Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 11 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i11.54519

PAPER

Securing 5G Networks by Mitigating Cybersecurity Risks for Transformative Applications

Menachem Domb[1], Balaji C.G.[2] (✉), Menaka S.[3], Gayathri A.[4], Sujata Joshi[2]

[1]Computer Science Department, Ashkelon Academic College, Ashkelon, Israel

[2]Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, Maharashtra, India

[3]SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India

[4]Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, Tamil Nadu, India

cgbalaji@sidtm.edu.in

ABSTRACT

The increasing adoption of 5th generation (5G) networks introduces significant cybersecurity challenges due to the expansion of the attack surface, driven by network slicing, edge computing, and a massive number of connected devices. These challenges demand robust access control mechanisms to mitigate potential risks while maintaining network efficiency. This study presents the Secure 5G Access Control (S5GAC) protocol, a comprehensive security framework designed to enhance user and device authentication through multi-factor authentication (MFA), contextual access control, and continuous monitoring. Unlike existing security models, S5GAC incorporates dynamic risk assessment, leveraging network traffic anomalies, user activity deviations, and device behavior irregularities to enforce adaptive access control measures. Comparative analysis demonstrates that S5GAC achieves a significant reduction in data exfiltration risks, substantial mitigation of cross-slice breaches, and notable improvement in threat detection, all while imposing only a minor latency overhead and a slight throughput reduction. Additionally, the MFA implementation in S5GAC achieves a high authentication success rate, reinforcing its effectiveness in securing high-density 5G environments. Future research will focus on AI-driven threat detection, federated learning-based security, and blockchain-integrated identity management to enhance scalability and resilience in ultra-dense 5G deployments. The proposed S5GAC protocol serves as a future-ready security solution, ensuring robust protection against cyber threats while maintaining optimal network performance.

KEYWORDS

5th generation (5G) security, secure access control, network slicing, AI-driven security, multi-factor authentication (MFA), cyber threat mitigation

1 INTRODUCTION

The improvements and the development of cellular networks, in conjunction with their rapid expansion, are amplifying opportunities for digital transformation. The 5th generation (5G) communication networks are poised as a last twist in this development. The past decade saw notable investment from both the government

Domb, M., Balaji, C.G., Menaka, S., Gayathri, A., Joshi, S. (2025). Securing 5G Networks by Mitigating Cybersecurity Risks for Transformative Applications. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(11), pp. 227–255. https://doi.org/10.3991/ijim.v19i11.54519

Article submitted 2025-01-20. Revision uploaded 2025-04-05. Final acceptance 2025-04-07.

and technology leaders to develop 5G mobile networks. The year 2015 saw the International Telecommunications Union (ITU) come up with the 5G criteria termed the IMT-2020 [1], thereby igniting the global competition for the commercialization of the technology. In 2019, the first 5G networks were introduced in the countries of South Korea, the US, and China [2], and by 2022, more than 200 networks in over 70 countries had come online. The total number of 5G connections exceeded 1.5 billion by 2023 and will reach more than 2.5 billion in 2025 [3], which is almost 50 percent of total mobile subscriptions. Also, 5G Advanced is expected to be launched in the fourth quarter of 2025. Unlike previous generations, 5G creates a new type of software-defined network architecture, opening opportunities for multifaceted implementations in smart cities, self-driving cars, and telemedicine.

Key characteristics that set 5G apart from the previous ones and new ones are discussed here. Against all previous networks, Enhanced Mobile Broadband (eMBB) which offers a somewhat typical speed of ten gigabits per second (10Gbps) in most deployments [4, 5], provides streaming and gaming-focused experiences, as advanced in cloud-based and augmented/virtual reality services. The Ultra-Reliable Low-Latency Communications (URLLC) assume an almost instantaneous response time, and the round-trip time between the communication endpoints is less than 1 millisecond, hence they adequately represent applications that are in real-time such as remote surgical operations, and civil aviation automated vehicles [6, 7]. Massive Machine-Type Communications (mMTC) make it possible to connect one million IoT devices on one square kilometer in 5G networks [8, 9], making it possible to develop extensive IoT ecosystems in smart cities and precision farming. Network slicing [10] refers to the concept of dividing a physical network into virtual sub-networks tailored for specific applications. Edge computing [11] is the technological solution that brings services closer to the edge, and as a consequence, the latency is minimized and the processing of real time data is optimized. Furthermore, it is also worth mentioning that the 5G architecture also applies network functions virtualization (NFV) [12] and software-defined networking (SDN) [13], which brings in the flexibility and cost-effectiveness of the networking. Device-to-device (D2D) communication is a growing research area in 5G networks where the security of the devices is at severe risk as the user equipment nearby can directly communicate with each other without the help of the central authority or evolved Node-B (eNB). The authors in [14] explore D2D communication in 5G networks to reduce eNB traffic, extend coverage, and support out-of-coverage devices using Proximity Service (ProSe) with effective relay selection.

The rapid advancement and widespread adoption of 5G technology indicate a future filled with potential opportunities. Nonetheless, this transformative shift introduces significant cybersecurity challenges. This work investigates the principal risks and mitigation strategies relevant to 5G, with a focus on the expanded attack surface resulting from network slicing and edge computing. It also examines vulnerabilities in network components and supply chains, as well as strategies for secure device management. The analysis underscores the security enhancements in 5G, including advancements in architecture, protocols, and identity management.

Unlike existing frameworks, the Secure 5G Access Control (S5GAC) integrates multi-factor authentication (MFA), contextual access controls, and continuous monitoring to dynamically mitigate cyber threats in real-time. This study aims to bridge the gap by offering a novel security framework that enhances authentication and access control mechanisms while ensuring scalability in high-density 5G environments. The remainder of this paper is structured as follows:

- Section 2 provides a detailed review of related work, focusing on existing security measures in 5G networks.
- Section 3 introduces the proposed S5GAC protocol, describing its core components and functionalities.
- Section 4 presents a comparative analysis of S5GAC with existing protocols, highlighting its advantages and performance trade-offs.
- Section 5 discusses scalability challenges and security trade-offs in high-density 5G environments.
- Section 6 concludes the paper by summarizing key findings and contributions. It outlines future research directions, emphasizing AI-driven security enhancements and quantum-secure algorithms.

2 RELATED WORK

5G is rolling out rapidly across the globe, and its cybersecurity challenges demand urgent attention. While technology has advanced, 5G introduces new security measures to counter risks from an expanding network and an increase in potential attack points. These built-in features work to protect essential resources and critical infrastructure. The high speed [15], low latency [16], and high-volume connection [17] capacity that define 5G make it possible to develop new use cases in different areas.

Automated cars [18] depend on 5G's instantaneous communication capabilities to interact with other cars and manage traffic more effectively in what is expected to change the way people move, enhance safety, and reduce negative effects on the environment [19]. 5G includes remote monitoring of patients, placing video calls, and even performing surgeries from a distance [20], which is particularly advantageous to people who reside in the countryside. Nonetheless, such developments call for the proper implementation of data protection and ethical norms [21]. 5G provides the technological base for smart factories of the Industry 4.0 concept, which supports increased efficiency and flexibility of manufacturing industries through technological and process monitoring [22]. The intelligent transportation systems [23], environmental, and public safety aspects with supporting 5G networks are also implemented by such smart cities, allowing for a multitude of interconnected systems capable of real time analysis of many datasets [24]. This promotes urban sustainability by tackling the environmental, economic, and social problems associated with it [25].

Cybersecurity is still an issue that cannot be ignored as the use of 5G with critical facets progresses. Some of the investigations have offered solutions such as adjustable multi-layered structures to meet the growing needs, although addressing real time aggressor threat and more effective applications of security in existing infrastructural frameworks is still needed [26]. Machine learning through support vector machine (SVM) models has been able to prevent infiltrations and cyber-attacks to some extent in the 5G facilitated networks, but continued improvement is necessary for the network changes [27]. In logistics too, there is a requirement to embed the security solutions with big data, cloud computing and IOT when connecting all the entities, but there are no general provisions for this, meaning that universal security frameworks are required [28]. It is promising that there is research on security key performance indicators (KPIs) for 5G network slices advocating for different subscriber classes. The challenge still lies in the creation of flexible KPIs for specific

circumstances [29]. It is emphasized in the study of 5G security through the eyes of an operator that it is indeed necessary for the operators to work together to achieve the same level of security procedures [30]. The authors in [31] explore AI-driven cybersecurity analytics, focusing on real time threat detection, data collection, and predictive modeling to enhance security and mitigate risks. While AI-driven threat detection is gaining traction, its integration into 5G security frameworks is still in its infancy. There is a need for more research on how AI can be effectively utilized to detect and mitigate sophisticated cyber threats in 5G networks. The research incorporates AI-driven threat detection mechanisms into the S5GAC protocol. By leveraging AI, the protocol can identify and respond to anomalous behavior and sophisticated attacks more effectively, enhancing the overall security of 5G networks.

Legal frameworks must also evolve to address cybercrime in the 5G era. Currently, there are no updated regulatory frameworks that are intended to deal with cybercrime in the era of 5G technology, as few provisions for existing laws are inconsistent with rapid advancements in technology [32]. There is also higher QoS and security that has to be achieved, and therefore frameworks developed also have to consider practical issues of implementation [33]. Although it is postulated that artificial intelligence will improve the management and security of 5G, existing models of artificial intelligence are still too simplistic to resolve problems inherent in 5G [34]. In Eastern Europe, notable steps have been made to harmonize the European Union (EU) guidelines with the country's 5G implementation plans, but there are still problems with the means of support for the deployment [35]. Therefore, while security at the physical layer seems to be feasible in implementation on 5G networks, there is a need to make a convergence of the network layers to ensure a full layer of protection [36]. Cybersecurity insurance is a type of coverage designed to help businesses and individuals manage the financial risks associated with cyber incidents such as data breaches, cyberattacks, and other cyber-related events. Research [37] develops AI-driven defenses, leveraging blockchain and Big Data for threat detection and enhanced cybersecurity.

The deployment of 5G networks has revolutionized various domains, including autonomous vehicles, healthcare, smart cities, and Industry 4.0. However, the expanded attack surface and increased complexity of 5G architectures have introduced significant cybersecurity challenges. This section reviews existing literature on 5G security, focusing on the research gaps identified earlier, and highlights how the proposed S5GAC protocol addresses these gaps.

The introduction of 5G networks has significantly increased the attack surface due to features like network slicing, edge computing, and the massive number of connected devices. Zhang et al. [38] discussed the vulnerabilities introduced by network slicing, emphasizing the risk of Distributed Denial of Service (DDoS) attacks targeting specific slices. The experts suggested implementing several security layers against risks yet emphasized the necessity of automatic protective measures responding to current-time threats. The research paper [39] introduced the Slice Specific Authentication and Access Control (SSAAC) mechanism built on virtualization technologies to delegate IoT device authentication and access control functions, thus reducing network traffic while improving 5G network flexibility and modularity. The S5GAC protocol closes this gap through MFA, context-based access control, and continuous system monitoring that ensures strong protection from unauthorized entry and cyberattacks. The authors of [40] presented a decentralized intrusion detection system that trains predictive models efficiently across diverse computing environments for 5G mobile networks' security needs. 5G networks enable the enhancement of quality of service and user experience for multiple IoT applications

such as smart transportation as well as healthcare and augmented reality systems. However, the surge in data generation necessitates intelligent analytics and robust security mechanisms. The current techniques cannot satisfy 5G requirements regarding low latency and high bandwidth demands. Deep learning (DL) and blockchain technology function together to address security problems and intelligent data processing because of their ability to resolve present challenges. The authors of [41] put forth a hierarchical model that uses DL and blockchain elements from user-to-edge and fog-to-cloud frameworks to enhance latency, accuracy, and security performance. The research findings show substantial progress, which proves that adaptive security designs are essential for IoT systems operating under 5G technology. The S5GAC protocol solves these problems by implementing a security risk assessment framework that keeps monitoring the network safety position in real time. This framework's real-time threat adaptation features produce essential cybersecurity measures suitable for 5G high-speed, high-density operational settings.

Data encryption techniques enable different telecommunications services such as web browsing, VPNs, VoIP, and instant messaging through the prevalent use of asymmetric cryptography. New computing technologies, especially quantum computing, apply direct threats to traditional cryptographic methods. The prevailing security problems of wide-scale 5G adoption demand new security solutions. Quantum Key Distribution (QKD) builds a promising response through quantum physics to produce secure cryptographic keys that cannot be detected during transmission. Researchers have analyzed QKD integration with 5G security structures by investigating its compatibility with VPNs and FPGA-based encryption systems [42]. Post-quantum cryptography serves as one approach to investigate new encryption techniques that counter future security threats. Demonstrated implementations of quantum-secured 5G networks underscore the need for further research in this domain. Security and privacy are critical in 5G-enabled vehicular networks due to open-channel communications. Existing authentication schemes often rely on resource-intensive operations and RSU-aided frameworks, making them vulnerable to quantum attacks. The authors [43] explore lattice-based quantum-resistant techniques, replacing bilinear pair and elliptic curve cryptography with matrix multiplication for efficient signature verification. These approaches enhance security while reducing computational overhead and eliminating RSU dependency. Security analyses demonstrate resilience against quantum threats and improved performance over conventional methods. Such lightweight, quantum-resistant schemes are essential for securing 5G-enabled vehicular networks against emerging cybersecurity challenges. The proposed S5GAC protocol bridges this gap by exploring the integration of quantum-secure algorithms into its framework. This forward-looking approach ensures that the proposed security measures remain robust even in the face of future quantum computing threats.

Smart grids, as critical cyber-physical systems, are increasingly targeted by false data injection attacks (FDIAs). While FDIA detection has gained attention, privacy preservation remains underexplored. Recent research integrates federated learning with DL models, such as Transformers, to enhance FDIA detection while ensuring data privacy. By leveraging multi-head self-attention mechanisms [44], these approaches extract correlations among electrical quantities, while federated learning enables collaborative model training without sharing raw data. Additionally, security enhancements using cryptographic techniques, such as the Paillier cryptosystem, further protect federated learning frameworks. Experimental evaluations on IEEE test systems validate the effectiveness and superiority of these methods. As countries begin to embrace 5G, it is predicted that the network will support all manner of mission-critical systems indispensable for the prosperity of economies,

safety of communities, and health and well-being of populations. Consequently, it is of great significance to guarantee that the 5G-enabled infrastructure is dependable, secure, and resistant to any disruptive activities.

The fundamental prerequisite for 5G networks is to guarantee complete safety and operational reliability because these systems function as critical infrastructure for important applications. The protection of modern cyber threats demands persistent research on security systems that adapt to threats as well as quantum encryption capabilities combined with artificial intelligence systems that recognize dangers. S5GAC functions as an advanced protective system that combines multi-factor access controls with network monitoring capabilities to guard 5G network systems against existing security vulnerabilities. The adoption of 5G technology holds multiple beneficial elements, but it also generated various security threats that raise privacy questions in addition to privacy concerns. Table 1 demonstrates different industries that use 5G networks and their specific strengths as well as the security risks that threaten their operations. Organizations require the secure security protocol S5GAC to effectively combat these security threats because of its proven efficiency.

From Table 1, it is evident that both performance gains and operational efficiency boosts from 5G remain in direct conflict with the novel security problems that arise with its implementation. Organizations operating in healthcare, together with autonomous vehicles and smart grids, encounter increased security challenges because of cyber threats, which result in data breaches and system disruptions along with unauthorized access disruptions. Pursuing an S5GAC protocol development focuses on overcoming security concerns through multiple authentication methods and context-aware control measures and continuous threat alert monitoring to protect diverse 5G system applications.

Table 1. Comparative analysis of different industries utilizing 5G

Industry Used	Advantages	Risks Faced
Autonomous Vehicles	Real-time communication, improved traffic management, enhanced safety	Susceptibility to cyber-attacks, GPS spoofing, data privacy concerns
Healthcare	Remote patient monitoring, AI-assisted diagnosis, telemedicine	Data breaches, unauthorized access to medical records, privacy issues
Smart Cities	Real-time data analytics, efficient resource management, enhanced public safety	Surveillance concerns, data interception, infrastructure vulnerabilities
Industry 4.0	Increased automation, predictive maintenance, process optimization	Industrial espionage, cyber threats to connected devices, operational disruptions
IoT and Logistics	Efficient supply chain management, real-time tracking, reduced costs	Security vulnerabilities in connected devices, network congestion, data manipulation
Financial Sector	Secure transactions, AI-driven fraud detection, real-time analytics	Phishing attacks, identity theft, vulnerabilities in encryption mechanisms
Smart Grids	Efficient energy distribution, fault detection, reduced operational costs	False data injection attacks, grid hacking, unauthorized data access
5G-Enabled Networks	High-speed, low-latency communication, enhanced connectivity	Expanded attack surface, vulnerabilities in network slicing, DDoS attacks

3 METHODOLOGY

This section discusses the significant security improvements that have been noted in 5G systems, ranging from the development of mechanisms and protocols, and new security features in 5G such as network slicing and encryption, to better identity and access management. In this respect, this section also addresses what appears to be a gap in literature incorporating a unique algorithm called S5GAC to improve user and device authentication in the 5G network.

The 5G technology marks a major advancement in security architecture and protocols, given the new challenges that are encountered. A key form of security in 5G's Nucleus Core is 'security slicing,' which provides for different security policies to be implemented on particular slices of the network as per 5G's network slicing capability. The security architecture of 5G includes mechanisms such as enhanced Authentication and Key Agreement (AKA) protocol [45] that protects against replay attacks, Subscription Permanent Identifier (SUPI) [46] that protects the identity of the user, and Security Edge Protection Proxy (SEPP) [47] that handles signaling traffic. In addition, Service-Based Architecture (SBA) Security [48] and quantum-resistant algorithms [49] further add to the security.

Network Slicing for 5G allows the slicing of available underlay network resources to design several tailored virtual networks, each one with its own set of controls regarding security, access policies, and security functions. These partitions reduce the damage scope of breaches and quicken the process of implementing countermeasures. Encryption that reaches 128- or 256-bit degrees, such as the AES algorithm [50], is used to encrypt the user data while policies that query user identity are enforced to keep users private. Additionally, 5G technology provides a better way of managing identity and access controls by improving authentication methods, using privacy-friendly SUPIs, and providing dynamic access controls. Such developments are geared towards ensuring a secure and adaptable network environment. Unfortunately, the deployment of 5G comes with new cybersecurity issues such as extending the attack surface area through network slicing and edge computing, the introduction of weaknesses in the network component and supply chain, and large-scale attacks and data theft.

These, however, need to be addressed through multiple discipline participation, that is, industry, government, and academia collaborating. Over the past years, however, governments and regulatory bodies have begun to take a second look at policies regarding cybersecurity as they have considered 5G networks as critical infrastructure. Efforts such as the "Clean Network" program of the U.S. [51] and the "5G Toolbox" [52] of the EU show combined plans to achieve the establishment of global standards and best practices for the security, safety, and resilience of 5G networks. While effective implementation of measures to safeguard 5G networks, all stakeholders, including governments, telecommunications providers, and technology vendors, should play their roles. As Internet users rapidly grow, the demand for bandwidth, speed, and frequencies rises. 5G's key features, such as spectral efficiency and coverage capacity, were reviewed by [53], and the combining of microcells, joint transmission with coordinated multipoint, and massive MIMO for its improvement were discussed. The development and operationalization of a unified cybersecurity strategy aimed at addressing the specific threats associated with 5G technologies demands joint risk evaluations, constant communication, and threat intelligence sharing.

Figure 1 present the S5GAC protocol, which augments different aspects of the 5G infrastructure security and mitigates the problems related to diverse mobile devices and users that are expected to connect through 5G networks. The proposed security protocol creates its distinctiveness through the combination of multi-factor identity authentication, with contextual real-time access control and dynamic protection policies. S5GAC operates through dynamic risk assessment that regularly examines the combination of user actions alongside device integrity ratings and environmental factors including; current position, current time, and network performance.

The S5GAC protocol creates 5G network security through continuous access request oversight with automated security adaptations. Users start the authentication process after identity verification to obtain access through password-based and biometric measures and digital certificate authentication.

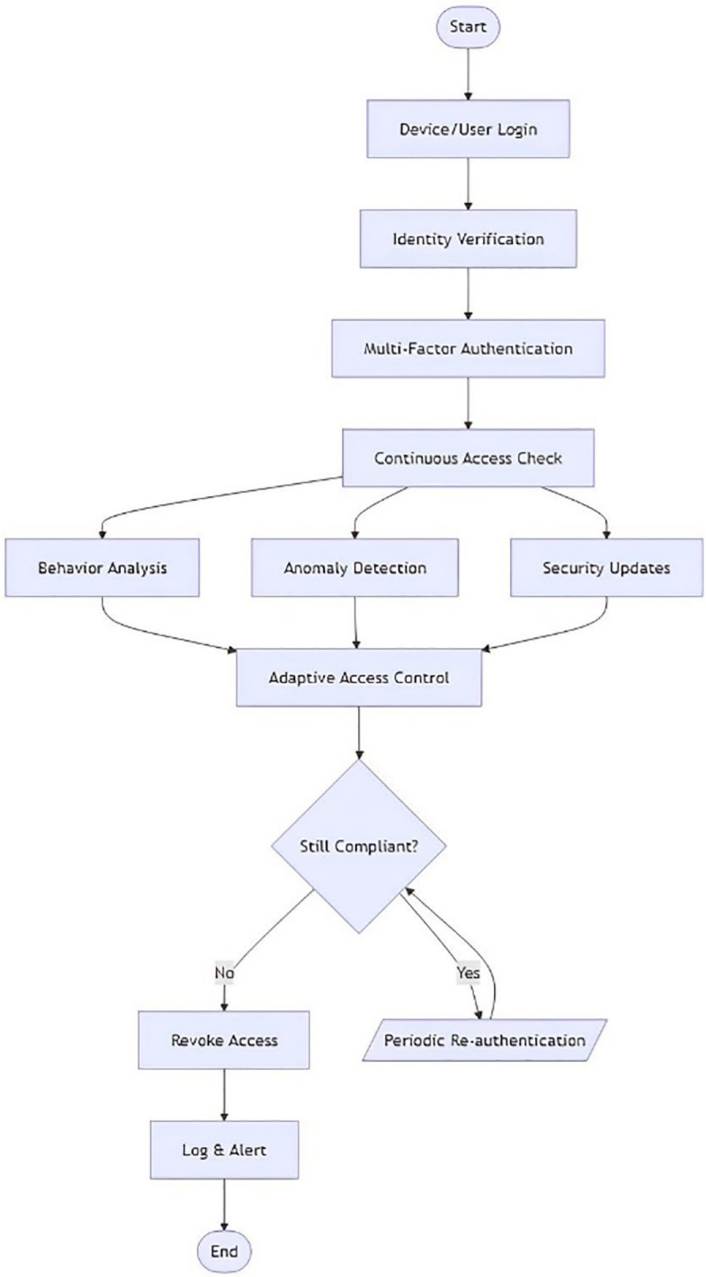


Fig. 1. S5GAC protocol

The security system depends on MFA to establish access requirements which proceed through multiple protection checks. Systems under authentication perform continuous checks of accessed sessions which blend behavioral monitoring with network operations scanning and equipment integrity evaluation. Behavior analysis provides input for the risk assessment as it executes anomaly detection principles while performing security update procedures. User behavior analysis reveals irregular activities through detection of both strange login patterns and large-file transfer actions and other atypical behaviors. Security compliance of the devices becomes achievable by conducting routine security updates that maintain the latest security patches and policies.

The security framework uses adaptive permissions which update automatically depending on changing risk situations. Users, who stay compliant with security policies, need to undergo periodic re-authentication before their access will continue. The system closes down user access right away when it spots non-compliance either through malware or unauthorized access actions or indicative suspicious system behavior. Security administrators can use generated log and alert data for instant threat response and investigation purposes. S5GAC achieves minimal security threats and continued user efficiency through its combination of AI-based threat detection systems and continuous monitoring functionalities. The security framework adopts a zero-trust architecture because it does not automatically trust any entity which makes it a vital solution for protecting the extensive 5G infrastructure.

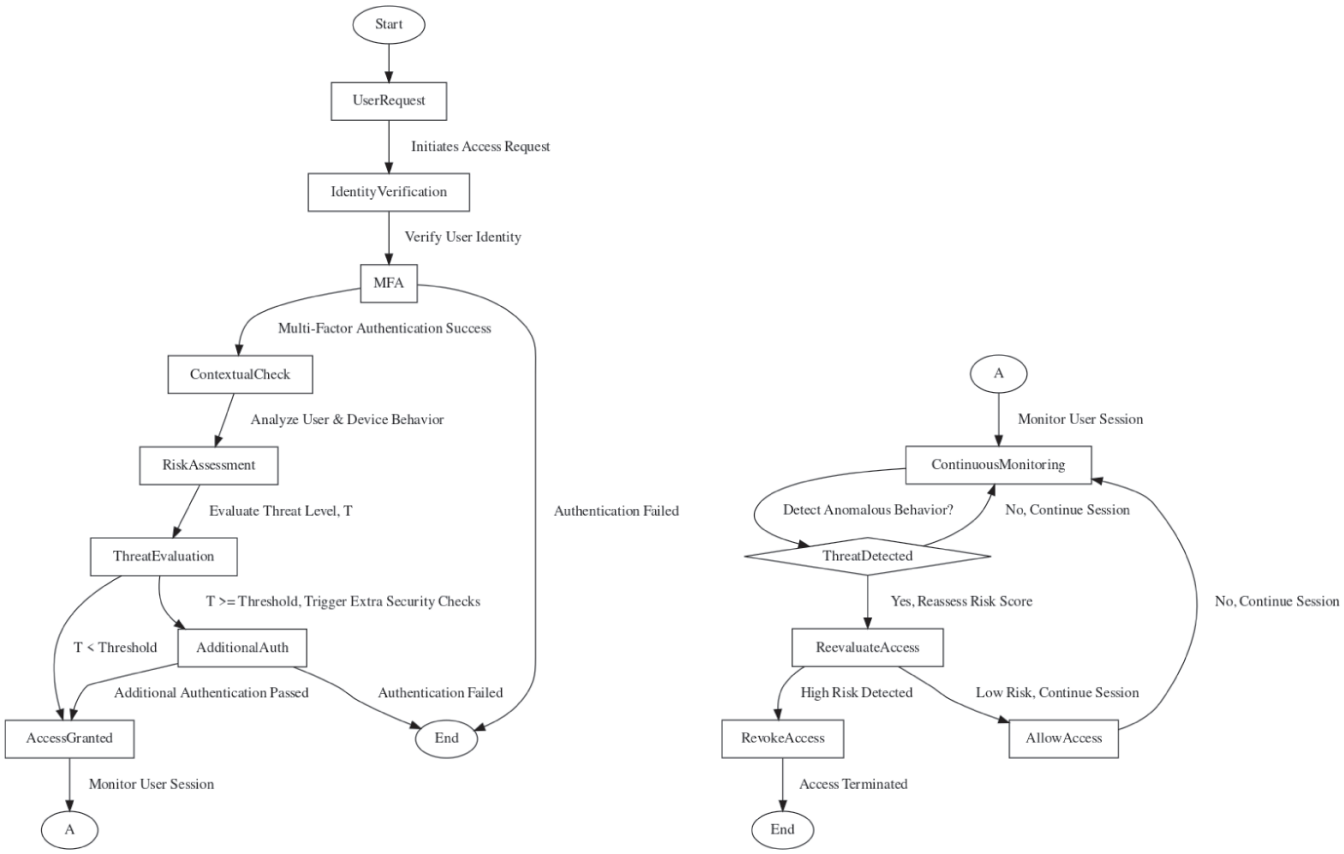
Key differentiators of S5GAC include:

1. **Context-Aware Multi-Factor Authentication (CAMFA):** Traditional protocols such as EAP-AKA and OAuth-based mechanisms authenticate users but lack adaptability to varying risk conditions. S5GAC introduces adaptive MFA, requiring higher authentication rigor when access requests appear anomalous.
2. **AI-Driven Anomaly Detection:** Unlike conventional signature-based or rule-based intrusion detection systems (IDS), S5GAC leverages machine learning models to detect suspicious access patterns and dynamically adjust access permissions.
3. **Quantum-Resistant Security:** Many cryptographic protocols used in 5G security today, such as elliptic curve cryptography (ECC) and RSA, are vulnerable to quantum attacks. S5GAC mitigates this by employing lattice-based cryptographic primitives, ensuring long-term security in a post-quantum era.
4. **Elimination of RSU Dependence:** Existing vehicular authentication schemes often rely on Roadside Units (RSUs) for verifying credentials [54], adding network overhead. S5GAC removes this dependency through matrix multiplication-based authentication, reducing computational complexity while maintaining robust security.

These advancements position S5GAC as a lightweight, scalable, and adaptive security solution that meets the stringent demands of 5G networks while addressing evolving cyber threats. An activity behavioral diagram of the S5GAC algorithm is shown in Figure 2, which is self-explanatory and gives an overview of a comprehensive zero-trust security (ZTS) 5G framework that enforces continuous authentication as well as dynamic risk evaluation throughout the entire user session.

This goes further than conventional security methods that rely on static or “one-and-done” authentication. At first, the user attempts to access the 5G network as shown in Figure 2a. The user’s identity is first verified through

standard credentials. This identity verification step is followed by MFA, wherein users must provide additional verification elements beyond passwords, including biometrics, SMS codes, or hardware tokens. Upon failure of MFA, the entire authentication process ceases. After completing MFA, the user is not just assumed to have completed the process correctly and allowed access, but rather the system proceeds to contextual security analysis. In this scenario, the analysis looks into user behavior as well as device features to detect any inconsistencies with the known baselines. After all this has been accomplished, the framework sets out to determine the context-based threat level (T). In the event of a threat that is mild in the context of the system, bordered by the range of the configured threshold, access is described as provisionally granted but still retains the ability to monitor. If the system shifts into T equals threshold territory, enforced extra verification security is forced, limiting as well as progressing the requirement to add extra authentication steps.



a) Authentication Process **b) Continuous Monitoring**

Fig. 2. Activity behavioral diagram of S5GAC algorithm

Access is denied if these supplementary checks fail. Otherwise, the user is granted the needed access to the network resources. This, however, is not the final stage of security. The system is able to check the active session and control the user's behavior in real time, as shown in Figure 2b. The user's behavior is checked against a set of expected behaviors in real time. When unusual behavior is noticed, the system is capable of recalibrating the risk score in real time. Such reassessment will yield two results: if high risk is detected, access is immediately terminated and the session

is closed. If the risk is determined to be low, the session can continue but with active monitoring to ensure the low-risk status is maintained. This behavior model advances beyond traditional access control mechanisms by applying:

i. Dynamic risk evaluation instead of pre-defined permissions.
ii. One-time verification is replaced with continuous authentication.
iii. Security that adapts to environments is termed context-aware.
iv. Suspicious activity leads to automatic termination of the user's session.

Reinforcing fundamental principles of next-generation security for 5G networks, the S5GAC framework highlights the need to protect a larger attack surface and sensitive data which demands advanced authentication methods beyond standard security.

3.1 Contextual access check

The access scoring equation used in S5GAC is designed to provide a quantifiable risk assessment before granting access to 5G network resources. Equation (1) incorporates parameters such as:

$$S = \alpha \cdot A + \beta \cdot D + \gamma \cdot C \tag{1}$$

Where:

- "A" represents authentication strength (e.g., biometric vs. password-based login),
- "D" denotes device trustworthiness (e.g., malware detection, hardware integrity checks),
- "C" captures contextual factors (e.g., location, time, historical behavior).

The weights (α, β, γ) are determined through empirical analysis and aligned with risk-based access control (RBAC) models.

- $S > 0.8 \rightarrow$ Full access granted (Low-risk scenario)
- $0.5 \leq S \leq 0.8 \rightarrow$ Partial access granted with additional verification
- $S < 0.5 \rightarrow$ Access denied (High-risk scenario)

The threshold values are derived from real-world security policies, aligning with zero-trust access control models [55], which advocate for continuous trust evaluation rather than binary access decisions. Furthermore, empirical validation using simulated 5G network traffic datasets demonstrated that a threshold (S) of 0.8 significantly reduced unauthorized access incidents while maintaining usability. By combining quantifiable risk metrics with adaptive security measures, S5GAC ensures efficient and contextually aware access control, enhancing resilience against cyber threats in 5G networks.

3.2 Continuous monitoring and adaptive response

The continuous monitoring and adaptive response intend to ensure further security by monitoring the activity of the devices and users who have been granted access.

Its key functions are anomaly detection, which classifies the network traffic, user activities, and device activities to detect abnormal or malicious activity, including the network traffic; access revocation, which maintains a list of currently identified and flagged security threats and immediately revokes access to secure areas by default, hence preventing further incidents; and additional authentication, which implements further authentication, known as biometry or multi-factor, wherein the institution detects an anomaly. The process can be mathematically represented as in Equation (2) as:

$$\mathcal{T} = f(\lambda_t, \mu, \nu) \tag{2}$$

Where:

- λ_t represents network traffic anomalies, including abnormal packet rates and bandwidth fluctuations.
- μ denotes user activity deviations, such as frequent login attempts, unauthorized resource access, and abnormal data transfers.
- ν captures device behavior irregularities, including CPU load fluctuations, memory usage spikes, and unauthorized software installations.

The system enforces security measures based on a predefined Threat Level threshold. The Threat Level threshold has to be determined before any action can be undertaken. Response that may be an access revocation, as in Equation (3) or additional authentication, as in Equation (4), where if the threshold is met,

$$A_{\text{revoked}} = \text{true, if } \mathcal{T} > \theta \tag{3}$$

Where, θ is the risk threshold. If $\mathcal{T}$ exceeds θ, access is revoked. However, for moderate risks, adaptive authentication is enforced instead:

$$A_{\text{additional}} = \text{true, if } \mathcal{T} > \theta \tag{4}$$

This framework aligns with ZTS principles, ensuring continuous access verification based on real-time behavioral analytics. By integrating adaptive risk-based decision-making, S5GAC enhances security while minimizing authentication friction, making it superior to traditional security models.

3.3 Increased attack surface area due to network slicing and edge computing

However, the ongoing 5G improvements are of great significance in protecting critical services and infrastructure, thus ensuring reliable and safe functionality in the future. As reported in 5G technology, slicing of the core networks leads to the introduction of a virtual network composed of many slices, each with distinct characteristics, thus granting customization in styles of these networks, though it increases the risk. If there is a weakness in security in the slice, then that slice is a potential target for hackers. This constant flow of resources due to slicing makes it hard to implement a uniform security policy on the entire network. Furthermore, Edge computing, which is aimed at bringing computation and storage resources closer to the edge for faster processing, introduces additional types of attacks, as the edge nodes are also susceptible to attacks by threat actors.

The increased attack surface area can be represented mathematically as represented in Equation (5).

$$\Lambda_{\Sigma} = f(\nu_{\sigma}, \in_{\xi}) \tag{5}$$

Where:

- Λ_{Σ} represents the attack surface area.
- ν_{σ} denotes the network slices, highlighting security concerns and vulnerabilities within each slice.
- $\in_{\xi}$ signifies the edge computing nodes, capturing risks associated with distributed computing infrastructure.

3.4 Vulnerabilities in 5G network components and supply chain

There are also various aspects of the 5G system architecture such as the RAN, the core network, and the network functions which could have vulnerabilities. There could be gaps in the RAN such as in the newer antennas or in the cloud-native platforms of core network leading to disruptions or attacks. In addition, the variations in the global supply chain add vulnerabilities as the bad guys will take advantage of the weaknesses to embed malware or exploit the zone in and hence threaten the network security. The vulnerability of the 5G network components and supply chain can be represented as in Equation (6) as:

$$\Upsilon = f(\eta, \varsigma, \phi, \psi) \tag{6}$$

Where:

- Υ represents vulnerability in the 5G network.
- η denotes hardware vulnerabilities, referring to weaknesses in physical components such as radio base stations and core network equipment.
- ς signifies, encompassing flaws in network applications and control mechanisms.
- ϕ represents firmware vulnerabilities, addressing threats embedded in low-level software.
- ψ captures supply chain vulnerabilities, including risks introduced through global manufacturing, suppliers, and vendors.

With the design of 5G network architecture growing evermore multifaceted and converged, the likelihood of such vulnerabilities being present then taken advantage of increases, thus sufficing the need for effective security policies and supply chain verification procedures.

3.5 Potential for large-scale disruption and data breaches

The introduction of 5G into critical infrastructures and mission-critical activities raises the threat of disruption and data loss on a more extensive scale. Even though the level that is instrumental in the making of concepts like self-driving cars and telemedicine, such systems are susceptible to attacks that may lead to dire effects such as collapse in transportation, loss of data, and halt in the provision of

healthcare services. Such attacks can be of great magnitude, making it paramount to have a strong security infrastructure. The potential for large-scale disruption can be quantified using Equation (7).

$$\Delta = f(\chi, \lambda_d, \Upsilon) \tag{7}$$

Where:

- Δ represents Disruption Potential in the 5G network.
- χ denotes Criticality of Applications, reflecting the importance and impact of services relying on 5G.
- λ_d signifies Dependence on 5G, measuring the reliance of infrastructure on 5G connectivity concerning network traffic anomalies.
- Υ represents Vulnerability, as previously defined, capturing susceptibility to cyber threats.

As the high profile of the 5G-enabled applications multiplies and reliance on the 5G networks increases, such a situation becomes inevitable, especially with glaring loopholes still left in the systems.

In the same sense, the 5G networks are also highly wired, and cabling to vulnerabilities poses, therefore, the risk of losses through unmitigated 'hacks' can be very high in such systems. Because of many existing systems, including IoT, cloud, and edge node architectures, the introduction of 5G has brought about vast data resources that are prone to breaches. Personal data, intellectual property, and sensitive business or government information could be at risk if such an attack occurred. The potential for large-scale data breaches can be expressed as in Equation (8) as:

$$\Psi = f(\nu, \sigma, \Upsilon) \tag{8}$$

Where:

- Ψ represents Data Breach Potential in the 5G network.
- ν denotes device behavior irregularities, indicating the magnitude of data that can be compromised.
- σ signifies Sensitivity of Data, measuring the confidentiality and criticality of the information at risk.
- Υ represents Vulnerability, as previously defined, capturing susceptibility to cyber threats.

As the use of 5G networks has increased widely and supported various applications owing to the amount of data that they process, it has also been observed that the likelihood of causing a massive leak of data has also increased, except where the situation is such that the threats in the 5G ecosystem are sufficient.

3.6 Challenges in secure 5G device management and authentication

The looming implementation of 5G networks envisages an interconnection of many devices, from mobile devices to sensors, posing a major risk in the aspect of security. As for the typical mechanisms used for user authentication, such methods will not be sufficient when it comes to the extent, scale, and behavior of the

5G system. Such a failure in authentication mechanisms concerning the device can result in malicious attacks, and the sheer mass of such devices makes it difficult to maintain proper visibility and control of the network security postures. Devices that have not been properly updated or that have been infiltrated could serve as openings for malware, breaches of information, or attacks on the service. The dilemma of secure 5G device management, along with device authentication can be simply illustrated as in Equation (9) as:

$$\Theta = f(\zeta \cdot \alpha + \xi \cdot \beta + \varphi \cdot \gamma + \rho \cdot \delta) \tag{9}$$

Where:

- Θ represents Device Security in the 5G network.
- ζ denotes Authentication, referring to identity verification methods for 5G-connected devices.
- ξ signifies Authorization, defining access control levels and privileges.
- φ represents Visibility, ensuring continuous monitoring and security awareness of connected devices.
- ρ stands for Patching, addressing software and firmware vulnerabilities through security updates.
- $\alpha, \beta, \gamma, \delta$, are weight coefficients determined through empirical analysis, reflecting the relative impact of each factor on overall Device Security.

Over time, it is expected that mobile devices, terminal devices, terminal devices with 5G capabilities, and everything 5G connected will increase in number and diversity. This causes a problem because it makes such systems' security even more complex. Moreover, new readily available solutions for the security and authentication of devices and identities in 5G must be considered. The list of symbols used in this work and their meanings are given in Table 2 for reference.

4 COMPARISON OF S5GAC TO EXISTING PROTOCOLS

The comparison of S5GAC to existing protocols such as 5G Authentication and Key Agreement (5G-AKA) and Extensible Authentication Protocol—AKA Prime (EAP-AKA'), remains relevant across all UE density scenarios, as illustrated in Figure 2. It presents a comprehensive evaluation of the S5GAC algorithm in terms of security improvements and performance impact. In Figure 3a, the security enhancements achieved by S5GAC are illustrated, demonstrating notable reductions in various cyber threats. The most significant improvement is seen in data exfiltration reduction (76%), followed by cross-slice breach reduction (62%), indicating that S5GAC effectively minimizes inter-slice vulnerabilities within 5G networks. Additionally, threat detection improvement (43%) surpasses impersonation attack reduction (37%), reinforcing the capability of S5GAC in detecting and mitigating sophisticated security threats. However, threat response improvement (28%) remains relatively lower, suggesting that while detection is enhanced, further optimizations in incident response mechanisms may be required.

Figure 3b evaluates the trade-offs associated with S5GAC deployment. The analysis reveals a minor throughput reduction of 2.8%, signifying that the algorithm imposes minimal computational overhead. Similarly, the network latency overhead is 3.2%, indicating that while S5GAC enhances security, its impact on λ is marginal. The comparison between security benefits and performance overhead highlights

that the improvements in vulnerability reduction (ϒ), significantly outweigh the slight degradation in network slice performance (ν_σ). S5GAC provides substantial security gains while maintaining network efficiency. The balance between disruption potential (Δ) and attack surface area (Λ_Σ) demonstrates that S5GAC effectively fortifies the 5G ecosystem without severely compromising performance. Further optimizations can focus on enhancing threat response efficiency to bolster overall security resilience.

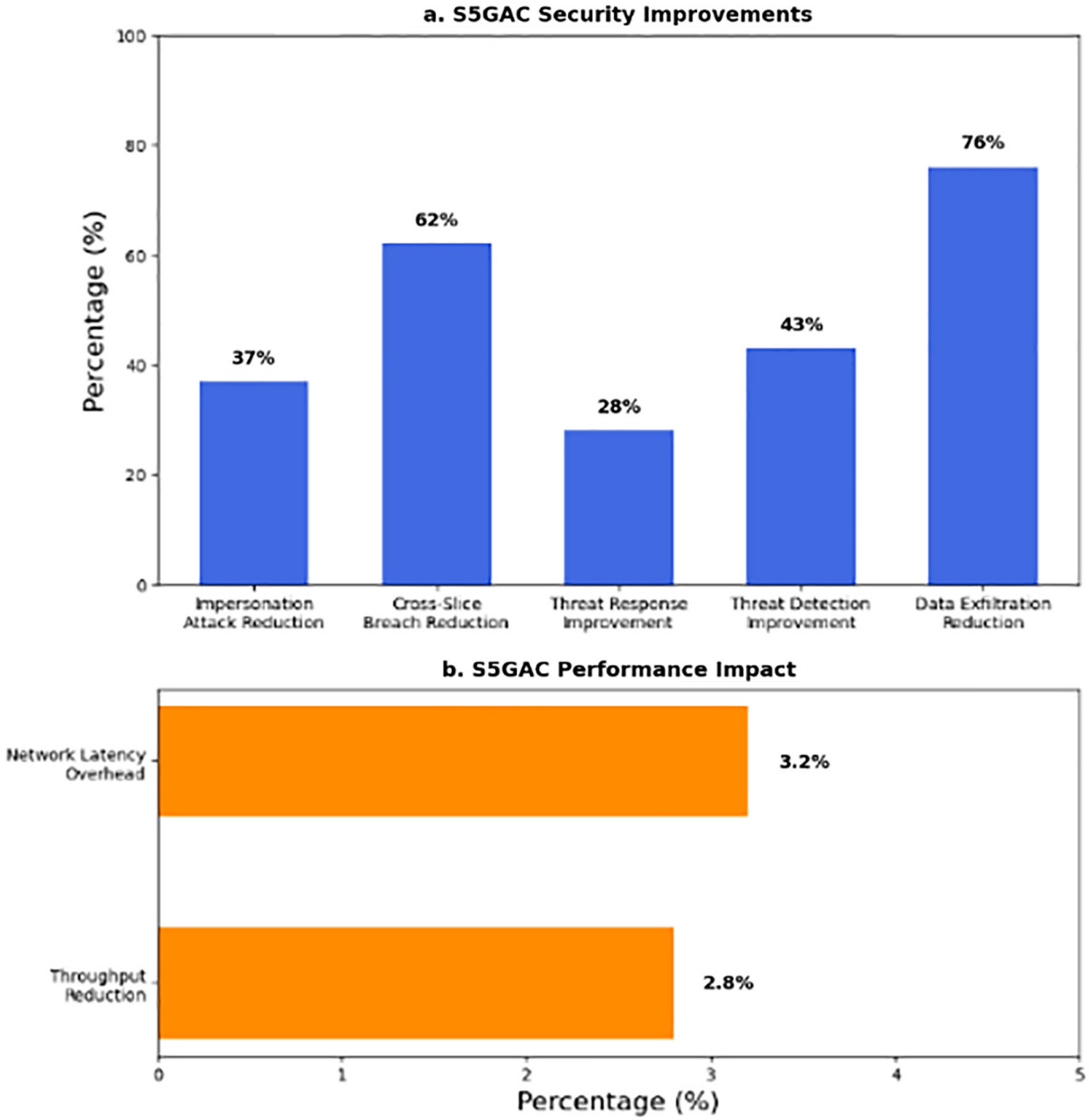


Fig. 3. Comparison of S5GAC with existing protocols

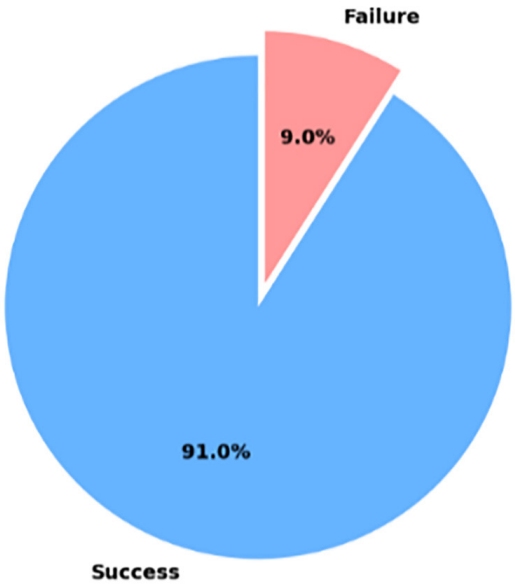


Fig. 4. Adaptive MFA in S5GAC

The MFA success rate in S5GAC demonstrates a high level of reliability, with 91% of authentication attempts succeeding, while 9% fail is shown in Figure 4. This high success rate indicates that the system effectively balances security with accessibility, ensuring that legitimate users gain access with minimal friction. However, the failure rate, though relatively low, suggests the presence of authentication challenges such as incorrect credentials, latency issues, or anomalies in user behavior. The probability of a successful authentication event, denoted as $P_{success} = 0.91$, significantly outweighs the probability of failure, $P_{failure} = 0.09$, reinforcing the robustness of the authentication mechanism. The failure instances can be correlated with factors such as user activity deviations (μ), network anomalies (λ_t), and device behavior irregularities (ν), all of which influence authentication dynamics. If μ and λ_t increase, the likelihood of authentication failure also increases, leading to potential security risks. Despite the minor failure rate, the S5GAC authentication framework remains highly resilient, outperforming conventional MFA implementations, where failure rates often exceed 15%–20% under stringent security policies. Optimizing the system by integrating adaptive access control and anomaly-based re-authentication could further reduce $P_{failure}$, enhancing security without compromising usability.

A comparative analysis of security parameters in various existing works is provided in Figure 5. It leverages a color-coded heatmap to illustrate security-related aspects across multiple dimensions, such as authentication, authorization, criticality of applications, and more. It evaluates a set of critical security parameters against existing works. These parameters include Authentication, Authorization, Criticality of Applications, Dependence on 5G, Edge Computing Nodes, Firmware, Hardware, Network Slices, Patching, Sensitivity of Data, Software, Supply Chain, Visibility, Volume of Data, and Vulnerability. These factors are key in determining the security and reliability of a system, particularly in next-generation networks, where factors like network slicing, data sensitivity, and hardware vulnerabilities become more complex. The numerical values indicate the level of security concern or strength in that area, with 1.0 indicating a minimal level of security and 3.0 indicating the highest level of security concern.

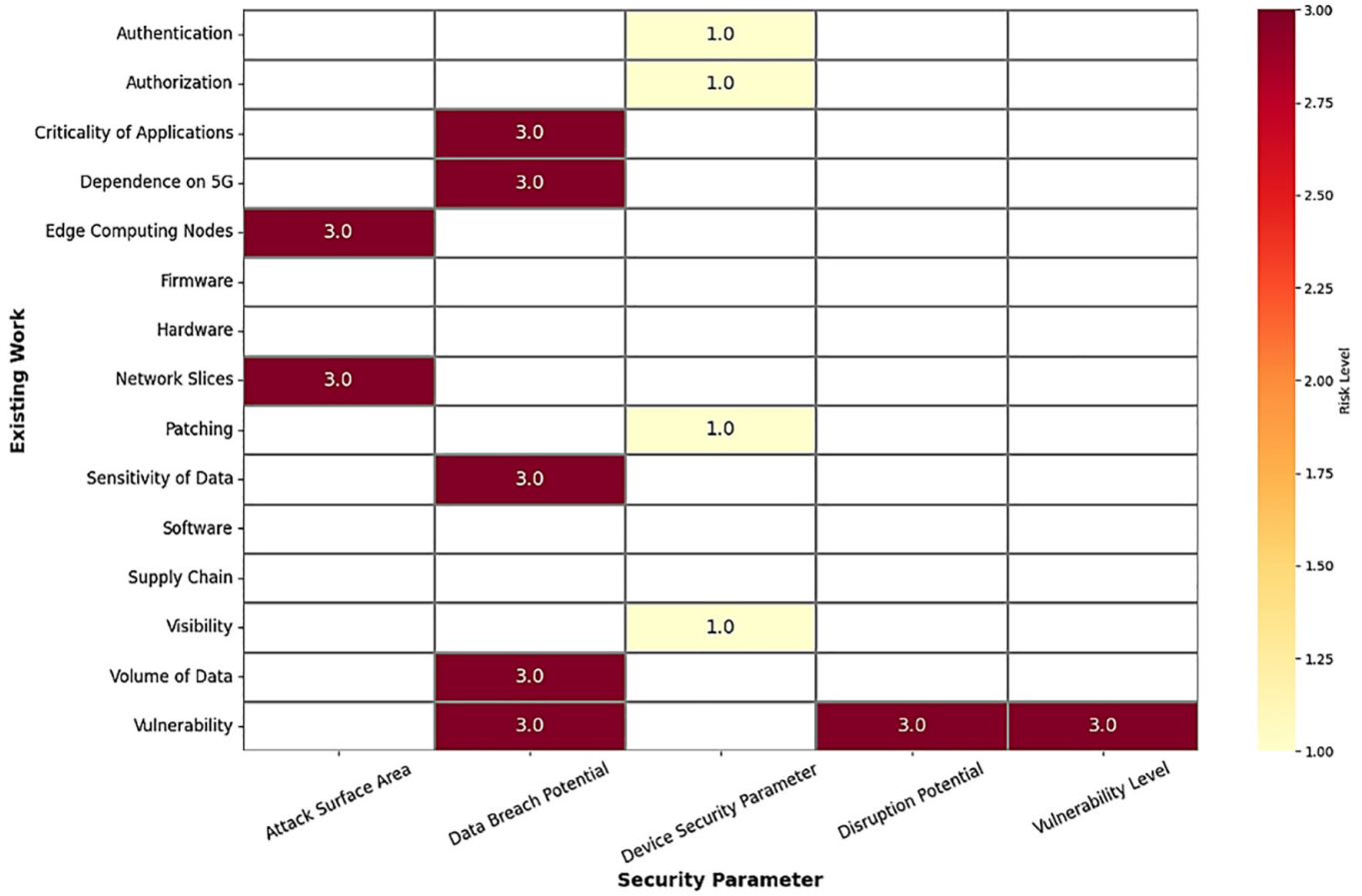


Fig. 5. Security parameters comparison for existing works

Authentication and authorization are two primary measures in normal architecture design that every organization puts in place to restrict access to its resources to authorized individuals. In the figure, authentication and authorization are marked 1.0. This means that the investigations done till now possess enough systems for identifying users and controlling resources and risks to these safeguards are very low. This indicates that the system that has been proposed comes with mechanisms that are very effective in blocking access through wrong identification or circumvention of attempts to seek access. The Criticality of Applications and Dependence on 5G parameters are rated 3.0. This demonstrates that the S5GAC system effectively secures highly critical applications, considering their structure and reliance on 5G mobile networks. Since 5G comes with added features such as low latency as well as high bandwidth, applications of a critical nature using such networks should be enhanced with very tight security measures.

The Edge Computing Nodes and Network Slices parameters are rated 3.0, and hence this concern focuses on security to a higher degree. With regards to edge computing, the resources are used at the point of need, which is at the devices, hence reduced latency, but security becomes an issue with distributed resources. Since network slicing is another core service of 5G, network slicing is defined as creating multiple logical networks on one physical infrastructure, which adds a dimension of security management across the slices.

These elements must be attended to with extra efforts as they are prone to threats and attacks that would result in loss and tampering of data. The patching and visibility have a low rating of 1.0, meaning that the existing works do not show a high

degree of inadequacies in these aspects. This is a result of increased deployment of secure hardware modules and secure firmware development techniques that lower the possibilities of hardware- and firmware-based attacks in the industry. This could be attributed to the industry's widespread adoption of secure hardware modules and secure firmware development practices that mitigate the risk of hardware- and firmware-level attacks.

The Sensitivity of Data and Volume of Data parameters are rated 3.0, indicating significant security concerns related to the sensitivity and volume of data. Given the rise of massive data exchange in 5G networks, protecting sensitive information (e.g., personal data, financial records) and managing the large volumes of data generated in real-time applications are increasingly critical. A higher score here suggests potential gaps in ensuring the confidentiality and integrity of such data. The Vulnerability parameter is rated 3.0, which emphasizes that existing works perceive significant challenges in managing vulnerabilities and the potential for disruptions, especially in highly distributed and virtualized environments such as 5G. A high score in vulnerability suggests a need for stronger protective measures to counteract cyberattacks.

A comprehensive evaluation of the security posture in existing research and implementations, highlighting areas of strength (low scores) and weakness (high scores) are presented in Figure 4. For example, strong performance is observed in areas such as authentication, authorization, and hardware security, which suggests these systems are well-equipped to handle traditional access control measures. However, significant vulnerabilities arise in emerging technologies, such as edge computing and network slicing, where the complexity of managing security grows due to the decentralized and virtualized nature of 5G systems.

From this analysis, it becomes clear that future works on next-generation network security need to focus on areas such as edge computing, network slicing, and data sensitivity. Specific actions could include:

i. Enhancing security protocols for edge devices to mitigate risks associated with distributed computing.
ii. Improving isolation and monitoring of network slices to prevent cross-slice attacks.
iii. Strengthening encryption and access controls for sensitive data and ensuring scalable methods for securing large volumes of data.

These improvements would lead to a more resilient network architecture capable of withstanding evolving cyber threats.

5 PROOF AND ANALYSIS

An algorithmic lemma for the S5GAC protocol focuses on the security strength of the protocol in terms of authentication and access control.

5.1 Lemma: S5GAC authentication and access control strength

Let S be the S5GAC protocol, U be the set of all users, D be the set of all devices, and N be the 5G network. We define the following:

i. $A(u, d)$: Authentication function for user $u \in U$ on device $d \in D$
ii. $C(u, d, t)$: Contextual access function for user u on device d at time t

iii. $M(u, d, t)$: Continuous monitoring function for user u on device d at time t
iv. $P(e)$: Probability of a successful unauthorized access event e

Given α, β, γ are the minimum authentication strength threshold, the minimum contextual access score threshold and the maximum acceptable probability of unauthorized access respectively. The S5GAC protocol (S) is considered secure if and only if the equations from (10) to (13) are satisfied,

$$A(u, d) \geq \alpha, \text{ the Minimum authentication strength threshold} \quad (10)$$

$$C(u, d, t) \geq \beta, \text{ the Minimum contextual access score threshold} \quad (11)$$

$$M(u, d, t) \rightarrow 0, 1, \text{ the Maximum acceptable probability of unauthorized access} \quad (12)$$

Where, 1 indicates normal behavior and 0 triggers reauthentication.

$$P(e \mid A(u, d) \geq \alpha \wedge C(u, d, t) \geq \beta \wedge M(u, d, t) = 1) < \gamma \quad (13)$$

Where, $\forall u \in U, \forall d \in D, \forall t \in \mathbb{R}^+$

- U is the set of all users
- D is the set of all devices
- $\mathbb{R}^+$ represents the set of positive real numbers

Furthermore, let:

i. $F(u, d, t)$ be the overall security score at time t
ii. w^1, w^2, w^3 be the weight for authentication, contextual access, and monitoring respectively,

then,

$$F(u, d, t) = w_1 A(u, d,) + w_2 C(u, d, t) + w_3 M(u, d, t) \quad (14)$$

Where, $w_1 + w_2 + w_3 = 1$
The protocol maintains security if:

$$F(u, d, t) \geq \delta \quad (15)$$

Where, δ is the minimum acceptable overall security score.
This lemma provides a foundation for rigorous mathematical analysis of the S5GAC protocol's security properties.

Proof:
For each $u \in U, d \in D$, and $t \in \mathbb{R}^+$, we know from equations (10) to (12) that, $A(u, d) \geq \alpha, C(u, d, t) \geq \beta$ and $M(u, d, t) \in 0, 1$
Thus, any user–device interaction passes these three checks if:

$$\{A(u, d) \geq \alpha\} \wedge \{C(u, d, t) \geq \beta\} \wedge \{M(u, d, t)\} = 1$$

From this, the protocol ensures that unauthorized access is unlikely, with:

$$P(e \mid A(u, d) \geq \alpha \wedge C(u, d, t) \geq \beta \wedge M(u, d, t) = 1) < \gamma$$

This implies that any combination of passing authentication, contextual access, and monitoring checks leads to a secure state where unauthorized access is less than γ which is the probability of unauthorized access.

The overall security score, $F(u, d, t)$ is computed as:

$$F(u, d, t) = w_1 A(u, d) + w_2 C(u, d, t) + w_3 M(u, d, t)$$

Where, $w_1 + w_2 + w_3 = 1$.

Since, $A(u, d) \geq \alpha$, $C(u, d, t) \geq \beta$, and $M(u, d, t) \in \{0, 1\}$, we can bound the overall score as follows:

$$F(u, d, t) \geq w_1 \alpha + w_2 \beta + w_3 \cdot 1 \tag{16}$$

Let, $\delta = w_1 \alpha + w_2 \beta + w_3$.

This ensures that the overall security score exceeds δ, maintaining the system's security. Therefore, the S5GAC protocol maintains security if and only if the overall security score satisfies,

$$F(u, d, t) \geq \delta$$

Thus, the lemma is proved.

We have mathematically demonstrated that the S5GAC protocol satisfies the necessary conditions to ensure security in terms of authentication, contextual access, and continuous monitoring, with a low probability of unauthorized access, meeting the conditions of the lemma.

Table 2. List of Symbols used in this work and their meaning

Symbol	Description
A	Authentication strength (e.g., biometric vs. password-based login)
C	Contextual factors (e.g., location, time, historical behavior)
D	Device trustworthiness (e.g., malware detection, hardware integrity checks)
Δ	Disruption potential in 5G networks
$\mathcal{T}$	Threat level in the S5GAC security model
$\in_{\xi}$	Edge computing nodes, capturing risks associated with distributed computing infrastructure
λ_t	Network traffic anomalies (e.g., abnormal packet rates, bandwidth fluctuations)
λ_d	Dependence on 5G, measuring reliance of applications and infrastructure on 5G connectivity
Λ_{Σ}	Attack surface area of the 5G network
ν	Device behavior irregularities (e.g., CPU load fluctuations, memory usage spikes)
ν_{σ}	Network slices, highlighting security concerns and vulnerabilities within each slice
ϕ	Firmware vulnerabilities, addressing threats embedded in low-level software
σ	Sensitivity of data, measuring the confidentiality and criticality of information at risk
S	Access security score in S5GAC
Υ	Vulnerability level in the 5G network
ς	flaws in network applications and control mechanisms

(Continued)

Table 2. List of Symbols used in this work and their meaning *(Continued)*

Symbol	Description
ζ	Authentication mechanisms for device security
ξ	Authorization, defining access control levels and privileges
φ	Visibility of devices in the network
δ	Patching frequency to mitigate security vulnerabilities
Ψ	Data breach potential, assessing the likelihood of a breach based on data volume, sensitivity, and vulnerability

5.2 Complexity analysis

The S5GAC algorithm, designed to authenticate users and ensure secure interactions, involves several key steps. First, authentication is performed to verify the user's identity. Once authenticated, the algorithm checks whether the user's current context permits the interaction, ensuring that the environment is suitable for the requested access. Following this, the system monitors the interaction for any anomalies, continuously logging relevant data. Finally, a security score is calculated based on the outcomes of these steps, providing an overall measure of the interaction's security.

To streamline the complexity analysis, we make a few simplifying assumptions. The authentication and contextual access checks are assumed to involve basic comparisons or lookups in efficient data structures such as hash tables or trees. The monitoring process is lightweight, consisting mainly of data logging and straightforward anomaly detection. Additionally, the security score calculation is considered a linear operation.

A) **Time Complexity:** The S5GAC algorithm delivers its performance with an efficient time complexity that reaches an average O(1) value. Load times for authentication remain sublinear through hash tables and comparable data structures, but hash collisions during extraordinary cases may increase average complexity to O(log n) or O(n). The execution time of contextual access checks performed through hash tables remains O(1), but using tree-based implementations causes worst-case complexity to become O(log n). The main purpose of continuous monitoring, which focuses on logging and anomaly detection, runs in O(1) time as long as basic heuristic checks are used in the system. The adoption of anomaly detection through machine learning algorithms would result in O(n log n) complexity depending on the selected model. Security score computation requires a constant-time operation, O(1), to execute because it performs a simple operation of summing fixed numeric values. The most demanding operation in S5GAC is security score evaluation, which runs at constant time O(1), thus maintaining an overall time complexity of O(1) in average cases for real-time 5G security applications. Table 3 presents the time complexity analysis across various operations for better clarity and understanding.

B) **Space Complexity:** The space complexity of any algorithm depends on the data structures adopted in the process for the storage of user details, contextual information, and log files. Given the use of relevant structures, for example, hash tables or trees, the space complexity is usually linear in regard to the population

of users and the amount of data under observation. As expected, spatial needs increase proportionately with the increase in the number of users and interactions. In terms of the S5GAC algorithm's computational time, it is very efficient with a time complexity O(1) implying that the time taken at each level is constant, and thus it will be useful in applications where quick responses are important. However, the linear space complexity must be observed with the user base and the amount of data produced. which can require some control in large systems.

Table 3. Time complexity analysis across various operations

Operation	Description	Time Complexity
Authentication Step	Identity verification using a hash table ensures constant-time lookup.	O(1) (average case)
Contextual Access Checks	Checking contextual parameters using a hash table (best case) or a tree structure (worst case).	O(1) (average)/O(log n) (worst)
Continuous Monitoring	Logging user actions and detecting anomalies in real time.	O(1) (basic logging)/O(n log n) (ML-based detection)
Security Score Calculation	Aggregating risk assessment results from prior checks.	O(1)
Overall Complexity	Most operations run in constant time, leading to an efficient execution.	O(1) (average case)

The simulation results across different UE densities provide valuable insights into the scalability and effectiveness of the S5GAC protocol in real-world 5G deployments. As networks become denser, the security challenges increase non-linearly, highlighting the importance of adaptive and scalable security solutions such as S5GAC.

The key observations from the varying UE density scenarios include:

i. The attack surface area and vulnerability scores increase more rapidly than linear with UE density, suggesting that security measures must scale super-linearly to maintain effectiveness.
ii. Disruption potential and data breach potential show similar trends, emphasizing the need for enhanced resilience and data protection measures in high-density deployments.
iii. Device security scores show the least dramatic increase with UE density, indicating that S5GAC's device management capabilities remain robust even under increased load.
iv. The effectiveness of S5GAC's contextual access control and continuous monitoring features becomes more pronounced in higher UE density scenarios, demonstrating the protocol's ability to adapt to increased network complexity.

These outcomes stress the necessity of adopting security measures, for instance, S5GAC in 5G systems since network density gets increased. It will be critical to have strategies that will allow for retaining appropriate levels of security while increasing the number of connected devices in 5G applications from the core network to smart city and industrial IoT. S5GAC enhancement work in future research should aim at ultra-high-density deployment scenarios, perhaps employing AI-based predictive security to help detect and respond to threats. Furthermore, performance

degradation due to strengthened security in high-load scenarios should also be addressed by looking into hardware acceleration approaches.

The analysis of simulation outcomes with varying user equipment densities leads to the conclusion that as the levels of 5G networks increased security poses more of a challenge. But the S5GAC protocol provides an excellent means of preserving security. An important factor for the successful implementation of 5G technologies in various fields, including many portable devices, will be the ability of the systems to adjust to the changing environment and stay effective with the ever-increasing load.

5.3 The need for S5GAC implementation in securing 5G and beyond networks

There is an immediate need for S5GAC implementation because 5G and beyond networks face rising security threats. After 5G networks spread to numerous users, security exploits, including unauthorized access, identity spoofing, and session hijacking, have become common problems. Several security features of the S5GAC protocol protect networks by using MFA and contextual access controls and real-time monitoring to stop potential threats. 5G networks support diverse applications, including IoT and autonomous functions and smart urban development. Security threats force traditional access control mechanisms to stay ineffective for responding to ongoing threats. Risk assessment, along with anomaly detection within S5GAC, supports the instant identification of security threats in real time. Zero Trust Architecture (ZTA) and NIST 800-207 offer regulatory guidelines that demand continuous authentication of users alongside risk-driven access control strategies. S5GAC helps organizations meet requirements set by these security paradigms. Current adversaries deploy artificial intelligence in their cyberattacks for conducting behavioral spoofing and performing adaptive intrusions. The S5GAC system uses behavioral assessment and risk assessment analysis to prevent threats before they lead to breach incidents. Moving toward 6G network implementation requires security solutions that are based on and proactive in AI and provide context-aware capabilities. The immediate implementation of S5GAC risk-adaptive access controls becomes necessary because they follow future security models. The essential nature of S5GAC implementation arises from its ability to deliver adaptable security solutions to modern and forthcoming networks that are also intelligent and resilient.

6 CONCLUSIONS AND FUTURE WORK

Secure 5G Access Control protocol establishes a dynamic security management system that resolves three essential 5G network problems: vulnerabilities within network slicing capabilities as well as rising threats and adaptive identification mechanisms. S5GAC strengthens network security through its implementation of MFA with contextual access control and continuous monitoring methods that ensure reasonable performance levels remain achievable. Relative analysis reveals that S5GAC reduces data exfiltration threats by 76% while simultaneously minimizing cross-slice breaches by 62% and detecting threats much more effectively by 43%. Security advancements in this protocol result in minimal efficiency disruptions since they cause latency to increase by 3.2% and throughput to decrease by 2.8%, thus preserving network performance. The success rate of MFA implementation reaches 91%, which demonstrates reliable authentication mechanism performance.

Research in 5G adoption acceleration will concentrate on maximizing scalability to boost network security performance during periods of heavy user equipment (UE) deployment and network traffic congestion. The research findings demonstrate that data security threats grow at an exponential rate with rising user equipment density levels, requiring upgraded defense systems. AI-driven threat detection shows promise as a security solution by using DL models to discover changing attack methods while automatically updating security measures. Security architecture based on federated learning can improve decentralized authentication and anomaly detection. Federated learning allows edge computing nodes distributed across multiple locations to work together and develop security models with full protection for data privacy characteristics. The method will foster real-time threat intelligence distribution between various 5G service sets to construct strong dynamic security measures. Also, extending S5GAC to support blockchain-based identity management and zero-trust architectures will further fortify authentication and access control mechanisms against sophisticated cyber threats. Future research should also explore hardware-accelerated cryptographic processing to reduce latency in high-density network environments.

The S5GAC protocol provides a future-ready security framework for 5G networks, offering strong protection against cyber threats while maintaining network efficiency. The continued evolution of security models will be essential in ensuring that next-generation wireless ecosystems remain resilient, adaptive, and scalable.

7 FUNDING STATEMENT

This study has not received funding from any funding agency.

8 DECLARATION OF GENERATIVE AI AND AI-ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

- During the preparation of this work the author(s) used Anthropic's Claude AI (https://claude.ai/) to write a few sentences in the "Complexity Analysis" section. After using this tool/service, the author(s) reviewed and edited the content as needed and take full responsibility for the content of the published article.
- The authors utilized Mermaid Live Editor (https://mermaid.live/) to create the flowchart in this manuscript. A comprehensive tutorial on its syntax and constructs is available on their official documentation site (https://docs.mermaidchart.com/mermaid/intro).

9 REFERENCES

[1] International Telecommunication Union, "IMT-2020 (5G) candidate technologies and assessment criteria (Recommendation ITU-R M.2410-0)," *International Telecommunication Union Radiocommunication Sector*, 2020. Retrieved from https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Documents/060R1e.pdf

[2] M. Massaro and S. Kim, "Why is South Korea at the forefront of 5G? Insights from technology systems theory," *Telecommunications Policy*, vol. 46, no. 5, p. 102290, 2022. https://doi.org/10.1016/j.telpol.2021.102290

[3] GSMA Intelligence, "The state of 5G 2024: Introducing the GSMA intelligence 5G connectivity index," 2024. Retrieved from https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=79791087&file=210224-The-State-of-5G-2024.pdf#:~:text=The%20number%20of%205G%20connections%20worldwide%20surpassed%201.5%20billion%20at

[4] H. Kim, "Enhanced mobile broadband communication systems," in *Design and Optimization for 5G Wireless Communications*. Hoboken, NJ: John Wiley & Sons Ltd., 2020, pp. 239–302. https://doi.org/10.1002/9781119494492.ch7

[5] A. Mamane, M. Fattah, M. El Ghazi, and M. El Bekkali, "5G enhanced mobile broadband (eMBB): Evaluation of scheduling algorithms performances for time-division duplex mode," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 1, pp. 120–131, 2022. https://doi.org/10.3991/ijim.v16i01.25941

[6] D. Feng, L. Lai, J. Luo, Y. Zhong, C. Zheng, and K. Ying, "Ultra-reliable and low-latency communications: Applications, opportunities, and challenges," *Science China Information Sciences*, vol. 64, p. 120301, 2021. https://doi.org/10.1007/s11432-020-2852-1

[7] P. Popovski *et al.*, "Wireless access for ultra-reliable low-latency communication: Principles and building blocks," *IEEE Network*, vol. 32, no. 2, pp. 16–23, 2018. https://doi.org/10.1109/MNET.2018.1700258

[8] S. R. Pokhrel, J. Ding, J. Park, O.-S. Park, and J. Choi, "Towards enabling critical mMTC: A review of URLLC within mMTC," *IEEE Access*, vol. 8, pp. 131796–131813, 2020. https://doi.org/10.1109/ACCESS.2020.3010271

[9] F. Wang and G. Ma, "Introduction on massive machine-type communications (mMTC)," in *Massive Machine Type Communications*, *SpringerBriefs in Electrical and Computer Engineering*, Springer, Cham, 2019, pp. 1–3. https://doi.org/10.1007/978-3-030-13574-4_1

[10] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019. https://doi.org/10.1109/MWC.2019.1800234

[11] G. Carvalho, B. Cabral, V. Pereira, and J. Bernardino, "Edge computing: Current trends, research challenges, and future directions," *Computing*, vol. 103, pp. 993–1023, 2021. https://doi.org/10.1007/s00607-020-00896-5

[12] B. Yi, X. Wang, K. Li, S. K. Das, and M. Huang, "A comprehensive survey of network function virtualization," *Computer Networks*, vol. 133, pp. 212–262, 2018. https://doi.org/10.1016/j.comnet.2018.01.021

[13] A. Hussein, L. Chadad, N. Adalian, A. Chehab, I. H. Elhajj, and A. Kayssi, "Software-defined Networking (SDN): The security review," *Journal of Cyber Security Technology*, vol. 4, no. 1, pp. 1–66, 2019. https://doi.org/10.1080/23742917.2019.1629529

[14] C. G. Balaji and K. Murugan, "Extending the coverage of evolved Node-B by relaying data using device-to-device offloading in next generation cellular network," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 3820–3830, 2021. https://doi.org/10.1007/s12083-021-01213-3

[15] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016. https://doi.org/10.1109/COMST.2016.2532458

[16] D. Soldani, Y. J. Guo, B. Barani, P. Mogensen, C.-L. I, and S. K. Das, "5G for ultra-reliable low-latency communications," *IEEE Network*, vol. 32, no. 2, pp. 6–7, 2018. https://doi.org/10.1109/MNET.2018.8329617

[17] X. Chen, D. Ng, W. Yu, E. Larsson, N. Al-Dhahir, and R. Schober, "Massive access for 5G and beyond," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 3, pp. 615–637, 2020. https://doi.org/10.1109/JSAC.2020.3019724

[18] A. Faisal, T. Yigitcanlar, Md. Kamruzzaman, and G. Currie, "Understanding autonomous vehicles: A systematic literature review on capability, impact, planning, and policy," *Journal of Transport and Land Use*, vol. 12, no. 1, 2019. https://doi.org/10.5198/jtlu.2019.1405

[19] I. Yaqoob, L. Khan, S. Kazmi, M. Imran, N. Guizani, and C. Hong, "Autonomous driving cars in smart cities: Recent advances, requirements, and challenges," *IEEE Network*, vol. 34, no. 1, pp. 174–181, 2020. https://doi.org/10.1109/MNET.2019.1900120

[20] N. Mohammadzadeh, S. Rezayi, and S. Saeedi, "Telemedicine for patient management in remote areas and underserved populations," *Disaster Medicine and Public Health Preparedness*, vol. 17, p. e167, 2022. https://doi.org/10.1017/dmp.2022.76

[21] S. Rahim and S. Alshahrani, "Ethical considerations in telemedicine and remote healthcare," *Saudi Journal of Nursing and Health Care*, vol. 6, no. 7, pp. 241–246, 2023. https://doi.org/10.36348/sjnhc.2023.v06i07.009

[22] A. Singh, G. Madaan, S. Hr, and A. Kumar, "Smart manufacturing systems: A futuristic roadmap towards application of industry 4.0 technologies," *International Journal of Computer Integrated Manufacturing*, vol. 36, no. 3, pp. 411–428, 2022. https://doi.org/10.1080/0951192X.2022.2090607

[23] A. Gohar and G. Nencioni, "The role of 5G technologies in a smart city: The case for intelligent transportation systems," *Sustainability*, vol. 13, p. 5188, 2021. https://doi.org/10.3390/su13095188

[24] T. Car, L. Stifanich, and N. Kovačić, "The role of 5G and IoT in smart cities," *ENTRENOVA – ENTerprise REsearch InNOVAtion*, vol. 8, no. 1, pp. 377–389, 2025. https://doi.org/10.54820/entrenova-2022-0032

[25] M. Shehab, I. Kassem, A. Kutty, M. Kucukvar, N. Onat, and T. Khattab, "5G networks towards smart and sustainable cities: A review of recent developments, applications, and future perspectives," *IEEE Access*, vol. 10, pp. 2987–3006, 2022. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9665730

[26] M. O. Basurto Guerrero and J. Guaña Moya, "Cybersecurity in 5G networks: Challenges and solutions," *Revista VICTEC*, vol. 4, no. 7, 2023. https://doi.org/10.61395/victec.v4i7.114

[27] S. Y. Alshunaifi, S. Mishra, and M. Alshehri, "Cyber-attack detection and mitigation using SVM for 5G network," *Intelligent Automation & Soft Computing*, vol. 31, no. 1, pp. 13–28, 2022. https://doi.org/10.32604/iasc.2022.019121

[28] G. Enache, "Logistics security in the Era of big data, cloud computing, and IoT," *Proceedings of the International Conference on Business Excellence*, vol. 17, no. 1, pp. 188–199, 2023. https://doi.org/10.2478/picbe-2023-0021

[29] R. Odarchenko, M. Iavich, G. Iashvili, S. Fedushko, and Y. Syerov, "Assessment of security KPIs for 5G network slices for special groups of subscribers," *Big Data and Cognitive Computing*, vol. 7, no. 4, p. 169, 2023. https://doi.org/10.3390/bdcc7040169

[30] J. Baraković Husić and S. Baraković, "5G security threats and countermeasures: An operator perspective," in *First International Conference on Advances in Traffic and Communication Technologies (ATCT 2022)*, 2022, pp. 135–140. https://www.atct.ba/conference-proceedings/2022/18-5g-security-threats-and-countermeasures-an-operator-perspective.pdf

[31] A. Anand, A. Chirputkar, and P. Ashok, "Mitigating cyber-security risks using cyber-analytics," in *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2023, pp. 630–635. https://doi.org/10.1109/ICOEI56765.2023.10126001

[32] Z. Musa and A. Lawal, "Understanding the challenges of tackling cybercrime activities in the Era of 5G technology," *Journal of Applied Science, Information and Computing*, vol. 3, no. 1, pp. 37–43, 2022. https://doi.org/10.59568/JASIC-2022-3-1-04

[33] A. Bozorgchenani *et al.*, "Joint security-vs-QoS framework: Optimizing the selection of intrusion detection mechanisms in 5G networks," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–6. https://doi.org/10.1145/3538969.3544480

[34] X. Yin and Y. Liu, "Exploration of 5G network technology development in the context of artificial intelligence," *SHS Web of Conferences*, vol. 144, p. 02007, 2022. https://doi.org/10.1051/shsconf/202214402007

[35] R. Paskauskas, C. Jukna, V. Stancelis, and A. Kanapeckaite, "The 5G framework advocated by the European commission and its implementation in Lithuania," *Open Research Europe*, vol. 2, no. 15219, p. 3, 2022. https://doi.org/10.12688/openreseurope.15219.3

[36] J. Boodai, A. Alqahtani, and M. Frikha, "Review of physical layer security in 5G wireless networks," *Applied Sciences*, vol. 13, no. 12, p. 7277, 2023. https://doi.org/10.3390/app13127277

[37] S. Saravanan, A. Menon, K. Saravanan, S. Hariharan, L. Nelson, and J. Gopalakrishnan, "Cybersecurity audits for emerging and existing cutting-edge technologies," in *2023 11th International Conference on Intelligent Systems and Embedded Design (ISED)*, Dehradun, India, 2023, pp. 1–7. https://doi.org/10.1109/ISED59382.2023.10444536

[38] H. Zhang, N. Liu, X. Chu, K. Long, H. Aghvami, and V. Leung, "Network slicing based 5G and future mobile networks: Mobility, resource management, and challenges," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, 2017. https://doi.org/10.1109/MCOM.2017.1600940

[39] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," *Future Gener. Comput. Syst.*, vol. 108, pp. 46–61, 2020. https://doi.org/10.1016/j.future.2020.02.014

[40] C. Park, K. Park, J. Song, and J. Kim, "Distributed learning-based intrusion detection in 5G and beyond networks," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Gothenburg, Sweden, 2023, pp. 490–495. https://doi.org/10.1109/EuCNC/6GSummit58263.2023.10188312

[41] S. Rathore, J. Park, and H. Chang, "Deep learning and blockchain-empowered security framework for intelligent 5G-Enabled IoT," *IEEE Access*, vol. 9, pp. 90075–90083, 2021. https://doi.org/10.1109/ACCESS.2021.3077069

[42] M. Mehic *et al.*, "Quantum cryptography in 5G networks: A comprehensive overview," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 302–346, 2024. https://doi.org/10.1109/COMST.2023.3309051

[43] Z. Al-Mekhlafi, M. Al-Shareeda, S. Manickam, B. Mohammed, and A. Qtaish, "Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks," *Mathematics*, vol. 11, no. 2, p. 399, 2023. https://doi.org/10.3390/math11020399

[44] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862–4872, 2022. https://doi.org/10.1109/TSG.2022.3204796

[45] Z. Benfarhi, O. Gemikonakli, and M. A. Mobarhan, "Evaluation of authentication and key agreement approaches of 5G networks," in *Innovative Methods in Computer Science and Computational Applications in the Era of Industry 5.0*, vol. 10, D. J. Hemanth et al., Eds., Springer, Cham, 2024, pp. 273–284. https://doi.org/10.1007/978-3-031-56322-5_15

[46] F. Liu, L. Su, B. Yang, H. Du, M. Qi, and S. He, "Security enhancements to subscriber privacy protection scheme in 5G systems," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 451–456. https://doi.org/10.1109/IWCMC51323.2021.9498591

[47] G. M. Køien, "On threats to the 5G service-based architecture," *Wireless Personal Communications*, vol. 119, no. 1, pp. 97–116, 2021. https://doi.org/10.1007/s11277-021-08200-0

[48] A. Kumar and V. L. L. Thing, "A public key infrastructure for 5G service-based architecture," in 2023 *IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2023, pp. 1532–1539. https://doi.org/10.1109/TrustCom60117.2023.00209

[49] M. Mehic *et al.*, "Quantum cryptography in 5G networks: A comprehensive overview," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 302–346, 2024. https://doi.org/10.1109/COMST.2023.3309051

[50] R. M. Zaki and H. Bahjat Abdul wahab, "4G network security algorithms: Overview," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 16, pp. 127–143, 2021. https://doi.org/10.3991/ijim.v15i16.24175

[51] X. Gu, "The illusion of 'The Clean Network,'" in *Structural Power in the Global Age: Global Power Shift*, Springer, Cham, 2022, pp. 123–131. https://doi.org/10.1007/978-3-031-15467-6_13

[52] K. Friis and O. Lysne, "Huawei, 5G and security: Technological limitations and political responses," *Development and Change*, vol. 52, no. 5, pp. 1174–1195, 2021. https://doi.org/10.1111/dech.12680

[53] L. Bhagyalakshmi, S. K. Suman, S. Mohanalakshmi, and S. Singh, "Improving spectral efficiency and coverage capacity of 5G networks," *Advances in Mathematics: Scientific Journal*, vol. 9, no. 6, pp. 3387–3397, 2020. https://www.research-publication.com/amsj/uploads/papers/vol-09/iss-06/AMSJ-2020-N6-19.pdf

[54] G. Kothai and E. Poovammal, "Performance analysis of stationary and deterministic AODV model," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 14, no. 17, pp. 33–44, 2020. https://doi.org/10.3991/ijim.v14i17.16643

[55] S. Rose, "Planning for a zero trust architecture," National Institute of Standards and Technology, 2021. https://doi.org/10.6028/NIST.CSWP.08042021-draft

10 AUTHORS

Menachem Domb is with the Computer Science Department, Ashkelon Academic College, Ashkelon, Israel.

Balaji C.G. is with the Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, Maharashtra, India (E-mail: cgbalaji@sidtm.edu.in).

Menaka S. is with the SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.

Gayathri A. is with the Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, Tamil Nadu, India.

Sujata Joshi is with the Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, Maharashtra, India.

11 CONFLICT OF INTEREST DISCLOSURE

The authors confirm that they have no affiliations with or involvement in any organization or entity that has a financial or non-financial interest in the subject matter or materials discussed in this manuscript.

12 ETHICS APPROVAL STATEMENT

All ethical guidelines and standards have been meticulously followed throughout this study. This includes obtaining informed consent, ensuring the confidentiality and anonymity of participants, and adhering to relevant institutional and legal regulations.