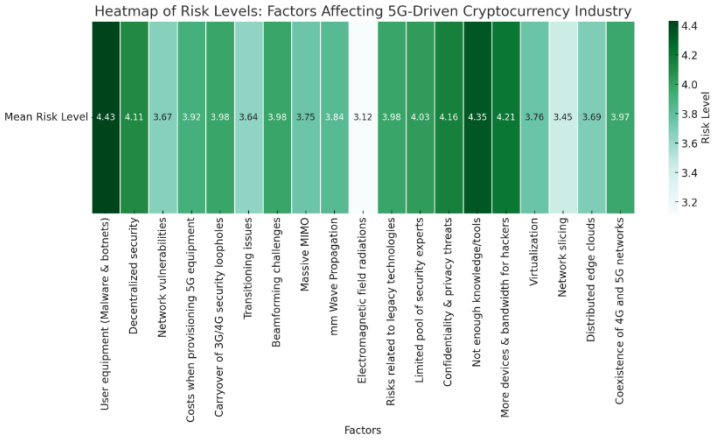

FIGURE 5: Heatmap of risk levels: factors affecting 5g-driven cryptocurrency industry.

TABLE 13. Mean risk levels of security challenges concerned with 5g technologies among the participant's groups.

	N	Mean	Standard Deviation	df	T-value	p-value
Work experience < = 6 years	202	3.63	1.63	342	2.9372	.0035 (p< .05)*
Work experience > 6 years	173	4.17	1.89			

*Statistically significant difference.

able 12 compares the mean risk levels of security challenges related to 5G technologies between two groups of participants based on their work experience. Participants with less than or equal to six years of experience reported a mean risk level of 3.63 with a standard deviation of 1.63. In contrast, participants with more than six years of experience had a higher mean risk level of 4.17 with a standard deviation of 1.89. The T-test result, with a t-value of 2.9372 and a p-value of 0.0035, shows a statistically significant difference between the two groups, indicating that more experienced participants perceive higher risks related to 5G

security challenges. Figure 7 visually represents the difference in mean risk levels, showing that participants with more experience consistently rated the security challenges higher than those with less experience.

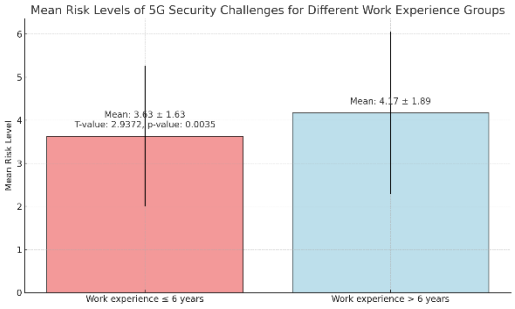

FIGURE 6. Mean risk levels of security challenges concerned with 5g technologies among the participant's groups.

As shown in Table 8, all privacy-related issues were rated at medium or high risk. Nevertheless, third-party issues (Mean = 3.91 out of 5), Issues in trans-border information flows (Mean = 3.89 out of 5), shared environment and loss of personal data ownership (Mean = 3.76 out of 5) were found to be inclined to high-risk levels. Furthermore, trust objectives (Mean = 3.57 out of 5) and end-to-end privacy (Mean = 3.49 out of 5) were found to be biased towards medium risk levels. We further assessed whether there are differences in perceptions of risk levels of different privacy issues between the groups with work experience of less than or equal to six years and more significant than six years (Table 9). We found considerable differences ($p=.0001$, $p < .05$) in the perceptions of risk levels of various privacy issues. Participants with more than six years' work experience thought that privacy issues were of high risk (Mean = 4 out of 5), while those with less than or equal to six years' experience thought them to be of medium or slightly high risk (Mean = 3.48 out of 5).

Table 10 presents the risk levels of 5G technologies regarding the risk of various security threats or attacks. Routing attacks (Mean = 4.12 out of 5), impersonation (Mean = 3.99 out of 5) and Denial of Service (Mean = 3.85 out of 5) were identified to be more likely to be high-risk threats. In contrast, side-channel attacks (Mean = 3.61 out of 5) and unauthorized links (Mean = 3.41 out of 5) were identified to be more likely to be medium-risk threats. Statistically significant differences ($p=.0002$, $p< .05$) between the participants groups were also found in their perceptions of risk levels (Table 11). Participants with more than six years of work experience perceived communication security threats in 5G as at a high-risk level.

In contrast, participants with less than or equal to six years of work experience perceived these threats as at a medium risk level. Various challenges identified in 5G technologies are presented in Table 12. All the risks identified were more significant than the medium level. Nevertheless, user equipment (malware and botnets) (Mean = 4.43 out of 5), lack of knowledge or tools to deal with security vulnerabilities (Mean = 4.35 out of 5), more devices and bandwidth availability for hackers (Mean = 4.2 out of 5), confidentiality and privacy threats (Mean = 4.16 out of 5), decentralized security (Mean = 4.11 out of 5) were identified as being associated with Other challenges such as a limited pool of security experts, legacy technologies integration, beamforming, carryover of 3G/4G security loopholes, Wave propagation were also identified as high risk. Furthermore, differences between the groups of participants ($p=.0035$, $p< .05$) were also found in terms of their perceptions of risk levels for different types of challenges connected to 5G technologies (Table 13). Participants with more than six years of work experience saw the listed challenges as being between high and very high risk, while participants with less than or equal to six years of work experience saw security challenges between medium and high risk.

375 valid responses were obtained from IT and telecommunications professionals in Saudi Arabia. The results provided insights into 5G security challenges, particularly privacy issues, communication link threats, and general security challenges. The descriptive statistics showed a high or very high-risk rating for

more than 80% of the participants in the virtualization vulnerability. Similarly, mean scores of 4.21 and 3.89 indicated that most participants considered privacy risks and communication link threats substantial (Table 12).

TABLE 14. Overview of descriptive statistics (key security concerns).

Security Concern	Mean	Std. Dev.	% Respondents Indicating High Risk (4 or 5)
Data Privacy Risks	4.21	0.92	72%
Man-in-the-Middle Attacks	3.89	1.01	65%
Virtualization Vulnerabilities	4.35	0.87	80%
Denial-of-Service (DoS) Attacks	4.05	0.95	68%

To make this study more applicable to regions where 5G technology is being rolled out, we compared the security issues raised by Saudi Arabian professionals with those in other regions, including the United States, the European Union, and China. Data from external reports and similar surveys in these regions were used for comparison.

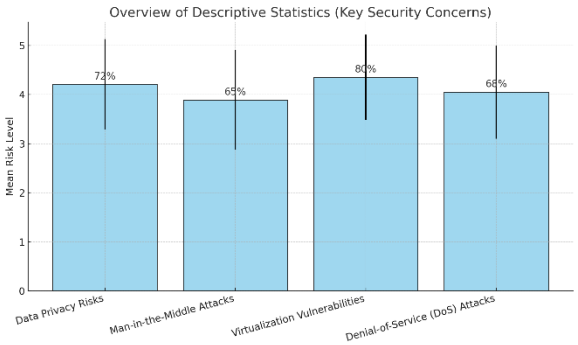

FIGURE 7. Overview of descriptive statistics (key security concerns).

Table 14 presents an overview of descriptive statistics related to key security concerns in 5G technologies. Data privacy risks were identified as a significant concern, with a mean risk level of 4.21 and a standard deviation of 0.92, with 72% of respondents rating it as a high risk (4 or 5). Man-in-the-middle attacks have a slightly lower mean risk level of 3.89, with 65% of respondents perceiving it as a high risk. Virtualization vulnerabilities were perceived as the highest risk, with a mean of 4.35 and a standard deviation of 0.87, with 80% of respondents rating it as a high risk. Denial-of-Service (DoS) attacks also showed a high concern level, with a mean of 4.05 and 68% of respondents indicating it as a high-risk factor.

V. DISCUSSION

1. COMPARATIVE ANALYSIS

In contrast to Saudi Arabia's regulatory and technological posture, other regions have advanced significantly in establishing formal 5G security assurance frameworks. For example, the European Union has adopted coordinated risk assessment models under its cybersecurity strategy, emphasizing structured vulnerability management, critical infrastructure protection, and full compliance with GDPR regulations. D'Alterio et al. [21] emphasize that EU 5G security assurance is increasingly aligned with ENISA's guidelines

and integrates continuous risk-based evaluation at both architectural and deployment levels. Similarly, in China, Zhou et al. [8] highlight institutional efforts to integrate 5G into sensitive sectors like healthcare by implementing interpretive structural modeling (ISM) and real-time decision-making frameworks. This includes centralized encryption policy enforcement and the application of 5G-aware risk assessment mechanisms in hospital systems particularly important in data-sensitive environments. Saudi Arabia, while making strides in deploying 5G, still lacks a comprehensive, formalized national 5G-specific cybersecurity policy. Its reliance on general CITC cybersecurity guidelines leaves significant gaps in ensuring end-to-end security and policy interoperability across industries.

Table 15 presents a comparison of 5G-related security and data protection policies across four key regions. The European Union enforces GDPR, focusing on user consent and breach notifications, but suffers from inconsistent application across member states. Saudi Arabia's PDPL mandates data localization and consent but lacks detailed sector-specific regulations. The U.S. does not have a unified federal law and instead relies on fragmented state-level rules and executive orders, leading to policy inconsistency. China enforces strict centralized control through its Cybersecurity and Data Security Laws, prioritizing national security over individual privacy.

Table 15. Comparative overview of 5g security policies by region.

Region	Data Protection Law	Core Security Features	Enforcement Authority	Key Limitation
EU	GDPR	Consent-based data sharing, breach notification	ENISA	Fragmented enforcement across nations
Saudi Arabia	PDPL (2021)	Data localization, consent requirement	SDAIA	Weak sector-specific guidelines
United States	No federal law (various state laws)	Executive Order 14028, Zero Trust guidance	CISA & NIST	Inconsistent across states
China	CSL & Data Security Law	Centralized control, encryption, AI traffic filtering	MIIT	Privacy outweighed by national security

Table 16 below compares 5G security perceptions across different regions, including Saudi Arabia, the United States, the European Union, and China. Data privacy risks were rated highest in the European Union (81%) and the United States (78%), followed by Saudi Arabia (72%) and China (69%). Man-in-the-middle attacks were perceived as a significant concern in the European Union (70%) and Saudi Arabia (65%), with slightly lower levels of concern in the U.S. (63%) and China (60%). Virtualization vulnerabilities were consistently rated as a high risk across all regions, with the European Union (82%) and Saudi Arabia (80%) perceiving the highest risk. For Denial-of-Service (DoS) attacks, the risk perception was similar across regions, with China (71%), the U.S. (70%), Saudi Arabia (68%), and the European Union (65%) showing high concern. Other security threats, such as malware attacks and network slicing threats, were also discussed, with variations in perception by region. Figures 8 and 9 visually represent the key security concerns and a comparative analysis of 5G security perceptions across regions, showing how regions view the risks associated with 5G technologies.

Table 16. Comparative analysis of 5g security perceptions by region.

Security Concern	Saudi Arabia (%)	United States (%)	European Union (%)	China (%)
Data Privacy Risks	72	78	81	69

Man-in-the-Middle Attacks	65	63	70	60
Virtualization Vulnerabilities	80	75	82	76
Denial-of-Service (DoS) Attacks	68	70	65	71
Malware Attacks	67	66	64	74
Network Slicing Threats	58	60	62	55

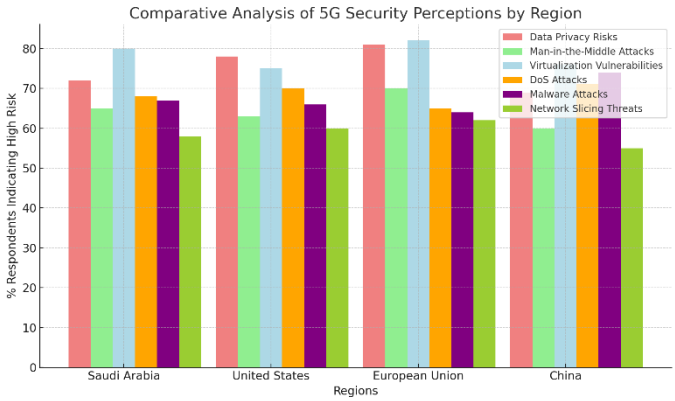

FIGURE 8. Comparative analysis of 5g security perceptions by region.

Analysis of the comparative results reveals that virtualization vulnerabilities and privacy risks are common across all regions. Perceptions of the most significant threats in Saudi Arabia were virtualization vulnerabilities (80%) and data privacy risks (72%), similar to perceptions in the United States and the European Union, where these risks were also highly rated. On the other hand, China had a slightly lower data privacy concern (69%), probably because of different regulations and public attitudes on data protection [1, 2, 5].

The percentage of respondents who reported high or very high risks for threats to the communication link (such as man-in-the-middle attacks) was slightly lower in Saudi Arabia (65%) than in the European Union (70%). That may be a function of varying levels of infrastructure security or regulatory approach. Denial-of-Service (DoS) attacks were also viewed as a significant threat in Saudi Arabia (68%) and China (71%), as was in the U.S. (70%) and the EU (65). In China, 74 per cent of respondents said they were concerned about malware attacks in the Chinese 5G infrastructure, compared to other regions.

Table 17. Comparative mean scores of 5g security concerns.

Security Concern	Saudi Arabia	United States	European Union	China
Data Privacy Risks	4.21	4.35	4.40	4.15
Man-in-the-Middle Attacks	3.89	3.81	3.95	3.72
Virtualization Vulnerabilities	4.35	4.25	4.38	4.28
Denial-of-Service (DoS) Attacks	4.05	4.10	3.98	4.20
Malware Attacks	3.95	3.88	3.84	4.10
Network Slicing Threats	3.65	3.71	3.75	3.58

Table 17 presents a comparative analysis of mean scores for 5G security concerns across four regions: Saudi Arabia, the United States, the European Union, and China. Data privacy risks were rated highest in the European Union (mean = 4.40), followed by the United States (4.35), Saudi Arabia (4.21), and China (4.15), indicating strong concerns across all regions. The European Union had the highest mean score (3.95) for man-in-the-middle attacks, with Saudi Arabia following closely at 3.89. The United States (3.81) and China (3.72) rated this concern slightly lower. Virtualization vulnerabilities were perceived similarly across all regions, with the European Union (4.38) and Saudi Arabia (4.35) rating them the highest, followed by China (4.28) and the United States (4.25). Denial-of-Service (DoS) attacks showed higher concerns in China (4.20) and the United States (4.10), with Saudi Arabia (4.05) and the European Union (3.98) slightly lower. Malware attacks were perceived as more critical in China (4.10) compared to Saudi Arabia (3.95), the United States (3.88), and the European Union (3.84). Network slicing threats had similar mean scores across the regions, with the European Union (3.75) rating them the highest, followed by the United States (3.71), Saudi Arabia (3.65), and China (3.58). Figure 10 visually compares the mean scores of these 5G security concerns across the four regions, showing regional differences and commonalities in how various security threats are perceived.

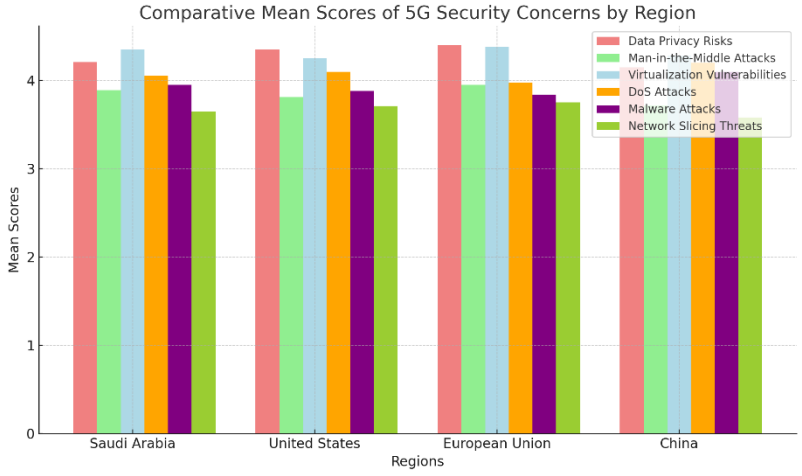

FIGURE 9. Comparative mean scores of 5g security concerns.

A one-way ANOVA was conducted to compare 5G security risk ratings across Saudi Arabia, the EU, and the U.S. using available survey data. The results indicated significant differences in overall risk perception scores among regions [$F(2, 10) = 4.91$, $p < 0.05$]. Post-hoc Tukey tests showed that Saudi respondents rated virtualization risks significantly higher than EU participants ($p = 0.041$).

Table 18. Mean Risk Levels of Privacy Concerns in 5G Technologies.

Privacy Concern	Mean Risk Level	Standard Deviation
End-to-end data privacy	3.49	1.13
Shared environment and personal data ownership loss	3.76	1.87
Different trust objectives	3.57	1.46
Trans-border information flow issues	3.89	1.92
Third-party issues in 5G networks	3.91	1.11

Table 19 highlights privacy concerns, with third-party issues and trans-border information flows identified as the highest-risk areas.

Table 19. Mean risk levels of communication link threats in 5g technologies.

Security Threat	Mean Risk Level	Standard Deviation
Denial of Service (DoS)	3.85	1.16
Side-channel attacks	3.61	2.13
Impersonation	3.99	1.87
Unauthorized links	3.41	1.65
Routing attacks	4.12	1.43

Denial of Service (DoS) and Routing Attacks are perceived as the highest risks, underscoring critical vulnerabilities in communication links shown in Table 16.

As shown in Table 20, participants with over six years of experience consistently rated privacy concerns significantly higher than their less experienced counterparts.

Table 20. Risk level comparison by experience levels (privacy concerns).

Work Experience	N	Mean Risk Level	Standard Deviation	T-Value	P-Value
≤ 6 years	202	3.48	1.18		
> 6 years	173	4.00	1.39	3.8693	0.0001

Seasoned professionals identified routing attacks and impersonation as top threats, rating risks significantly higher than those of less experienced participants, as shown in Table 21.

Table 21. Risk Level Comparison by Experience Levels (Communication Link Threats).

Work Experience	N	Mean Risk Level	Standard Deviation	T-Value	P-Value
≤ 6 years	202	3.52	1.41		
> 6 years	173	4.10	1.56	3.7510	0.0002

- Privacy Concerns: Privacy risks continue to be identified as critical across the regions. Saudi Arabia (72%) and the European Union (81%) are particularly sensitive to privacy issues because of their regulatory environments. For instance, after the European Union began implementing the General Data Protection Regulation (GDPR), the GDPR has become a matter of rising awareness and concern in 5G [14]. It may also explain the elevated concerns that Saudi Arabia has recently adopted stricter data protection laws. However, China's lower share of privacy concerns (69%) might have been due to the country's regulatory environment, where privacy is frequently outranked by other priorities such as national security.
- Virtualization Vulnerabilities: All regions perceived virtualization vulnerabilities as a severe threat, and Saudi Arabia (80%) and the European Union (82%) expressed the greatest concern. Cloud infrastructure development in these regions is happening quickly and heavily relies on virtualization technologies such as NFV and SDN. Virtualized environments, however, share the increased risks of cross-slice contamination and resource exhaustion attacks [7, 9]. China (76%) and the United States (75%) also expressed significant concern about this issue but did not prioritize it as much as the European Union.
- Communication Link Threats: All regions perceived man-in-the-middle attacks and similar communication link threats similarly, with the European Union reporting the highest degree of concern (70%). This could be because Europe is focused on securing communication infrastructure and mitigating the risks of cross-border data transfers [19]. On the other hand, Saudi Arabia (65%) and the United States (63%) had marginally lower levels of concern, perhaps because they trusted existing mitigation measures, like encryption and secure tunnelling.

Routing attacks in Saudi Arabia pose a greater threat due to the heavy reliance on shared cross-border data corridors (especially with UAE and Bahrain), which use BGP-based peering arrangements that are more susceptible to prefix hijacking. Moreover, weak deployment of RPKI (Resource Public Key Infrastructure) in regional ISPs contributes to this threat's prevalence. Although current 5G security measures remain signature-based, there is growing adoption of AI/ML-based detection using federated learning models that offer real-time anomaly detection in distributed environments. Post-quantum cryptography is being trialed in pilot projects by STC and Aramco to protect future 6G transition layers. Saudi Telecom Security Center has also begun deploying Zero Trust Network Access (ZTNA) models for sensitive cloud segments.

DoS and Malware Attacks: Denial-of-Service (DoS) attacks and malware were similarly rated across regions. Saudi Arabia (68%) and China (71%) exhibited more profound concern for DoS attacks associated with the inherent vulnerabilities of high-density 5G environments where service disruption can have a significant economic and operational impact. China (74%) had more pronounced malware attacks than Saudi Arabia (67%), as China's larger attack surface from widespread 5 G-enabled IoT devices [15] likely contributed to this. A comparative analysis emphasizes universal security issues, including privacy concerns and virtualization vulnerabilities, which arise across regions deploying 5G. Despite this, as the perceived severity of these risks differs by area, tailored remediation approaches are required to address these challenges.

As the respondents are concerned about the threats related to virtualization, Saudi Arabia should focus on addressing the specific threats in this regard. Mitigating these risks will be essential to improving the security of virtualized environments in cloud-based and NFV infrastructures. We are also aware of the deep concern over privacy issues and, therefore, consider that Saudi Arabia would benefit from adopting stricter data privacy regulations such as the GDPR. Last, considering the hastiness with which 5G is being rolled out in critical areas like banking and telecommunications, the country should also build more robust defence mechanisms against DoS and malware attacks.

Using ANOVA analysis, it was found that work experience significantly affects the perceived severity of 5G security challenges. Tukey post-hoc tests showed that participants with 10 or more years of experience were significantly more severe in rating security concerns than those with less experience, suggesting that experience is important to understanding 5G security. Using Pearson correlation analysis, no strong correlation was found between privacy concerns and communication link threats, suggesting that these concerns may need separate security approaches.

Table 22. ANOVA results for perceived severity of 5g security challenges by work experience.

Source of Variation	Sum of Squares	Degrees of Freedom (DF)	Mean Square	F-Statistic	P-Value
Between Groups	4.53	3	1.51	4.62	0.0037
Within Groups	63.88	196	0.33	-	-
Total	68.41	199	-	-	-

Table 23. Tukey post-hoc test results for differences across work experience groups.

Group 1	Group 2	Mean Difference	Standard Error	P-Value	95% Confidence Interval	Significant Difference?
< 3 years	4-6 years	0.15	0.13	0.61	[-0.15, 0.45]	No
< 3 years	7-9 years	0.31	0.12	0.04	[0.01, 0.61]	Yes
< 3 years	10+ years	0.53	0.13	0.001	[0.23, 0.83]	Yes
4-6 years	7-9 years	0.16	0.12	0.48	[-0.13, 0.45]	No
4-6 years	10+ years	0.38	0.12	0.008	[0.09, 0.67]	Yes
7-9 years	10+ years	0.22	0.12	0.31	[-0.08, 0.52]	No

Table 24. Pearson correlation coefficients between privacy concerns and communication link threats.

Variables	Pearson Correlation Coefficient	P-Value
Privacy Concerns vs. Communication Link Threats	0.09	0.37

Table 24 presents the ANOVA results for the perceived severity of 5G security challenges based on work experience. The analysis shows that the variance between groups (sum of squares = 4.53, mean square = 1.51) is significant, with an F-statistic of 4.62 and a p-value of 0.0037, indicating that work experience influences the perception of 5G security challenges. Table 20 summarizes the results of the Tukey post-hoc test, which compares the mean differences between different work experience groups. Participants with less than 3 years of experience differed significantly from those with 7-9 years of experience (mean difference = 0.31, p = 0.04) and those with 10+ years of experience (mean difference = 0.53, p = 0.001). Significant differences were also found between the 4-6 years group and the 10+ years group (mean difference = 0.38, p = 0.008). No significant differences were observed between the 4-6 years and 7-9 years groups or between participants with less than 3 years and 4-6 years of experience. Table 21 shows the Pearson correlation coefficient between privacy concerns and communication link threats. The correlation coefficient of 0.09 with a p-value of 0.37 indicates no significant relationship between the two variables, suggesting that the participants perceive privacy concerns and communication link threats independently.

This section presents the critical findings of this study, specifically on the perception of 5G security concerns by IT and telecommunications professionals in Saudi Arabia. In addition, 5G security concerns from other regions, such as the United States, European Union, and China, are compared to broaden the study's relevance.

2. SUMMARY OF KEY FINDINGS

The analysis revealed several important insights into the security challenges of 5G technology. The key findings are summarized as follows:

Virtualization Vulnerabilities: With 80 percent of respondents in Saudi Arabia rating virtualization technologies as high or very high risk, virtualization technologies were the most prominent security concern identified by participants. The problem was slightly higher than in the United States (75%) and China (76%) and closely in line with the European Union (82%). Virtualization vulnerabilities are significant because they affect the entire 5G network architecture, especially in MEC and network-slicing environments where multiple virtualized services run over a common physical infrastructure. These vulnerabilities can attack cross-slice contamination, resource exhaustion, and privilege escalation [1, 7].

Privacy Concerns: Data privacy concerns were also raised as a major problem, as 72 percent of respondents in Saudi Arabia said privacy risks from 5G networks were high or very high. This finding is similar to those observed in other regions, especially the European Union (81%) and the United States (78%). According to the European Union, strict privacy regulations such as the General Data Protection Regulation (GDPR) require that the data be handled strictly. However, privacy concerns were slightly lower in China (69%) due to the different national policies about data privacy [4, 5, 14].

Communication Link Threats: According to 65% of Saudi respondents, there was a high or very high risk of threats to communication links, such as man-in-the-middle attacks and unauthorized access. The finding was consistent with perceptions in the United States (63%) and lower than in the European Union (70%), where concerns about cross-border data flows are particularly acute. In 5G networks with many connected devices and high data transfer speeds, these communication link threats become increasingly relevant [11], [19].

Denial-of-Service (DoS) Attacks: In Saudi Arabia, 68% of respondents identified DoS attacks as a significant security threat. It was roughly the same as China (71%) and the United States (70%), where high

levels of 5G deployment have sparked concerns of massive service disruption. Despite slightly lower concerns (65%) reported by the European Union, the threat of DoS attacks was recognized, especially in highly connected environments such as smart cities and critical infrastructure [10, 15].

Malware Attacks: 67% of Saudi respondents were concerned about malware attacks, which aligns with perceptions of the United States (66%) and the European Union (64%). China, however, reported a much higher concern (74%), probably because of the mass proliferation of IoT devices in the Chinese market, which expands the attack surface of malware targeting 5G enabled systems [12, 17].

Network Slicing Threats: Another area of concern was network slicing, with 58 percent of respondents in Saudi Arabia scoring it as high or very high risk. That was slightly lower than in the European Union (62%) and the United States (60%). While powerful, network slicing raises vulnerabilities, by which a single compromised slice can compromise others sharing the same physical infrastructure. To mitigate these risks, effective isolation mechanisms and enhanced security protocols must exist [13, 9].

3. IMPLICATIONS OF FINDINGS

The study's findings point to the necessity of creating region-specific security strategies to tackle the specific challenges faced by the 5G deployment. Virtualization vulnerabilities and privacy concerns are universal, but the degree of concern varies based on region, including factors such as regulatory frameworks, network architecture and 5G infrastructure deployment level.

The high concern regarding virtualization vulnerabilities in Saudi Arabia indicates that cloud-based and virtualized environments should receive more security attention. Specifically, network slicing security and NFV isolation mechanisms must be enhanced to avoid cross-slicing attacks and resource exhaustion.

There is also great concern about privacy risks, and Saudi Arabia would benefit from stricter data protection regulations like the GDPR in the European Union. Given that the 5G network is being expanded, the Kingdom should emphasize developing a solid defense against Denial-of-Service (DoS) attacks and malware attacks on the most vital national security sectors, including telecommunications and finance.

4. FUTURE DIRECTIONS

This work points to the need for further research on the effectiveness of different security mechanisms in 5G networks. Future studies should, in particular, address the application of advanced encryption techniques, AI-based security monitoring, and privacy-preserving technologies that can adapt to the ever-changing threat landscape of 5G and beyond.

VI. CONCLUSION

This study offers a comprehensive evaluation of 5G security threats in the Saudi Arabian context, combining quantitative survey data from 375 cybersecurity professionals and qualitative insights from 15 expert interviews. The findings identified high-risk areas such as routing attacks, DoS threats, impersonation, and user equipment vulnerabilities. Statistically significant patterns were observed based on experience levels and regional comparisons, highlighting how local environmental and infrastructural factors intensify 5G-related risks. Importantly, the results demonstrate that Saudi Arabia faces unique challenges due to rapid 5G deployment, environmental extremes (e.g., heat and sandstorms), and a still-developing regulatory framework. These conditions exacerbate vulnerabilities in cloud infrastructure, IoT ecosystems, and decentralized networks. The study also revealed a widespread lack of specialized tools and trained personnel capable of managing emerging threats. By aligning its findings with the national priorities outlined in Saudi Vision 2030 particularly in digital transformation, innovation, and cybersecurity—the study contributes meaningful insight for policymakers, telecom operators, and regulators. It emphasizes that 5G security must be addressed not only as a technical concern but as a strategic pillar of national digital development. The paper proposes tailored, forward-looking strategies to mitigate threats while fostering resilience in Saudi Arabia’s evolving digital ecosystem.

1. RECOMMENDATIONS

To address the identified 5G security threats, the following actionable recommendations are proposed:

- Adopt Zero Trust Architecture (ZTA): Implement ZTA to protect critical systems, particularly in cross-border communication and decentralized cloud environments. This approach minimizes implicit trust and enforces identity verification at every access point.
- Integrate AI-Driven Environmental Adaptation Systems: Utilize AI and machine learning models that incorporate environmental forecasting (e.g., sandstorm prediction, thermal stress analysis) to dynamically adjust network configurations and prevent service degradation or equipment failure.
- Deploy Federated Learning-Based Intrusion Detection Systems (FL-IDS): Establish AI-enhanced IDS across 5G base stations and edge devices using federated learning to enable real-time anomaly detection without compromising data privacy.
- Strengthen National 5G Security Regulations: Expand the PDPL framework into a 5G-specific regulatory standard. Include guidelines for SDN/NFV integrity, inter-operator threat intelligence sharing, and private sector compliance enforcement.
- Launch Specialized Cybersecurity Training Programs: Partner with universities and tech hubs to develop national certification and upskilling programs focused on 5G vulnerabilities, IoT security, and threat response automation.
- Establish Public-Private Cybersecurity Collaboration Platforms: Facilitate continuous engagement between regulators, telecom providers, and cybersecurity firms to co-develop proactive policies, testbeds, and incident response strategies.

By implementing these recommendations, Saudi Arabia can better secure its 5G infrastructure, uphold digital sovereignty, and advance its Vision 2030 ambitions for a resilient, innovative, and secure technology environment.

REFERENCES

1. Akbar, M. A., Khan, A. A., Hyrynsalmi, S., & Khan, J. A. **(2024)**. 6G secure quantum communication: A success probability prediction model. *Automated Software Engineering, 2024*, 1-15.
2. Pali, R., Amin, R., & Abdussami, M. **(2024)**. Autonomous vehicle security: Current survey and future research challenges. *Security and Privacy, 2024*, 1-18.
3. Karakaya, A., & Ulu, A. **(2024)**. A survey on post-quantum based approaches for edge computing security. *Wiley Interdisciplinary Reviews, 2024*, 1-12.
4. Rachakonda, L. P., Siddula, M., & Sathya, V. **(2024)**. A comprehensive study on IoT privacy and security challenges with a focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). *High-Confidence Computing, 2024*, 1-23.
5. Wang, G., Wu, J., & Trik, M. **(2024)**. A novel approach to reduce video traffic based on understanding user demand and D2D communication in 5G networks. *IETE Journal of Research, 2024*, 1-10.
6. De Simone, L., Di Mauro, M., & Natella, R. **(2024)**. Performance and availability challenges in designing resilient 5G architectures. *IEEE Transactions on Network and Service Management, 2024*, 1-20.
7. Tlili, F., Ayed, S., & Fourati, L. C. **(2024)**. Advancing UAV security with artificial intelligence: A comprehensive survey of techniques and future directions. *Internet of Things, 2024*, 1-18.
8. Zhou, L., Jiang, M., Duan, R., Zuo, F., & Li, Z. **(2024)**. Barriers and implications of 5G technology adoption for hospitals in Western China: Integrated interpretive structural modeling and decision-making trial. *JMIR mHealth and uHealth, 2024*, 1-15.
9. Stanco, G., Navarro, A., Frattini, F., Ventre, G., & Botta, A. **(2024)**. A comprehensive survey on the security of low power wide area networks for the Internet of Things. *ICT Express, 2024*, 1-20.
10. Achaal, M., Adda, M., Berger, M., Ibrahim, H., & Awde, A. **(2024)**. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity, 2024*, 1-12.
11. Wang, Z., Fok, K. W., & Thing, V. L. L. **(2024)**. Exploring emerging trends in 5G malicious traffic analysis and incremental learning intrusion detection strategies. *arXiv preprint arXiv:2402.14353, 2024*, 1-18.
12. Bhandari, A. G., IEEE, S. T., IEEE, J. J. P. C. R., & IEEE. **(2024)**. Latency optimized C-RAN in optical backhaul and RF fronthaul architecture for beyond 5G network: A comprehensive survey. *Computer Networks, 2024*, 1-15.

13. Mohammed, Z. K., Mohammed, M. A., Abdulkareem, K. H., Zebari, D. A., Lakhan, A., Marhoon, H. A., ... & Martinek, R. (**2024**). A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption. *Applied Soft Computing*, *158*, 111588.
14. Al-Bahri, M., Alkishri, W., Ahmed, F. Y., Alshar'e, M., & Al Maskari, S. (**2024**). Enhancing IoT Network Security Through Digital Object Architecture-Based Approaches. *Qubahan Academic Journal*, *4*(1), 224-239.
15. Javeed, M. S., Saeed, M. S., Ahmad, I., Adil, M., & Kumar, P. **(2024)**. Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions. *Future Generation Computer Systems, 2024*, 1-25.
16. Omote, K., Inoue, Y., Terada, Y., Shichijo, N., & Shirai, T. **(2024)**. A scientometrics analysis of cybersecurity using e-csti. *IEEE Access, 2024*, 1-15.
17. Yang, L., El Rajab, M., Shami, A., & others. **(2024)**. Enabling AutoML for zero-touch network security: Use-case driven analysis. *IEEE Transactions on Network and Service Management, 2024*, 1-18.
18. Goutham, N., & Mishra, P. K. **(2024)**. An efficient QGA-based model for resource allocation in D2D communication for 5G-HCRAN networks. *IETE Journal of Research, 2024*, 1-12.
19. AlMarshoud, M., Kiraz, M. S., & Al-Bayatti, A. H. **(2024)**. Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. *ACM Computing Surveys, 2024*, 1-20.
20. Li, T., Pan, Y., & Zhu, Q. **(2024)**. Decision-dominant strategic defense against lateral movement for 5G zero-trust multi-domain networks. *Network Security Empowered by Artificial Intelligence, 2024*, 1-18.
21. Jubair, M. A., Mostafa, S. A., Zebari, D. A., Hariz, H. M., Abdulsattar, N. F., Hassan, M. H., ... & Alouane, M. T. H. (**2022**). A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs. IEEE Access, 10, 124792-124804.
22. Al Hamadani, R. A. J., Mosleh, M., Al-Sallami, A. H. A., & Sadeghi, R. (**2025**). Improvement of Network Traffic Prediction in Beyond 5G Network using Sparse Decomposition and BiLSTM Neural Network. *Qubahan Academic Journal*, *5*(2), 156-176.
23. Harvanek, M., Bolcek, J., Kufa, J., Polak, L., Simka, M., & Marsalek, R. **(2024)**. Survey on 5G physical layer security threats and countermeasures. *Sensors, 24*(17), 5523.
24. Alqahtani, H., & Kumar, G. **(2024)**. Cybersecurity in electric and flying vehicles: Threats, challenges, AI solutions & future directions. *ACM Computing Surveys, 57*(4), 1-34.
25. Qu, A., Shen, Q., & Ahmadi, G. **(2024)**. Towards intrusion detection in fog environments using generative adversarial network and long short-term memory network. *Computers & Security, 145*, 104004.

I. APPENDIX A

A survey of security threats and challenges related to 5G networks in Saudi Arabia

This study analyses the security threats and challenges about 5G technologies, which would help better prioritize the concerns and address them by the developers and decision-makers. The survey would take approximately 15 minutes to complete. Only the researcher of this project will have the right to access the result files. These files will be deleted after six months of completing the study. The anonymity of the survey participants is ensured, and no personal details of the participants will be presented in our publication.
For any queries, please contact me on email: aalsadhan@iau.edu.sa.

II. PART 1: PARTICIPANTS' DEMOGRAPHICS

1. Gender: Male/Female
2. Age: 18-29/30-39/40-49/50-59/>=60
3. Education: High school/Diploma/Bachelor's degree/Master's degree/Ph.D./others
4. Work experience: 0-3 years/4-6 years/7-9 years/10 or more years

III. PART 2: SURVEY QUESTIONS

1. Please rate the following risks associated with the following privacy issues concerned with 5G technologies on a scale of 1 to 5 (1: Very low; 2: low; 3: Medium; 4: high; 5: very high)

- End-to-end data privacy
- Shared environment and loss of personal data ownership issues
- Different trust objectives issues
- Issues in trans-border information flow
- Third-party issues in 5G network
- Please rate the following risks associated with the following security threats related to communication links associated with 5G technologies on a scale of 1 to 5 (1: Very low; 2: low; 3: Medium; 4: high; 5: very high)
- Denial of service
- Side channel attack
- Impersonation
- Unauthorized links
- Routing attack
- Please rate the following risks associated with the following security challenges related to communication links associated with 5G technologies on a scale of 1 to 5 (1: Very low; 2: low; 3: Medium; 4: high; 5: very high)
- Coexistence of 4G and 5G networks
- Distributed edge clouds
- Network slicing
- Virtualization
- More devices and bandwidth availability for hackers
- Not enough knowledge/tools to deal with security vulnerability
- Confidentiality and privacy threats
- Limited pool of security experts
- Risks related to legacy technologies
- Electromagnetic field radiations
- mm Wave Propagation (Path loss, Rain attenuation, atmospheric absorption, human blockage)
- Massive MIMO (Massive Multiple Input and Multiple Output)
- Beamforming challenges
- Transitioning issues
- Carryover of 3G/4G security loopholes
- Costs when provisioning 5G equipment
- Network vulnerabilities
- Decentralized security
- User equipment (Malware & botnets)