Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2025.059170

REVIEW

Zero Trust Networks: Evolution and Application from Concept to Practice

Yongjun Ren[1], Zhiming Wang[1], Pradip Kumar Sharma[2], Fayez Alqahtani[3], Amr Tolba[4] and Jin Wang[5,*]

[1]School of Computer Science, School of Cyber Science and Engineering, Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing, 210044, China

[2]Department of Computing Science, University of Aberdeen, Aberdeen, AB243FX, UK

[3]Software Engineering Department, College of Computer and Information Sciences, King Saud University, Riyadh, 12372, Saudi Arabia

[4]Computer Science Department, Community College, King Saud University, Riyadh, 11437, Saudi Arabia

[5]Sanya Institute of Hunan University of Science and Technology, Sanya, 572024, China

*Corresponding Author: Jin Wang. Email: jinwang@hnust.edu.cn

Received: 29 September 2024 Accepted: 16 December 2024 Published: 17 February 2025

ABSTRACT

In the context of an increasingly severe cybersecurity landscape and the growing complexity of offensive and defensive techniques, Zero Trust Networks (ZTN) have emerged as a widely recognized technology. Zero Trust not only addresses the shortcomings of traditional perimeter security models but also consistently follows the fundamental principle of "never trust, always verify." Initially proposed by John Cortez in 2010 and subsequently promoted by Google, the Zero Trust model has become a key approach to addressing the ever-growing security threats in complex network environments. This paper systematically compares the current mainstream cybersecurity models, thoroughly explores the advantages and limitations of the Zero Trust model, and provides an in-depth review of its components and key technologies. Additionally, it analyzes the latest research achievements in the application of Zero Trust technology across various fields, including network security, 6G networks, the Internet of Things (IoT), and cloud computing, in the context of specific use cases. The paper also discusses the innovative contributions of the Zero Trust model in these fields, the challenges it faces, and proposes corresponding solutions and future research directions.

KEYWORDS

Zero trust; cybersecurity; software-defined perimeter; micro-segmentation; internet of things

1 Introduction

1.1 Origin and Development

In 2010, Kindervag et al. introduced the term Zero Trust [1], advocating for a data-centered, inside-out network design for greater efficiency. Google launched the BeyondCorp project in 2011 [2], based on this concept, to enable seamless work without VPN access from untrusted networks, completing it by 2017. In 2013, Gartner highlighted Zero Trust in its Information Security Market Maturity Model, and the Cloud Security Alliance (CSA) introduced the Software Defined Perimeter (SDP) [3], with

the standard released in 2019. Gartner's 2019 report forecasted that by 2023, 60% of enterprises would replace most VPNs with Zero Trust Network Access (ZTNA). Zero Trust was adopted by U.S. federal agencies in 2014, and in 2017, Alibaba launched the "Zero Trust Security Lab," while 360 Group introduced the "360 Security Brain" [4].

In 2018, Forrester Research recognized Zero Trust as crucial for enterprises facing growing risks and proposed the ZTX architecture [5]. The National Institute of Standards and Technology (NIST) finalized the Zero Trust Architecture in August 2020 [6]. The U.S. Office of Management and Budget (OMB) released a strategy in January 2022 to drive Zero Trust adoption in government cybersecurity, aligning with Executive Order 14028 [7]. The development of Zero Trust is shown in Fig. 1.

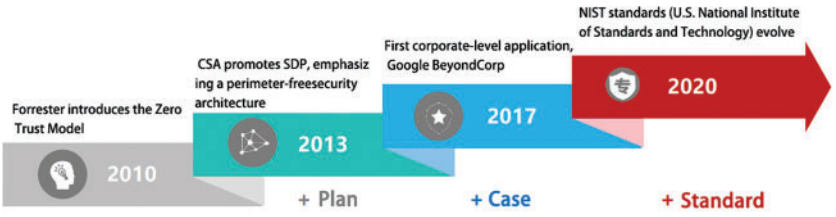

Figure 1: Evolution of zero trust

Numerous private companies have also designed and delivered cutting-edge Zero Trust network security solutions. For example, Microsoft delivers Azure [8] and 365 Security. Citrix provides Workspace [9], Palo Alto Networks supplies Next-Generation Firewalls [10] and VMware offers NSX Advanced Threat Detection [11,12].

1.2 Basic Concepts

Zero Trust Network (ZTN) [6] is a security model based on the principle of "never trust, always verify." It treats all users, devices, and systems—whether internal or external—as potential threats. Consequently, every access request undergoes strict authentication, privilege verification, and security assessment before granting access. ZTN maintains network security by continuously monitoring and analyzing network activities, dynamically adjusting security policies to prevent unauthorized access and potential attacks.

1.2.1 Core Principles

(1) Distrust, Authenticate Everything: The Zero Trust model asserts that no user, device, or network is inherently trusted, requiring strict authentication and authorization for all access requests.

(2) Least Privilege Principle: This model limits access to the minimum necessary to reduce risk and ensure compliance with privacy regulations such as GDPR and HIPAA [13].

(3) Dynamic Access Control: Zero Trust evaluates user, device, and environment status in real time, adjusting access control policies to ensure that only authenticated entities are granted appropriate access [14].

(4) Fine-grained Authentication and Authorization: The model emphasizes detailed user and device authentication to prevent unauthorized access to resources.

1.2.2 Basic Architecture

In Zero Trust network models [15], a three-element architecture is commonly used [16], consisting of subjects, controllers, and objects. A subject (e.g., user or service) sends an access request to the controller, which authenticates and evaluates policy commands. After validating the subject's identity, the controller authorizes access to the object service (e.g., file or application) through the object gateway. The subject then requests data, which the object gateway transfers. This process ensures each access request is evaluated, preventing attackers from bypassing the controller, even if parts of the network are compromised.

This architecture separates the control plane from the data plane, with the controller port fully open to the network, enabling access management and supervision. The controller, central to authentication and access control, also executes policy-based commands. The triangular interaction among subjects, controllers, and objects ensures secure access to services, enhancing network security and resource protection. As shown in Fig. 2.

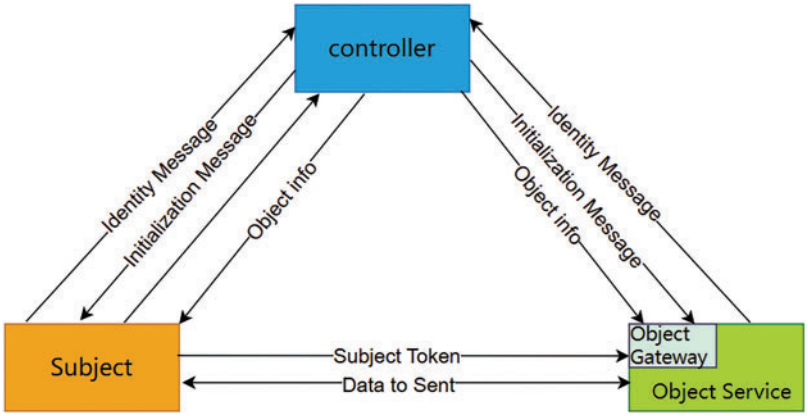

Figure 2: Basic zero trust architecture

Zero Trust represents a shift from the traditional "castle" model, which assumes internal networks are secure while external networks are insecure. The Zero Trust model recognizes that attackers can come from within and can bypass boundary defenses, hence the need for security measures at every corner of the organization. This approach is particularly important for modern enterprises [17] as they frequently adopt cloud services and remote work [18], factors that blur traditional network boundaries. The Zero Trust architecture provides an adaptive and responsive security approach better suited to modern network environments and threat models. This is the reason we came to summarize the zero-trust cybersecurity model [19].

1.3 Contributions

Existing literature on Zero Trust Networks has some limitations. Yan et al. [20] explore zero-trust deployment in IoT, cloud platforms, and big data but lack an in-depth analysis of specific applications' effects and limitations. Sarkar et al. [21] discuss Zero Trust cloud networking, emphasizing its advantages and limitations, but focus primarily on cloud computing, neglecting other areas. He et al. [22] compare core technologies like authentication and access control in Zero Trust architectures, identifying challenges and future research trends, but their review mainly covers technical aspects without examining real-world applications.

In contrast, this dissertation integrates the most recent research results on cutting-edge technologies and applications in the field of zero trust network in various areas, and cites the most recent literature. Aiming to provide new insights and solutions for academia and industry. Our main contributions include:

(1) We provide a systematic comparison of traditional security models and the Zero Trust cybersecurity model, detailing the strengths and weaknesses of the Zero Trust model.

(2) We analyze the key technologies of zero trust, summarizing the principles behind their application, highlighting potential shortcomings in practical implementations, and suggesting directions for future improvements.

(3) We offer a comprehensive overview of the latest research on the application of Zero Trust Networks in network security, 6G networks, the Internet of Things, and cloud computing environments. We explore the innovations and challenges it brings to these fields, and propose possible future solutions and research directions to address current issues. We have selected highly cited or recently published references that cover different aspects of these four fields.

This paper is organized as follows: Section 2 compares the traditional border security model with the Zero Trust security model. Section 3 introduces core Zero Trust technologies, discussing their principles, implementation methods, and applications. Section 4 reviews recent research on Zero Trust in network security, 6G, IoT, and cloud computing, analyzing application cases and experimental results. Finally, the conclusion summarizes the research and presents future outlooks and potential applications.

2 Models of Cybersecurity

Based on whether trust is established on network boundaries, network security models can be divided into two categories: the traditional boundary security model and the zero trust security model Dhiman et al. [23] provided a detailed introduction. The traditional boundary security model protects sensitive resources within the network by constructing multiple layers of defenses. In contrast, the zero trust security model abandons the concept of boundary security and establishes short-term connections through robust authentication, variable trust, and dynamic security risk assessments, using complex security strategies.

2.1 Model of Border Security

The border security model relies on physical and logical boundaries, such as isolating internal and external networks, to protect sensitive resources. It uses devices like Network Address Translation (NAT) to control communication between internal and external networks. While providing defense in depth and coarse-grained access control, the model's reliance on hierarchical network architectures can create a disconnect between security measures and operational realities. Furthermore, attackers can exploit vulnerabilities in boundary devices to penetrate the network and launch attacks from within.

For example, Huawei's internal network security strategy employs a border protection model to prevent unauthorized external access, using firewalls and intrusion detection systems at the network borders. Once an employee successfully logs into the corporate network via VPN, they can access all internal systems without further authentication. While this simplifies access management and improves usability, it also poses risks—if an attacker breaches the boundary, they can move freely within the internal network, posing significant threats.

The border security model has evolved alongside the development of internet technologies and is now mature. Its primary advantage is deep defense capability and coarse-grained access control between different trust domains. However, its reliance on layered internet architecture and regional divisions leads to a lack of integrated security measures within each layer, leaving security largely dependent on the designer's or user's awareness and capabilities. Despite remaining a key security architecture, the increasing complexity of network threats and intelligent attack methods reveal the model's limitations.

2.2 Model of Zero Trust Security

The model of Zero Trust security starts with defending against advanced and internal threats, no longer relying on physical or logical boundaries to define security policies. It embeds security controls into data and resource access decisions, enhancing security through real-time identity verification, access control, and behavioral analysis [24]. The Zero Trust model divides the network into control plane, user plane, and data plane [25] to achieve secure control from access requests to resources. The control plane is responsible for formulating and issuing access policies, the user plane handles identity and device verification, while the data plane is responsible for implementing these policies and controlling data flow. The core of this model is continuous verification and the implementation of the principle of least privilege for every request to address ubiquitous network threats.

For enterprises looking to integrate Zero Trust Network Architecture (ZTN) into their traditional infrastructure, adopting a hybrid model and phased implementation strategy serves as an effective transition approach. During the transition, the coexistence of traditional infrastructure and ZTN is a common practice. Through the hybrid model, enterprises can gradually introduce zero trust principles without fully replacing existing systems. For example, prioritizing the deployment of zero trust in high-risk areas while continuing to use traditional security methods in low-risk areas helps minimize the impact on current operations. Meanwhile, the phased implementation strategy breaks down the deployment of ZTN into multiple stages, allowing enterprises to expand from core systems to edge devices incrementally. With this gradual implementation, businesses can adjust strategies based on feedback, reducing transition risks and more effectively adapting to a zero trust environment.

Although the Zero Trust model is effective, it also presents challenges. Its reliance on user and device identity verification exacerbates the risk of identity theft, although the model mitigates such threats through multiple verifications [26]. Additionally, Zero Trust does not directly mitigate distributed denial of service (DDoS) attacks and requires additional traffic filtering measures for defense. This model retains a significant amount of network data to aid traffic analysis but may also expose system architecture to hackers. While it poses new security challenges, Zero Trust addresses several weaknesses of traditional boundary models and can enhance privacy protection through methods such as site-to-site tunnels [27]. Table 1 presents a comparison of the main functions between the perimeter security model and the zero trust security model.

3 Key Technologies for Zero Trust Networks

The National Institute of Standards and Technology (NIST) in the United States summarized the core technologies of Zero Trust Networks in its "Zero Trust Architecture (ZTA)" white paper [4], referred to as "SIM." These three core technologies include Software-Defined Perimeter (SDP), Enhanced Identity Management (IAM), and Micro-segmentation. Each technology is a key component in implementing a Zero Trust Network. The SIM technology framework is shown in Fig. 3.

Table 1: Comparison of model of border security and Zero Trust security

Category	Model of border security	Model of Zero Trust security
Trust basis	Implicit trust within the network	No implicit trust, verification required for each access
Access control	Mainly at the perimeter, less control internally	Granular controls throughout the network
Threat perception	Focus on external threats	Focus on both internal and external threats
Key mechanism	Firewall	Dynamic and context-aware access control
Security principle	Security is based on network segmentation	Security is based on strict user and device verification
Implementation	Implementation tied to network architecture, hard to change	Flexible implementation, adapts to various environments
Data handling	Data security mainly through network controls	Data security through encryption and rigorous access policies
Operational complexity	Management mainly at network level, simpler for internal operations	High complexity due to continuous verification requirements

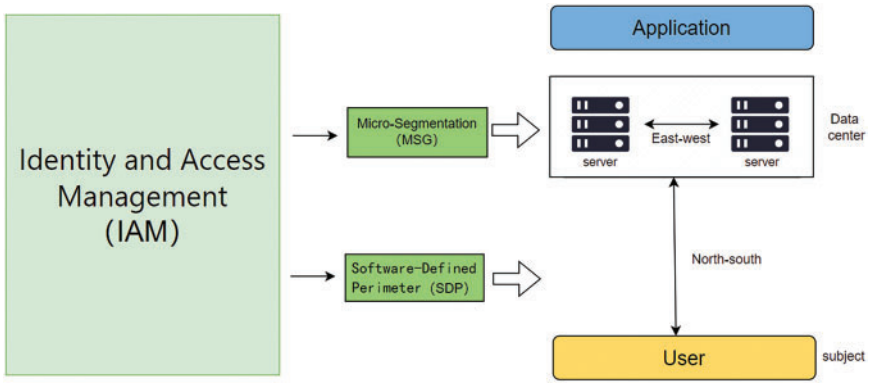

Figure 3: SIM technology framework

In this architecture, all communication flows and access permissions are strictly controlled. IAM ensures that all user identities are rigorously verified, and SDP technology is used to implement fine-grained access control policies to manage north-south traffic between users and servers. Meanwhile, east-west traffic between internal servers is micro-segmented using MSG technology, ensuring that even internal requests are rigorously checked, significantly reducing the possibility of internal threats. This architecture reflects the core ideas of Zero Trust principles: no longer defaulting to trust within the network, but always maintaining verification and least-privilege principles, providing a detailed security framework for network safety. Table 2 provides a concise and easily understandable introduction to the three major technologies.

Table 2: Key Technologies (SIM)

Technology	Main function	Advantages
Software Defined Perimeter (SDP)	Identity-based access control, protect external accessk	Minimize attack surface, protect critical assets
Identity and Access Management (IAM)	Manage user identities, control resource access permissions	Centralized management of user identities, enhances security and compliance
Micro-Segmentation (MSG)	Divides the network into micro-nodes, controls traffic flow	Fine-grained control, prevents lateral movement

3.1 Software-Defined Perimeter (SDP)

Software-Defined Perimeter (SDP) is a next-generation network security model based on Zero Trust philosophy [28]. It uses software to create virtual boundaries, utilizing identity-based access control mechanisms to cloak applications and services, thus protecting corporate data security [29]. SDP enhances access control management and sets standards for user access, network access, and system authentication. SDP is not intended to replace existing identity and access management solutions but rather to strengthen access control by integrating authentication and authorization with other security components, reducing potential attack surfaces. Yan et al. [30] proposed a decentralized SDP mechanism leveraging blockchain technology. Multiple SDP controllers form a blockchain network, tasked with authenticating and authorizing hosts. The authorization policies are defined by the hosts that adopt SDP.

SDP technology is rooted in the concept of Software Defined Networking (SDN) [31], separating the control layer from the data layer to achieve flexible control and management of the network. The SDP architecture consists of three main components: SDP hosts, SDP controllers, and SDP gateways. SDP client hosts initiate connections, SDP gateways accept connections, and SDP controllers manage these connections. These operations are managed through a secure control channel interacting with SDP controllers, thus achieving separation of the control plane and data plane for a fully scalable system. The core of SDP is the use of Single-Packet Authorization (SPA) technology to hide business systems and employ an "IP whitelist" access control model, preventing unauthorized clients from accessing business resources. The SDP architecture is shown in Fig. 4.

In this architecture, the SDP controller is responsible for conducting authentication prior to access and manages the opening and closing of data channels between hosts. Consequently, SDP can effectively protect against remote virtual machine manager attacks, virtual machine hopping, and port scanning [32]. Moreover, to facilitate scalability and ensure normal use, all components can be multiple instances. In use, each server is hidden behind a remote access gateway device. Before the authorization service is visible and allowed access, the user must undergo identity verification. SDP adopts the logical model used in segmented networks and integrates this model into standard workflows.

The future improvements of SDP technology can be summarized in four key areas: First, with the widespread adoption of cloud computing, edge computing, and IoT devices, the SDP architecture needs further optimization to support data management and dynamic application processing in distributed environments. Second, SDP should enhance fine-grained access control, using more

detailed policy designs to address complex and dynamic security scenarios, thereby improving the defensive effectiveness of the zero trust architecture. Additionally, SDP must deeply integrate with emerging technologies such as artificial intelligence and DevSecOps to ensure security protocols are aligned during development and operations, addressing the challenges of integrating traditional and modern systems. Lastly, by introducing adaptive threat detection mechanisms and incorporating machine learning models, SDP can improve its dynamic isolation and defense against new types of attacks, such as customized malware.

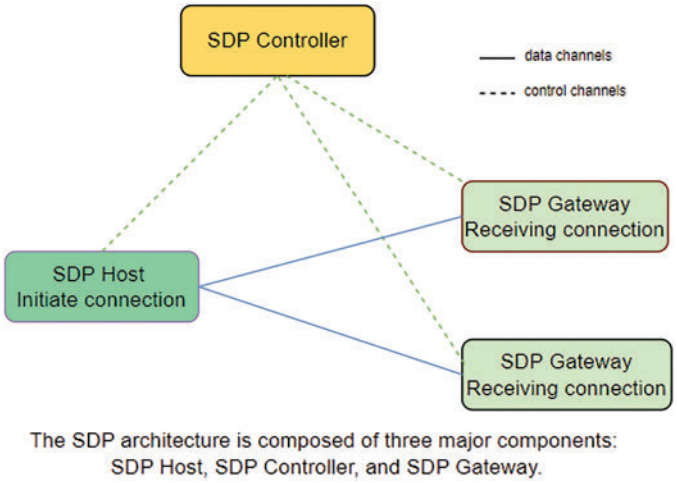

Figure 4: SDP architecture diagram

3.2 Identity and Access Management (IAM)

IAM systems are a crucial element of Zero Trust architecture, tasked with managing user identities and access permissions [33,34] to ensure that the correct individuals access appropriate resources in the proper manner and at the right time. Traditional authentication and authorization mechanisms are foundational to IAM, but modern IAM systems also incorporate security technologies such as multi-factor authentication, behavioral analysis, and fine-grained access control policies.

Through multi-factor authentication (MFA), IAM systems require users to provide multiple authentication factors (e.g., password, mobile code, fingerprint) [35], enhancing security and ensuring compliance with privacy regulations such as GDPR and HIPAA. Implementing a Zero Trust architecture in large organizations presents challenges, particularly regarding the impact of continuous verification on network performance, potentially increasing latency. Optimizing the authentication process, adopting MFA, and using risk-based verification can mitigate this burden. However, selecting and configuring authentication factors remains a challenge for both administrators and users. Preuveneers et al. [36] proposed AuthGuide, a framework that increases abstraction in MFA configuration through a series of questions integrated into IAM's authentication workflows. Behavioral analysis can detect anomalies by monitoring user behavior patterns, while fine-grained access control policies allow dynamic adjustment of permissions based on factors like identity, device status, and network environment, providing more precise control. Xu et al. [37] proposed a fine-grained access control and data sharing scheme for dynamic user groups to improve cloud data sharing among authorized users.

In a Zero Trust network environment, the challenges faced by Identity and Access Management (IAM) cannot be resolved by a single new technology but require the integration and optimization

of existing Access Control (AC) technologies. Access control is a key mechanism for maintaining information security, aimed at preventing unauthorized access both inside and outside an organization and effectively managing the granting and revocation of user permissions. This mechanism ensures that only authorized individuals, processes, and systems can access sensitive resources. Access control models are precisely defined in their enforcement mechanisms and security policies, implemented internally according to the specific goals and needs of the organization.

Traditional access control models, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC), form the foundation of access control. On top of traditional models, a series of hybrid access control models have been developed. Due to the numerous hybrid models, they will not be elaborated here. Aftab et al. [38] conducted an in-depth examination of access control models and compared traditional and hybrid access control models based on their respective access control standards.

Currently, IAM technology still faces some potential shortcomings. As the scale of networks and users expands, IAM may encounter difficulties in scaling and management, particularly in multi-cloud and hybrid environments. Secondly, dynamic threat response may lag, especially when facing complex attack behaviors, where the speed and accuracy of IAM systems may have limitations, indicating areas for optimization. Additionally, there may be conflicts between authentication and privacy protection in IAM, especially when handling sensitive biometric data, increasing the potential for future legal and compliance risks. While enhancing security, the decline in user experience is also a challenge, as complex authentication processes could affect user satisfaction. Finally, IAM relies on the integration of various technologies, and issues with cross-platform interoperability could result in access control failures or security vulnerabilities. These challenges suggest that IAM needs continuous optimization under the Zero Trust architecture to address these concerns.

3.3 Micro-Segmentation

Micro-segmentation technology transforms the network from a single security zone into multiple small, manageable segments, each capable of being independently controlled and protected. Initially used in Ethernet, its main purpose was to limit broadcast domains and reduce collisions. As technology has evolved, micro-segmentation has gradually been applied to virtualization [39] and cloud computing environments [40]. By adopting software firewalls internally, logical isolation is achieved within the data center, thereby establishing a secure boundary [41,42].

We summarize the specific advantages of micro-segmentation:

(1) Reduced Attack Surface: Segmenting the network into numerous small security zones can decrease the overall network attack surface, making it challenging for attackers to access all sensitive information simultaneously.

(2) Improved Lateral Movement Security: Each security segment can be independently controlled and protected, preventing the spread of malicious activity within the network and enhancing the detection and prevention of lateral movements.

(3) Security for Critical Applications: Micro-segmentation can be used to protect security-critical applications, ensuring they do not affect the normal operation of other non-critical applications if compromised.

(4) Improved Regulatory Compliance: Dividing the network into multiple security segments can better meet regulatory and compliance requirements, ensuring the secure storage and transmission of sensitive data.

Micro-segmentation is widely applicable and can be specifically applied to different targets, such as CPU time, memory access, network access, etc. It can be implemented in a virtualized environment and also found in shared kernel environments such as container technology [43], providing flexible and powerful security controls. In the Zero Trust model, micro-segmentation plays a role in defending against and limiting lateral movement attacks. Zhang et al. [44] designed a security control strategy called "Light Verification" to restrict east-west traffic between devices or components based on Zero Trust model principles, helping to reduce detection costs with ease. Through MSG technology, the Zero Trust model achieves more detailed, dynamic, and controllable network segmentation, offering higher levels of network security and data protection.

In the Zero Trust network architecture, Micro-segmentation, as a key implementation technique [45], has the core objective of providing effective security capabilities for protected service resources in an environment where boundaries are gradually disappearing [46]. Due to the different research directions of researchers and technical backgrounds of vendors, the specific implementations of Microsegmentation vary. However, the various implementation approaches all aim to solve this core problem. Table 3 shows the current implementation methods of micro-segmentation technology in the Zero Trust architecture and its potential future improvement solutions.

Table 3: Current implementation methods of micro-segmentation technology

Current implementation methods	Isolation method	Challenges	Solutions
Virtual Network-based Microsegmentation	VLANs, virtual switches	Complex configuration, poor scalability	Automated tools, cross-cloud management
Host-based Microsegmentation	Host firewalls, policy controls	Errors in large-scale workloads	AI optimization, dynamic load handling
Container-based Microsegmentation	Container networks, security policies	Cluster communication, misconfigurations	Granular policies, automated orchestration
Application-based Microsegmentation	App-level policies, authentication	Complex access control, security risks	Identity-based control, blockchain verification
Network Segmentation-based Microsegmentation	SDN segmentation	Management complexity, manual lag	Automated tools, real-time policy adjustment
Service Mesh-based Microsegmentation	Service mesh policies	Complex configuration	Lightweight mesh, concurrency optimization

Taken together, micro-isolation technology combines the reliability of hardware devices, the fine-grained control of agent software, the flexibility of software exchange, and the isolation capability of virtualization through the above several implementations, forming a multi-level, multi-dimensional security and protection system, and providing a solid foundation for the Zero Trust Network Architecture.

4 Application Scenarios of Zero Trust Network

4.1 Network Security

The fundamental concept of Zero Trust security is that no person, device, or system inside or outside the network should be trusted by default. Instead, network security should be reestablished based on authentication and authorization mechanisms [47]. Zero Trust abandons the traditional network security architecture which assumes internal networks are safe and constructs digital moats around enterprises with firewalls, WAFs, IPS, and other perimeter security products while neglecting the security of the internal network [48].

The National Institute of Standards and Technology (NIST) describes Zero Trust Architecture as an end-to-end approach to network/data security in its publication Zero Trust Architecture. NIST criticizes traditional security solutions for focusing only on perimeter defenses and providing overly broad access to authenticated users. The primary goal of a Zero Trust Architecture is to implement fine-grained access controls based on identity to reduce the growing risk of unauthorized lateral movement. With these perspectives in mind, NIST has defined a Zero Trust Architecture that provides a set of concepts, principles, components, and their interactions designed to eliminate uncertainty in making precise access decisions about information systems and services.

In the book "Zero Trust Networks" [49], authors Evan Gilman and Doug Barth outline Zero Trust Architecture based on five core assumptions: the network is always vulnerable; threats exist both inside and outside the network; network location does not imply trustworthiness; all devices, users, and network traffic must be authenticated and authorized; and security policies must be dynamic and derived from multiple data sources.

In network security practice, the Zero Trust model introduces a variety of technological means to provide comprehensive protection strategies. For example, The design and prototype implementation of the NEUTRON Policy Framework is presented by Katsis et al. [50]. A flexible, graph-based approach to defining and sharing complex, fine-grained cybersecurity policies is employed, providing an automated end-to-end policy pipeline for specification, management, testing, and deployment. Kholidy et al. [51] proposed a dynamic, data-driven Zero Trust Security Framework (ZTSF) designed to reliably deploy and securely manage 5G network slices. A multi-criteria approach is used to quantify the end-to-end trust of 5G open architecture entities, taking into account security factors such as vulnerability, exploitability, and attackability, as well as service level agreement (SLA) breaches and user experience assessments for network slices (NS) and virtualized network functions (VNF). Yan et al. [30] point out that Zero Trust network security is a strategy against frequent attacks in current network environments. In the big data field, potential security risks can be identified and intercepted by constructing user identity models and auditing network traffic information. In cloud networks, introducing trusted third-party assessments of cloud network security and implementing a network of trust among users is crucial. In the public cloud Infrastructure as a Service (IaaS) platform, it helps build, evaluate, and manage trust relationships between users and cloud service providers. In the IoT environment, malicious attacks and security issues in network environments can be addressed by establishing context-aware trust management systems and applying blockchain technology [52].

The application of the Zero Trust model in network security has shown its innovation and effectiveness across multiple domains. For example, Surantha et al. [53] analyzed a Kubernetes application for a financial service company in Indonesia aimed at improving their digitally serviced applications developed using a microservices architecture. By applying Kubernetes in the enterprise's digital service applications, they successfully integrated new technologies and services. Anderson et al. [54] noted that as the COVID-19 pandemic pushed businesses and employees towards remote work, important

questions about the security of remote access arose. This paper explores the role of BYOD (Bring Your Own Device) in remote work and presents the challenges and opportunities of implementing Zero Trust concepts in BYOD security. A Zero Trust access control policy specification for BYOD was proposed, and a corresponding network architecture was designed to support enterprise Zero Trust BYOD use cases. Further applications include Zero Trust security monitoring [55], industrial IoT [56], healthcare [57], metaverse [58], environmental monitoring networks, commercial banking, government units, university networks, and airport networks, demonstrating the applicability and effectiveness of Zero Trust architecture in facing specific needs and challenges.

4.2 6G Networks

As technological advancement and digital transformation accelerate, our reliance on Information Technology (IT) continues to grow, especially in terms of solutions, devices, systems, networks, and processes. In this context, the sixth generation (6G) network technology has been proposed, marking an important direction of development—creating purpose-built networks. Unlike previous network designs, 6G networks are envisioned to be designed starting from specific application use cases, rather than making application demands adapt to network capabilities.

While 6G technology aims to deepen the integration of digital and physical worlds, this advancement also introduces unprecedented security challenges. Breaches in information security are not limited to data loss, loss of device control, or financial damages; more critically, they could pose threats to personal safety and cause massive property damage [59]. To address these security challenges and ensure the reliability of 6G networks, the adoption of a Zero Trust security architecture becomes necessary. In a Zero Trust Network environment, all devices or terminals must undergo a security assessment before connecting to the network to ensure they meet security requirements. With this embedded trust mechanism, 6G networks will offer a level of security far surpassing current network technologies.

6G networks will become a core platform for the integration of physical and virtual worlds, by integrating processing, communication, intelligence, sensing, and storage capabilities to enable seamless collaboration between devices and their digital twins (DT) during service provision. In this context, digital twins become an indispensable part of 6G networks, not only providing a virtual representation of physical elements and their dynamics and functions but also playing a key role in driving the intelligence and adaptability of the network. To address security and scalability issues in 6G networks, Ridhawi et al. [60] proposed an innovative framework that combines the Zero Trust security architecture with 6G networks supported by digital twins. Unlike traditional Zero Trust solutions, this framework adopts a decentralized approach and integrates blockchain technology, successfully resolving issues related to the scalability and security of physical devices and their digital twins.

Additionally, Chen et al. [61] designed a new Zero Trust architecture based on Software-Defined Perimeter (SDP), aimed at enhancing the network's collaborative defense against threats. In this architecture, relying on trust assessments from Third-Party Security Services (TPSS), the community can achieve highly complex access control for visitor user equipment (UE), while implementing distributed identity management through an innovative digital certificate system, enhancing the overall network's security and resilience.

Faced with the challenges of Zero Trust vehicular networks in 6G [62], Hao et al. [63] proposed an efficient and trustworthy access method and security architecture, successfully solving the issues of vehicle verification and authorization, providing a solid foundation for secure communication in vehicular network environments. This study also emphasizes the importance of further reducing

authentication latency as a future focus for vehicular network research, highlighting key directions for optimizing network performance and enhancing user experience.

Existing Zero Trust architectures are unable to overcome the security challenges faced by 6G networks:

(1) Current Zero Trust architectures use fine-grained access control strategies to protect all data resources and computational services. This feature cannot meet the challenges brought about by the massive scale of 6G networks.

(2) Existing Zero Trust architectures are primarily designed for single network domains with a logical centralized controller. They cannot be applied to heterogeneously managed 6G networks with decentralized architectures.

(3) For existing Zero Trust architectures, end-to-end encryption is mandatory. Due to resource limitations, the massive IoT terminals in 6G networks cannot meet this requirement.

(4) While emerging software-defined perimeter (SDP) technology has extended Zero Trust architectures to the network and transport layers, other challenges remain largely unaddressed. Customizing Zero Trust architectures to the security needs of large-scale 6G networks has become a critical issue.

4.3 Internet of Things (IoT)

With the rapid development of Internet of Things (IoT) technology, the interconnection between IoT devices has formed a vast, diverse, and dynamic distributed network. In this complex network, establishing an effective security mechanism is as crucial as enhancing IoT performance.

Facing the efficiency of IoT data storage, Wang et al. [64] proposed an efficient blockchain-based IoT data storage scheme (S-BDS) by integrating sharding. They developed an insertable vector commitment (IVC) within bilinear groups and substituted Merkle trees with IVC to store IoT data on the blockchain. This approach effectively reduces communication congestion to address the complexity of heterogeneous and interoperable data generated by smart homes, smart grids, and remote information processing in IoT environments. It enhances the stability and security of IoT systems. Han et al. [65] constructed a blockchain-based Zero Trust Data Storage (ZT-BDS) for 6G edge IoT that proposes using a Porosity-based Renewable Polynomial Commitment (PoR) scheme instead of PoW, to collect and store data at the 6G edge of IoT. They introduced an improved distributed storage scheme using PoR as the consensus algorithm, replacing Merkle trees with dynamic accumulators to enhance storage and bandwidth capabilities. Future work will focus on privacy protection.

Facing Data Security of IoT, The development of the power IoT architecture raises higher demands for data layer data security storage. To achieve fine-grained access control of data resources in distributed databases within the power IoT, Huang et al. [66] proposed a scheme to protect data resources using Zero Trust architecture components. This involves using dynamic trust management to make real-time, context-aware decisions and authorizations on access requests, implementing fine-grained access control methods to minimize authorization to access subjects, and finally, discussing methods to optimize access control performance through multi-granularity policy matching and permission expansion. Liu et al. [67] proposed a novel blockchain-based data sharing solution within a Zero Trust environment, utilizing smart contracts, effective voting, and consensus mechanisms to filter out forged information and prevent unauthenticated participants from sharing junk data. They also propose that reducing communication delay and computational overhead of protocols is one of

the future research directions. Awan et al. [68] discuss fundamental cyber threats and vulnerabilities in smart environments and propose the ZAIB (Blockchain-based Zero Trust and ABAC for IoT) new security framework. The framework monitors and facilitates inter-device communication through different levels of access control mechanisms based on environmental parameters and device behavior. Issues such as user privacy, device authentication and authorization are addressed. Colombo et al. [69] presented a set of requirements that IoT access control solutions need to meet to be in line with ZT principles. The proposed requirements involve the access control models adopted.

Combining blockchain technology, Zero Trust management is evolving toward higher levels of security policies. For instance, Khan [70] proposes a Fabric-IoT access control system based on Zero Trust blockchain to address security and scalability issues in IoT device resource access control. Traditional centralized methods rely on a single server or central node, leading to single points of failure, low reliability, and poor scalability. This approach leverages blockchain's distributed storage and smart contracts, using consensus mechanisms to ensure secure data sharing and dynamic handling of access control. This method not only eliminates single points of failure but also enhances system security and data consistency, thereby managing resource access for IoT devices more effectively. Further, Zhao et al. [71] introduced a novel authentication scheme that uses blockchain technology to elevate smart devices from untrusted to trusted status. This introduces a new perspective on device authentication and security certification, allowing devices to confirm their trustworthiness in a decentralized and tamper-proof environment.

Challenges in the IoT environment include:

(1) Heterogeneous Devices and Multiple Protocol Environment: Different devices and the use of multiple heterogeneous protocols increase the sensitivity of the IoT network to data leaks [72].

(2) Limitations of the Sensing Layer: Devices in the sensing [73] layer typically have limited computational resources, high mobility, and widespread geographic distribution, which increases the complexity of authentication and access control.

(3) Malicious Code and Software Attacks: IoT networks and devices are susceptible to malicious code injections, malware attacks, and sinkhole and wormhole attacks.

(4) Expansion beyond Secure Network Boundaries: IoT networks have expanded beyond the organization's predefined secure network boundaries, increasing the difficulty of regulation. By adopting a Zero Trust architecture, utilizing methods such as dynamic policy adjustments, network microsegmentation, and automated security management, the authentication and access control of devices and users can be strengthened.

(5) Openness and Diversity of Protocols at the Transport Layer: The openness of the transport layer and support for multiple protocols make it susceptible to RF interference and jamming attacks.

In response to these issues, Dhar et al. [74] proposed an innovative security framework based on Zero Trust principles and blockchain technology, aimed at enhancing the security of IoT devices. This framework introduces a novel risk scoring method and five recommendations for IoT security management, providing solutions for addressing security issues.

4.4 Cloud Environment

In cloud computing, the concept of Zero Trust provides new solutions to address the increase in internal attacks within the cloud environment. Traditional security boundaries, which merely divide the network into trusted internal and untrusted external parts, fail to effectively protect against internal threats, especially the potential for data loss, theft, and damage due to lateral attacks within the cloud.

Consequently, scholars have introduced the concept of Zero Trust into cloud environments and have made adjustments to existing technologies.

The classification and application of Zero Trust Network mechanisms in cloud computing are crucial components in ensuring the security of cloud environments. Ahmadi et al. [75] explored the implementation of Zero Trust Architecture (ZTA) in addressing security challenges within cloud networks. Using qualitative research methods, including a systematic literature review from 2020 to 2024, they examined insights from diverse sources such as journal articles, academic literature, and case studies. The study reveals ZTA's impact on mitigating lateral movement, reducing the probability of insider threats, enhancing network micro-segmentation, and improving identity and access management. Traditional trust management mechanisms are static, but these relationships tend to deteriorate when meeting the dynamic requirements of cloud services. To address this challenge, Mehraj et al. [76] proposed a conceptual Zero Trust strategy for cloud environments. This model provides a conceptual type for establishing perceptions and philosophies of trust in cloud services and discusses the importance and challenges of establishing trust in cloud computing.

The practice of Zero Trust Network architecture is a key issue in the current field of cloud security. Ferretti et al proposed a novel survivable Zero Trust architecture [77], aimed at ensuring the necessary security levels within the cloud computing environment. This architecture not only guarantees a high level of security and robustness but also tolerates intrusions and recovers from failures and successful attacks under certain conditions.To address the deficiencies of existing authenticated key exchange (AKE) schemes in mobile cloud computing environments, particularly regarding resistance to chosen-ciphertext attacks (IND-CCA) and protection against malicious private key generators (mPKG), Hossain et al. [78] proposed a public key encryption (PKE) scheme based on the ADOW trapdoor function. This scheme employs signaling technology and projection functions to achieve key-dependent message security (KDM), pseudo-random ciphertext property (PCP), and reproducible randomness property (RRP), while ensuring IND-CCA security. Furthermore, a zero-trust architecture-based secure authentication scheme, ASMCC+, was constructed based on this PKE scheme, effectively safeguarding the privacy of consumer electronics users (CEU) and cloud servers. With the rise of cloud microservices, attackers can exploit cross-service dependencies to propagate laterally within data centers. To address this challenge, Zaheer et al. [79] proposed eZTrust, a network-agnostic microservice method. eZTrust allows data center tenants to specify access control policies based on fine-grained workload identities and uses the extended Berkeley Packet Filter (eBPF) to verify these identities, effectively preventing cross-service dependency attacks. However, this network has less accountability and oversight over its overall security and remains passive. To address this issue, emerging technologies like Zero Trust Network Architecture (ZTNA) have restructured cloud network security methods. Sarkar et al. [21] surveyed several implementations of cloud network models based on Zero Trust and compared the novel features used by the latest research models for specific needs. They investigated various methods and applications for authenticating and authorizing key services in trust-based cloud networks and identified several challenges with transitioning from existing system architectures to implementing Zero Trust in cloud environments. The most significant obstacle identified was the human factor. Compared to other security architectures, Zero Trust focuses more on fine control over data but also may pose risks to privacy. In today's dominant storage and management environments, the security of the cloud is crucial. Therefore, when deploying Zero Trust, appropriate architectures and methods must be designed for data privacy.

In specific domains, Jasim et al. [80] proposed a method to protect location-based service (LBS) data privacy using cloud services in a specific domain. Based on zero trust, they achieve data privacy protection by managing system access rights. The method stores user location data on a secondary

server rather than in untrustworthy third-party applications. The study ensures user data privacy on each server by distributing data from different sources to different servers through data partitioning and a multi-level policy model that allows access to third-party applications only on specified servers. Zero trust is significantly used in distributed volunteer cloud networks, Albuali et al. [81] proposed a client-server model for verifying the trust level of nodes. The system introduces a behavior-based adaptive system that assigns tasks to the most trusted nodes and manages their lifecycle. Nodes with low trust level are blacklisted and assigned secondary tasks or no tasks.

There are many challenges to realizing a Zero Trust network in a cloud environment, and the following are three relatively important challenges that may be faced today:

(1) Dynamic Scalability: The dynamic and elastic nature of cloud environments allows the number, location, and configuration of resources and services to constantly change, making it difficult for traditional static security policies to adapt. This dynamic scalability requires a Zero Trust architecture that can update and adapt security policies in real-time to accommodate new resources and services. This not only increases the complexity of policy management, but also requires efficient automation and orchestration mechanisms to dynamically manage policy rules and ensure that security controls are applied in a timely and effective manner when resources or services change.

(2) Cross-Cloud Interoperability: In multi-cloud or hybrid cloud environments [82], applications and data may be distributed across different cloud provider platforms, which raises the issue of cross-cloud security controls and policy consistency. Security models and interfaces vary across cloud providers, complicating the implementation of a unified Zero Trust policy. Standardized interfaces and protocols across clouds need to be established to ensure consistency and interoperability of security policies across different cloud environments while maintaining efficient access control and monitoring capabilities to address complex cross-cloud security challenges.

(3) Data Privacy and Compliance: Data storage and processing in cloud environments involves multiple legal and regulatory frameworks, especially in cross-border data transfer and processing scenarios. Zero Trust architectures need to ensure data privacy protection and compliance during transmission, storage, and processing, which includes stringent requirements for data encryption, access control, data minimization, and compliance auditing. In addition, data segregation and privacy protection in multi-tenant environments need to be addressed to prevent data leakage and unauthorized access.

5 Conclusion

Since the concept of Zero Trust network was proposed in 2010, it has experienced a remarkable transformation from theory to practical application, and has not only been deeply explored in the field of theoretical research, but also widely used in practice. The Zero Trust model has gradually become an indispensable part of modern network security, promoted by companies such as John Cates and Google. Through continuous development, the Zero Trust model has evolved from a simple concept to a comprehensive security strategy that encompasses a variety of key technologies such as software-defined perimeter (SDP), enhanced identity management (IAM), and microisolation. Together, these technologies have resulted in a security model that emphasizes continuous authentication and authorization regardless of user, device, or network location.

The application of the Zero Trust security model continues to expand from the initial cybersecurity domain to emerging technologies such as 6G networks, IoT, and cloud computing. With the acceleration of technological advances and digital transformation, these areas are facing increasing

security challenges, and the Zero Trust model provides an adaptable and responsive security protection approach that is more suitable for modern network environments and threat models. Especially in 6G networks and IoT environments, the Zero Trust model not only effectively responds to the security challenges posed by large-scale and heterogeneous networks, but also enhances the reliability and protection of the network through a decentralized approach and blockchain technology.

Overall, the research and application of Zero Trust network demonstrates the cutting-edge development trend in the field of network security, which is of great significance for improving the level of network security and responding to the increasingly complex network threats. In the future, with the continuous progress of technology and security needs, the Zero Trust model will continue to evolve, bringing more innovations and challenges to the field of cybersecurity.

Acknowledgement: Thanks to the anonymous reviewers and editors for their hard work.

Funding Statement: This work was supported by the National Natural Science Foundation of China (Grants Nos. 62473146, 62072249 and 62072056), the National Science Foundation of Hunan Province (Grant No. 2024JJ3017), the Hunan Provincial Key Research and Development Program (Grant No. 2022GK2019), and by the Researchers Supporting Project Number (RSP2024R509), King Saud University, Riyadh, Saudi Arabia.

Author Contributions: The authors confirm their contribution to the paper as follows: Conceptualization and Design: Yongjun Ren, Amr Tolba, Jin Wang; Methodology: Yongjun Ren; Software: Yongjun Ren, Fayez Alqahtani; Investigation: Zhiming Wang; Data Curation: Zhiming Wang, Fayez Alqahtani; Funding Acquisition: Pradip Kumar Sharma, Jin Wang; Project Administration: Pradip Kumar Sharma, Jin Wang; Writing—Original Draft: Zhiming Wang, Yongjun Ren, Fayez Alqahtani; Writing—Review & Editing: Zhiming Wang, Jin Wang; Supervision: Amr Tolba, Jin Wang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: No datasets were used or generated during the current study.

Ethics Approval: This study did not involve any human or animal subjects, and therefore, ethical approval was not required.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] J. Kindervag *et al.*, *Build Security into Your Network's DNA: The Zero Trust Network Architecture*, Forrester Research Inc., 2010, vol. 27, pp. 1–16.

[2] R. Ward and B. Beyer, "BeyondCorp: A new approach to enterprise security," *USENIX SAGE*, vol. 39, no. 6, pp. 6–11, 2014.

[3] C. S. A. (CSA), "SDP specification v1.0," 2014. Accessed: Aug. 20, 2024. [Online]. Available: https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

[4] H. Zhou, "360 security brain leads the intelligent era of security protection," (in Chinese), *Cybersecur. Informatizat.*, vol. 3, no. 6, p. 18, 2018.

[5] M. Katzer, "Azure and office 365 security," in *Securing Office 365*. Apress, Berkeley, 2018. pp. 43–96, 2018.

[6] V. Stafford, "Zero trust architecture," NIST Special Publication 800-207, 2020. doi: 10.6028/NIST.SP.800-207.

[7] S. D. Young, "Moving the US government toward zero trust cybersecurity principles," The White House's Office of Management and Budget, 2022.

[8] B. Wilder, *Cloud Architecture Patterns: Using Microsoft Azure*. Sebastopol, CA: O'Reilly Media, Inc., 2012.
[9] A. Halfpenny, *Welcome to Citrix Workspace (PC)*. Road Fort Lauderdale, USA: Policy, 2023.
[10] P. Perminov, T. Kosachenko, A. Konev, and A. Shelupanov, "Automation of information security audit in the information system on the example of a standard "cis palo alto 8 firewall benchmark"," *Int. J.*, vol. 9, no. 2, pp. 2085–2088, 2020. doi: 10.30534/ijatcse/2020/182922020.
[11] S. Keeriyattil, "Zero trust networks with VMware NSX: Getting started," in *Zero Trust Networks with VMware NSX*, Berkeley, CA: Apress, 2019. doi: 10.1007/978-1-4842-5431-8_3.
[12] J. Pettit *et al.*, "Bringing platform harmony to VMware NSX," *2018 ACM SIGOPS Oper. Syst. Rev.*, vol. 52, no. 1 , pp. 123–128, 2018. doi: 10.1145/3273982.3273994.
[13] R. Das, *The Zero Trust Framework and Privileged Access Management (PAM)*. Milton Park, Oxfordshire, USA: CRC Press, 2024.
[14] K. Hatakeyama, D. Kotani, and Y. Okabe, "Zero trust federation: Sharing context under user control towards zero trust in identity federation," in *2021 IEEE Int. Conf. Pervasive Comput. Commun. Workshops other Affiliated Events (PerCom Workshops)*, IEEE, 2021, pp. 514–519.
[15] S. Wang, B. Zhang, B. Shi, and Y. Shen, "Analysis and inspiration of key elements of zero trust network architecture," in *2024 2nd Int. Conf. Mechatron., IoT Industr. Inform. (ICMIII)*, IEEE, 2024, pp. 938–941.
[16] 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, 2023, Art. no. 1595. doi: 10.3390/e25121595.
[17] O. Sheridan, "The state of zero trust in the age of fluid working," *Netw. Secur.*, vol. 2021, no. 2, pp. 15–17, 2021.
[18] W. Kou, H. Zhou, and J. Du, "Research on telecommuting security solution based on zero trust architecture," in *Int. Conf. Comput. Eng. Netw.*, Springer, 2023, pp. 82–89.
[19] Y. Bobbert and J. Scheerder, "Zero trust validation: From practical approaches to theory," *Sci. J. Res. Rev.*, vol. 2, no. 5, pp. 830–848, 2020. doi: 10.33552/SJRR.2020.02.000546.
[20] X. Yan and H. Wang, "Survey on zero-trust network security," in *Artif. Intell. Secur.: 6th Int. Conf., ICAIS 2020*, Hohhot, China, Springer, Jul. 17–20, 2020, pp. 50–60.
[21] 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, 2022, Art. no. 11213. doi: 10.3390/su141811213.
[22] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wirel. Commun. Mob. Comput.*, vol. 2022, no. 1, 2022, Art. no. 6476274. doi: 10.1155/2022/6476274.
[23] P. Dhiman, *et al.*, "A review and comparative analysis of relevant approaches of zero trust network model," *Sensors*, vol. 24, no. 4, 2024, Art. no. 1328. doi: 10.3390/s24041328.
[24] J. Seaman, "Zero trust security strategies and guideline," in *Digital Transformation in Policing: The Promise, Perils and Solutions*. Cham, Switzerland: Springer, 2023, pp. 149–168.
[25] Q. Wang, Q. Yuan, F. Li, and L. Xia, "Review of zero trust networks and their key technologies," (in Chinese), *J. Comput. Appl.*, vol. 43, no. 4, 2023, Art. no. 9.
[26] L. Meng, D. Huang, J. An, X. Zhou, and F. Lin, "A continuous authentication protocol without trust authority for zero trust architecture," *China Commun.*, vol. 19, no. 8, pp. 198–213, 2022. doi: 10.23919/JCC.2022.08.015.
[27] D. Barth and E. Gilman, "Zero trust networks: Building trusted systems in untrusted networks," Accessed: Aug. 20, 2024. [Online]. Available: 2017. https://dl.acm.org/doi/book/10.5555/3161337
[28] A. Moubayed, A. Refaey, and A. Shami, "Software-defined perimeter (SDP): State of the art secure solution for modern networks," *IEEE Netw.*, vol. 33, no. 5, pp. 226–233, 2019. doi: 10.1109/MNET.2019.1800324.
[29] J. Kindervag, *Applying Zero Trust to the Extended Enterprise*. Cambridge, MA, Forrester Research, pp. 1–8, 2011.

[30] J. Yan, B. Yang, L. Su, and S. He, "Blockchain based software defined perimeter (SDP) in support of authentication and authorization," in *2022 Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS)*, IEEE, 2022, pp. 40–42.
[31] A. Sallam, A. Refaey, and A. Shami, "On the security of SDN: A completed secure and scalable framework using the software-defined perimeter," *IEEE Access*, vol. 7, pp. 146577–146587, 2019. doi: 10.1109/ACCESS.2019.2939780.
[32] J. Singh, A. Refaey, and A. Shami, "Multilevel security framework for nfv based on software defined perimeter," *IEEE Netw.*, vol. 34, no. 5, pp. 114–119, 2020. doi: 10.1109/MNET.011.1900563.
[33] I. A. Mohammed, "Intelligent authentication for identity and access management: A review paper," *Int. J. Manag., IT Eng. (IJMIE)*, vol. 3, no. 1, pp. 696–705, 2013.
[34] I. A. Mohammed, "Systematic review of identity access management in information security," *Int. J. Innov. Eng. Res. Technol.*, vol. 4, no. 7, pp. 1–7, 2017.
[35] Y. G. Wu, W. H. Yan, and J. Z. Wang, "Real identity based access control technology under zero trust architecture," in *2021 Int. Conf. Wirel. Commun. Smart Grid (ICWCSG)*, IEEE, 2021, pp. 18–22.
[36] D. Preuveneers, S. Joos, and W. Joosen, "AuthGuide: Analyzing security, privacy and usability trade-offs in multi-factor authentication," in *Trust, Privacy Secur. Digital Bus.: 18th Int. Conf., TrustBus 2021*, Sep. 27–30, Springer, 2021, pp. 155–170.
[37] S. Xu, G. Yang, Y. Mu, and R. H. Deng, "Secure fine-grained access control and data sharing for dynamic groups in the cloud," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 2101–2113, 2018. doi: 10.1109/TIFS.2018.2810065.
[38] M. U. Aftab *et al.*, "Traditional and hybrid access control models: A detailed survey," *Secur. Commun. Netw.*, vol. 2022, no. 5, pp. 1–12, 2022. doi: 10.1155/2022/1560885.
[39] C. Hamou, R. Brouk, and S. McAllister, U.S. patent no. 10,375,121, 2019.
[40] D. Klein, "Micro-segmentation: Securing complex cloud environments," *Netw. Secur.*, vol. 3, pp. 6–10, 2019.
[41] L. Ni, H. Cui, M. Wang, D. Zhi, K. Han and W. Kou, "Construction of data center security system based on micro isolation under zero trust architecture," in *2022 2nd Asia-Pacific Conf. Commun. Technol. Comput. Sci. (ACCTCS)*, IEEE, 2022, pp. 113–116.
[42] N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "Towards a zero-trust micro-segmentation network security strategy: An evaluation framework," in *NOMS 2022—2022 IEEE/IFIP Netw. Operat. Manag. Symp.*, IEEE, 2022, pp. 1–7.
[43] S. Raveenthiran, "Secure lightweight NFV architecture analysis for IoT edge computing," 2022. Accessed: Aug. 20, 2024. [Online]. Available: https://www.researchgate.net/publication/366920311
[44] P. Zhang *et al.*, "Dynamic access control technology based on zero-trust light verification network model," in *2021 Int. Conf. Commun., Inf. Syst. Comput. Eng. (CISCE)*, IEEE, 2021, pp. 712–715.
[45] N. Sheikh, M. Pawar, and V. Lawrence, "Zero trust using network micro segmentation," in *IEEE INFOCOM 2021—IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, IEEE, 2021, pp. 1–6.
[46] L. Xie, F. Hang, W. Guo, Y. Lv, and H. Chen, "A micro-segmentation protection scheme based on zero trust architecture," in *ISCTT 2021; 6th Int. Conf. Inf. Sci., Comput. Technol. Transp.*, VDE, 2021, pp. 1–4.
[47] D. Eidle, S. Y. Ni, C. DeCusatis, and A. Sager, "Autonomic security for zero trust networks," in *2017 IEEE 8th Annual Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, IEEE, 2017, pp. 288–293.
[48] 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.
[49] E. Gilman and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. Beijing, China: Posts & Telecom Press, 2019.
[50] C. Katsis, F. Cicala, D. Thomsen, N. Ringo, and E. Bertino, "NEUTRON: A graph-based pipeline for zero-trust network architectures," in *Proc. Twelfth ACM Conf. Data Appl. Secur. Privacy*, 2022, pp. 167–178.

[51] H. A. Kholidy *et al.*, "Toward zero trust security in 5G open architecture network slices," in *MILCOM 2022—2022 IEEE Military Commun. Conf. (MILCOM)*, IEEE, 2022, pp. 577–582.
[52] Y. Ren, Y. Leng, Y. Cheng, and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Math. Biosci. Eng.*, vol. 16, no. 4, pp. 1874–1892, 2019. doi: 10.3934/mbe.2019091.
[53] N. Surantha, F. Ivan, and R. Chandra, "A case analysis for kubernetes network security of financial service industry in Indonesia using zero trust model," *Bull. Electr. Eng. Inform.*, vol. 12, no. 5, pp. 3142–3152, 2023. doi: 10.11591/eei.v12i5.4240.
[54] J. Anderson, Q. Huang, L. Cheng, and H. Hu, "BYOZ: Protecting byod through zero trust network security," in *2022 IEEE Int. Conf. Netw., Archit. Storage (NAS)*, IEEE, 2022, pp. 1–8.
[55] X. Liu, W. Chen, J. Liu, and J. Qian, "Zero-trust security monitoring of intelligent distribution network terminals based on 5G communication technology," *Int. Conf. Electron. Inf. Eng. Data Processing (EIEDP 2023)*, vol. 12700, pp. 264–267, 2023. doi: 10.1117/12.2682685.
[56] C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," *Ad Hoc Netw.*, vol. 156, no. 5, 2024, Art. no. 103414. doi: 10.1016/j.adhoc.2024.103414.
[57] G. Vukotich, "Healthcare and cybersecurity: Taking a zero trust approach," *Health Serv. Insights*, vol. 16, 2023, Art. no. 11786329231187826. doi: 10.1177/11786329231187826.
[58] R. Cheng, S. Chen, and B. Han, "Toward zero-trust security for the metaverse," *IEEE Commun. Mag.*, vol. 62, no. 2, pp. 156–162, 2024. doi: 10.1109/MCOM.018.2300095.
[59] H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection framework to secure 6G edge computing," *IEEE Netw.*, vol. 38, no. 1, pp. 196–202, 2024. doi: 10.1109/MNET.131.2200513.
[60] I. A. Ridhawi, S. Otoum, and M. Aloqaily, "Decentralized zero-trust framework for digital twin-based 6G," 2023, *arXiv:2302.03107*.
[61] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero trust architecture for 6G security," *IEEE Netw.*, vol. 38, no. 4, pp. 224–232, Jul. 2024. doi: 10.1109/MNET.2023.3326356.
[62] J. Anderson, Q. Huang, L. Cheng, and H. Hu, "A zero trust architecture for connected and autonomous vehicles," *IEEE Internet Comput.*, vol. 27, pp. 7–14, Sep.–Oct. 2023. doi: 10.1109/MIC.2023.3304893.
[63] M. Hao, D. Ye, R. Yu, J. Wang, and J. Liao, "Trusted access solution for 6G zero trust vehicular networks empowered by blockchain," *J. Electron. Inf. Technol.*, vol. 44, no. 9, pp. 3004–3013, 2022.
[64] J. Wang, J. Chen, N. Xiong, O. Alfarraj, A. Tolba and Y. Ren, "S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–23, 2023. doi: 10.1145/3511902.
[65] C. Han, G. -J. Kim, O. Alfarraj, A. Tolba, and Y. Ren, "ZT-BDS: A secure blockchain-based zero-trust data storage scheme in 6G edge IoT," *J. Internet Technol.*, vol. 23, no. 2, pp. 289–295, 2022.
[66] J. Huang, R. Yu, and D. Mao, "Fine-grained access control based on zero trust in distributed databases in the context of power internet of things," *J. Inf. Secur. Res.*, vol. 7, no. 6, p. 535, 2021.
[67] Y. Liu, *et al*., "A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things," *IEEE Trans. Comput.*, vol. 72, no. 2, pp. 501–512, 2023. doi: 10.1109/TC.2022.3157996.
[68] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, "A blockchain-inspired attribute-based zero-trust access control model for IoT," *Information*, vol. 14, no. 2, 2023, Art. no. 129. doi: 10.3390/info14020129.
[69] P. Colombo, E. Ferrari, and E. D. Tümer, "Access control enforcement in IoT: State of the art and open challenges in the zero trust era," in *2021 Third IEEE Int. Conf. Trust, Privacy Secur. Intell. Syst. Appl. (TPS-ISA)*, IEEE, 2021, pp. 159–166.
[70] A. R. Khan, "Zero trust-based blockchain based IoT security with consensus and access control framework," *J. Intell. Syst. Internet Things*, vol. 12, no. 1, 2024, Art. no. 110.
[71] S. Zhao, S. Li, F. Li, W. Zhang, and M. Iqbal, "Blockchain-enabled user authentication in zero trust internet of things," in *Secur. Privacy in New Comput. Environ.: Third EAI Int. Conf., SPNCE 2020*, Lyngby, Denmark, Springer, Aug. 6–7, 2020, pp. 265–274.

[72] D. Greenwood, "Applying the principles of zero-trust architecture to protect sensitive and critical data," *Netw. Secur.*, vol. 2021, no. 6, pp. 7–9, 2021. doi: 10.1016/S1353-4858(21)00063-5.
[73] T. Dimitrakos *et al.*, "Trust aware continuous authorization for zero trust in consumer internet of things," in *2020 IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, IEEE, 2020, pp. 1801–1812.
[74] S. Dhar and I. Bose, "Securing IoT devices using zero trust and blockchain," *J. Organ. Comput. Electron. Commerce*, vol. 31, no. 1, pp. 18–34, 2021. doi: 10.1080/10919392.2020.1831870.
[75] S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," *J. Eng. Res. Rep.*, vol. 26, no. 2, pp. 215–228, 2024. doi: 10.9734/jerr/2024/v26i21083.
[76] S. Mehraj and M. T. Banday, "Establishing a zero trust strategy in cloud computing environment," in *2020 Int. Conf. Comput. Commun. Inf. (ICCCI)*, IEEE, 2020, pp. 1–6.
[77] L. Ferretti, F. Magnanini, M. Andreolini, and M. Colajanni, "Survivable zero trust for cloud computing environments," *Comput. Secur.*, vol. 110, 2021, Art. no. 102419. doi: 10.1016/j.cose.2021.102419.
[78] M. J. Hossain *et al.*, "ASMCC+: A secure authentication scheme for mobile cloud computing environment based on zero trust architecture," *IEEE Trans. Consum. Electron.*, 70, no. 3, pp. 6236–6249, 2024.
[79] Z. Zaheer, H. Chang, S. Mukherjee, and J. Van der Merwe, "eZTrust: Network-independent zero-trust perimeterization for microservices," in *Proc. 2019 ACM Symp. SDN Res.*, 2019, pp. 49–61.
[80] A. C. Jasim, I. A. Hassoon, and N. Tapus, "Cloud: Privacy for locations based-services' through access control with dynamic multi-level policy," in *2019 6th Int. Conf. Control, Decision Inf. Technol. (CoDIT)*, IEEE, 2019, pp. 1911–1916.
[81] A. Albuali, T. Mengistu, and D. Che, "ZTIMM: A zero-trust-based identity management model for volunteer cloud computing," in *Cloud Comput.—CLOUD 2020: 13th Int. Conf., Held Part Services Conf. Federation, SCF 2020*, Honolulu, HI, USA, Sep. 18–20, 2020, Springer, 2020, pp. 287–294.
[82] S. Rodigari, D. O'Shea, P. McCarthy, M. McCarry, and S. McSweeney, "Performance analysis of zero-trust multi-cloud," in *2021 IEEE 14th Int. Conf. Cloud Comput. (CLOUD)*, IEEE, 2021, pp. 730–732.