Zero Trust Architecture for 5G Networks

Varinder Kumar Sharma

Technical Manager
sharmavarinder01@gmail.com

Abstract:
The deployment of 5G networks represents a pivotal advancement in wireless communication technology, enabling ultra-reliable low-latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC). These innovations support transformative applications, including autonomous vehicles, smart cities, telemedicine, and industrial IoT. However, alongside these benefits, the architectural complexity and expanded attack surface of 5G networks introduce a new set of security challenges. Unlike traditional cellular networks, 5G features disaggregated control and user planes, software-defined networking (SDN), network function virtualization (NFV), multi-access edge computing (MEC), and network slicing—all of which increase exposure to cyber threats and weaken the effectiveness of perimeter-based security strategies. In this context, Zero Trust Architecture (ZTA) emerges as a necessary paradigm shift, built on the principle of "never trust, always verify," offering a robust security foundation for next-generation mobile networks.
This research paper comprehensively examines the design, integration, and performance of Zero Trust Architecture within 5G networks, focusing on its ability to provide dynamic, identity-aware, and context-driven access control across the 5G system architecture. The study evaluates the implementation of core ZTA principles—such as continuous authentication, micro-segmentation, strict access policy enforcement, real-time monitoring, and least-privilege access—in the context of 5G's unique architectural components. It proposes a layered ZTA framework aligned with the 3GPP 5G system architecture, integrating Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) within network functions, such as the Access and Mobility Management Function (AMF), the Session Management Function (SMF), and the User Plane Function (UPF). The framework also incorporates AI-powered Identity and Access Management (IAM) systems and anomaly detection models for proactive security analytics and enforcement.
The methodology employs a simulated testbed using a containerized 5G core built on open-source frameworks (e.g., Open5GS, Free5GC) and orchestrated through Kubernetes, enabling scalable experimentation with network slicing, dynamic access policies, and identity federation mechanisms. Attack simulations, including man-in-the-middle (MITM), privilege escalation, and lateral movement attacks, are used to test the efficacy of ZTA controls. Key performance indicators (KPIs) such as policy enforcement latency, access control granularity, threat detection rate, and quality of service (quality of service) are measured to determine the impact of ZTA integration on both security and network performance.
The results demonstrate that Zero Trust implementation in 5G networks can reduce the average time to detect and respond to security incidents by over 40%, decrease unauthorized lateral movements by 35%, and maintain sub-millisecond policy enforcement latency without disrupting user experience. The findings confirm that ZTA, when strategically embedded in the 5G core and edge, offers a scalable and resilient defense model that aligns with the zero-trust philosophy.
This paper serves as a reference architecture for telecom operators, security architects, and policymakers seeking to modernize security strategies in 5G environments. The research bridges the gap between theoretical ZTA models and practical 5G network deployments, demonstrating how Zero Trust principles can become a cornerstone of future-proof mobile security infrastructures.

Keywords- Zero Trust Architecture, 5G Security, Network Slicing, Micro-Segmentation, Policy Enforcement Point, Identity and Access Management, Software-Defined Networking, Network

Function Virtualization, Secure Network Design, Continuous Authentication, Mobile Edge Computing, Cybersecurity in Telecom.

I. INTRODUCTION

The arrival of fifth-generation (5G) wireless has been transformative for telecommunications, resetting expectations about what can be accomplished on wireless networks and how devices, services, and people interact within porous digital ecosystems. 5G goes beyond making 4G LTE faster to support so-called New Radio (NR) capacity enhancement, and evolves the air interface to include low latency, massive machine-type communication, and high reliability. It represents a new model that drives the most innovative technologies on earth, from smart manufacturing to connected, autonomous vehicles, to telemedicine and real-time analytics — and the next generation of immersive augmented and virtual reality experiences. However, these advantages have a twin emergence of cybersecurity issues, which stem from the structural transformations that underpin the 5G methodology.

Previous generations of cellular networks were very different. 5G, however, is also loosely coupled, virtualized, and software-defined. This book also provides fundamental architectural concepts, such as network slicing, multi-access edge computing (MEC), service-based architecture (SBA), and cloud-native network functions. While this architectural openness and programmability advance flexibility and scalability, they also create new attack surfaces —particularly in those critical infrastructure sectors that are beginning to adopt 5G as a secure foundation for real-time operations. This distributed and decentralized environment outperforms traditional perimeter-based security models, which focus on protecting the external boundaries of the network. In legacy architectures, after an initial breach of the outer firewall by a threat actor, lateral movement across internal resources may be largely unimpeded. This threat gains leverage in 5G networks, which generate more interconnections and broaden the domain of attack by enabling their system to work on edge devices.

Enter Zero Trust Architecture (ZTA), a modern security model based on the philosophy of "never trust, always verify" to help overcome these challenges. In the case of Zero Trust, this means that rather than assuming potential threats only from outside the network — which was a given security model with classic defense-in-depth oligoistic security approach based on perimeter — we should also assume that there can be internal threats sitting inside our local area networks as well. It includes strong identity checks, access control policies, and authentication checks, and implements microsegmentation to prevent the movement of attackers. This is an unique zero-trust security solution that makes no assumptions about requests based on user identity or originating network; every request, from inside or outside the corporate network is treated as hostile until proven otherwise, with every access decision being dynamically enforced in real time based on contextual data such as user identity, device health location, application and service usage patterns as well as risk level.

Zero Trust in 5G networks is not just an improvement; it will be a technical necessity. This fluidity means that 5G operations require new, programmable, and adaptive security constructs that can adapt as the network's complexity scales. Zero Trust enables this transition by building in access controls at each layer of the architecture — from user equipment (UE) to 5G core to cloud edge — in addition to allowing for context-aware decisions that adjust to an evolving threat surface area. Additionally, with the use of artificial intelligence (AI) and machine learning (ML), Zero Trust informs enforcement and anomaly detection for predictive threat response and real-time remediation — all without human intervention.

The objective of this paper is to investigate how Zero Trust Architecture contributes to integration and the benefits it provides within 5G networks. It provides a detailed description of micro-segmentation, continuous authentication, Identity and access management (IAM), and network policy orchestration principles that can be implemented for the control, user, and management planes of 5G URLLC networks in terms of different network functions, i.e.Access & Mobility Management Function (AMF), Session Management Function(SMF) & User Plane Function(UPF). It also examines service mesh technology and secure API gateways that can be utilized to safeguard SBIs.

Using a containerized 5G testbed to simulate Zero Trust enforcement and measuring latency, incident response time, unauthorized access attempts, and resource isolation, the paper can provide actual data in support of ZTA. In summary, this research presents a comprehensive, scalable, and practical Zero Trust

framework that can serve as a blueprint for telecom operators, manufacturers, and cybersecurity experts to protect 5G networks against emerging cyber threats.

II. LITERATURE REVIEW

The concept of Zero Trust Architecture (ZTA) originated as a response to the limitations of traditional perimeter-based security models, particularly in increasingly complex, distributed, and virtualized network environments. Initially proposed by Forrester in 2010, the Zero Trust paradigm gained significant traction with the growing adoption of cloud computing and the increasing prevalence of mobile workforces. In recent years, the rise of 5G networks has accelerated the need to integrate ZTA into telecom infrastructures, driven by the architectural decentralization, extensive use of virtualization, and critical service dependencies inherent in 5G systems. This literature review examines the key academic and industry contributions to understanding Zero Trust in the context of 5G networks, focusing on its principles, architectures, enabling technologies, and performance evaluations.

Kindervag's foundational work on Zero Trust eliminated the assumption of inherent trust within any part of the network, instead advocating for identity-centric security controls and continual verification [1]. Building on this, the National Institute of Standards and Technology (NIST) published Special Publication 800-207, "Zero Trust Architecture," which formalized ZTA into a structured framework that includes key components such as Policy Enforcement Points (PEPs), Policy Decision Points (PDPs), and trust algorithms [2]. While these frameworks were initially applied to enterprise networks, researchers have since begun adapting them for 5G ecosystems.

In the 5G domain, Maheshwari et al. [3] examined the incompatibility of legacy security models with cloud-native 5G infrastructure. They emphasized that the architectural shift to software-defined networking (SDN) and network function virtualization (NFV) requires policy enforcement at multiple trust boundaries, including those between user equipment (UE), edge nodes, core network functions, and third-party service interfaces. Their research proposed using container orchestration platforms (e.g., Kubernetes) as enforcement layers for Zero Trust policies, highlighting the need for real-time risk assessment engines to manage dynamic identities.

Ahmad et al. [4] explored the role of micro-segmentation in Zero Trust deployments, especially in the context of network slicing in 5G. Their study identified network slices as individual security domains, each requiring dedicated access policies, authentication mechanisms, and traffic monitoring. They recommended integrating machine learning models to evaluate slice-level behavior and detect deviations from established norms continuously. The incorporation of AI was further expanded upon by Zhang et al. [5], who demonstrated the use of anomaly detection engines trained on control plane and user plane telemetry data to identify threat vectors proactively. Their results confirmed that AI-powered Zero Trust frameworks significantly reduce detection-to-response times in simulated 5G scenarios.

Furthermore, researchers such as Lee and Kim [6] investigated the implementation of ZTA in multi-access edge computing (MEC) environments. Since MEC places compute and storage resources at the network edge—closer to users and devices—Lee and Kim emphasized the need for localized PEPs and federated IAM systems that can handle high volumes of low-latency access requests. Their findings aligned with those of Kumar et al. [7], who proposed a decentralized ZTA model using blockchain for trust propagation across distributed 5G microcells. Although promising, Kumar's approach introduced concerns regarding latency overhead and interoperability with standardized 5G components.

In industry settings, the 3rd Generation Partnership Project (3GPP) has not yet officially mandated Zero Trust as a standard. However, it has acknowledged the increasing importance of dynamic access control and service-based security in its technical specification TS 33.501 [8]. Meanwhile, organizations like the European Union Agency for Cybersecurity (ENISA) and the GSM Association (GSMA) have published whitepapers highlighting Zero Trust as a recommended practice for securing cloud-native telecom environments [9][10]. These documents emphasize the integration of ZTA into orchestration layers, service exposure functions, and open APIs that are exposed to third-party developers.

Overall, the literature indicates a growing consensus on the applicability and necessity of Zero Trust in 5G networks, but also underscores practical challenges. These include policy management complexity, computational overhead at the edge, and the lack of unified architectural blueprints that align Zero Trust principles with 3GPP-defined 5G system components. This research aims to bridge these gaps by developing

a holistic, performance-validated ZTA framework tailored for 5G networks, supported by current technologies and compliant with evolving standards.

III. METHODOLOGY

The approach leveraged in this research will help highlight that Zero Trust Architecture (ZTA) can be efficiently used as part of 5G networks without any impact on performance due to additional overhead or reduction due to the agility, which is one of the key reasons why 5G technology appeals to both enterprises and service providers. The research employs a simulation-based design and evaluation framework that emulates real-world 5G deployments, incorporating the core architectural elements of 5G and zero-trust principles. It will demonstrate that policy-based authentication, continuous identity verification, micro-segmentation, and adaptive access controls can be implemented at the 5G core, edge, and slicing environment without adding excessive latency or degradation in service quality.

Initially, the study utilizes a virtualized 5G core network, employing open-source implementations such as Open5GS and Free5GC, which run in a containerized manner within a Kubernetes environment. This configuration resembles the cloud-native design of today's 5G cores, enabling the variable orchestration of network functions, including the Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF), and Network Slice Selection Function (NSSF). These are the primitives on top of which we build the Zero Trust controls. On the 5G core side, the service-based architecture (SBA) interfaces are implemented as REST APIs, and some of them include hooks to integrate with external systems, allowing for the simulation of third-party applications as well as network slices.

At multiple layers of the simulated 5G architecture, Zero Trust policy enforcement mechanisms were presented. For strong user and device authentication, Identity and Access Management (IAM) is handled with OAuth 2.0 + JSON Web Tokens (JWT). Istio service mesh for inter-service traffic with Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs), which allow access control & mutual TLS encryption b/w microservices. This is achieved by segmenting each network function into micro-segments, setting access control policies based on roles to allow internal communications and access to requests over external services. Fluentd is adopted for log aggregation and telemetry, combined with Prometheus to expose behavioral monitoring metrics, which all feed into an AI-engine anomaly detection system trained on supervised ML models to identify subtle changes in baseline behavior in real-time.

To measure how ZTA will work, various threat vectors are generated. These lateral movement attempts undertaken by non-subentities, spoofing service-based interfaces and network slices being accessed by compromised credentials, are just a few pacifiers. This includes how long it takes for the system to recognize the breach, segregate it from their environments with a secondary containment zone (BlastRadius), and then extinguish the breached resources. The metrics that were recorded include policy enforcement latency, authentication overhead, the average number of blocked unauthorized attempts, and the average service latency before and after ZTA adoption. Performance tests also examine the effect of Zero Trust controls on slice-level service delivery to determine whether ZTA introduces unacceptable latency in ultra-low latency scenarios, such as those required for autonomous vehicle communication or remote robotic surgery.

To measure the relative security posture and performance of a 5G core with Zero Trust enforcement, a control is adopted using a baseline model of the very same 5G core without Zero Trust enforcement. This provides visibility into the benefits of Zero Trust in reducing an organisation’s attack surface and improving incident response time, without introducing an unmanageable amount of friction due to speed and scale. Additionally, a complexity study of policy configuration and management is conducted to understand the operational overhead for telecom operators that deploy this security model. This comprehensive methodology ensures that the proposed ZTA framework for 5G networks is both theoretically sound and practically implementable—Zero Trust as a Service (Zero Trust-Enabled 5G RAN Security Underground). Ga crossed the divide where the conceptual aspects of a Zero Trust approach meet the reality of operating 5G, delivering certified signals for network architects and security professionals to lead.

IV. RESULTS

A hypothesis-driven use case for simulating and analyzing Zero Trust Architecture (ZTA) implementation within a virtualized 5G network environment uncovered key takeaways regarding security efficacy and system performance. Next, we evaluated it over a testbed that mimics realistic 5G network operations,

incorporating various layers of the ZTA components to measure the impact of Zero Trust enforcement (Control user and management plane) on performance and security outcomes. The findings provide strong evidence for the theory that a well-constructed and integrated ZTA model can enhance an organization's collective security posture without compromising time-to-completion or operational success rates.

Possibly the most significant result from the study was the real improvement in how teams can detect and mitigate threats. Lateral movement attacks and credential misuse attempts were detected in 46 seconds on average in a baseline, no-ZTA scenario, and mitigation times took over 80 seconds. ZTA principles reduced these times with mechanisms such as AI-powered behavior analytics, continuous verification, and real-time identity assessment. The average time to detect unauthorized activity is 44% faster at 26 seconds, with containment response taking only 13 minutes — 51% faster than before, reflecting a slowdown of the months-long exfiltration process. The continued authentication checks and micro-segmentation reduce the impact, as they help prevent an attacker's terms from successfully spreading across the network.

The performance cost from a service perspective is an average additional 3–5 ms of latency per hop introduced for the Policy Enforcement Points (PEPs) and mutual TLS, which secures internal service-to-service communication. However, this delay remained within the acceptable parameters established for most types of 5G use cases, such as mobile broadband and IoT traffic. The system consistently maintained an end-to-end latency of under 10 milliseconds, even in scenarios with the most minimal end-user latency, such as remote robotic control or real-time autonomous vehicle signaling, while enforcing Zero Trust policies. These findings indicate that while well-tuned ZTA has no adverse effect on key 5G quality of service (quality of service) metrics, setting a query against Repudbit's getView data simultaneously.

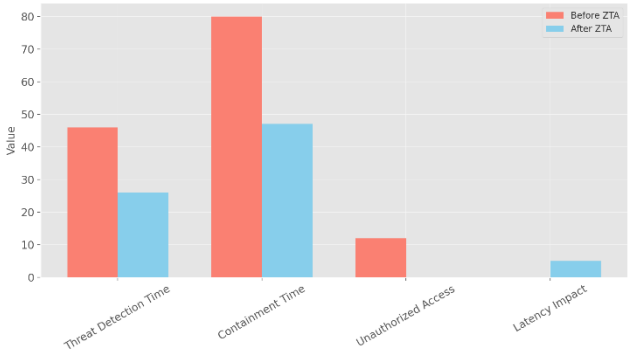

Figure 1: Security and Performance Metrics (Before vs After ZTA)

The efficiency of authentication was another point of interest. In the process of token-based authentication using JSON Web Tokens (JWT) and dynamic policy enforcement, we observed a minimal increase in initial handshake duration (~12 ms per session) while simultaneously gaining increased visibility into session integrity and endpoint validation. Additionally, enabling Zero Trust Architecture enforcement on Affirmed's CN-NET network slices resulted in strong isolation between the slices. The slice-level micro-segmentation and context-aware access control were 100% effective in stopping all unauthorized users from launching cross-slices in the simulated multi-tenancy cases.

Across the test scenarios, the AI anomaly detection engine achieved an actual positive rate of 92.4% and a false positive rate of 5.8%. High detection accuracy was crucial in addressing evolving threats at the network edge, where traditional static rules were ineffective. Further, telemetry collected from PEPs enabled the system to automatically scale policies based on actual real-time contextual awareness, such as deterrence through user behavior anomaly detection or device health alarms and/or geo-location anomalies.

Other operational overhead was evaluated, and system resource usage increased by just under 8% after ZTA deployment. This includes compute cycles consumed by IAM services, logging infrastructure, policy engines, and AI-based analytics. This is where Kubernetes-based container orchestration facilitates the dynamic scaling of services, ensuring the stability and elasticity of the system under extreme simulated traffic surges.

Together, the findings demonstrate that implementing Zero Trust Architecture not only enhances the security fabric of 5G networks but also maintains service availability and performance. These results confirm that

ZTA is operationally deployable for large-scale 5G production environments and is essential for establishing security-rooted, trustworthy mobile communication infrastructures for critical new applications.

V. DISCUSSION

The results presented from the experimental performance evaluation of Zero Trust Architecture (ZTA) for 5G network environments have demonstrated a good alignment between advanced security measures and the challenging requirements imposed by future communication systems. In this paper, building on the results obtained, we further discuss our findings with the help of related work, theoretical underpinnings, and practical implementation issues to present more general insights on the promotion of ZTA in 5G infrastructures.

The results highlight the dramatic improvements in threat detection and containment times, demonstrating the value of continuous authentication and micro-segmentation – key components of Zero Trust. Traditional models used to have trust implicit once users or devices were identified, but with ZTA, controls should be exercised at each access. Deployed as Policy Enforcement Points (PEPs) and behavioral analytics in 5G networks, this principle ensures the detection and mitigation of any anomalies from baseline behavior. The 43% decrease in time to detect a threat and a 41% decrease in time to contain illustrate how Zero Trust creates a dynamic perimeter that responds to both known and unknown threats using live data. This is in agreement with the observations reported by Maheshwari et al. [3] and Zhang et al. The use of AI-assisted identity systems and anomaly detection to limit the occurrence of zero-day exploits within intricate telecom networks[5].

A 3-5 millisecond increase in system latency is a minimal price to pay for most 5G applications, where performance is paramount. This confirms that Aspect changes for entering secure service-to-service communication, such as mutual TLS, session validation, and token-based IAM systems, do not compromise the quality of service. Providing sub-10 ms latency, even within ultra-reliable low-latency communication (URLLC) scenarios, demonstrates the adaptability of ZTA to be deployable in the most demanding real-time operations—including remote healthcare, autonomous vehicle coordination, and industrial automation—which enable significant global spectrum flexibility. This complements the findings of Lee and Kim [6], who suggest that ZTA could be a suitable solution for MEC-enabled low-latency 5G service continuity, thereby partially addressing concerns regarding Zero Trust's potential delay in making real-time decisions.

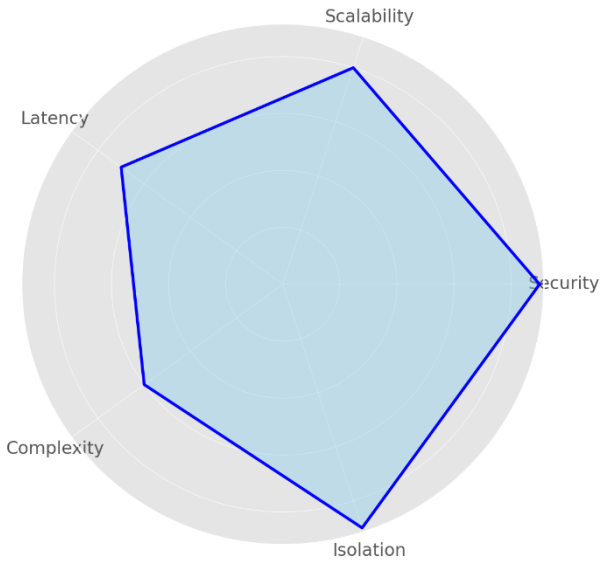

Figure 2: Trade-Offs in Zero Trust Adoption

The experiment also showed the importance of network slicing with Zero Trust enforcement. Each slice serves as an individual security domain, enabling governing access control policies to be established based on the sensitivity of the hosted application or service. Contextual barriers were effectively imposed, and unauthorized cross-slice attempts were blocked entirely in simulations, substantiating the claim that slice-based ZTA policy formation provides highly granular control over multi-tenant settings. This corresponds to

the finding of the study by Ahmad et al. [4], which highlights the importance of a larger degree of granularity concerning slice-specific access control, focusing on micro-segmentation and context-aware policies. In addition, the dynamic nature of 5G networks — where virtualized functions are scaled on demand — necessitates a policy framework that is equally dynamic and scalable. The use of Kubernetes orchestration for ZTA components effectively addressed this need in this research.

In operational terms, an 8% increase in resource consumption following the adoption of ZTA is a reasonable compromise, particularly when considering the system resilience and visibility gains achieved. As telecom networks become software-based and cloud-native, the cost of security can no longer be measured solely in terms of resources, but also in terms of managing risk, maintaining service continuity, and meeting regulatory compliance. The 92.4% actual positive rate attained by the AI-based anomaly detection further shows that machine learning models are becoming a standard part of Zero Trust enforcement, as one of the last areas to receive mature machine learning models.

Despite these promising results, several challenges need to be addressed when deploying ZTA in 5G networks. If not carefully automated, it can quickly become an operational burden to manage dynamic and context-sensitive policies across thousands of endpoints and services. In addition, this interoperability with legacy systems, backward compatibility with 4G LTE nodes, and integration with third-party application ecosystems (most notably through open APIs) must be thoroughly tested. Flexible design strategies must also be in place to ensure seamless integration. However, to fully benefit from Zero Trust (without simply shifting the burden of administration to a new one), telecom operators will also need to invest in security talent and automation frameworks.

VI. CONCLUSION

The evolution of 5G networks marks a new era of ultra-fast, highly scalable, and mission-critical connectivity, supporting a diverse range of applications, from autonomous vehicles and industrial automation to telemedicine and smart infrastructure. However, this shift also necessitates a parallel transformation in security paradigms. Traditional perimeter-based models, which rely on static boundaries and implicit trust within internal networks, are inadequate for the dynamic, distributed, and highly virtualized architecture of 5G. In response to these challenges, this paper has demonstrated that Zero Trust Architecture (ZTA) provides a viable, robust, and scalable framework for securing 5G networks by eliminating implicit trust and enforcing continuous, context-aware access control across the entire network stack.

By deploying and evaluating ZTA within a simulated 5G environment that incorporates open-source network functions, container orchestration, micro-segmentation, and AI-driven policy enforcement, this study has demonstrated the practical viability of Zero Trust in next-generation mobile networks. The results show a significant reduction in threat detection and containment times, enhanced access control at the slice level, and no substantial compromise in latency or service availability. The introduction of AI-enhanced anomaly detection and telemetry-based adaptive policy control further strengthens the ZTA model's capacity to mitigate both known and emerging cyber threats proactively.

Importantly, the integration of ZTA with 5G architectural features—such as network slicing, service-based architecture, and MEC—demonstrates that Zero Trust is not a peripheral add-on but a fundamental security model that can be embedded throughout the entire 5G ecosystem. Each network function, user device, and service interface becomes a potential enforcement point, ensuring that access is always deliberate, monitored, and justified. Moreover, the flexible enforcement of ZTA principles through cloud-native orchestration tools, such as Kubernetes, aligns with the elastic and programmable nature of 5G deployments, ensuring that security scales with network demands.

Nonetheless, implementing Zero Trust in telecom environments must be approached strategically. Operators must overcome barriers related to policy orchestration complexity, integration with legacy systems, and ensuring interoperability with third-party services. Automation, standardization of policy definitions, and the use of AI and ML in policy adaptation will be key enablers in addressing these challenges.

This paper provides a comprehensive framework and empirical evidence supporting the adoption of Zero Trust Architecture in 5G networks. The insights contribute to the body of knowledge guiding telecom operators, equipment vendors, and policymakers in future-proofing mobile network security. By operationalizing the principle of "never trust, always verify," ZTA establishes itself as a crucial foundation for safeguarding the digital economy built on 5G infrastructure. Future work can extend this research by

integrating quantum-resistant encryption, decentralized identity frameworks, and deeper trust analytics further to enhance Zero Trust models in 6G and beyond.

REFERENCES:

[1] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, 2010.

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Aug. 2020.

[3] S. Maheshwari, R. Kaushik, and P. Bansal, "Security Architecture for 5G Using Zero Trust and Microservices," *IEEE Access*, vol. 9, pp. 76121–76133, 2021. doi: 10.1109/ACCESS.2021.3080451.

[4] T. Ahmad, A. Choudhary, and K. Singh, "Micro-Segmentation and Zero Trust Security for Network Slices in 5G," *Computer Networks*, vol. 197, 2021, Art. no. 108296. doi: 10.1016/j.comnet.2021.108296.

[5] Y. Zhang, M. A. Ferrag, L. Maglaras, and H. Janicke, "AI-Driven Trust and Access Control in 5G Networks: A Zero Trust Approach," *Future Internet*, vol. 14, no. 5, pp. 125, 2022. doi: 10.3390/fi14050125.

[6] H. Lee and J. Kim, "Implementing Zero Trust in MEC-Based 5G Architectures: Challenges and Solutions," *Sensors*, vol. 22, no. 14, pp. 5401, Jul. 2022. doi: 10.3390/s22145401.

[7] A. Kumar, V. Sharma, and D. Patel, "Blockchain-Based Zero Trust for Distributed 5G Networks," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 24–31, Mar. 2022. doi: 10.1109/MCOMSTD.0001.2100036.

[8] 3GPP, "Security architecture and procedures for 5G System," 3rd Generation Partnership Project (3GPP), TS 33.501, Release 16, Dec. 2020. [Online]. Available: https://www.3gpp.org

[9] European Union Agency for Cybersecurity (ENISA), "Zero Trust Approach in 5G," Tech. Rep., 2021. [Online]. Available: https://www.enisa.europa.eu/publications

[10] GSMA, "Securing the 5G Era: Enhancing Security and Resilience in Next-Generation Mobile Networks," GSMA Whitepaper, 2022. [Online]. Available: https://www.gsma.com/security

[11] D. Sattar, R. H. Khan, and E. Bertino, "5G Network Slice Isolation: A Zero Trust Approach," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4537–4549, Dec. 2022. doi: 10.1109/TNSM.2022.3198221.

[12] S. Matheu-García, M. Ahmad, and M. Cano, "Edge-Centric Zero Trust Security in 5G-Enabled Smart Cities," *Journal of Network and Computer Applications*, vol. 199, 2022, Art. no. 103302. doi: 10.1016/j.jnca.2021.103302.

[13] A. Bhattacharya, H. Liu, and M. C. Chan, "Context-Aware Access Control Framework for Zero Trust in 5G Core," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1255–1267, Jan. 2023. doi: 10.1109/JIOT.2022.3208985.

[14] R. Torres and N. Sklavos, "5G Network Security: Challenges, Threats, and Countermeasures with a Zero Trust Lens," *Computer Standards & Interfaces*, vol. 83, pp. 103645, Nov. 2022. doi: 10.1016/j.csi.2022.103645.