A Survey on Zero Trust Architecture

Yuxin Yang, yuxiny@wustl.edu
(A paper written under the guidance of Prof. Raj Jain)

Download 

Abstract

With the rapid development of cloud services and mobile networking, the increasing openness and complexity of networking provide attackers with more opportunities to exploit vulnerable entry points to access the internal network. Concerns about cybersecurity have consequently grown. Traditional security systems operate on the assumption that all entities within a defined perimeter are trustworthy, protecting enterprises from external threats originating beyond the network boundary. However, the security of this approach is no longer guaranteed, as attacks can originate from any source, including from within the network perimeter itself. To address this challenge, the concept of zero trust emerges as a potential solution. It is a more secure system that holds the principle “Never trust, always verify.” This paper gives an overview of the zero trust framework and discusses the implementations of zero trust in different scenarios. Then walks through the migration frameworks from the traditional system to the zero-trust architecture. This paper also discusses the possible challenges of the future 6G era and has a future scope of how ZTA will be implemented in the 6G era.

Keywords

Zero Trust, Zero Trust Architecture, Policy Enforcement, ZTA, PEP, IoT, 6G, 6G Security

Table of Contents:

- 1. Introduction
  - 1.1 Traditional Security System
  - 1.2 Zero Trust System
- 2. Zero Trust Architecture
  - 2.1 ZTA Framework
  - 2.2 How ZTA works
  - 2.3 ZTA Implementations
- 3. Migration from Traditional Model to ZTA
  - 3.1 Migration of ZTA
  - 3.2 Challenges in Migration
  - 3.3 Migration Frameworks
- 4. Next Trend: ZTA in 6G
  - 4.1 What is 6G
  - 4.2 Key Challenges in 6G
  - 4.3 Future Scope of ZTA in 6G
- 5. Conclusion

- 6. List of Acronyms
- 7. References

1. Introduction

With the fast development of the Internet of Things (IoT), nowadays, people around the world enjoy the convenience of cloud services and mobile networking. However, the rapid growth in networking openness and complexity brings new security challenges to traditional security systems. Attackers have more opportunities to exploit vulnerable entry points to access the internal network. Many researchers point out that the old security model is no longer reliable and propose a new idea, “zero trust”, which will be introduced in detail in the following sections.

1.1 Traditional Security System

Traditional security system, such as firewalls and Virtual Private Network (VPN), assumes that everything inside is safe once their identification is verified. It is similar to a building guarded only at the entrance. A guard checks identification at the gate and allows those with valid identification to enter, and they are trusted completely to access the entire building, which means there is no further security check inside the building. However, if a thief sneaks in through a window, the guard would not notice. In this case, the internal security risk occurs, and the traditional system fails to handle it. The “always trust” principle here is vulnerable in a connected world where unauthorized access can come from anywhere.

1.2 Zero Trust System

The concept of zero trust is introduced to handle these internal security risks. This approach assumes that nothing is trustworthy. Instead of trusting users and devices, the system continuously verifies trust in every access. Once the access is verified, zero trust system limits the access scope and duration according to the principle of least privilege [Syed22]. It also follows a dynamic risk assessment policy to continuously monitor risk levels of usage patterns. In the building example, instead of relying on the guard at the entrance, many internal checkpoints, such as keycard access, are added at every important doorway. In Figure 1, a simple zero trust system is shown. The request is sent to the policy enforcement point (PEP), and PEP checks if the access is trustworthy. The region between the user device and the PEP is an untrusted zone; every access will be marked as untrusted. If the access is allowed, the user can then access the resources. PEP will limit the access time and scope of the resources.

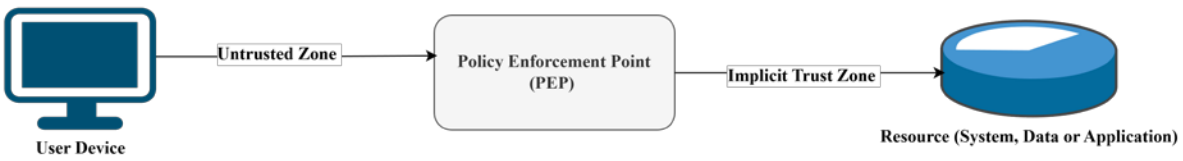


Figure 1. Zero Trust System

This is the basic idea of zero trust, and why we need zero trust instead of the traditional system. Later this paper will introduce what the zero-trust architecture is, how to migrate from the

traditional system to the zero-trust system, and what the trends of the zero-trust system are in the coming 6G era.

2. Zero Trust Architecture

This section is going to introduce the zero-trust architecture (ZTA). Through the introduction, the idea that zero trust is a concept is introduced, but the basic framework of zero trust is clearly defined by the National Institute of Standards and Technology (NIST). However, there are currently no detailed standards on how to implement a ZTA. With the guidance of the NIST framework, many enterprises choose their own way to change the basic framework and build their own ZTA.

This section will first have an overview of the NIST ZTA framework, looking at the key components and explaining how they work in sections 2.1 and 2.2. Section 2.3 will review some advanced ZTA models from research studies.

2.1 ZTA Framework

The NIST document explains that there are mainly two categories of components: the core logic components and the data source component. As shown in Figure 2, core logic components include the policy administrator (PA), policy engine (PE), and the policy enforcement point (PEP). The data components are used as input to help PE make better decisions, which include the continuous diagnostics and mitigation (CDM) system, industry compliance system (ICM), threat intelligence sources, network and system activity logs, data access policies, public key infrastructure (PKI), ID management system, and security information and event management (SIEM) system [NIST]. In the next section, this paper will explain what function each component has and how they work together to grant or deny access.

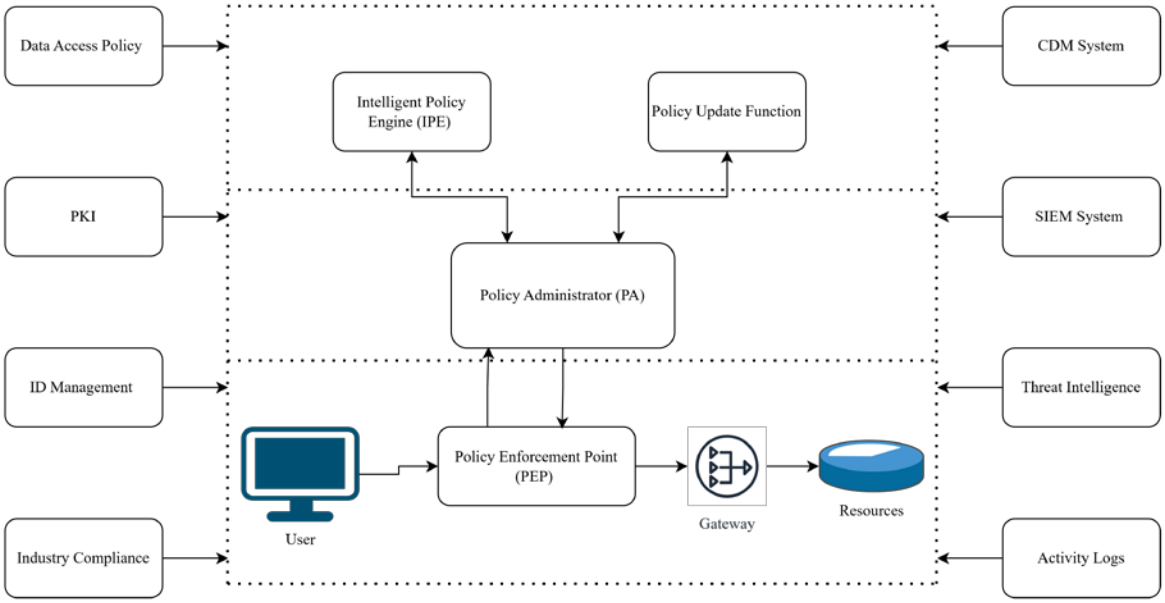


Figure 2. Components of ZTA Framework

2.2 How ZTA works

Generally speaking, the core logic components are the brain of ZTA, and the data components are factors that affect the decision-making strategy. For core logic components, PE decides to allow or deny the user's access based on the policy set. PA creates or shuts down the connection between the user and resources based on PE's decision. PEP monitors the whole ZTA and reports to PA if a wrong connection is established or shut down [Qazi22]. For data components, the CDM system checks if the user has any known vulnerabilities or software integrity issues. If new vulnerabilities or incomplete software are found, the threat intelligence will send out a warning to PE. ICM and data access policy affect the policy rules in PE, depending on which organization is making the access and what resources they want to access. Activity logs, ID management system, and PKI record various information, such as real-time feedback about traffic actions, the information of certificates and user information. SIEM collects security information and warns of potential attacks [Trendmicro].

As shown in Figure 2, when a user device asks to access specific resources, the request is sent to PEP, then PEP forwards it to PA. PA decides to create or shut down the user connections based on the decision made by PE. PE determines whether to allow or deny access based on the policy set. Here, IPE and the policy update function work together as a PE. IPE shows that PE can be driven by artificial intelligence (AI), and the policy update function shows that the policy inside PE can be dynamic by continuously evaluating the collected information from the data components and adjusting access policies accordingly. If the access is allowed, the user can pass the gateway and access resources.

After reviewing how the basic ZTA framework works, section 2.3 moves further and introduces various implementations of ZTA, some of which add more components to the basic framework, and some make adjustments to adapt ZTA to their own services.

2.3 ZTA Implementations

Due to various factors such as different application purposes, target users, application scenarios, etc., the corresponding network environments vary greatly. Therefore, a large number of personalized ZTAs have emerged.

In the cloud computing field, [Mehraj20] adds a new core logic component called "trust engine", which dynamically evaluates the integrated trust score of a user, device, or application in a particular network. In the mobile networking field, [Liu24] exploits AI and novel air interface technologies to help reduce the computing resources used in core logic components, enhancing ZTA's ability to handle a vast amount of information in the 6G era. In the smart healthcare field, [Chen21] constructs a security protection model based on 4 dimensions, which achieves end-to-end security enforcement of data, users, and services. The key components in ZTA implementations are core logic components. To improve their performance, [Hussain24] applies fedfratfd learning (FL), which is a distributed artificial intelligence (DAI) approach, to ZTA. FL is used to improve the efficiency of PEP. Methodologies such as Multi-Factor Authentication and data encryption are widely used in PE. [Guha25] constructs a combined verification method by balancing the policy weights, ensuring real-time adaptability.

Although there are many practical implementations of the zero-trust model, in reality, people are still extensively using the vulnerable traditional security systems and have no idea about upgrading the systems, that is, how to migrate to the zero-trust model. In the next section, this paper will discuss the migration from traditional systems to ZTA.

3. Migration from Traditional Model to ZTA

Migrating from a traditional model to ZTA is important to strengthen the security of data. However, this transformation may be challenging, which requires system compatibility. How to effectively accomplish the migration becomes a problem. In the following sections, this paper will introduce the concept of ZTA migration and the potential challenges in it. Then, have a review of useful existing migration knowledge from leading enterprises such as Microsoft, Cisco, and Google.

3.1 Migration of ZTA

Before the real migration, we need to know what the deterministic factors are in the migration of ZTA. Deploying ZTA is not accomplished by simply updating the tools, but requires a continuous process. In Figure 3, [NIST] divides the deployment steps into three main steps: assessment, risk assessment and prioritization, and deployment and review. The assessment identifies participants and assets and then decides whether to start the migration or not. Prioritization means that migration will first be applied to tasks with a low level of importance, in order to reduce potential risk. Deployment follows security policies, includes monitoring, and uses feedback to refine future migrations.

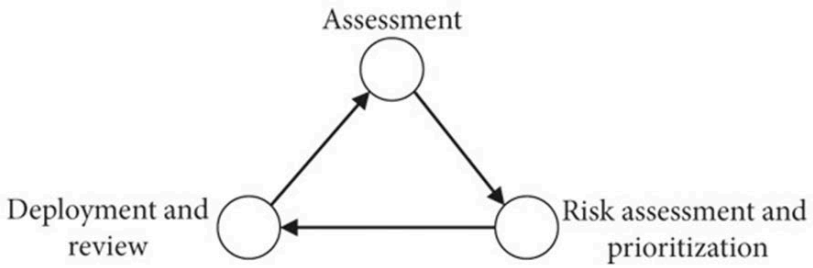


Figure 3. ZTA Migration Cycle [NIST]

After investigating the migration cycle, next section is going to discuss the possible challenges in ZTA migration.

3.2 Challenges in Migration

To successfully implement a good ZTA, there are many challenges to overcome. Here are three main categories of challenges [Phiayura23].

Technical and architectural challenge. Technically, traditional systems may have issues with adopting zero-trust principles. Redesigning the entire system would be costly. It is also difficult to

define reasonable trust levels. Architecturally, this entire migration requires the enterprise to have a full awareness of its IT equipment. However, due to management problems, it is very hard to have a full assessment of every device.

Policy and governance challenges. Policy challenges occur because of the lack of unified standards, which makes it hard to benchmark and test ZTA implementations. Unfortunately, the standards may remain fragmented because of the dynamically changing deployment environment of ZTA. Governance challenges occur because of the incomplete regulations. ZTA is still a relatively new concept in the regulatory domain; more time is needed to refine the regulations in this area.

Organizational and strategic challenges. For organizational challenges, migration needs time, which means users are not able to use the services normally during that period. This may lead to the loss of users. For strategic challenges, migration puts the company at high risk of experiencing vendor lock-in. Some providers may use methods such as pricing incentives to discourage the migration.

To overcome these challenges, it's better refer to the experiences of successful cases; many leading enterprises have been on their journey to ZTA, and they offer valuable lessons for future adopters.

3.3 Migration Frameworks

This section will introduce the ZTA migration frameworks from leading companies such as Cisco, Microsoft, and Google, and recent studies.

In Cisco's migration framework, the ability to establish visibility into all users, devices, and applications is highly valued [Cisco]. SecureX integration is used to provide unified visibility and SSO capabilities. Their approach first builds central control of identifications, then extends zero trust across the network, and finally adopts continuous trust evaluation and policy enforcement.

Microsoft divides the migration into six steps [Microsoft]. Define strategy, plan, ready, adopt, govern, and manage. The define strategy phase means building a business case aligned with their security risks. The plan phase focuses on identifying quick wins by using existing technology to achieve clear outcomes. The ready phase prioritizes early actions based on business needs and identifies possible adjustments. The adopt implements the strategy. The govern phase measures the success of the system. Finally, the manage phase monitors the network and continuously refines the function.

Google BeyondCorp's ZTA migration includes building the plan and a five-step zero trust implementation. Building the plan means identifying the first mover criteria and outcome. The zero trust implementation steps include defining the protect surface, mapping the transaction flows, building a zero trust architecture, creating a zero trust policy, and monitoring and maintaining the network [Google].

Aside from migration frameworks from enterprises, recent studies also focus on the ZTA migration. [Phiayura23] gives a comprehensive ZTA migration framework in Figure 4. It mainly

divides the migration process into two parts. In the plan, develop, and test part, the first phase is to strategize zero trust. The second phase is to do context assessment, and the third phase is to architect ZTA. In the deploy and operate part. The fourth phase is to conduct zero trust transformation. The fifth phase is to monitor and maintain the network. The final phase is to optimize ZTA security. Then the whole lifecycle will iterate and continuously extend zero trust principles to the entire applications. The proposed framework can serve as a reference model for an effective migration to a ZTA.

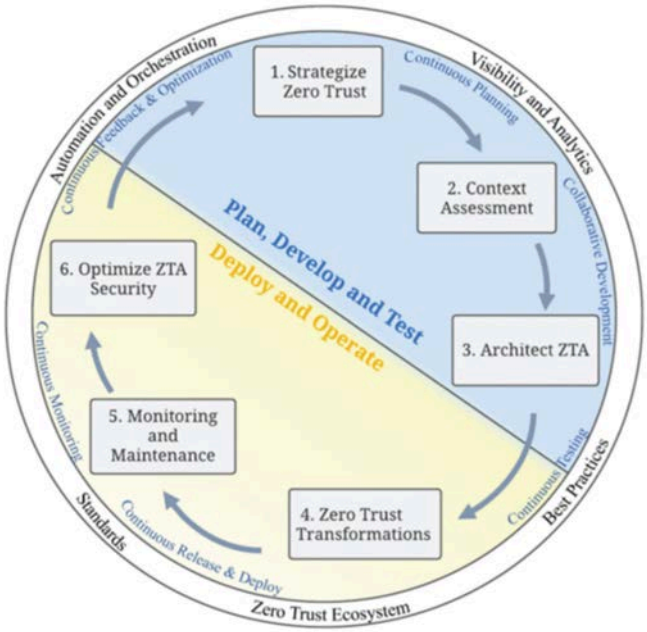


Figure 4. A Comprehensive Framework for ZTA Migration [Phiayura23]

Many enterprises have enhanced their security and prevented cyberattacks and data leaks by implementing a zero-trust architecture migration. However, networking is changing so fast, and their ZTA may need a huge update in the coming 6G era.

4. Next Trend: ZTA in 6G

In the previous sections, this paper discussed the development and current state of ZTA. Now it's going to turn our attention to the future. The sixth-generation (6G) era is coming, and the networking environment is expected to undergo a huge change. How will Zero Trust Architecture adapt to this new landscape? In the following sections, this paper will first introduce the concept of 6G and then the possible challenges. Finally, a future scope of ZTA in the 6G world will be discussed.

4.1 What is 6G

The Sixth Generation (6G) network is an integrated heterogeneous network system that contains various types of wireless networks [Sedjelmaci24]. As shown in Figure 5, there are four types of wireless networks: satellite networks, air networks, terrestrial networks, and marine networks. 6G

is expected to have massive connectivity and a high level of openness, which means a more complex network with more possible vulnerabilities [Nahar24]. Decentralization is another property of 6G, which means instead of a single unified identification system, 6G is going to have multiple central systems, which makes traditional identity authentication methods based on digital certificates fail to handle the 6G system.

Because 6G has new properties that are different from the current 5G, the ZTA, which adapts to the 5G network, faces new challenges and needs to be refined. In the later section, this paper will introduce the potential challenges in the 6G network.

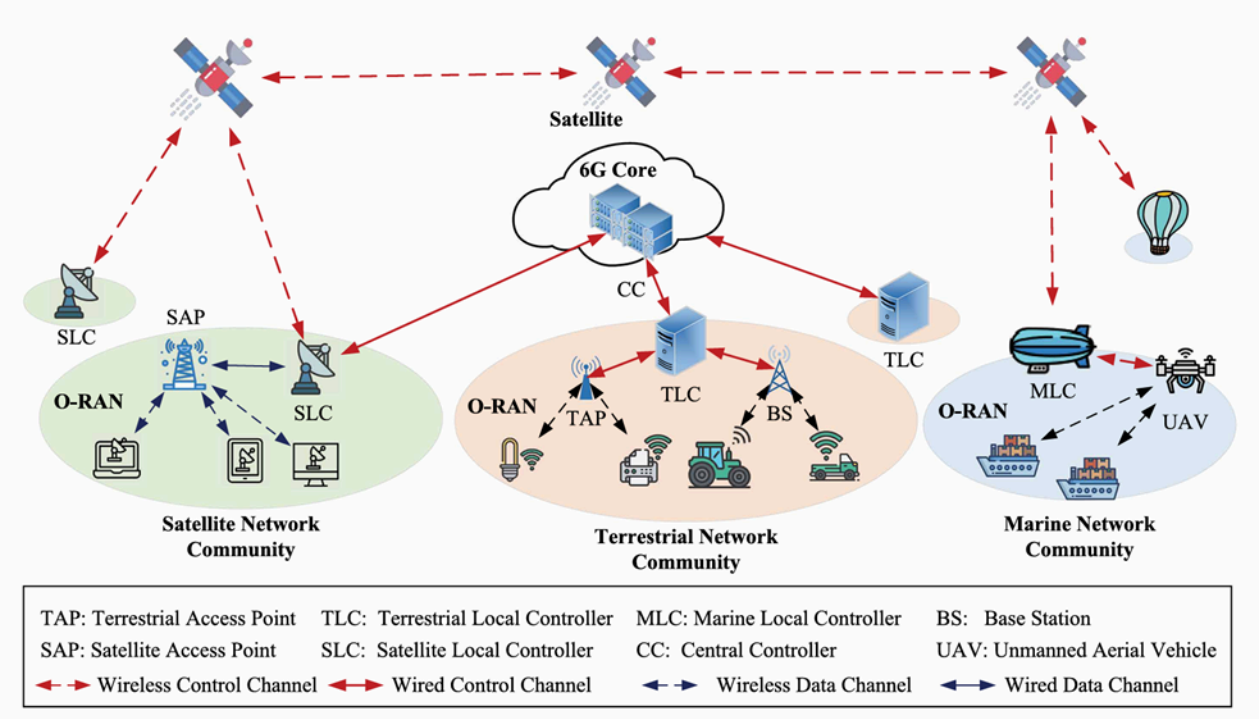


Figure 5. The Network Architecture of 6G [Chen24]

4.2 Key Challenges in 6G

Due to the properties of the 6G network. There are three main challenges that the current ZTA may fail to handle. The first challenge is the decentralized management system; the current ZTA is designed for a single network domain. How to transform a single domain into multiple domains is a problem. The second challenge is the high level of openness. High openness challenges the trust policy defined in PEP. How to grant secure access control while maintaining a high level of openness is a problem. The last challenge is the limit of resources. End-to-end encryption is used to protect ZTA from malicious attacks. However, the massive connectivity in the 6G network requires massive encryption. And ZTA may fail to handle this problem.

These three challenges limit the performance of ZTA in the future 6G network. Based on these limitations, we can refine the existing ZTA and propose a new potential ZTA framework. In the next section, this paper will have a discussion on the future scope of ZTA.

4.3 Future Scope of ZTA in 6G

Some researchers try to overcome the limitations mentioned in section 4.2. [Chen24] introduces a distributed ZTA with a decentralized identity management and a trust evaluation system. In Figure 6, the 6G network is divided into four communities managed by a local software-defined networking (SDN) controller, which acts as a PEP inside the community. Third-party security services (TPSSs) act as the data components in the ZTA framework, which are responsible for providing the vulnerability list and detecting malicious behaviors. TPSSs are built on public blockchain infrastructure. These components work together to conduct real-time trust assessment across heterogeneous network domains. The trust evaluation system calculates the trust score based on the historical behaviors.

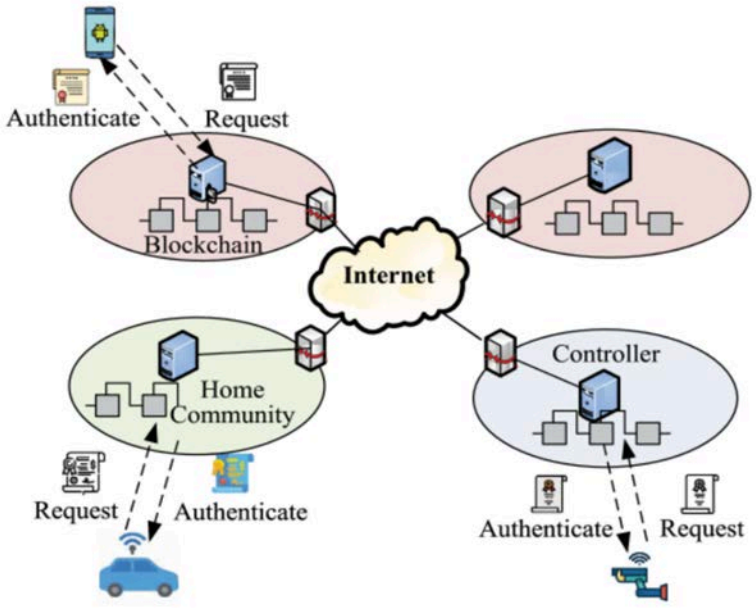


Figure 6. Decentralized Identity Authentication Method [Chen24]

The refined ZTA is now a decentralized system, which meets the requirements of a decentralized 6G network. However, the problem of computing resources limitation due to massive connectivity remains unsolved.

5. Conclusion

Compared with traditional security systems, ZTA enhances overall security by reducing internal security threats. This paper introduces the concept of zero trust and elaborates on the zero trust model and its operation principle. To address increasingly severe security challenges, more enterprises should recognize the limitations of traditional systems and migrate to the ZTA system. This paper summarizes the existing advanced migration frameworks, which can help enterprises minimize losses and maximize benefits during the migration process. Looking to the future, the upcoming 6G brings more challenges to ZTA. This article points out these challenges and discusses the practical research directions for implementing ZTA in a 6G environment.

6. List of Acronyms

IoT	Internet of Things
ZTA	Zero Trust Architecture
PA	Policy Administrator
PE	Policy Engine
PDP	Policy Decision Point
PEP	Policy Enforcement Point
VPN	Virtual Private Network
PKI	Public Key Infrastructure
IPE	Intelligent Policy Engine
CDM	Continuous Diagnostics and Mitigation System
SIEM	Security Information and Event Management System
AI	Artificial Intelligence
FL	Federated Learning
DAI	Distributed Artificial Intelligence
NIST	National Institute of Standards and Technology
SSO	Single Sign-On
6G	Sixth-Generation
SDN	Software-Defined Networking
TPSSs	Third-Party Security Services

7. References

[Chen21]	"Baozhan Chen et al., "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture", IEEE Internet of Things Journal, 2021, vol. 8, no. 13, pp. 10248–10263," / https://doi.org/10.1109/JIOT.2020.3041042
[Chen24]	"Xu Chen et al., "Zero Trust Architecture for 6G Security", IEEE Network, 2024, vol. 38, no. 4, pp. 224–232," / https://doi.org/10.1109/MNET.2023.3326356
[Cisco]	"Cisco Zero Trust Architecture Guide. An overview of the Cisco Zero Trust Framework," / https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-ag.html
[Google]	"Google Zero Trust Security. An overview of Google Zero Trust Security," / https://workspace.google.com/security/zero-trust/
[Guha25]	"Debanksh Guha et al., "A Practical Implementation of Zero Trust Architecture for Securing Web-Based Applications", 2025 International Conference on

	Advancements in Smart, Secure and Intelligent Computing (AS-SIC), 2025, pp. 1–6," / https://doi.org/10.1109/ASSIC64892.2025.11158196
[Hussain24]	"Mukhtar Hussain et al., "Federated Zero Trust Architecture using Artificial Intelligence", IEEE Wireless Communications, 2024, vol. 31, no. 2, pp. 30–35," / https://doi.org/10.1109/MWC.001.2300405
[Liu24]	"Yiliang Liu et al., "Zero Trust-Based Mobile Network Security Architecture", IEEE Wireless Communications, 2024, vol. 31, no. 2, pp. 82–88," / https://doi.org/10.1109/MWC.001.2300375
[Mehraj20]	"Saima Mehraj and M. Tariq Banday, "Establishing a Zero Trust Strategy in Cloud Computing Environment", 2020 International Conference on Computer Communication and Informatics (ICCCI), 2020, pp. 1–6," / https://doi.org/10.1109/ICCCI48352.2020.9104214
[Microsoft]	"Zero Trust Guidance Center. An overview of the Microsoft Zero Trust model," / https://learn.microsoft.com/en-us/security/zero-trust
[Nahar24]	"Nurun Nahar et al., "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks", IEEE Access, 2024, vol. 12, pp. 94753–94764," / https://doi.org/10.1109/ACCESS.2024.3425350
[NIST]	"NIST, "Zero trust architecture", NIST Special Publication 800.207, 2020, pp. 800–207," / https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
[Phiayura23]	"Pacharee Phiayura and Songpon Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture", IEEE Access, 2023, vol. 11, pp. 19487–19511," / https://doi.org/10.1109/ACCESS.2023.3248622
[Qazi22]	"Farhan A Qazi, "Study of Zero Trust Architecture for Applications and Network Security", 2022 IEEE 19th International Conference on Smart Communities (HONET), 2022, pp. 111–116," / https://doi.org/10.1109/HONET56683.2022.10019186
[Sedjelmaci24]	"Hichem Sedjelmaci and Nirwan Ansari, "Zero Trust Architecture Empowered Attack Detection Framework to Secure 6G Edge Computing", IEEE Network, 2024, vol. 38, no. 1, pp. 196–202," / https://doi.org/10.1109/MNET.131.2200513
[Syed22]	"Naeem Firdous Syed et al., "Zero Trust Architecture (ZTA): A Comprehensive Survey", IEEE Access, 2022, vol. 10, pp. 57143–57179," / https://doi.org/10.1109/ACCESS.2022.3174679
[Trendmicro]	"What Is Zero Trust Architecture? An introduction to Zero Trust Architecture," / https://www.trendmicro.com/en_us/what-is/what-is-zero-trust/zero-trust-architecture.html

---

Last modified on November 17, 2025
This and other papers on recent advances in networking are available online at
http://www.cse.wustl.edu/~jain/cse5700-25/index.html
Back to Raj Jain's Home Page