Zero Trust in 5G Networks: Principles, Challenges, and Opportunities

Moyan Lyu, *Student Member, IEEE* and Junaid Farooq, *Member, IEEE*

***Abstract*—The deployment of fifth-generation (5G) networks across various industry verticals is poised to transform communication and data exchange, promising unparalleled speed and capacity. However, the security concerns related to the widespread adoption of 5G, particularly in mission-critical sectors, present significant challenges. This article investigates the potential of a Zero Trust (ZT) security philosophy as a viable countermeasure to these concerns. It delves into the practicalities of implementing ZT principles within 5G networks, with a specific focus on harnessing AI/ML technologies for proactive security measures, dynamic policy adaptations, and advanced risk assessments. Further, the article underscores the importance of developing a tailored ZT maturity model for 5G networks. Furthermore, the paper outlines key future research directions aimed at improving the ZT maturity of 5G deployments, contributing to the safe and secure integration of 5G technology in various sectors.**

I. Introduction

As the pivotal technological foundation for industrial transformation, 5G wireless technology is catalyzing digital advancement and enhancing global communication networks [1]. However, the promise of 5G extends far beyond the prospect of accelerated internet connections. It fosters unprecedented advancements across three fundamental areas: (i) the dramatic increase in speed to accommodate large data volumes, (ii) the reduction of latency for a more responsive network, and (iii) the capacity to link a wide range of devices concurrently.

Endpoint devices in a 5G network, often known as user equipment (UE), encompass an array of technology, from smartphones and tablets to the Internet of Things (IoT). These devices connect to the core network via the radio access network (RAN), consisting of radio base stations that bridge the gap between users and the network's heart. The core network (CN) effectively routes data from devices to their designated destinations, offering greater flexibility and seamless integration with Internet and cloud services. One of the most transformative aspects of 5G is the incorporation of edge computing, or multi-access edge computing (MEC), which significantly reduces latency by bringing computation and data storage closer to the areas they serve. This technological shift enables real-time interactions for demanding applications, enhancing the user experience and overall network efficiency.

5G and beyond networks usher in an era of groundbreaking capabilities, ranging from ultra-high data rates and superior reliability to minimal latency and increased device connectivity. These developments pave the way for innovative applications such as Industry 4.0, augmented and virtual reality (AR/VR), teleportation, and autonomous vehicles. To deliver on these promises, 5G and its successors leverage cutting-edge technologies like software-defined networks (SDN), network function virtualization (NFV), network slicing, and artificial intelligence (AI). These tools enable the creation of highly adaptable, programmable, and autonomously managed network infrastructures, adept at meeting the rigorous performance demands of future services.

Transforming network functions into software enhances portability and flexibility, facilitated by decoupling the control plane from the data forwarding plane in SDN. This strategic decoupling drives innovation through abstraction while also simplifying network management. NFV acts as the bedrock for dynamically distributing network functions across various areas as needed, eliminating the necessity for specialized hardware for individual functions or services. SDN and NFV dramatically improve network adaptability, streamline control and management, and move beyond the limitations of vendor-specific proprietary solutions. They are seen as crucial for the future evolution of networks. Nevertheless, despite these technological leaps, network security and user privacy remain significant challenges, necessitating vulnerability assessments and the development of countermeasures to these new security risks.

The key contributions of this article are threefold. It outlines the key cybersecurity challenges in 5G networks and identifies shortcomings in traditional defense mechanisms. It then provides an overview of the emerging ZT paradigm in cybersecurity and its implementation in the context of 5G networks. Finally, it presents an architecture for achieving ZT security in 5G networks

Moyan Lyu and Junaid Farooq are with the Department of Electrical & Computer Engineering, College of Engineering and Computer Science, University of Michigan-Dearborn, Dearborn, MI 48128 USA. E-mails: {moyanlyu, mjfarooq}@umich.edu.

This work was supported in part by the National Science Foundation (NSF) under Grant # ITE-2226232.

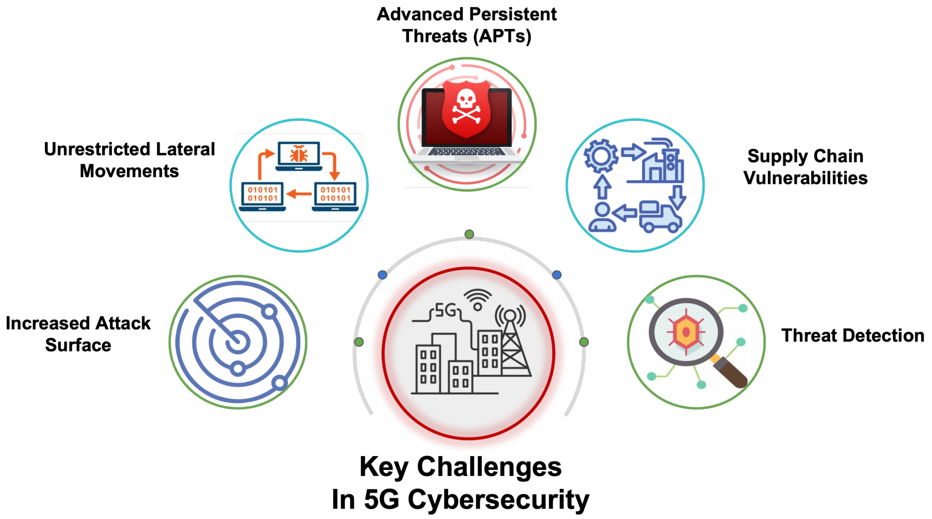
Advanced Persistent Threats (APTs)
Unrestricted Lateral Movements
Supply Chain Vulnerabilities
Increased Attack Surface
Threat Detection
5G
010101
010101
Key Challenges In 5G Cybersecurity

Fig. 1: Overview of key challenges in the cybersecurity of 5G Networks.

along with a review of key enabling functions and technologies.

II. Key 5G Security Challenges

While 5G offers unprecedented technological advancements and opportunities, its characteristics also introduce a higher degree of cybersecurity challenges than its predecessors [2]. Fig. 1 illustrates some of the key challenge areas in the cybersecurity of 5G networks.

A. Increased Attack Surface

The architecture of 5G networks inherently increases the attack surface for potential security threats. This is primarily due to its heavy reliance on virtualization and SDN technologies, which, while providing scalability and flexibility, also open up new avenues for security risks. 5G's extensive connectivity capabilities enable it to link a vast array of devices and IoTs, creating numerous potential entry points for cyber threats. Further, the implementation of new technologies like network slicing contributes to this expanded attack surface. In addition, the growing use of edge computing, which brings computation and data storage closer to the network edge, introduces further vulnerabilities and broadens the range of potential targets. Therefore, each connected device, network slice, and edge node represent potential access points for malicious actors, significantly increasing the attack surface compared to previous network generations.

B. Advanced Persistent Threats

Advanced persistent threats (APTs) are sophisticated, long-term cyber attacks orchestrated by highly skilled and motivated adversaries, such as nation-state actors or organized cyber criminal groups. These threats target specific organizations or entities to gain unauthorized access, extract sensitive information, or cause disruption [3]. In 5G networks, APTs can exploit the massive number of entry points and potential vulnerabilities. They can target vulnerabilities within network slices, potentially gaining unauthorized access to sensitive data or disrupting critical services. Moreover, APTs can target any weak link in this 5G ecosystem, including the supply chain, to gain unauthorized access or inject malicious code into network components.

C. Unrestricted Lateral Movements

Lateral movement is the ability of malicious actors or malware to move within a network once it has gained initial access [4]. In 5G networks, this can be a significant challenge since their inherent design allows high interconnectivity and supports a broad array of devices, which offers an attacker numerous potential paths for movement within the network after breaching one device or system. Additionally, attackers may exploit specific features such as network slicing and edge computing to gain access to multiple network slices and resources once they are inside the network. These lateral moves are much harder to detect since they typically leverage legitimate accesses.

D. Supply Chain Vulnerabilities

5G networks involve multiple vendors supplying hardware, software, and services, each with its own potential vulnerabilities. Furthermore, these networks often integrate third-party software and services to deliver

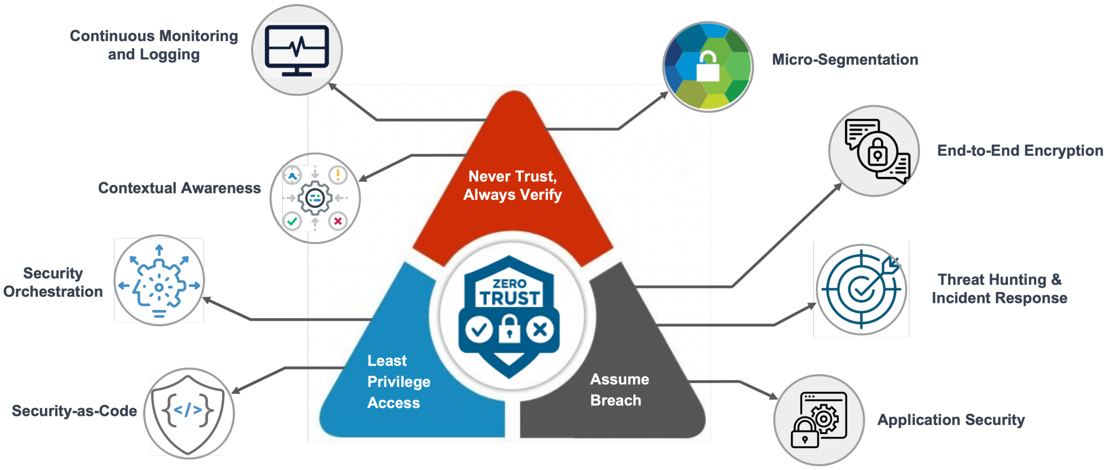

Fig. 2: Core principles of Zero Trust and implementation tenets.

advanced functionalities. However, the security practices of these third-party providers may not be up to par with the standards of the network operator, creating potential vulnerabilities [5]. Critical parts of the network, such as RAN, CN, and UEs, rely on hardware and firmware components, which can be tampered with or contain built-in vulnerabilities that can be exploited. Ensuring the integrity and authenticity of these components throughout the supply chain becomes critical, as tampered hardware can introduce vulnerabilities and compromise the security of the network.

E. Threat Detection

Threat detection is a key challenge for 5G cybersecurity due to the high volume, velocity, and variety of data generated. 5G networks generate a massive volume of data due to the increased number of connected devices and the high-speed data transfer capabilities. Analyzing this enormous volume of data in real-time to detect threats can be challenging, especially without sufficient human analysts. Also, the data in 5G networks is generated rapidly, requiring threat detection systems to process and analyze the data in near real-time. The speed at which data is generated demands efficient algorithms and scalable solutions that can keep up with the velocity of data. In addition, 5G networks consist of various configurations, vendors, data formats, and protocols. This diversity introduces complexity to threat detection because the security systems must be designed to handle and understand different types of data across different network environments.

III. Conventional Security Approach

Traditional cybersecurity mechanisms fail to cope with the emerging cyber threats and challenges of 5G networks. This section provides an overview of traditional cyber defense approaches.

A. Perimeter-based Defense

Traditional network security methods often rely on safeguarding network perimeters using tools such as firewalls and systems designed to prevent intrusion. These tools aimed to safeguard the network by creating a secure border between the internal networks we trust and the external networks that might pose a threat. However, this strategy is fraught with potential flaws that hackers can exploit. For example, as the number of services and applications grows, so does the complexity of setting up and maintaining this secure perimeter. This increased complexity makes the system more prone to errors, offering only a limited defense against threats from within the network and providing minimal insight into network traffic.

Moreover, the idea of a network ‘perimeter’ is becoming obsolete with the advent of 5G. The rise of cloud-based services, the trend towards remote working, the proliferation of internet-connected devices, and policies encouraging employees to bring their own devices to work, all contribute to broadening the potential avenues of attack, taking them beyond the scope of traditional defenses.

B. IP-based Access Control

Traditional defense mechanisms primarily rely on IP-based access control, fall short when interfacing with dynamic and sophisticated 5G networks. These systems often lack granularity, i.e., managing access control broadly based on IP addresses rather than focusing on individual users or devices. This approach hampers the ability to protect network resources effectively as it

Feature	**Traditional Defense**	**Zero Trust Security**
Trust Philosophy	Trust but verify	Never trust, always verify
Security Focus	*Perimeter-based, inside network is trusted*	*No implicit trust, verification needed at every point*
Resource Access	Generally unrestricted within network	Requires authentication and verification for every resource
Attack Exposure	High, once perimeter breached	Low, as each segment is independently secured
Adaptability to 5G	Limited, does not leverage the full potential of 5G	High, fully exploits the network slicing feature of 5G
Scalability	Challenge with growing network complexity	High, as each segment can be individually managed and secured

TABLE I: Comparison of Traditional and Zero Trust Security for 5G Networks

fails to differentiate between various activities from the same IP. Moreover, these defenses are typically unable to monitor intricate components like cloud workloads, processes, and applications. This limitation can pose significant security risks since 5G interactions are predominantly application-focused and data-driven. Furthermore, conventional methods frequently use pairwise access control, defining permissions between pairs of entities rather than ensuring comprehensive, end-to-end access control. As a result, proxies can bypass these controls, leading to potential security vulnerabilities.

IV. Preliminaries of Zero Trust

Traditional cyber defense approaches lack the ability to continuously monitor the network, meaning ongoing threats might go undetected for long periods of time, leaving the network exposed to advanced persistent threats. Also, these defenses are ill-equipped for end-to-end flow tracking, making it challenging to trace access history and verify compliance with established rules. These challenges necessitate more robust, dynamic, and fine-grained cybersecurity solutions that can cater to the complexity and demands of modern 5G networks. ZT is an innovative cybersecurity strategy developed to meet the increasing complexity and demands of modern network environments, including the emerging 5G networks [6]. Rejecting traditional reliance on network boundaries for security, ZT shifts focus to protecting data, assets, and services. This revolutionary approach operates on three fundamental principles [7]: “Never trust, always verify”, “Assume breach”, and “Least privilege access” as shown in Fig. 2. A summary of the key differences between traditional defense mechanisms and ZT security is provided in Table I. The following describes the core ZT principles and tenets for effective implementation.

A. Never Trust, Always Verify

This principle eliminates the notion of inherent trust based on a network location or prior access [8]. In the ZT model, each access request is treated as potentially malicious regardless of its origin. ZT requires continuous verification and validation of each user, device, and network component. This principle integrates *contextual awareness*, monitoring the situational and environmental factors of each access request, such as the time of the request, geographical location, and network behavior patterns. *Continuous monitoring and logging* of network activity facilitate real-time threat detection and aid in traceability during post-incident analysis. *Micro-segmentation*, another essential aspect of this principle, divides the network into smaller zones to control traffic flow, restrict lateral movement, and reduce the attack surface.

B. Assume Breach

This principle operates under the presumption that breaches can, and will, occur. This anticipation motivates a proactive approach to security. *Threat hunting and incident response* activities are integral to this principle, ensuring early detection of threats and rapid reaction to security incidents. *End-to-end encryption* is enforced to safeguard data integrity and confidentiality, even in the event of a breach. *Application security* measures such as secure coding practices, application firewalls, and real-time vulnerability scanning help protect applications from being the weak link in the security chain. This principle fosters a heightened state of alert, empowering organizations to minimize the impact of security incidents.

C. Least Privilege Access

This rule stipulates that users, devices, and network components should only have the minimal access rights required for their specific roles or tasks, thereby reducing the potential attack surface. *Security orchestration and automation* streamline the implementation of this principle, allowing for dynamic access management based on real-time context. This methodology also helps ensure rapid response and adjustments to changes in network behavior, roles, and access requirements. Furthermore, the practice of *security-as-code* allows for the integration of security measures early in the development lifecycle. By encoding security policies, compliance can be ensured programmatically, and security practices can be consistently applied across the entire digital infrastructure.

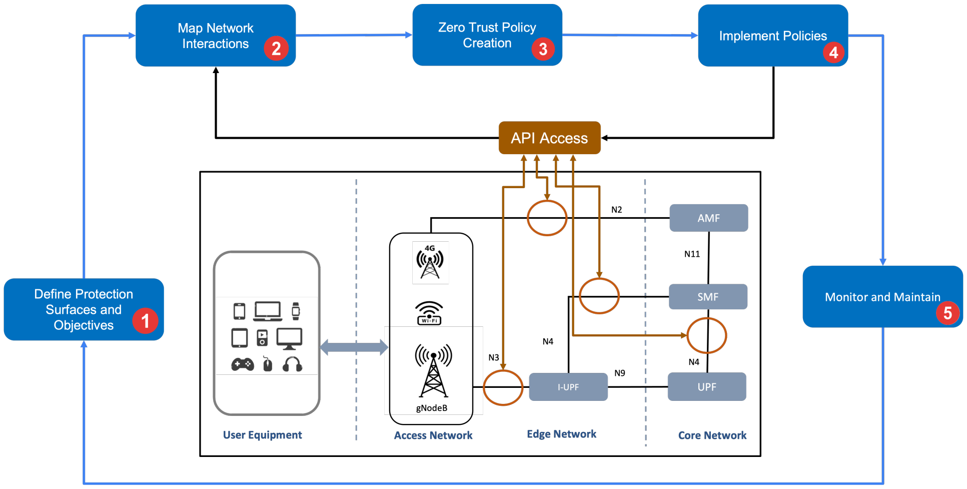

Fig. 3: Workflow of implementing ZT over 5G networks. The 5G network is accessed and controlled via API calls to the northbound interfaces in the core network.

V. Implementing ZT over 5G Networks

Implementing ZT over 5G networks requires a principled approach involving various enabling tools and technologies. We first present a workflow for implementing ZT in 5G networks, followed by a detailed architecture and components involved.

A. *Workflow for Zero Trust in 5G*

The following components form the ZT lifecycle, where the 5G network is accessed through APIs on various northbound interfaces as shown in Fig. 3.

1) Define Protection Surfaces and Objectives: The initial step in setting up ZT involves defining what must be protected - the devices, network interactions, and data. Each device represents a potential attack entry point, making their identification and monitoring vital [9]. Network scanning tools serve as indispensable aids to identify devices and understand typical traffic patterns. Moreover, categorizing data based on sensitivity level is crucial. For instance, customer information and intellectual property might require more stringent protection compared to public marketing materials. Tools like Asset Management Systems and access logs play a key role in maintaining a current inventory of devices and understanding access patterns. In mobile networks, the identity is associated with traffic flows, not merely an IP address. These identities, including Subscriber ID (or subscriber permanent identifier (SUPI)), Equipment ID (or permanent equipment identifier (PEI)), and Slice ID, provide critical details for monitoring and protection in 5G networks.

2) Map Network Interactions: Once the protection objectives are defined, it is essential to map how systems interact across the network. The movement of data and transactions, particularly concerning protected surfaces, dictates the required protection measures. Such an understanding is gleaned through network scanning and charting of transaction flows. The ZT approach espouses a flow-centric architecture. Flow maps, reflecting the design and operation of systems, highlight areas where controls must be inserted.

3) Zero Trust Policy Creation: Following the network architecture, the supporting ZT policies must be created, detailing the who, what, when, where, why, and how of network access and actions. Policy frameworks in 3GPP-based systems are used to regulate access across different security domains. The policies also guide the implementation of authentication and authorization procedures and the establishment of secure communication channels. In the 5G service-based architecture (SBA), ZT principles identify network function (NF) service consumers and producers, improving communication security significantly over previous generations of mobile networks.

4) Implementation of Policies: Policy implementation within a ZT framework involves an intricate process, carefully curated to meet a network's unique needs. This stage starts with establishing role-based access control (RBAC), granting access privileges per individual role to align with the principle of least privilege. The incorporation of end-to-end encryption and network micro-segmentation further secures sensitive data and isolates potential threats. The policies also include robust application security measures, ranging from regular vulnerability assessments to the deployment of application firewalls. To keep up with the dynamic network environments, security measures are automated using security orchestration and security-as-code practices. These automated systems enforce and update ZT policies in real-time. Lastly, the definition of policy enforcement points, such as access and mobility management function (AMF) in 5G networks, is crucial to enforcing access controls effectively.

5) Monitor and Maintain: The final and ongoing step is to monitor and maintain the network. This involves a continuous review of all internal and external logs up to Layer 7 and focusing on the operational aspects of ZT. A ZT network requires all traffic to be inspected and logged. Implementing ZT may involve a continuous diagnostics and mitigation (CDM) system, which continuously monitors digital assets' status and applies necessary updates. Threat Intelligence Feeds provide updates about new threats, informing policy decisions. Meanwhile, security information and event management (SIEM) Systems collect security-centric information for policy refinement.

B. A Zero Trust Security Architecture for 5G

A ZT architecture specifies the interconnection of various network functions, tools, and data sources needed to achieve ZT in 5G [10]. An overview of the main components involved is shown in Fig. 4. The three core functions of this architecture are as follows:

1) Continuous Monitoring: The concept of continuous monitoring forms a pivotal pillar in the establishment and maintenance of a ZT security architecture. It consists of four critical functions as follows:

- **Network Scanning:** This involves the use of *observability tools* and technologies to identify all the devices connected to the network. Network scanning extends beyond traditional computers and servers to incorporate various network hardware and IoT devices along with individual processes, workloads, and interactions in the cloud, providing a comprehensive view of the network landscape. By understanding what devices are present on the network, potential vulnerabilities can be better identified and addressed.
- **End-to-end Micro-segmentation:** After network scanning generates a comprehensive inventory of components in a 5G network, the subsequent step involves decoding communication patterns among these components. The network scanning results then allow for multiple segmentation strategies. For instance, grouping similar device types, like smartphones or IoT devices, into one segment allows tailoring of specific security policies to their unique characteristics and vulnerabilities. Moreover, segmentation could also hinge on user roles or access levels, with administrators, regular employees, or guests having distinct device groupings.
- **Access Provisioning:** Once the identity is verified, the network evaluates the user or device's access rights based on pre-defined roles or policies. These policies can be dynamically adjusted based on real-time network conditions, ensuring stringent security and flexibility. Advanced technologies such as artificial intelligence and machine learning can further bolster access provisioning by continually monitoring and learning from network behavior, enabling adaptive and proactive access control.
- **Zero Trust Compliance:** ZT compliance checking in 5G networks can be conducted by leveraging AI and machine learning (ML) algorithms. These algorithms can observe network activities, configurations, and cross-verify them with established ZT principles, continually ensuring that only validated users and devices have access to network resources. Compliance checks can also extend to the implementation of micro-segmentation, wherein the network is divided into separate zones, and all communication across these zones is treated as untrusted.

2) Data Analytics: This core function involves analyzing the collected metadata from the network and assessing for potential vulnerabilities. The main components involved are as follows:

- **Threat Modeling:** Threat modeling in 5G networks can be efficiently performed using the MITRE adversarial tactics, techniques & common knowledge (ATT&CK) [11] and 5G hierarchy of threats (FiGHT) [12] frameworks. The MITRE ATT&CK framework provides a comprehensive matrix of adversarial tactics, techniques, and procedures (TTPs) that attackers may utilize across the lifecycle of an attack. By leveraging this matrix, security teams can emulate potential cyber threat scenarios, predict possible vulnerabilities in the 5G architecture, and develop robust mitigation strategies. On the other hand, the FiGHT Matrix is a specific cybersecurity dataset that can be utilized to train machine learning models to recognize and anticipate various cyber threats in a 5G environment.
- **End-to-End Risk Assessment:** Once the risks are identified, their impact and likelihood are analyzed to calculate the overall risk level. Mitigation strategies are then proposed based on the calculated risk, prioritizing higher risks first. As 5G networks are inherently dynamic, the risk assessment is not a one-off process but a continuous one, requiring regular reassessment to ensure newly introduced vulnerabilities are identified and mitigated promptly. AI and ML technologies can greatly enhance the efficiency and effectiveness of risk assessments by automating data analysis and detection of anomalous

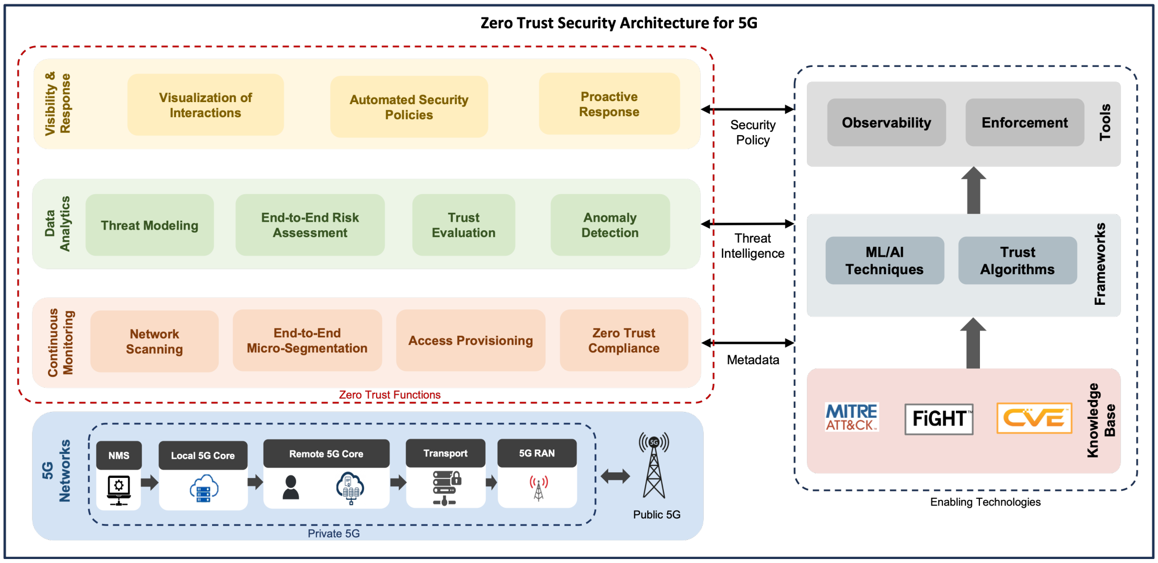

Fig. 4: A Zero Trust architecture for 5G networks mapping functions and enabling technologies.

patterns. In summary, end-to-end risk assessment in 5G networks is a crucial process that promotes network security by identifying, evaluating, and addressing potential vulnerabilities throughout the network.

- **Trust Evaluation:** User behavior, device characteristics, data transmission patterns, and other relevant parameters are continuously monitored and analyzed. Anomalies and unusual patterns in these factors could suggest potential security threats, triggering further examination. Additionally, trust evaluation may incorporate the assessment of network elements like user equipment, software applications, and network nodes [13]. This involves examining their security attributes, operational behavior, past activity logs, and adherence to security policies and procedures. Any deviations or anomalies can lead to a decrease in trust score, and in some cases, may prompt re-authentication or revoking of access privileges.
- **Anomaly Detection:** Regular traffic flows, user behavior, and standard device interactions have a specific pattern. Once these baseline patterns are established, the system can then identify any deviations from the norm, which could indicate potential security threats or anomalies. For example, unusual traffic spikes, unfamiliar devices accessing the network, or unexpected changes in user behavior could all be flagged as anomalies. In a 5G network, the high-speed, low-latency characteristics allow for real-time data analysis and immediate anomaly detection, enabling swift and proactive response to potential security incidents.

3) Visibility and Response: The third main function focuses on understanding the network's operations, generating security policies, and enabling proactive responses.

- **Visualization of Network Interactions:** Having visibility into the interactions between network devices, processes, and workloads is crucial to understanding the network dynamics of. Visualization tools can provide a clear picture of network activity, making identifying potential vulnerabilities or ongoing threats easier.
- **Automated Generation of Security Policies:** AI/ML algorithms can analyze various factors such as user behavior, device characteristics, location data, and contextual information to establish continuous authentication. By continuously evaluating and verifying user identities and device integrity, networks can ensure access privileges are granted based on real-time assessments rather than relying solely on initial authentication [14].
- **Proactive Response:** This function enables the system to react to identified threats promptly. A proactive response can limit the impact of an attack, ensuring quick recovery and preventing further damage. This is enabled through advanced security systems capable of detecting threats early and responding swiftly and effectively.

VI. Future Research Directions

To tackle the burgeoning security challenges inherent in complex 5G networks, several research directions are recommended to enhance current practices and explore novel solutions.

A. Refining Proactive Security Measures

While AI/ML has been instrumental in advancing proactive security, there is a need for more in-depth exploration to enhance their predictive accuracy and speed. Future research can focus on integrating multidimensional data sources, such as user behaviors, network traffic patterns, and application interactions, to enhance the models' contextual awareness and threat prediction capabilities. Emphasis can be placed on interpreting the complexities of 5G-specific attack vectors and exploiting the potential of real-time analytics.

Enhanced threat modeling frameworks could also be a focus area, aiming to deepen the understanding of the attack lifecycle and develop anticipatory security mechanisms. Refining the integration of databases like CVE into AI/ML models could offer real-time threat intelligence, while concurrently updating the AI/ML models to counter emerging threats.

B. Advanced Dynamic Policy Adaptation

Future research can delve deeper into the realm of dynamic policy adaptation, focusing on improving real-time risk evaluation and policy modification. Research could be directed towards the development of AI/ML models that can understand and respond to changes in the network environment, user behaviors, and real-time threat intelligence. As 5G networks become more complex and dynamic, developing intelligent, automated policy adaptation mechanisms could be a game-changer. Efforts can be made to decentralize AI capabilities across the network, enabling dynamic policy adaptation at the edge while ensuring overall network security. This could potentially increase the network's resilience, reducing latency and the time taken to respond to threats.

C. Next Generation AI-Based Risk Assessment

Future work could be directed towards optimizing AI-based risk assessment methodologies. The goal could be to build predictive models capable of accurately forecasting potential threats by integrating various data types, such as network patterns, user behaviors, and device states. Research could be focused on real-time risk assessment, aiming to develop AI models that can assess, prioritize, and respond to threats as they emerge. The development of explainable AI for risk assessment can help elucidate the AI's decision-making process, fostering trust and reliability. Moreover, understanding the interconnectedness of risks across various domains is an unexplored research area. Cross-domain risk assessment can offer a comprehensive understanding of the threat landscape, helping in the development of holistic security measures.

D. Developing a 5G-Specific Zero Trust Maturity Model

An essential future research direction could be the development of a ZT Maturity Model tailored specifically for 5G networks [15]. The model could serve as a road map for organizations, providing a structured approach towards the full implementation of ZT principles in their 5G network. This maturity model could detail stages of ZT adoption, from initial understanding and planning to full integration into 5G infrastructure and operational processes. The model could also factor in the automation of processes via AI/ML, facilitating efficient threat detection, policy enforcement, and continuous adaptation to the changing threat landscape. Developing such a maturity model requires collaboration among industry stakeholders, academic researchers, and regulatory bodies. This cooperative effort can lead to a robust framework that ensures the security, resilience, and trustworthiness of future 5G networks.

VII. Conclusion

The forthcoming years will witness a significant proliferation of 5G networks across a myriad of industry sectors. These advancements, while promising, bring forth considerable cybersecurity challenges, potentially hampering the broad integration of 5G networks into mission-critical applications. It is in response to these concerns that the ZT philosophy emerges as a viable and proactive approach in the domain of cybersecurity. In this article, we have delved into the intricate process of implementing ZT principles over 5G networks. We examined the potential role of AI/ML in refining proactive security measures, advancing dynamic policy adaptations, and improving risk assessments. We further discussed the necessity of developing a ZT maturity model specifically tailored to 5G networks. Notably, this study underscores that while significant progress has been made in aligning 5G networks with ZT, there remains an ample scope for future research. Key areas include refining AI/ML for improved security insights, enhancing real-time threat response, creating robust cross-domain risk assessment models, and designing a comprehensive 5G-specific ZT maturity model. By exploring these avenues, we can navigate the cybersecurity challenges posed by the evolving 5G landscape, ultimately enabling a safe and secure adoption of 5G technology across all sectors.

References

[1] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201–1221, 2017.

[2] N. I. of Standards and T. (NIST), "5G cybersecurity volume b: Approach, architecture, and security characteristics," NIST Special Publication, Tech. Rep. 1800-33B, 2022. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf

[3] J. Liu, Y. Shen, M. Simsek, B. Kantarci, H. T. Mouftah, M. Bagheri, and P. Djukic, "A new realistic benchmark for advanced persistent threats in network traffic," *IEEE Networking Letters*, vol. 4, no. 3, pp. 162–166, 2022.

[4] H. A. Kholidy, A. Karam, J. Sidoran, M. A. Rahman, M. Mahmoud, M. Badr, M. Mahmud, and A. F. Sayed, "Toward zero trust security in 5G Open architecture network slices," in *IEEE Military Communications Conference (MILCOM 2022)*, 2022, pp. 577–582.

[5] National Institute of Standards and Technology (NIST), "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," National Institute of Standards and Technology, Tech. Rep. NIST SP 800-161 Rev. 1, April 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

[6] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57 143–57 179, 2022.

[7] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," Available from: https://csrc.nist.gov/publications/detail/sp/800-207/final, National Institute of Standards and Technology, NIST Special Publication 800-207, 2020.

[8] C. Benzaïd, T. Taleb, and M. Z. Farooqi, "Trust in 5G and beyond networks," *IEEE Network*, vol. 35, no. 3, pp. 212–222, 2021.

[9] Y. Ge and Q. Zhu, "MUFAZA: Multi-source fast and autonomous zero-trust authentication for 5G networks," in *IEEE Military Communications Conference (MILCOM 2022)*, 2022, pp. 571–576.

[10] K. Ramezanpour and J. Jagannath, "Intelligent Zero Trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Computer Networks*, vol. 217, p. 109358, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128622003929

[11] MITRE, "MITRE adversarial tactics, techniques, and common knowledge (ATT&CK)," 2023. [Online]. Available: https://attack.mitre.org/

[12] MITRE, "5G hierarchy of threats (FiGHT)," https://fight.mitre.org, 2022.

[13] S. Huang, Z. Zeng, K. Ota, M. Dong, T. Wang, and N. N. Xiong, "An intelligent collaboration trust interconnections system for mobile information control in ubiquitous 5G networks," vol. 8, no. 1, 2021, pp. 347–365.

[14] C. Benzaïd and T. Taleb, "AI for beyond 5G networks: A cybersecurity defense or offense enabler?" *IEEE Network*, vol. 34, no. 6, pp. 140–147, 2020.

[15] Cybersecurity and I. S. A. C. Division, "Zero trust maturity model version 2.0," Cybersecurity and Infrastructure Security Agency, Tech. Rep., 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf