5thGeneration Security and Zero Trust Importance

Subjects: Telecommunications

Contributor: Paul Scalise , Matthew Boeding , Michael Hempel , Hamid Sharif , Joseph Delloiacovo , John Reed

The expansion of 5G technologies has ushered in a new era of communications with promises for high-speed mobile broadband communications, ultra-low latency applications, massive device connectivity, Internet of Things (IoT) support, and more. As 5G usage and coverage continue to increase in the near future for industries and consumers alike, it also brings with it a new range of security challenges and considerations.

5G security survey Zero Trust architecture confidentiality integrity availability

1. Security Focuses in 5thGeneration

To enhance the security of 5thGeneration (5G) cellular networks, 3rd Generation Partnership Project (3GPP) released an updated Technical Standard (TS) 33.501 [1] for security architecture and procedures. The security architecture through three different strata and six separate security domains are outlined, as shown in **Figure 1**. These security domains and the sections of this research that discuss their respective research areas are listed below:

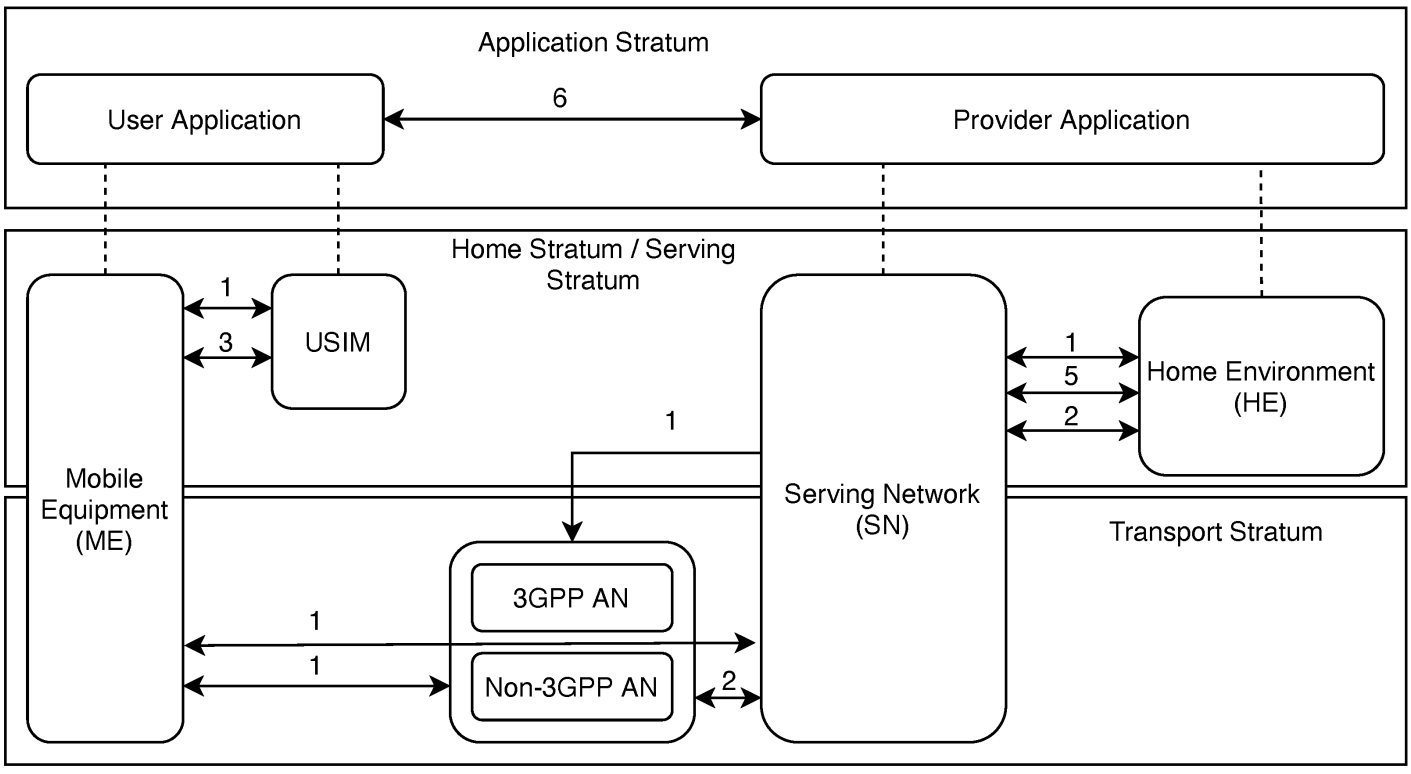

Figure 1. 3GPP security domains defined in TS 33.501. The interfaces are relative to the list 1–6 above.

(1) Network Access Security focuses on UE authentication and secure network services access with a particular focus on attacks against the physical/radio interface. This domain includes both 3GPP and trusted non-3GPP access and the access security between the Serving Network (SN) and Access Network (AN). In the context of this research, sections covering authentication, 5G access, RAN, and UE physical layer security will review the current state of research in each of these areas. These sections will outline current research enhancements, vulnerabilities, and future research directions to align with the TS 33.501 standard.

(2) Network Domain Security encompasses security for network nodes that enables the secure exchange of signaling data and user plane data. Sections covering the topics of non-3GPP co-existence, SDN, NFV, and MEC will discuss research in this domain later in this research.

(3) User Domain Security contains the security features that secure the user's access to mobile equipment. Discussed later are general resources and security measures listed by the National Institute of Science and Technology (NIST) on identifying areas of concern for user security at the device end.

(4) Application Domain Security entails security for the user domain to the application provider domain in order to be able to exchange messages securely. Application domain security is not within the scope of TS 33.501, but this research will discuss blockchain technology and post-quantum cryptography for applications specific to 5G networks.

(5) Service-Based Architecture (SBA) Domain Security is the set of security features that enables network functions to securely communicate within the serving network domain and with other network domains. Such features include network function registration, discovery, and authorization security aspects as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to TS 33.401 [2]. These security features will be discussed in the SBA section with specific subsections corresponding to the various network functions in a 5G system.

(6) Visibility and Configurability of Security spans the set of features that inform the user whether a security feature is in operation. Visibility and configurability are mentioned within this survey in the sections discussing the user equipment, the Core Network, and O-RAN (Open-RAN).

2. 5thGeneration Security Research

As 5G expands its presence worldwide, the scientific literature evaluating the security aspects of 5G has grown, especially regarding surveys into specific areas of 5G's implementation. For example, in [3], the current research and challenges of security for different aspects of cloud services, RAN, MEC, and network slicing are investigated. The insights presented in this research are focused on the need to deploy future 5G networks while taking great care of the vast security aspects. Understanding that these networks will serve applications to a wide range of

consumers, they need to provide adaptability, resilience, and flexibility, embodied and provided by Software-Defined Networking (SDN) and Network Function Virtualization (NFV), in order to be able to provide and enforce comprehensive security measures. The authors of [4] focus their security research on access, handover, IoT, D2D, V2X, and 5G network slicing, whereas in [5], the focus is on architecture and design, attacks on 5G, physical security, and V2X. Both of these publications showcase potential vulnerabilities to the security mechanisms within architecture, specifically for authentication and network slicing, and thereby emphasize the need for more fine-grained security control in the network. A comparative analysis of 5G security mechanisms is discussed in [6][7], which includes a wide survey into the overall 5G security framework, Core Network, Radio Access Network, cloud infrastructure, and the Internet of Things. IoT protocols for 5G are reviewed in [8]. An overview of the threats to, and vulnerabilities of, both 5G and 6G, is presented in [9] with a specific focus on SDN, NFV, and MEC in 5G networks. The security issues of network coexistence are investigated in [10] with a focus on 5G/6G coexistence with WiFi 6. Application-specific attacks are outlined in [11] with a focus on cyber–physical systems, fog computing, and SDNs. The contributions from these primary surveys showcase the need for continued research and a strong focus on improving the adoption and implementation of security mechanisms. For confidential communication and heightened network monitoring and security, a Zero Trust Architecture (ZTA) is recommended, particularly in a 5G setting. ZTA opens the door for operations in which the assumption is that the attacker is always one step ahead of the fix or patch to a network issue.

3. Zero Trust Importance

ZTA focuses on a shift in security perspective from perimeter defense to defending each transaction within a network [12]. It is built around the assumption that the attacker may already have penetrated into the network and established a foothold. In ZTA environments, therefore, each transaction is individually scrutinized to ensure the integrity of every communication attempt and enforce strict policy compliance. This shift in network security is vitally important to 5G networks that inherently operate in an untrusted environment [13]. The added security of a ZTA can be used for a variety of applications, including military applications shown in [13][14]. **Table 1** lists and describes the tenets of ZTA provided by the National Institute of Science and Technology (NIST), including backbone considerations for the deployment of a ZTA system.

Table 1. ZTA tenets.

Zero Trust Architecture Tenets from NIST [12]	
Tenet	**Explanation**
(1) “All data sources and computing services are considered resources”.	A network can comprise different classes of devices, which can have different footprints and functions. A personal device can also be seen as a resource if it can access the enterprise-owned network.
(2) “All communication is secured regardless of network location”.	Any equipment attempting to obtain access to a network, whether on-site or remote, must be authenticated. Network location alone does not imply trust. Confidentiality and integrity need to be protected.

Zero Trust Architecture Tenets from NIST [12]	
Tenet	**Explanation**
(3) “Access to individual enterprise resources is granted on a per-session basis”.	Prior to accessing an asset, the user will be identified and verified. Only the minimum resources should be given in order to complete a task. Successful authentication and access to one resource does not grant access to other resources on the network without further permissions.
(4) “Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes”.	It is necessary for an organization to protect resources by defining what resources it has, who its members are, and what access to resources those members need. Requesting asset state can include device characteristics such as software versions installed, network location, time/date of request, previously observed behavior, and installed credentials. Resource access and action permission policies can vary based on the sensitivity of the resource/data.
(5) “The enterprise monitors and measures the integrity and security posture of all owned and associated assets”.	No access within the network or remote can be inherently trusted. Devices should be monitored using continuous diagnostics and mitigation (CDM), and patches/fixes should be applied when necessary. Devices that do not match this criteria can be completely rejected from making any connections with the network.
(6) “All resource authentication and authorization are dynamic and strictly enforced before access is allowed”.	A ZTA needs to be adaptive and continually reevaluate trust with devices and their open sessions. Identity, Credential, and Access Management (ICAM) and asset management systems are an expectation of the ZTA. Continual monitoring with possible reauthentication and reauthorization occurs throughout user transactions, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.
(7) “The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture”.	Any data on the network that can be captured should be. This allows for the improvement of the policy creation and enforcement.

unity ever since the term was coined in 1994 by Stephen Paul Marsh [15]. Since then, the idea of limiting the trust shown to users of a network or networked resource to zero has gained popularity, especially over the past few years. **Figure 2** shows the rapid increase in publications that mention the term ‘Zero Trust’ per year, giving weight to ZTA and the exploration of its feasibility in real-world deployments across different network and application implementations. This search was conducted using Google Scholar with the search phrase of “network, security, “zero trust” -game -health -mechanical”. The negated words are used to exclude publications that are not within this domain of literature. Topics akin to the excluded keywords initially showed up in the study but were excluded after their relevance was seen to be outside of this search domain. Researchers then looked at the incorporation of both ZTA and 5G/6G in publications and see a similar growth in interest in the past few years. **Figure 3** illustrates the increasing amount of publications including ZTA and 5G/6G, providing more weight to the importance of ZTA and the discovery of applications in a 5G or 6G network environment with each category growing in popularity at a rate that is nearly doubling year-over-year. This search was similarly conducted using Google Scholar with the search phrase of “network, security, 5G OR 6G, ‘zero trust’ -game -health -mechanical”.

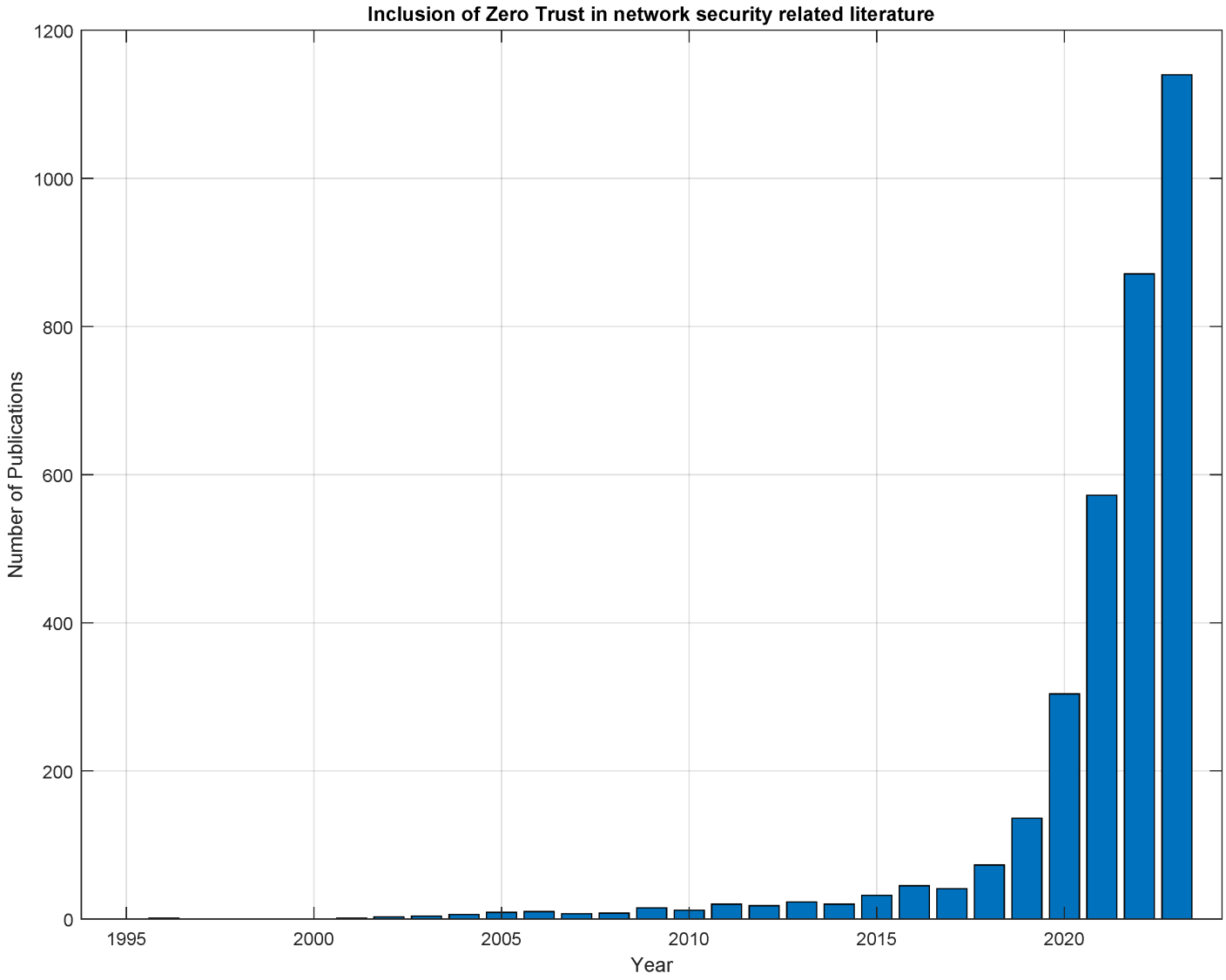

Figure 2. Mentions of the term ‘Zero Trust’ in network security oriented research publications starting from the year 1994.

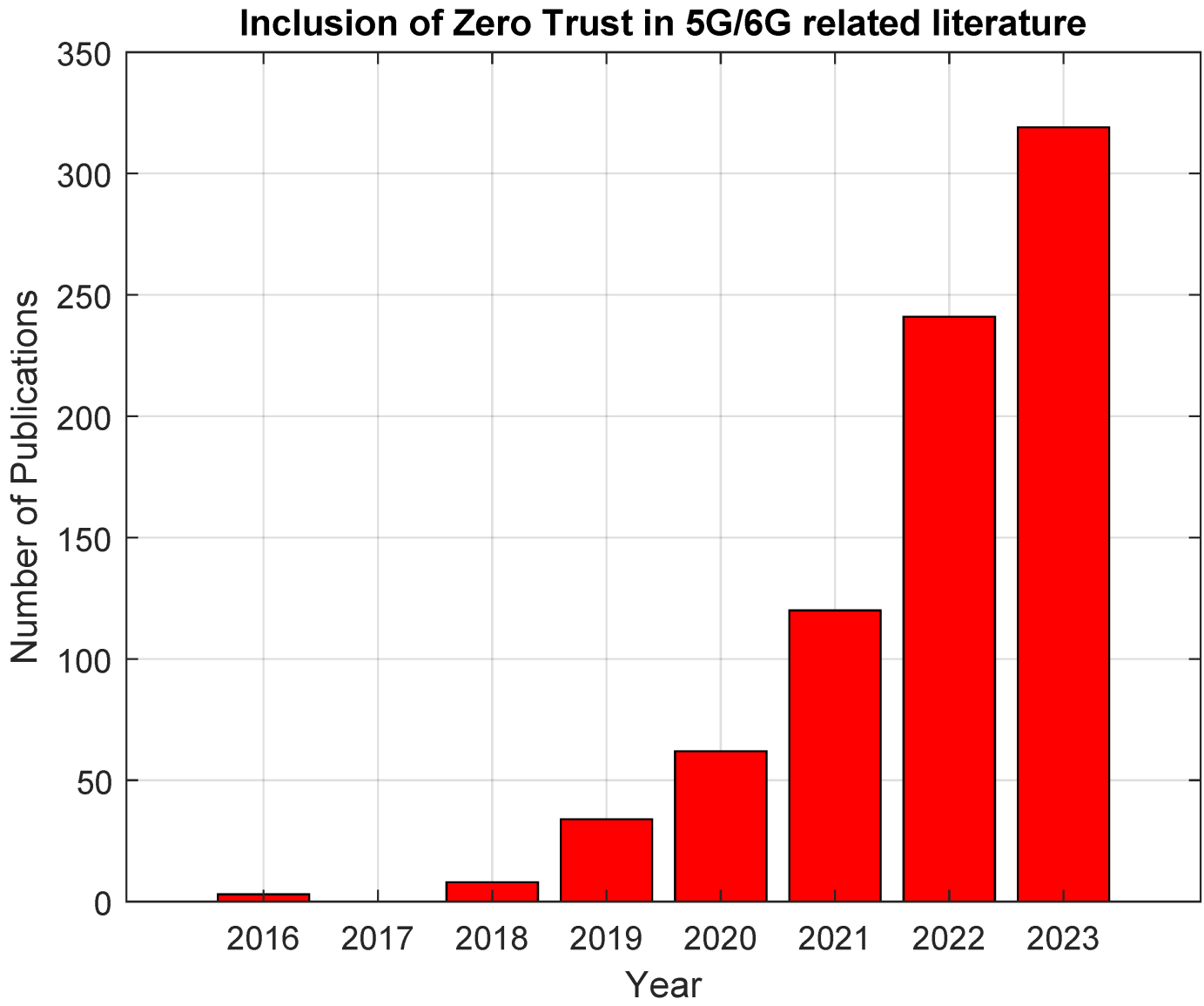

Figure 3. Mentions of the term 'Zero Trust' in conjunction with either 5G or 6G in network security-oriented research publications, starting from the year 2016.

References

1. TS 33.501; Security Architecture and Procedures for 5G System. 3GPP: Valbonne, France, 2023. Available online: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/ (accessed on 10 August 2023).
2. TS 33.401; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evoltuion (SAE); Security Architecture, Release 17, V17.4.0. 3rd Generation Partnership Project: Valbonne, France, 2023.

3. Dutta, A.; Hammad, E. 5G Security Challenges and Opportunities: A System Approach. In Proceedings of the 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 10–12 September 2020; pp. 109–114.
4. Cao, J.; Ma, M.; Li, H.; Ma, R.; Sun, Y.; Yu, P.; Xiong, L. A Survey on Security Aspects for 3GPP 5G Networks. IEEE Commun. Surv. Tutor. 2020, 22, 170–195.
5. de Castro Nunes Borges, V.O.; Rosa, R.L. General Aspects of Information Security in 5G Networks: Survey. Available online: https://infocomp.dcc.ufla.br/index.php/infocomp/article/view/3072 (accessed on 16 February 2024).
6. Sachdeva, T.; Kumar, S.; Diwakar, M.; Singh, P.; Pandey, N.K.; Choudhary, S. Comparative Analysis of 5G Security Mechanisms. In Proceedings of the 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 3–4 March 2023; pp. 1–4.
7. Zhang, S.; Wang, Y.; Zhou, W. Towards secure 5G networks: A Survey. Comput. Netw. 2019, 162, 106871.
8. Tashtoush, Y.; Darweesh, D.; Karajeh, O.; Darwish, O.; Maabreh, M.; Swedat, S.; Koraysh, R.; Almousa, O.; Alsaedi, N. Survey on authentication and security protocols and schemes over 5G networks. Int. J. Distrib. Sens. Netw. 2022, 18, 15501329221126609.
9. Ounza, J.E. A taxonomical survey of 5G and 6G security and privacy issues. Glob. J. Eng. Technol. Adv. 2023, 14, 042–060.
10. Ramezanpour, K.; Jagannath, J.; Jagannath, A. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. Comput. Netw. 2023, 221, 109515.
11. Park, J.H.; Rathore, S.; Singh, S.K.; Salim, M.M.; Azzaoui, A.; Kim, T.W.; Pan, Y.; Park, J.H. A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions. Hum.-Centric Comput. Inf. Sci. 2021, 11.
12. Stafford, V. Zero trust architecture. Nist Spec. Publ. 2020, 800, 207.
13. Ramezanpour, K.; Jagannath, J. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. Comput. Netw. 2022, 217, 109358.
14. Bhardwaj, A. 5G for Military Communications. Procedia Comput. Sci. 2020, 171, 2665–2674.
15. Marsh, S.P. Formalising Trust as a Computational Concept. Available online: https://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf (accessed on 16 February 2024).