IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 June 2024, accepted 28 June 2024, date of publication 9 July 2024, date of current version 18 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3425350

SURVEY

A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks

NURUN NAHAR, KARL ANDERSSON, (Senior Member, IEEE), OLOV SCHELÉN, (Member, IEEE), AND SAGUNA SAGUNA
Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 931 87 Skellefteå, Sweden

Corresponding author: Nurun Nahar (nurun.nahar@ltu.se)

This research work has been financially supported by the Interreg Aurora program and the Arctic 6G project, award no. 20357901.

ABSTRACT As sixth-generation (6G) cellular networks emerge, promising unparalleled connectivity and capabilities, yet it amplifies concerns regarding security vulnerabilities. These networks include a broader array of devices and sensors compared to earlier generations, increasing the potential for attackers to exploit weaknesses. Existing security frameworks contribute to safeguarding enterprises against external threats that originate beyond the network perimeter. These frameworks operate under the assumption that all entities inside the defined perimeters are reliable, and their primary objective is to authorize access to resources based on assigned roles and permissions. However, this strategy could be more effective today since attacks might originate from any source, including within the network perimeter. To address this issue, a zero-trust architecture (ZTA) could be a potential solution that assumes neither users nor devices can be inherently trusted, and it consistently evaluates potential risks to decide whether to allow access to resources. This article will explore the zero-trust approach and its significance in contemporary network security. We describe the role of authentication and access control in ZTA and present an in-depth discussion of state-of-the-art authentication and access control techniques in different scenarios. This article examines the applicability of the zero-trust concept in 6G networks and analyzes the associated challenges and opportunities. This article also examines case studies demonstrating the practical application of the zero trust paradigm in 6G or comparable networks. It explores the research scope and tries to identify relevant research gaps in this area.

INDEX TERMS Zero-trust architecture, 6G networks, multi-factor authentication, perimeter-based security.

I. INTRODUCTION

The arrival of 6G technology marks the beginning of an exciting new age in wireless communication, which is set to transform connectivity like never before. With anticipated data speeds reaching a staggering ten terabits per second and minimal latency, this technology is poised to redefine the boundaries of what is possible in communication [1]. Its expansive network coverage and advanced features promise to unlock many opportunities across diverse applications. The integration of robust artificial intelligence alongside support for emerging technologies such as augmented reality and virtual reality holds the potential to reshape industries and elevate user experiences to unparalleled heights. It is projected to fuel innovation across multiple sectors, for example, enhanced mobile broadband to advanced health-care services, innovative infrastructure, and autonomous vehicles [2]. As the demand for data continues to surge, this technology aims to meet this growing need through innovative utilization of higher frequency bands and spectrum resources. The proliferation of connected devices is expected to soar, with projections indicating a staggering 43 billion connected devices by 2023 [3]. Furthermore, the collective data generated by mobile users and Internet of Things (IoT) devices is forecast to surpass 850 zettabytes by 2021 [4], underscoring the monumental scale of data processing and transmission that this communication network is poised to accommodate.

Some potential challenging features of 6G may include higher data rates, lower latency, enhanced connectivity,

The associate editor coordinating the review of this manuscript and approving it for publication was Yiqi Liu.

advanced spectrum usage, AI integration, and energy efficiency [5]. This technology is expected to achieve data rates that are significantly higher than current 5G technology. Reduced latency will be crucial for applications that require real-time responsiveness, such as augmented reality, virtual reality, and critical communication systems. The technology is also expected to improve connectivity in challenging environments, expand coverage in rural areas, and support new use cases. The technology is likely to use higher frequency bands and explore new spectrum resources to meet the increasing demand for data. Artificial intelligence will be more prominent, facilitating intelligent and adaptive network management and supporting various applications [6]. Energy efficiency will also be a key focus area, which will be crucial for powering a growing number of connected devices and reducing the environmental impact of wireless communication. New technologies, such as intelligent beamforming and energy-efficient modulation schemes, are being developed to optimize energy consumption [7].

However, as 6G networks become more intricate and interconnected, they may become susceptible to novel cybersecurity threats [8]. Single Sign-On (SSO) offers convenience by allowing users to access multiple applications with a single set of credentials [9]; unfortunately, it also presents inherent security challenges. SSO relies on a centralized authentication server; compromising this central point can have severe consequences. For example, a breach in the centralized authentication system could expose a vast array of services and sensitive information. If a device or credentials are compromised, an attacker can access multiple applications and services [10]. The complexity and interconnectedness of 6G communication networks pose significant security challenges. As the latest technology advances to support unprecedented data speeds, ultra-low latency, and a massive number of connected devices, it also creates new attack vectors for malicious actors to exploit. Threats to these networks include sophisticated cyberattacks targeting critical infrastructure, such as distributed denial-of-service (DDoS) attacks, ransomware, and advanced persistent threats (APTs) [11]. Moreover, integrating artificial intelligence and the extensive use of data in these networks introduce additional vulnerabilities, including AI-driven attacks and data breaches [12]. The growing reliance on higher frequency bands and spectrum resources increases the susceptibility to interference and signal jamming attacks. As these networks facilitate critical applications across various sectors, ranging from healthcare and transportation to smart cities and autonomous systems, the potential impact of security breaches becomes increasingly significant [13]. This underscores the urgent need for robust security measures and proactive defense mechanisms, as the window of opportunity for malicious actors to exploit these vulnerabilities is rapidly closing.

To tackle the security challenges the 6G network poses, it is crucial to implement additional security measures such as encryption, continuous monitoring, and multi-factor authentication (MFA) [14]. However, implementing MFA in this network environment can be challenging due to the need for seamless user experience and compatibility with various devices. Striking a balance between security and user experience becomes challenging when complex authentication processes cause user frustration and resistance to compliance. To adapt to dynamic user behaviors and changing security threats, 6G networks may require continuous authentication, which can be technically challenging and resource-intensive [15].

Hence, implementing a Zero Trust Architecture (ZTA) could be effective scope for 6G networks due to this advanced communication technology's heightened complexity, interconnectivity, and potential security risks [16]. Unlike traditional security models that rely on perimeter-based defenses, 6G networks, with their vast array of connected devices and applications, demand a more dynamic and adaptive approach [17]. Zero Trust assumes that no entity, whether internal or external, can be inherently trusted, and thus, every user and device must continually authenticate and validate their identity and permissions [18]. In this landscape, where critical applications span diverse sectors like healthcare, transportation, and manufacturing, adopting a zero-trust Trust Architecture becomes crucial to prevent lateral movement of threats within the network. By enforcing rigorous access controls, continuous monitoring, and real-time risk assessments, ZTA ensures that only authorized entities can access specific resources, mitigating the potential impact of compromised devices or malicious actors. Given the dynamic nature of this technology, where devices and users frequently join or leave, Zero Trust provides a proactive and adaptive security paradigm, aligning with the need for robust, flexible, and resilient cybersecurity in the face of evolving threats in this highly interconnected ecosystem [19]. The main contributions of this paper include:

(a) Providing a comprehensive survey on the applications and challenges of ZTA in the context of 6G network security. Offering insights into the background and literature study of 6G network security, highlighting the vulnerabilities of legacy perimeter-based security models and the need for more adaptive and sophisticated security approaches.
(b) Introducing the zero-trust model and its principles, emphasizing the significance of continuous verification, least privilege access, assuming breach, and micro-segmentation in enhancing network security.
(c) Presenting case studies and applications of ZTA in 6G or comparable networks.
(d) Identifying potential future research directions for the successful integration of ZTA in critical infrastructures.

These contributions collectively provide a comprehensive understanding of the significance, challenges, and potential applications of Zero Trust Architecture in the evolving landscape of 6G network security. The paper is structured as follows: In Section II, we offer a literature study and background information on 6G network security. Next, Section III examines various security aspects of the 6G network. In Section IV, we introduce the zero-trust model and principles. We delve into some case studies and applications of ZTA in Section V. Section VI provides insights into future trends and research, and the paper concludes with Section VII.

II. BACKGROUND

Based on the perimeter defense strategy, the traditional cybersecurity model assumes that all users and devices within the network are trusted [20]. The boundaries between internal and external networks have become increasingly blurry due to remote work, cloud computing, and the growth of internet-connected gadgets in the modern cybersecurity landscape, necessitating a revision of this approach. The rise of sophisticated cyberattacks, such as ransomware and data breaches, has highlighted the vulnerabilities of legacy perimeter-based security [21]. These attacks often exploit compromised credentials or vulnerabilities in software to gain unauthorized access to an organization's network. Once inside, attackers can move laterally across the network, compromising sensitive data and disrupting operations.

Perimeter-based security safeguards networks by establishing a defined boundary, or perimeter, and securing it against external threats [22]. This model assumes that entities within the perimeter are trusted, while those outside are potential threats. For instance, firewalls, intrusion detection systems, intrusion prevention systems, and virtual private networks are real-life examples of traditional perimeter-based security. Firewalls are the most common perimeter security devices. They are a barrier between the secure internal network and the untrusted outside world. Firewalls can filter network traffic based on various rules, such as source and destination IP addresses, ports, and protocols. Intrusion Detection Systems (IDSs) monitor network traffic for suspicious activity, such as unusual patterns or traffic from unknown sources [23]. IDSs can raise alerts when they detect suspicious activity, but they do not take any action to stop the attack. Intrusion Prevention Systems (IPSs) are similar to IDSs, but they can take action to stop attacks. IPSs can block traffic from suspicious sources, modify traffic to make it less harmful, or even disconnect infected devices from the network [24]. Virtual Private Networks (VPN) allow users to access the corporate network securely and remotely [25]. VPNs encrypt traffic between the user's device and the corporate network, making it difficult for attackers to intercept or steal sensitive data.

While this method has been influential in the past, it has significant tradeoffs. One major drawback is its inability to address internal threats effectively. Once an attacker breaches the perimeter, often achieved through tactics like phishing or exploiting vulnerabilities, they can move laterally within the network undetected. Additionally, perimeter-based security must accommodate the rise of remote work, mobile devices, and cloud services, as these resources operate beyond the traditional network boundaries. As organizations increasingly adopt decentralized architectures, the limitations of perimeter-based security become apparent [26], prompting the need for more adaptive and sophisticated security models like Zero Trust Architecture, which assumes a "never trust, always verify" approach to enhance resilience against evolving cyber threats. The limitations of perimeter-based security are as follows [27] and [28]:

(a) **Single Point of Failure:** Perimeter defense relies on a single barrier to protect the entire network, making it vulnerable to attacks that breach the perimeter.

(b) **Static Nature:** Perimeter defenses are often static and cannot adapt to the dynamic nature of modern networks, where users and devices frequently change their locations and roles.

(c) **Lack of Continuous Verification:** Perimeter defenses do not continuously verify the identity and trustworthiness of users and devices, leaving them susceptible to attacks that exploit compromised credentials or vulnerabilities.

(d) **Difficult to Enforce Least Privilege Access:** Perimeter defenses make it challenging to enforce least privilege access, granting users and devices more access than they need, which increases the risk of data breaches.

(e) **Limited Lateral Movement Prevention:** Perimeter defenses often lack the ability to effectively prevent lateral movement, allowing attackers to move freely within the network after gaining initial access.

As 6G networks are expected to have unprecedented connectivity with many devices and sensors, the issue of perimeter-based security presents unique challenges and considerations [29]. Traditional perimeter defenses may be less effective as the proliferation of interconnected devices expands the attack surface, risking the network's security. Moreover, the architecture of this network is likely to be highly distributed and decentralized, leaving it vulnerable to sophisticated attacks. The increased reliance on AI and ML technologies in 6G networks introduces new security challenges. While these technologies can enhance network efficiency and performance, they also introduce potential vulnerabilities that attackers could exploit to launch targeted attacks or manipulate data, risking the network's integrity and security. Furthermore, the sheer volume of data generated and transmitted over the networks presents privacy and security concerns. Considering the potential implications of data breaches or unauthorized access in highly interconnected environments, sensitive data must be protected. A paradigm shift is needed in cybersecurity approaches for 6G networks to overcome these challenges [30]. Organizations must adopt a holistic security strategy encompassing threat detection, response, and resilience. They should implement advanced AI-driven security solutions, employ encryption and authentication mechanisms, and adopt a zero-trust security model that assumes no entity, inside or outside the network perimeter, can be trusted inherently. The security challenges in current network architecture require organizations to adapt to the changing cybersecurity landscape.

In response to the limitations of perimeter-based security, ZTA emerged as a new security paradigm. ZTA breaks away from the assumption of trust, requiring continuous authentication and authorization for all users and devices, regardless of their location or network affiliation. We will discuss more on ZTA features, frameworks and tradeoffs in the later sections.

III. SECURITY ASPECTS OF 6G NETWORKS

The evolution from 4G to 6G networks presents new challenges and security considerations. While 4G networks addressed the issue of spoofing through fake base stations, vulnerabilities in user equipment (UE) identities remained exploitable by attackers [31]. 5G architecture introduced improvements such as unified data management and concealed identifiers, yet these enhancements primarily focused on authentication and fell short of resolving 6G network security challenges [32]. The openness of 6G networks, with integrated access networks and enterprise applications, complicates authentication mechanisms and cross-domain security. Traditional protocols like 5G AKA are insufficient in preventing compromised UEs from malicious activities. Although Transport Layer Security (TLS) secures end-to-end channels, it doesn't guarantee security of communication behavior. In 6G, threats emerge from network openness, virtualization, adversarial machine learning, and unauthorized user information utilization. Due to these diverse trends, establishing a uniform defense architecture at the application level is challenging [33]. Instead, focusing on network layer access control mitigates threats from abnormal access behavior. Future 6G networks may face severe attacks like DDoS, malware spread, and zero-day exploits, requiring robust access control mechanisms and proactive security measures [34]. DDoS attacks pose threats solely through access behaviors, which are expected to worsen with the proliferation of both devices. Malware, including viruses and ransomware, can compromise network integrity. At the same time, zero-day exploits exploit software vulnerabilities, especially with the increased use of open-source software in 6G networks, compromising network functions [35].

As shown in Figure 1, security challenges and concerns of the 6G network are closely related to the prominent use-case scenarios. From our literature study, we categorized the application use-case areas of the 6G network as AI/ML, Quantum communication, Radio Access Networks, and Decentralized & Distributed Solutions. 6G networks promise to revolutionize robotics by providing ultra-low latency communication, high bandwidth, and integration with edge computing, enabling robots to operate with unparalleled speed, precision, and autonomy [36]. With seamless collaboration, advanced perception capabilities, and enhanced safety features, 6G-powered robots can tackle various tasks, from industrial automation and telepresence to disaster response and exploration, ushering in a new era of innovation and efficiency. In the realm of AI and machine learning (ML), autonomous vehicles stand as a testament to the power of real-time decision-making and predictive analytics, reshaping the future of transportation [37]. Similarly, predictive maintenance models, fueled by ML algorithms, analyze data streams from critical infrastructure, such as power grids or transportation systems, preempting equipment failures and ensuring uninterrupted operations. In the healthcare sector, personalized treatment recommendations and early disease detection have become achievable goals through the analysis of individual health data. Wearable devices and medical records serve as information repositories, empowering AI-driven systems to deliver tailored healthcare solutions [38]. Meanwhile, the fusion of ML algorithms and IoT sensor data revolutionizes farming practices, optimizing crop yields and resource management for sustainable agricultural practices [39].

Quantum communication heralds a new era of secure and efficient data transmission. Quantum cryptography and key distribution protocols provide unbreakable encryption, ensuring the confidentiality and integrity of communication channels. Beyond secure communications, quantum networked computing unlocks unprecedented computational power, enabling distributed quantum computing tasks across interconnected processors. Additionally, quantum-enhanced sensors pave the way for precise measurements in navigation, environmental monitoring, and medical imaging. In radio access networks, cutting-edge technologies promise enhanced connectivity and coverage. Massive MIMO techniques leverage advanced antenna technologies to increase spectral efficiency and network capacity, catering to the growing demands for high-speed data transmission. Beamforming technologies optimize signal strength and reduce interference, particularly in densely populated urban areas. Furthermore, network slicing techniques enable the customization of network segments to meet specific application requirements, ensuring optimal performance for diverse use cases. Finally, decentralized and distributed solutions redefine the paradigms of computing and communication. Edge computing resources, deployed closer to end-users, minimize latency and bandwidth usage, facilitating real-time data processing for latency-sensitive applications. Blockchain technology underpins secure and transparent transactions in various domains, including finance, supply chain management, and digital identities.

Based on these scenarios, we characterize the security challenges for 6G networks as the follows:

(a) **Vast Scale Complexity**: The immense scale of 6G networks brings forth concerns regarding scalability in security architecture design. Conventional intricate systems may prove inefficient or unfeasible for managing such expansive networks, urging the need for novel and streamlined security solutions capable of seamless scalability.

(b) **Diverse Network Landscape**: The heterogeneous nature of 6G networks, with multiple operators managing varied networks, presents complexities in network

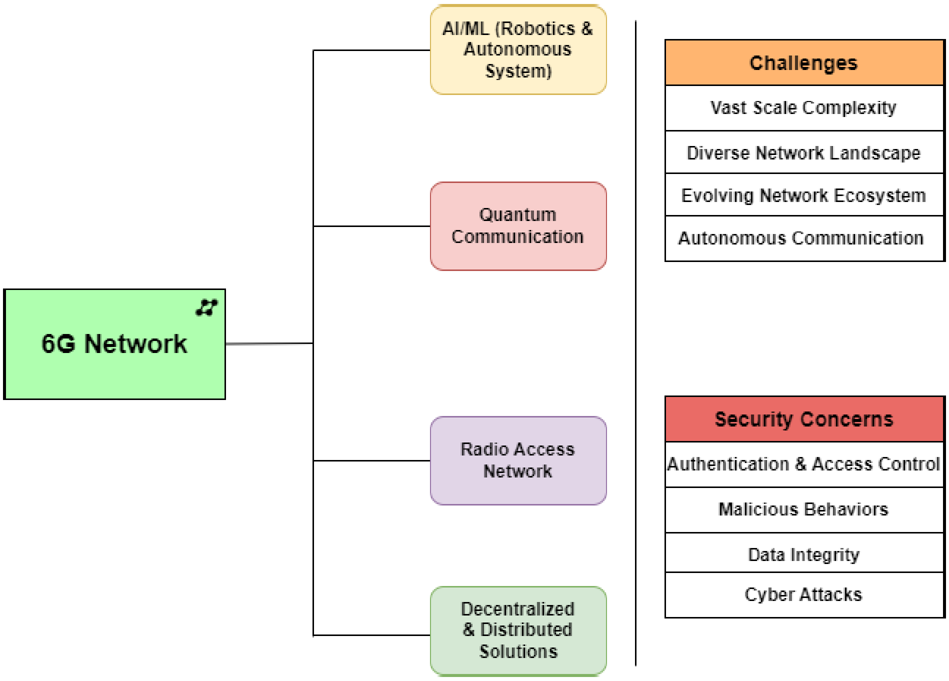


FIGURE 1. Challenges and security concerns in 6G networks.

management and signaling systems. Collaborative efforts among diverse control domains are indispensable for crafting robust security architectures. Furthermore, the diverse array of user equipment adds another layer of intricacy, demanding adaptable and versatile security design approaches.

(c) **Evolving Network Ecosystem**: The incorporation of Open Radio Access Network (O-RAN) components in 6G introduces new interfaces and network elements from diverse vendors, fostering an environment of openness. However, this openness also introduces challenges such as system fragility, heightened security risks, and the potential for additional points of failure. It underscores the critical need for robust security measures to safeguard against these vulnerabilities in an open and interconnected 6G landscape.

(d) **Autonomous Communication Dynamics** : Machine-to-machine (M2M) communication, a prevalent feature in 6G networks, facilitates autonomous interactions among intelligent devices. These interactions, devoid of human supervision, pose inherent risks that necessitate meticulous monitoring. Security architectures must employ granular access control mechanisms to effectively mitigate the associated risks and ensure the integrity of autonomous interactions in 6G networks.

Security concerns in 6G networks include authentication & access control, malicious behaviors, data integrity, and cyber attacks.

(a) **Authentication and Access Control:** As 6G networks connect many devices and services, ensuring robust authentication mechanisms and access controls is paramount. Weak authentication protocols can lead to unauthorized access to network resources, compromising data confidentiality and system integrity.

(b) **Malicious Behaviors:** The proliferation of connected devices in 6G networks increases the attack surface for malicious actors seeking to exploit vulnerabilities. Malicious behaviors such as malware, ransomware, and botnet attacks can disrupt services, steal sensitive information, or hijack devices for malicious purposes.

(c) **Data Integrity:** Maintaining the integrity of data transmitted and stored within 6G networks is crucial to prevent tampering, manipulation, or unauthorized modification. Without proper safeguards, malicious actors could alter data packets, falsify sensor readings, or inject malicious code into network traffic, leading to erroneous decisions and compromised operations.

(d) **Cyber Attacks:** 6G networks are susceptible to various cyber attacks, including distributed denial-of-service (DDoS) attacks, man-in-the-middle attacks, and spoofing attacks. These attacks can disrupt network connectivity, intercept sensitive data, or impersonate legitimate users or devices, undermining the trust and reliability of the network infrastructure.

IV. ZERO-TRUST MODEL AND PRINCIPLES

The Zero Trust Model is a cybersecurity strategy that questions the traditional concept of trust in network boundaries. Zero Trust operates on the premise of ‘‘never trust, always verify’’ in contrast to typical security models that depend on the assumption of trust once inside the network [40]. According to this architecture, rigorous authentication and permission procedures consistently confirm resource access rather than granting it automatically based on the user's location or network. This method assumes that risks may arise from external and internal sources. It emphasizes safeguarding vital assets by implementing the principle of least privilege, micro-segmentation, and ongoing monitoring. The Zero Trust Model advocates for a thorough and flexible security approach that aligns with the ever-changing nature of cybersecurity risks. John Kindervag, a former Forrester Research analyst, popularized the notion of Zero Trust in 2010 [41]. He offered this framework as a solution to the limitations of traditional security approaches in effectively dealing with advancing cyber threats.

The Zero Trust Model is based on assumptions that challenge traditional security paradigms [42], [43]. ZTA is built on the following basic assumptions:

(a) **No Implicit Trust:** The foundational assumption of the Zero Trust Model is that trust is not automatically granted based on the location of a user or device within the network. Every access request is treated with skepticism and subject to verification.

(b) **Threats Exist Both Inside and Outside:**Unlike traditional security models that focus on external threats, the Zero Trust Model assumes that threats can originate both from external sources and from compromised entities within the network. This assumption drives the need for continuous monitoring and a proactive security stance.

(c) **Continuous Monitoring is Essential:** The assumption that continuous monitoring is essential reflects the understanding that the security landscape is dynamic and threats can evolve over time. Continuous monitoring helps identify and respond to emerging security risks.

(d) **Network Perimeter is Not a Reliable Boundary:** The concept of a network perimeter as a secure boundary is challenged in the Zero Trust Model. The assumption is that a determined attacker can breach traditional perimeter defenses, necessitating a more granular and dynamic approach to security.

(e) **Data-Centric Focus:** The assumption that a data-centric focus is crucial implies that protecting sensitive data is a prty. Zero Trust emphasizes securing access to data rather than relying solely on protecting the network. Security policies should be adaptable and formulated using a wide range of data sources.

The zero trust model is thought to adhere to the following fundamental principles, based on the aforementioned assumptions:

(a) **Verify Explicitly:** The principle of "Verify Explicitly" emphasizes the need for continuous verification of the identity of users, devices, and systems. Access is not granted based solely on network location or assumed trust; instead, verification occurs at every step.

(b) **Least Privilege Access:** Users and systems are granted the minimum level of access required to perform their specific tasks. This principle minimizes the potential impact of a security breach by limiting the privileges of compromised accounts.

(c) **Assume Breach:** The "Assume Breach" principle challenges the traditional security posture that assumes everything within the network is secure. In a Zero Trust Model, it is assumed that a security breach is always possible, and security measures are designed with this assumption in mind.

(d) **Micro-Segmentation:** Networks are divided into small, isolated segments or zones, and access between these segments is strictly controlled. Micro-segmentation helps contain potential threats, preventing lateral movement within the network.

(e) **Conditional Access & Continuous Monitoring:** Access decisions are based on various contextual factors, including user identity, device health, location, time of day, and more. Policies can be dynamically adjusted to respond to changing conditions, ensuring that access is granted only when specific criteria are met. Real-time monitoring and analysis of user and system behavior are fundamental to the Zero Trust Model. Continuous monitoring helps detect anomalies and potential security threats, allowing for timely responses.

A. ZERO-TRUST ARCHITECTURE

ZTA's core consists of a policy enforcement point (PEP) and a policy decision point (PDP) [44]. The PEP serves as the initial contact for access requests. It establishes the link between the subject and the requested resource when access is granted. The PDP, assisted by the policy administrator (PA), makes the decision on access approval. The decision-making process relies on all accessible internal and external information regarding the security status of the subject and network assets. The ZTA core relies on data from multiple peripheral modules to establish and oversee a connection, as seen in Figure 2. We categorize these modules into static (on the right side of the picture) and dynamic (on the left side). The static modules consist of data access policy, public key infrastructure (PKI), identity (ID) management, and industry compliance. These modules jointly establish the security policy rules for secure communication and integrity check rules. The ZTA core can dynamically modify the policy rules. ZTA is characterized by its unique dynamic modules. The components consist of continuous diagnostics and mitigation (CDM), threat intelligence for detecting new security vulnerabilities, activity logs providing behavioral data on users, assets, and network traffic, and security information and event management (SIEM) for gathering information on the overall security status and possible threats. The processing engine of PDP is an intelligent policy engine (IPE) that uses static and dynamic rules to make judgments about allowing access. ZTA separates the network into three distinct logical and perhaps physical planes [45]. Data communication between the subject and network resources occurs in the data plane, which encompasses the subject's

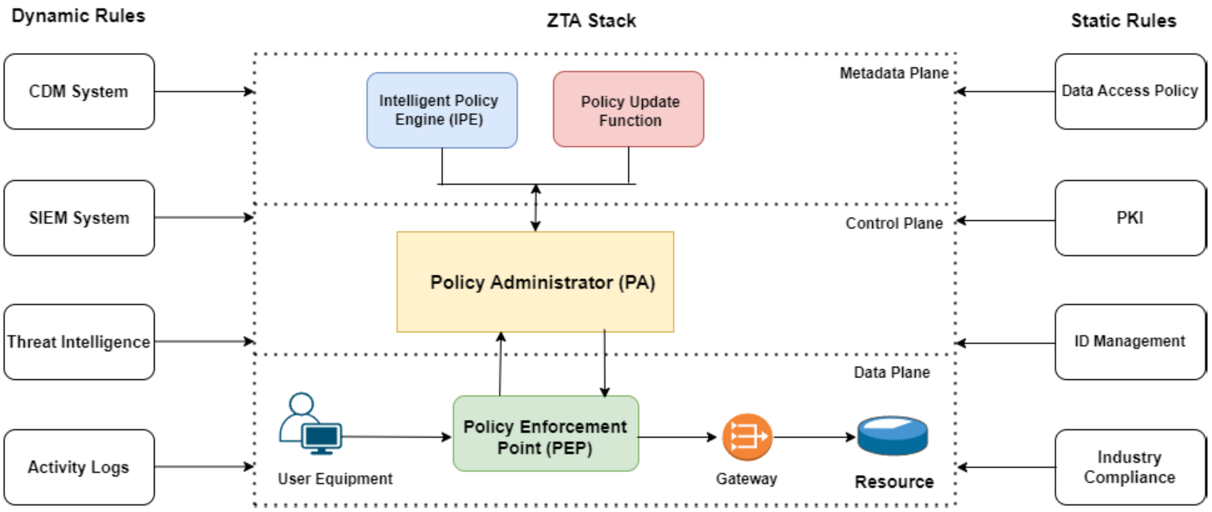


FIGURE 2. Logical components of ZTA stack.

initial access request. The ZTA components, PEP and PDP, interact in the control plane to make choices and set up connections. These two planes are also present in the current 5G network topologies. The third plane of the ZTA is the metadata plane, which is utilized for transmitting all necessary data to the AI engines. The arrangement of blocks in this figure represents the logical interaction of components and may not correspond to their physical placements in the network. This article employs the following language when discussing the ZTA. A subject refers to any entity, such as a user, application, or service, that seeks permission to access a network resource. Network assets encompass all devices, network infrastructure, and processes, including cloud services, that are involved in communication. The network resource holds sensitive information that needs to be safeguarded against unauthorized access.

B. ZTA MIGRATION

Many businesses intend to execute the ZTA migration to improve security and protect against cyberattacks and data breaches. We gathered relevant published research on ZTA migration from various sources, including government, business, and academic institutions.

NIST SP 800-207 recommends implementing a pilot program and an incremental strategy [56]. After choosing the first round of applicants, an organization moves on to the subsequent phases. This study emphasizes how important it is to identify assets, business processes, and risk management. CISCO's technological guidelines prioritize device visibility and fostering user trust [43]. Three main perspectives are involved in their ZTA migration: operational, managerial, and strategic. The methods and tactics for migrating to Zero Trust Architecture (ZTA) must be better documented.

Google BeyondCorp's ZTA migration focuses on technical migration strategies that show how to install devices, set up users, and manage the network in the ZT environment [52]. Iterative steps are taken to move the migration forward, beginning with a small pilot and progressively adding more candidates as time goes on. Microsoft ensures that all stakeholders are involved in the ZTA migration and helps define the scope of execution by concentrating on managerial tactics for the migration [26]. The four separate components of the Zero Trust Architecture (ZTA) implementation are identity, device, access, and service [57]. Table 1, illustrates the comparison among different ZTA architectures considering the framework and tradeoffs.

Implementation studies for Zero Trust Architectures frequently list the essential steps in switching to a Zero Trust Architecture. Establish the protective surface first, paying particular attention to the data, assets, applications, and services. Transaction flows will then be connected with the protected surface. In addition, the network's architectural layout needs to support micro-segmentation. Zero Trust policies are established and carried out by an organization. The last phase entails managing and maintaining the Zero Trust Architecture to protect the company safely and successfully. The majority of studies need a theoretical foundation for their migration techniques. Certain studies focus primarily on migration from managerial or technological perspectives. Dynamic and comprehensive frameworks or techniques that demonstrate the smooth and effective transition to ZTA take time to come by.

ZTA migration is shifting from conventional network security frameworks, which usually depend on perimeter-based defences, to a paradigm where no entity, whether inside or external to the network, is automatically trusted [58], [59]. This method considers that dangers may come from within or outside an organization, and access restrictions are implemented according to identity authentication and situational details. The migration procedure usually includes multiple crucial steps:

TABLE 1. Comparison among different zero-trust model architecture.

Zero Trust Model Architecture	Description	Benefits	Drawbacks
NIST Zero Trust Architecture [46] [47]	A comprehensive framework for implementing a zero-trust architecture covers identity and access management, network segmentation, data protection, and endpoint security.	• Provides a structured approach to Zero Trust implementation, aligning with industry best practices. • Emphasis on risk management and continuous monitoring.	• Can be complex and require significant resources to implement. • Implementation can be resource-intensive.
Google BeyondCorp [48] [49] [50]	A zero-trust approach that emphasizes the use of identity and context to control access to resources rather than relying on traditional network boundaries.	• Highly scalable and cloud-native, making it well-suited for modern enterprise environments. • Device-independent access, continuous authentication, and reduced attack surface	• May require significant changes to existing infrastructure and processes. • Resource-intensive to implement and initial setup can be complex. • Requires a mature identity and access management system.
Microsoft Zero Trust [51] [52]	A holistic zero-trust strategy that encompasses identity, devices, applications, data, and infrastructure. Integrates with Microsoft's existing security products and services, providing a unified approach to Zero Trust.	• Users and devices are continuously verified before granting access, reducing the risk of unauthorized access. • Users and devices are granted the minimum level of access necessary to perform their tasks, limiting potential damage in case of a security breach.	• Can be expensive and may require additional licensing for some features. • Strict access controls, especially if not well-tailored, may impact the user experience by introducing additional authentication steps.
Forrester Zero Trust Model [53]	A simplified model that focuses on three core principles: assume breach, use granular access, and continuously assess and monitor.	• Prioritizes the protection of sensitive assets. • Integrates with existing security investments.	• Requires a strong security culture and user education. • Initial deployment may disrupt existing workflows.
Gartner Zero Trust Network Access (ZTNA) [54] [55]	A specific implementation of zero trust that focuses on securing access to applications and services.	• Focused on securing access to applications and services. • Provides a granular approach to access control. • Can be deployed in cloud, on-premises, or hybrid environments.	• Requires careful planning and implementation to avoid introducing new security vulnerabilities. • May not be as cost-effective as other zero trust models.

(a) **Assessment and Planning:** Evaluate the current network architecture, security protocols, and access restrictions to pinpoint weaknesses and areas that need enhancement. Create a migration strategy detailing the objectives, schedules, and resources needed to apply Zero Trust principles.

(b) **Identity and Access Management (IAM):** Enhance IAM capabilities to guarantee strong authentication, authorization, and access control techniques. Utilise multi-factor authentication (MFA), least privilege access controls, and continuous monitoring to confirm user identities and apply access policies dynamically.

(c) **Micro-segmentation:** Micro-segmentation involves dividing the network into smaller isolated zones to reduce the spread of threats and contain the impact of a security breach. UseÂ network segmentation techniques to establish secure micro-perimeters around critical resources and applications.

(d) **Continuous Monitoring and Threat Detection:** Utilise sophisticated security analytics technologies for continuous monitoring of network traffic, user behaviour, and application activities in real-time. Utilise machine learning and AI technology to detect abnormalities, identify security threats, and respond promptly to security issues.

(e) **Security Policy Enforcement:** Ensure security policies are consistently applied throughout the full network architecture, encompassing cloud environments, remote endpoints, and IoT devices. Enforce policy-based access controls and automate security policy enforcement to adhere to Zero Trust principles.

(f) **Employee Training and Awareness:** Deliver thorough training and awareness programmes to instruct staff on Zero Trust concepts, security best practices, and their responsibilities in upholding a safe network environment. Promote a culture of security knowledge and accountability within the organisation.

(g) **Regular Evaluation and Improvement:** Employee Training and Awareness:Â Consistently evaluate the efficiency of Zero Trust measures, track security KPIs, and do routine audits to pinpoint deficiencies and opportunities for enhancement. Revise the migration plan considering insights gained and new security risks.

Organisations can move to a Zero Trust Architecture gradually by following these steps and adopting a staged strategy, which helps minimise disruption to business operations and enhance security posture.

C. SECURITY THREATS AND CHALLENGES

While the Zero Trust Model is designed to enhance the security by assuming that threats may exist both inside and outside the network, there are still several security threats and challenges associated with its implementation [60], [61]. Some of these include:

(a) **Credential Compromise:** If user credentials are compromised, either through phishing, credential stuffing, or other means, attackers may gain unauthorized access, bypassing the assumed zero trust posture.

(b) **Insider Threats:** Malicious or unintentional actions by employees or individuals with privileged access can pose a significant threat. Insiders could abuse their legitimate access to compromise sensitive data or systems.

(c) **Device Vulnerabilities:** Devices, including endpoints and IoT devices, may have vulnerabilities that could be exploited by attackers. Inadequate device security may result in unauthorized access or compromise of the Zero Trust Model.

(d) **Man-in-the-Middle Attacks:** Attackers may attempt to intercept and manipulate communication between users and resources, potentially gaining access to sensitive information. Secure communication channels and encryption are crucial to mitigating this threat.

(e) **Dependencies on Identity Management:** A robust identity and access management system is fundamental to the Zero Trust Model. If identity management is weak or compromised, it can undermine the entire security framework. Regularly updating and strengthening identity management practices is essential.

V. CASE-STUDIES OF ZERO TRUST MODEL

While specific details of Zero Trust implementations may be confidential due to security concerns, several well-known organizations have publicly discussed adopting Zero Trust principles.

(a) **Google**: Google's implementation of Zero Trust, known as the "BeyondCorp" model, is a well-documented case study. Instead of relying on a traditional network perimeter, BeyondCorp focuses on user and device identity, implementing strict access controls and continuous authentication [62]. This approach enhances security and allows employees to access resources securely from any location.

(b) **Cisco**: Cisco is another organization that has embraced the Zero Trust Model. Cisco's approach involves continuous monitoring and assessment of user and device behavior [63]. The company uses a combination of identity verification, adaptive access controls, and machine learning to detect and respond to potential threats in real-time.

(c) **Capital One**: Capital One, a financial services company, has publicly discussed its journey towards adopting a Zero Trust architecture [64]. Capital One focuses on continuous monitoring, dynamic risk assessments, and least privilege access principles. The company uses multi-factor authentication and conditional access policies to enhance security.

(d) **Adobe**: Adobe has shared insights into its implementation of a zero-trust security model [65]. Adobe's approach involves identity verification, least privilege access, and continuous monitoring. The company has implemented a phased approach to transitioning from traditional security models to a more zero-trust-oriented framework.

(e) **Wells Fargo**: Wells Fargo has outlined its commitment to the Zero Trust Model in enhancing security [66]. The financial institution emphasizes identity verification, least privilege access, and continuous monitoring to protect against evolving cyber threats. This includes implementing strong authentication measures and adopting a data-centric security approach.

It's important to note that the specific implementations and details of Zero Trust models can vary based on organizational needs, industry regulations, and the technology landscape. Organizations often tailor Zero Trust principles to fit their unique requirements and risk profiles. While these case studies provide insights into the principles and approaches of Zero Trust adoption, organizations considering such a shift should carefully assess their specific security needs and compliance requirements.

VI. RESEARCH TRENDS AND FUTURE SCOPE

Zero Trust security model has been gaining traction and is expected to continue evolving in response to emerging cybersecurity threats and technological advancements. Some of the potential research scope and trends are listed below [67], [68], [69]:

(a) **Integration with Cloud Security:** Zero Trust is increasingly being integrated with cloud security solutions to address the challenges posed by cloud-based environments. Researchers are exploring ways to ensure that the principles of Zero Trust can be effectively applied in dynamic and distributed cloud architectures.

(b) **Zero Trust for IoT:** With the proliferation of Internet of Things (IoT) devices, researchers are investigating how Zero Trust principles can be adapted to secure IoT ecosystems. This includes securing the communication between devices and implementing access controls based on device behavior.

(c) **Machine Learning and Automation:** Researchers are exploring the integration of machine learning and automation in Zero Trust architectures to enhance threat detection and response capabilities. This involves developing models that can analyze user and device behavior to identify anomalies and potential security risks.

(d) **Zero Trust in 5G/6G Networks:** With the deployment of 5G/6G networks, researchers are expected to explore how Zero Trust can be implemented to secure the increased connectivity and communication speeds, especially considering the diverse range of devices and applications that will be supported.

(e) **Enhanced User Experience:** Future developments may focus on improving the user experience within Zero Trust environments. This involves finding ways to minimize friction for legitimate users while maintaining a high level of security through adaptive and context-aware access controls.

VII. CONCLUSION

Adopting ZTA represents a fundamental shift in cybersecurity paradigms, advocating for a more proactive and granular approach to network security. By challenging the traditional notion of perimeter-based defenses and embracing principles such as continuous verification and least privilege access, ZTA offers a robust framework for mitigating internal threats and enhancing overall security posture. Within the context of 6G networks, where the proliferation of connected devices and data interconnections amplifies security challenges, the principles of ZTA become even more pertinent. As organizations transition towards 6G technologies, it is imperative to recognize the limitations of legacy security models and embrace more adaptive and sophisticated approaches. This necessitates ongoing research efforts to address the challenges and security threats posed by 6G networks, focusing on refining ZTA implementations and fostering a culture of security awareness and resilience.

This article provides a comprehensive overview of the applications and challenges of Zero-Trust Architecture (ZTA) in the context of 6G network security. It highlights the vulnerabilities of the traditional perimeter-based security models and the need for more adaptive and sophisticated security approaches. The article introduces the zero-trust model and its principles, emphasizing the importance of continuous verification, least privilege access, assuming breaches, and micro-segmentation in enhancing network security. Furthermore, the article discusses future research directions for successfully implementing ZTA in critical infrastructures such as 6G networks.

REFERENCES

[1] H. H. H. Mahmoud, A. A. Amer, and T. Ismail, "6G: A comprehensive survey on technologies, applications, challenges, and research problems," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 4, Apr. 2021, Art. no. e4233.

[2] P. R. Singh, V. K. Singh, R. Yadav, and S. N. Chaurasia, "6G networks for artificial intelligence-enabled smart cities applications: A scoping review," *Telematics Informat. Rep.*, vol. 9, Mar. 2023, Art. no. 100044.

[3] F. Dahlqvist, M. Patel, A. Rajko, and J. Shulman, "Growing opportunities in the Internet of Things," McKinsey & Company, Chennai, India, Tech. Rep., 2019, pp. 1–6.

[4] D. Xu, T. Li, Y. Li, X. Su, S. Tarkoma, T. Jiang, J. Crowcroft, and P. Hui, "Edge intelligence: Empowering intelligence to the edge of network," *Proc. IEEE*, vol. 109, no. 11, pp. 1778–1837, Nov. 2021.

[5] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, 2020.

[6] M. Andronie, G. Lăzăroiu, M. Iatagan, C. Uță, R. Ștefănescu, and M. Cocoşatu, "Artificial intelligence-based decision-making algorithms, Internet of Things sensing networks, and deep learning-assisted smart process management in cyber-physical production systems," *Electronics*, vol. 10, no. 20, p. 2497, Oct. 2021.

[7] Z. Yang, M. Chen, W. Saad, W. Xu, M. Shikh-Bahaei, H. V. Poor, and S. Cui, "Energy-efficient wireless communications with distributed reconfigurable intelligent surfaces," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 665–679, Jan. 2021.

[8] J. R. Bhat and S. A. Alqahtani, "6G ecosystem: Current status and future perspective," *IEEE Access*, vol. 9, pp. 43134–43167, 2021.

[9] A. Mahnamfar, K. Bicakci, and Y. Uzunay, "ROSTAM: A passwordless web single sign-on solution mitigating server breaches and integrating credential manager and federated identity systems," *Comput. Secur.*, vol. 139, Apr. 2024, Art. no. 103739.

[10] K. Thomas, J. Pullman, K. Yeo, A. Raghunathan, P. G. Kelley, L. Invernizzi, B. Benko, T. Pietraszek, S. Patel, D. Boneh, and E. Bursztein, "Protecting accounts from credential stuffing with password breach alerting," in *Proc. USENIX Secur. Symp.*, Aug. 2019, pp. 1556–1571.

[11] A. Sharma, B. B. Gupta, A. K. Singh, and V. K. Saraswat, "Advanced persistent threats (APT): Evolution, anatomy, attribution and countermeasures," *J. Ambient Intell. Hum. Comput.*, vol. 14, no. 7, pp. 9355–9381, Jul. 2023.

[12] A. Haddaji, S. Ayed, and L. C. Fourati, "Artificial intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey," *Comput. Electr. Eng.*, vol. 104, Dec. 2022, Art. no. 108460.

[13] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustain. Cities Soc.*, vol. 39, pp. 499–507, May 2018.

[14] P. H. Basha, G. Prathyusha, D. N. Rao, V. Gopikrishna, P. Peddi, and V. Saritha, "AI-driven multi-factor authentication and dynamic trust management for securing massive machine type communication in 6G networks," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 1s, pp. 361–374, 2024.

[15] Y. Wang, X. Kang, T. Li, H. Wang, C.-K. Chu, and Z. Lei, "SIX-trust for 6G: Toward a secure and trustworthy future network," *IEEE Access*, vol. 11, pp. 107657–107668, 2023.

[16] 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," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109358.

[17] P. Scalise, M. Boeding, M. Hempel, H. Sharif, J. Delloiacovo, and J. Reed, "A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas," *Future Internet*, vol. 16, no. 3, p. 67, Feb. 2024.

[18] 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. 57143–57179, 2022.

[19] E. A. Shaikh Ashfaq, "Zero trust security paradigm: A comprehensive survey and research analysis," *J. Electr. Syst.*, vol. 19, no. 2, pp. 28–37, Jan. 2024.

[20] R. Rapuzzi and M. Repetto, "Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model," *Future Gener. Comput. Syst.*, vol. 85, pp. 235–249, Aug. 2018.

[21] Z. Adahman, A. W. Malik, and Z. Anwar, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," *Comput. Secur.*, vol. 122, Nov. 2022, Art. no. 102911.

[22] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and application of zero trust security: A brief survey," *Entropy*, vol. 25, no. 12, p. 1595, Nov. 2023.

[23] S. Hajj, R. El Sibai, J. B. Abdo, J. Demerjian, A. Makhoul, and C. Guyeux, ''Anomaly-based intrusion detection systems: The requirements, methods, measurements, and datasets,'' *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 4, Apr. 2021, Art. no. e4240.

[24] P. R. Chandre, P. Mahalle, and G. Shinde, ''Intrusion prevention system using convolutional neural network for wireless sensor network,'' *IAES Int. J. Artif. Intell.*, vol. 11, no. 2, p. 504, Jun. 2022.

[25] S. Jingyao, S. Chandel, Y. Yunnan, Z. Jingji, and Z. Zhipeng, ''Securing a network: How effective using firewalls and VPNs are?'' in *Proc. Future Inf. Commun. Conf. (FICC)*, vol. 2. San Francisco, CA, USA: Springer, 2019, pp. 1050–1068.

[26] C. Itodo and M. Ozer, ''Multivocal literature review on zero-trust security implementation,'' *Comput. Secur.*, vol. 141, Jun. 2024, Art. no. 103827.

[27] S.-K. Park, ''Development of software-defined perimeter-based access control system for security of cloud and IoT system,'' *J. Inst. Internet, Broadcast. Commun.*, vol. 21, no. 2, pp. 15–26, 2021.

[28] I. Anjum, D. Kostecki, E. Leba, J. Sokal, R. Bharambe, W. Enck, C. Nita-Rotaru, and B. Reaves, ''Removing the reliance on perimeters for security using network views,'' in *Proc. 27th ACM Symp. Access Control Models Technol.*, Jun. 2022, pp. 151–162.

[29] I. A. Alimi, R. K. Patel, A. Zaouga, N. J. Muga, Q. Xin, A. N. Pinto, and P. P. Monteiro, ''Trends in cloud computing paradigms: Fundamental issues, recent advances, and research directions toward 6G fog networks,'' in *Moving Broadband Mobile Communications Forward: Intelligent Technologies for 5G and Beyond*, vol. 3. London, U.K.: IntechOpen Limited, 2021.

[30] S. Zhang and D. Zhu, ''Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities,'' *Comput. Netw.*, vol. 183, Dec. 2020, Art. no. 107556.

[31] C. Yu, S. Chen, F. Wang, and Z. Wei, ''Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers,'' *Comput. Netw.*, vol. 201, Dec. 2021, Art. no. 108532.

[32] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, ''Security requirements and challenges of 6G technologies and applications,'' *Sensors*, vol. 22, no. 5, p. 1969, Mar. 2022.

[33] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, ''Security and privacy for 6G: A survey on prospective technologies and challenges,'' *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[34] X. Chen, W. Feng, N. Ge, and Y. Zhang, ''Zero trust architecture for 6G security,'' *IEEE Netw.*, early access, Oct. 20, 2022, doi: 10.1109/MNET.2023.3326356.

[35] Md. A. Rahman and M. S. Hossain, ''A deep learning assisted software defined security architecture for 6G wireless networks: IIoT perspective,'' *IEEE Wireless Commun.*, vol. 29, no. 2, pp. 52–59, Apr. 2022.

[36] R. Chataut, M. Nankya, and R. Akl, ''6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges,'' *Sensors*, vol. 24, no. 6, p. 1888, 2024.

[37] A. Mekrache, A. Bradai, E. Moulay, and S. Dawaliby, ''Deep reinforcement learning techniques for vehicular networks: Recent advances and future trends towards 6G,'' *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100398.

[38] S. Nayak and R. Patgiri, ''6G communication technology: A vision on intelligent healthcare,'' in *Health Informatics: A Computational Perspective in Healthcare*. Singapore: Springer, 2021, pp. 1–18.

[39] F. Zhang, Y. Zhang, W. Lu, Y. Gao, Y. Gong, and J. Cao, ''6G-enabled smart agriculture: A review and prospect,'' *Electronics*, vol. 11, no. 18, p. 2845, Sep. 2022.

[40] M. J. Khan, ''Zero trust architecture: Redefining network security paradigms in the digital age,'' *World J. Adv. Res. Rev.*, vol. 19, no. 3, pp. 105–116, Sep. 2023.

[41] J. Kindervag, S. Balaouras, and L. Coit, ''Build security into your networks' DNA: The zero trust network architecture,'' Forrester Res., Cambridge, MA, USA, 2010, vol. 27.

[42] N. Papakonstantinou, D. L. Van Bossuyt, J. Linnosmaa, B. Hale, and B. O'Halloran, ''A zero trust hybrid security and safety risk analysis method,'' *J. Comput. Inf. Sci. Eng.*, vol. 21, no. 5, Oct. 2021, Art. no. 050907.

[43] P. Phiayura and S. Teerakanok, ''A comprehensive framework for migrating to zero trust architecture,'' *IEEE Access*, vol. 11, pp. 19487–19511, 2023.

[44] Q. Shen and Y. Shen, ''Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach,'' *Comput. Secur.*, vol. 136, Jan. 2024, Art. no. 103537.

[45] E. B. Fernandez and A. Brazhuk, ''A critical analysis of zero trust architecture (ZTA),'' *Comput. Standards Interfaces*, vol. 89, Apr. 2024, Art. no. 103832.

[46] J. Seefeldt, *What's New in NIST Zero Trust Architecture*, NIST Standard SP 800-207, Mar. 2021, p. 207.

[47] O. C. Edo, T. Tenebe, E.-E. Etu, A. Ayuwu, J. Emakhu, and S. Adebiyi, ''Zero trust architecture: Trend and impacton information security,'' *Int. J. Emerg. Technol. Adv. Eng.*, vol. 12, no. 7, p. 140, 2022.

[48] P. Assunção, ''A zero trust approach to network security,'' in *Proc. Digit. Privacy Secur. Conf.*, Porto, Protugal, 2019, pp. 65–72.

[49] I. Ahmed, T. Nahar, S. S. Urmi, and K. A. Taher, ''Protection of sensitive data in zero trust model,'' in *Proc. Int. Conf. Comput. Adv.*, Jan. 2020, pp. 1–5.

[50] D. A. E. Haddon, ''Zero trust networks, the concepts, the strategies, and the reality,'' in *Strategy, Leadership, and AI in the Cyber Ecosystem*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 195–216.

[51] V. N. S. S. Chimakurthi, ''The challenge of achieving zero trust remote access in multi-cloud environment,'' *ABC J. Adv. Res.*, vol. 9, no. 2, pp. 89–102, Dec. 2020.

[52] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, ''Security of zero trust networks in cloud computing: A comparative review,'' *Sustainability*, vol. 14, no. 18, p. 11213, Sep. 2022.

[53] J. Kindervag, ''No more chewy centers: Introducing the zero trust model of information security,'' Forrester Res., Cambridge, MA, USA, Tech. Rep., 2010, vol. 3.

[54] S. van der Walt and H. Venter, ''Research gaps and opportunities for secure access service edge,'' in *Proc. Int. Conf. Cyber Warfare Secur.*, 2022, vol. 17, no. 1, pp. 609–619.

[55] F. A. Qazi, ''Study of zero trust architecture for applications and network security,'' in *Proc. IEEE 19th Int. Conf. Smart Communities, Improving Quality Life Using ICT, IoT AI (HONET)*, Dec. 2022, pp. 111–116.

[56] V. Stafford, *Zero Trust Architecture*, NIST Standard 800-207, 2020.

[57] E. S. Hosney, I. T. A. Halim, and A. H. Yousef, ''An artificial intelligence approach for deploying zero trust architecture (ZTA),'' in *Proc. 5th Int. Conf. Comput. Informat. (ICCI)*, Mar. 2022, pp. 343–350.

[58] S. Teerakanok, T. Uehara, and A. Inomata, ''Migrating to zero trust architecture: Reviews and challenges,'' *Secur. Commun. Netw.*, vol. 2021, pp. 1–10, May 2021.

[59] T. Muhammad, M. T. Munir, M. Z. Munir, and M. W. Zafar, ''Integrative cybersecurity: Merging zero trust, layered defense, and global standards for a resilient digital future,'' *Int. J. Comput. Sci. Technol.*, vol. 6, no. 4, pp. 99–135, 2022.

[60] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, ''A security awareness and protection system for 5G smart healthcare based on zero-trust architecture,'' *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10248–10263, Jul. 2021.

[61] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, ''Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust,'' *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102436.

[62] H. Nguyen, Y. Lim, M. Seo, Y. Jung, M. Kim, and W. Park, ''Strengthening information security through zero trust architecture: A case study in South Korea,'' in *Proc. Int. Conf. Intell. Syst. Data Sci.* Can Tho, Vietnam: Springer, 2023, pp. 63–77.

[63] D. Haddon and P. Bennett, ''The emergence of post COVID-19 zero trust security architectures,'' in *Information Security Technologies for Controlling Pandemics*. Cham, Switzerland: Springer, 2021, pp. 335–355.

[64] M. Lacity, E. Carmel, and A. University, ''Self-sovereign identity and verifiable credentials in your digital wallet,'' *MIS Quart. Executive*, vol. 21, no. 3, pp. 241–251, 2022.

[65] S. A. Kawalkar and D. B. Bhoyar, ''Design of an efficient cloud security model through federated learning, blockchain, ai-driven policies, and zero trust frameworks,'' *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 10s, pp. 378–388, 2024.

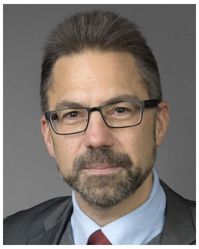
[66] J. Gogia and D. Chakraborty, ''Open banking: A revolution in the tech-fin industry,'' *Int. J. Electron. Banking*, vol. 3, no. 2, p. 100, 2022.

[67] S. Li, M. Iqbal, and N. Saxena, ''Future industry Internet of Things with zero-trust security,'' *Inf. Syst. Frontiers*, pp. 1–14, Mar. 2022.

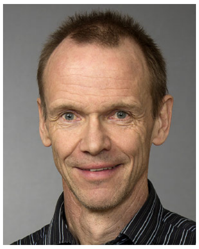
[68] M. A. Enright, E. Hammad, and A. Dutta, ''A learning-based zero-trust architecture for 6G and future networks,'' in *Proc. IEEE Future Netw. World Forum (FNWF)*, Oct. 2022, pp. 64–71.

[69] H. Sedjelmaci, N. Kaaniche, and K. Tourki, "Secure and resilient 6G RAN networks: A decentralized approach with zero trust architecture," *J. Netw. Syst. Manage.*, vol. 32, no. 2, pp. 1–23, Apr. 2024.

NURUN NAHAR received the B.Sc. (Engg.) and M.Sc. (Engg.) degrees in computer science and engineering from the University of Chittagong, Bangladesh, and the M.Sc. degree in computer science and engineering from the South China University and Technology (SCUT), Guangzhou, China. She is currently pursuing the Ph.D. degree in cybersecurity with the Luleå University of Technology, Sweden. Her research interests include artificial intelligence, machine learning, 6G communication, and zero-trust architecture.



KARL ANDERSSON (Senior Member, IEEE) received the M.Sc. degree in computer science and technology from the Royal Institute of Technology, Stockholm, Sweden, and the Ph.D. degree in mobile systems from the Luleå University of Technology, Sweden. After being a Postdoctoral Research Fellow with the Internet Real-Time Laboratory, Columbia University, New York, NY, USA, and a JSPS Fellow with the National Institute of Information and Communications Technology, Tokyo, Japan. He is currently a Chair Professor of cybersecurity with the Luleå University of Technology. His research interests include green and mobile computing, the Internet of Things, cloud technologies, and information security.



OLOV SCHELÉN (Member, IEEE) received the Ph.D. degree in computer networking from the Luleå University of Technology, Sweden. He has more than 20 years of experience in industry and academia. He is currently a Professor with the Luleå University of Technology and also the CEO of Xarepo AB. His research interests include mobile and distributed systems, software orchestration, computer networking, artificial intelligence, and blockchain.

SAGUNA SAGUNA received the master's degree in information technology from Monash University, Clayton, VIC, Australia, in 2008, and the dual Ph.D. degree in information technology from Monash University and in media technology from the Luleå University of Technology (LTU), Luleå, Sweden, in 2013, as a part of the Cotutelle Program between the two universities. She has interned with the IBM Research Laboratory, Gurgaon, India, and CSIRO, Canberra, Australia, during the Ph.D. studies. She is currently an Associate Professor with the Luleå University of Technology, Skellefteå, Sweden. Her research interests include human activity recognition, the IoT, elderly healthcare, anomaly detection, applied machine learning, and cybersecurity within smart city contexts. She was awarded the Promising Young Researcher Award at LTU, in 2018.