**ISSN:** 2583-9888
**DOI:** doi.org/10.51219/JAIMLD/anvesh-gunuganti/133

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 2

*Research Article*

# Identity Based - Zero Trust

**Anvesh Gunuganti***

Anvesh Gunuganti, USA

**Citation:** Gunuganti A. Identity Based - Zero Trust. *J Artif Intell Mach Learn & Data Sci 2023*, 1(2), 492-497. DOI: doi.org/10.51219/JAIMLD/anvesh-gunuganti/133

**Received:** 03 May, 2023; **Accepted:** 28 May, 2023; **Published:** 30 May, 2023

***Corresponding author:** Anvesh Gunuganti, USA, E-mail: maverickanvesh@gmail.com



## ABSTRACT

A dynamic cybersecurity threat growth, further enhanced by the rise in the work-from-home model and the increasing complexity of IT systems, prompts an urgent change in the tackling of cyber threats. The existing perimeter-oriented security practices have demonstrated to be insufficient in addressing challenges such as the distributed workforce, cloud relocation and highly organized cyber-attacks. The subsequent Zero Trust Architecture (ZTA) is another paradigm with the focus on the continuous verifying and using identity-based access controls to access the information. The purpose of this particular research work is to examine the use of Identity-Based Zero Trust Architecture (ZTA) that is implemented along with the FIDO2 passwordless authentication platform in order to boost cybersecurity robustness while remote work and distributed workforce model is applied. The research is illustrated via an examination of the chosen case studies, and a literature review It also discusses the various strategies for implementing ZTA, operational challenge and the effect on security posture. The resultant outcomes demonstrate that ZTA implements the best solution for security as it gets rid of static passwords, which besides strengthens user authentication, secures the authentication factor, and tackles modern cyber security challenges. One major recommendation is the promotion of user education by emphasizing interoperability standards and next in line research directions in optimizing ZTA implementation. Thus, the research can be considered as one of crucial components that drive the development of cybersecurity policies designed to adapt to the changing IT environments.

**Keywords:** Zero Trust Architecture (ZTA), Identity-based security, Cybersecurity resilience, Passwordless authentication

## 1. Introduction

In recent years, cybersecurity adversary has undergone dramatically brought forth by the frenzied rate of adoption of remote work and the intricate complexity of IT infrastructure. Organizations all over the globe cope with nonlinear dynamic cyber threats environment, which is characterized by multiplying sophisticated cyberattacks, cloud migration, surprisingly vast distributed networks. The issue of the conventional network-based security model, dependent on the VPN and the network border, has emerged as the main problem when it comes to safeguarding of the modern enterprises. In a time of huge shifts in the networks environment and having so many threats, the Zero Trust Architecture comes as a strategic paradigm shift, which is reorientation the organizations concerns from their assets in a completely different way.

## 2. Overview of Evolving Cybersecurity Challenges

As a result of the pandemic, the cybersecurity landscape has been going through significant transformational moves with remote work becoming the norm and the increasing complexity of the IT environments[1]. Organizations are now pressed with a variety of issues that are more numerous than they have ever been and the traditional approach is unable to provide effective solutions for them. These challenges include:

1. **Remote Work and Distributed Workforces:** The matter of fact is that the work from home has simply destroyed the notion of perimeter which, once again, better is flexible corporate networks to employee's home, café and other remote locations. Privacy and security risks will become more prominent due to the increased attack area, where most of the outside devices do not achieve the necessary security control standards.
2. **Cloud Adoption:** The migration of critical business systems to the clouds comes with complexities in data regulation and access. Organizations are under an obligation to realize data security in cloud environments and to benefit whoever is involved in these organizations by providing an uninterrupted and secure access.
3. **Rise of Insider Threats:** Organization exact handling of internal risks that could be either targeted or unintentional, involves the nature of insider threats to companies. Remote work can be considered a fertile ground for insider threats as it allows for more flexible working hours and increased risks of misusing the access in cases of privileged users.
4. **Sophisticated Cyberattacks:** Cyber criminals rely more and more on the deployment of complicated ways, like ransomware and supply chain assaults, to prey on flaws and breach networks. Modern-day conventional forms of defense are markedly inefficient to combat the increasing number of modern threats.

### 2.1. Shift to Remote Work and Distributed Workforce

The COVID-19 pandemic has accelerated remote work, which consequently meant that companies who needed to securely allow remote access to corporate resources had to do this very quickly[2]. This moment brought forward a point that earlier security techniques, such as VPNs, had their limitations due to the fact that they were relying heavily on perimeter defenses. Giving remote workers the freedom to access confidential info over unreliable networks highlighted the urgent necessity to implement a robust and identity-based approach to security.

### 2.2. Limitations of Traditional Security Approaches like VPNs

The Virtual Private Networks (VPNs) stem this tunnel for many years, the encrypted shortcut for securing the communications between remote nodes and main companies' networks[3]. However, VPNs have several inherent limitations in today's dynamic threat landscape:

1. **Broad Access Once Inside:** VPNs present a threat as user just need to gain entry and then he/she can access it extensively as locations is the only factor considered for trust. Such an absolutist principle can be dangerous as it can easily backfire if someone's login as well as devices details are compromised or any malware is installed.
2. **Complexity and Scalability:** Implementation of a VPN infrastructure for a remote employee's population can become as complicated and even costly as the managing of a large server farm. Scalability is the barrier sets as the organizations are having the capabilities of dealing with the expanding number of remote users and devices.
3. **Visibility and Control:** Despite VPNs' ability to keep track of users' activities and devices for security purposes, they may provide limited insight into user behavior as opposed to granular visibility, only at the level of initial authentication. The obstacle of limited range for suitable visibility does not help in efficient threat detection and response.

### 2.3. Introduction to Zero Trust Architecture (ZTA)

ZTA is a new cybersecurity strategy approach that brings a paradigm shift away from the traditional idea of a perimeter to strict and dynamic identity-based security [4]. ZTA assumes that the threats are both "inside and outside" the network boundaries and follows the rule of "Never Trust – Always Verify."

### 2.4. Definition and Core Principles of Zero Trust

Zero Trust Architecture (ZTA) is characterized by several core principles aimed at mitigating security risks and enhancing resilience:

**Identity-Centric Security:** ZTA is committed to Identity as the Key Containment Zone in its security posture. User's internet activity is matched not to network proximity but to verified identity instead [5].

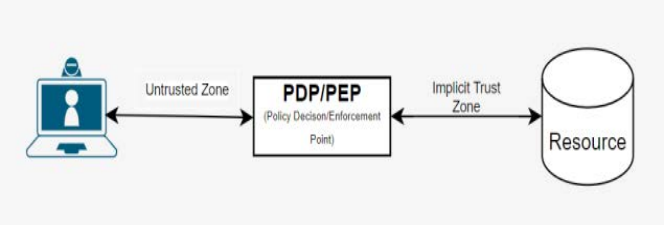


**Figure 1:** Zero trust Access

**Source:** Adapted From[9]

**Least Privilege Access:** Users are given least privilege necessary for their assigned tasks, hence limiting the damage of any hack-which could lead to a compromise.

**Continuous Monitoring and Authentication:** ZTA is constantly monitoring trust trustworthiness during user sessions by adding and removing privileges as assessments for potential threat changes and as the contextual factors evolve.

### 2.5. Importance of Continuous Verification and Least Privilege Access

Continuous verification provides the assurance that access is appropriate, at all times, with changing situations, like user behaviour, device posture etc. This proactive method reduces the likelihood that an unauthorised person can take advantage of the system and intruders can hack the system. Least privilege is a great measure for limiting the scope of security compromises by providing access to only what is required by the privileges and scale back the magnitude of possible security incidents[6].

### Research Question

How does the adoption of Identity-Based Zero Trust Architecture (ZTA) enhance cybersecurity resilience and mitigate risks associated with remote work and distributed workforce environments?

## 3. Literature Review

The development of cyber security structures follows a natural regimen of the changes in technology and online attacks. Classical security model grounded in physical boundaries, aware of networking internals, devoted the fences and guarded gateways to protecting valuable assets placed within the active zones of a trusted internal environment. Though the defences, these are created to cyberattacks, the attackers use advanced

methods, like exploitation of the remote workforce, Cloud computing, and attacking weak points in an organization's IT infrastructure. This change has had ZTA emerge as an evaluative and as an alternative paradigm for the evolution of cybersecurity. ZTA, on the other hand, takes the opposite route to the regular credo of implicit faith within reported limitations of system perimeter; rather ZTA proposes adherence to on-going verification and identification-based controls irrespective of the location of communication network[1]. The rise of zero trust principles and their relevance in the today's cybersecurity can be fully seen once we have understood the historical context which has framed cybersecurity strategies and reviewed the studies that emphasize the effectiveness of zero trust in addressing the emerging security threats.

### 3.1. Evolution of Cybersecurity Paradigms

The cybersecurity paradigm evolution is driven by technology game-changers and changing crown and prison landscape. A predominantly outward facing traditional approach was based on a binary nature of the network where trusted internal networks were distinguished from entrusted external networks. The model which is represented by VPNs and firewalls is the traditional one which involves securing the network interrogation points by just blocking access to certain places rather than protecting raised assets. It should be pointed out, though, that in today's world the border of a company changes when people work from home, using cloud computing facility, and an enterprise inevitably comes face to face with sophisticated cyberattacks.

The concept of Zero Trust Architecture (ZTA) is implemented to markedly differ from the classical methods. ZTA contradicts the traditional way of trust inside network perimeters which is just by authentication but ZTA proposes identity-based controls for every verification process. The development of such security perimeters demonstrates the wider trend of a dynamic system instead of a static one concerning web traffic and the primary focus of securing data and assets rather than location.

### 3.2. Historical Context of Perimeter-Based Security vs. Zero Trust

The historical context of cybersecurity emphasizes the difference of perimeter-based securities and why we should adopt the zero trust principles. Security models that defined border protection were useful when IT environment was static and in-house, mostly resources could be accessed within well-maintained network perimeter. While decentralized working forces and the cloud-based services development cause the physical barrier weaknesses, this is what fosters successful security breaches.

Zero-Trust, having been described by John Kindervag, a Forrester Research analyst, in 2010, became one of the ground-breaking approaches to cyber defense[7]. The main principles of Kindervag's models were the assumption that it is not just geolocation that provides a good basis to trust and the need to assume that every access request is authenticated first and then authorized based on identity and context. Through this puzzling mindset, a ground work for a variety of research and applications of the concept of Zero Trust Architecture were created to cater for different industries.

### 3.3. Review of Key Studies and Research on ZTA Adoption and Effectiveness

Recent research proves that the spread and acceptance of the concept of Zero Trust Architecture has allowed companies to keep up with the latest technological developments in their cybersecurity field. Organizations in domains like banking, education, the public sector, are seeing the importance taking steps in ZTA to protect the latest purposes and environment. Notable research has focused on:

1. **Implementation Strategies:** Studies reveal the pragmatic invention of ZTA implementation through security tools such IAM solution, micro-segmentation and continuous monitoring technologies[7].
2. **Impact on Security Posture:** Research studies the effectiveness of ZTA in the area of disarming the attack surfaces, improving the detection capabilities as well as countering the insider threats.
3. **Operational Challenges and Best Practices:** Researchers learn operational difficulties of deploying ZTA caused by users, scalability, and compatibility of the network with security[7].
4. **Comparative Analysis:** Comparative analytics assess how much more effective ZTA is as compared to traditional security models and thereby show the noteworthy improvements that can be achieved by implementing a Zero Trust policy.

## 4. Conceptual Framework

### 4.1. Understanding Identity-Based Zero Trust

Identity-Based Zero Trust as a new paradigm in security, it is oriented on continuous verification of access rights as well as the contextual factors of the user, being in the center of the security model. In contrast to the perimeter-based security architecture that takes a location-based belief as a grant, the ZTA works differently with a preventive approach that requires access to be authenticated and regulated for every request even from within the network[4] . Such an approach, elaborates the fundamental principle of "Never Trust, Always Verify", which stresses the need for the verification of the users, devices and applications before granting them the access to the critical resources.

### 4.2. Role of Identity Verification and Access Controls in ZTA

Identity verification is the basis of Zero Trust Architecture which is network less, based on decision making solely on the identity. Robust identity verifications mechanisms like MFA (Multi-factor authentication) and transaction authentication are used for performing identification tasks at the start of session and also each stage inside the process, and thus creating a secure environment [8]. Access controls undoubtedly are the very heart of the ZTA as they implement the principle of least privilege assuring that no user has beyond the minimal level of access to do what is requested. ZTA does this by enforcing the one-time-passwords that are used to authenticate the identity of the user and applying a high level of access controls that make it difficult for the attackers to find a way into the network and causing lateralization.

### 4.3. Components of ZTA Architecture

Zero Trust Architecture comprises several key components that collectively enable continuous verification and adaptive access controls:

1. **Policy Engine:** Policy engine refers to the engine that specifies as well as control application access based on

identity, device posture, and contextual attributes. It examines access requests in real-time against preset security policies and based upon its output it can authenticate, deny or to further scrutinize[6].

2. **Policy Enforcement Points (PEPs):** PEPs are one of the enforcement tools placed at important points in the network structure of devices or sensors. These include end-points, gateways and cloud services, in which enforcement of the access decisions are supported by certain policies defined by the policy engine.
3. **Continuous Monitoring and Analytics:** ZTA utilizes constant assessment based on monitoring and data analytics to establish the credibility of session underway. Through the utilization of behavioral analytics and anomaly detection algorithms a flagging process is enabled, that respond to potential threats with the aid of adaptive access controls and risk-based masks[7].
4. **Micro-Segmentation:** Micro-Segmentation, virtual network segmentation, is achieved by dividing the network resources into security segments with fine-grained boundaries assigned to workload characteristics or data sensitivity. It also guarantees that even if a particular part gets exposed to a damaging agent, lateral movement would be limited, which minimizes the dangerous effects of probable attacks.
5. **Authentication and Authorization Services:** By means of strong authentication and authorization services such as identity providers and access management modules, ZTA facilitates the differentiation between those who are authorized and those who are not in such a manner as to effectively implement the access control mechanism[8].

### 4.4. Tenets of Zero Trust Architecture (ZTA)

1. **Resource Protection:** Hereby principle is implied that data sources, computing services, no matter if they are situated inside or outside of the company's network, are assets that must be protected as that by default[5]. Apart from this, it provides resource identification and allows limited access only to authorized persons to avoid unrelated viewing.
2. **Secure Communication:** The ZTA divides information into three introductory security levels and ensures that there are mechanisms to detect and prevent breaches like attachment removal, spam filter, and smashing.
3. **Session-Based Security:** ZTA requires that within each session, resource access will be provided only on-demand in which means that only the concerned authentication and authorization are carried out for each session, without a span to other resources automatically[6]. This way includes the management of authorized sessions to have the session started and ended securely. Many other outcomes are also arising as the result of this behavior so that the unauthorized access becomes a rare event.
4. **Dynamic Access Control:** Access decisions processing is carried out dynamically considering contextual elements for instance, user identity, application context, and security posture of the interacting/transacting device. This motion implements access to request in a real-time fashion; only authentic ones are allowed on time, thus the overall security posture is promoted.
5. **Comprehensive Security Measures:** A minimum level of organizational NOC/SOC maturity must be maintained in all owned and associated devices and these continuously updated and monitored security measures must be used to diminish the existence of any security holes[11]. The certification ensures that devices matching the security standards are the only ones allowed to access the restricted data.
6. **Continuous Authentication and Monitoring:** To achieve the goal of Zero Trust we implement stringent authentication and authorization processes without fail, that together with IDAM (Identity Credential Access Management) and MFA (Multi-Instructor Authentication). That technique gives a coreless re-authentication and as the security context of the user changes simultaneously, it will adapt to it.
7. **Effective Logging and Analysis:** A logging of the entire network infrastructure and the communications activities is also a crucial aspect to be effective in detecting threats that may be encountered in the shortest span of time. Moreover, it will enhance the security posture of the organization[9]. Exploring and utilizing the log information shapes risk assessment, and measures to mitigate any found risks are implemented.

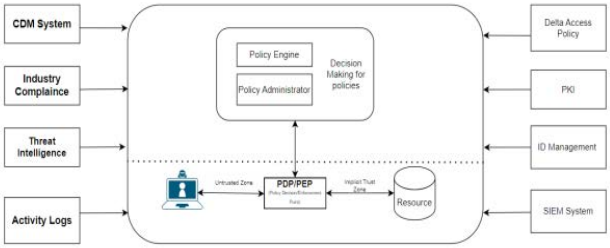


**Figure 2:** Core Zero Trust Logical Components

Source: Adapted from[9]

## 5. Research Methodology

The research methodology uses the case study investigating their adoption, approaches and solutions in the organizations that employ the Zero Trust Network (ZTN) implementation. This method gives us a good opportunity to implant the cases into real world situations for an in-depth analysis and the assessment of the performance of ZTN in complex environments.

**Case Study Analysis:** The case study will focus on analysis of several examples to identify key factors and challenges associated within ZTN implementations. Each case study will act as a lens that will highlight how ZTN adoption process went, the challenges that came out during the implementation, and how ZTN has been carried out in different organizational situations.

**Selection Criteria for Case Studies:** Cases for selecting the ZTN implementation are based on relevancy of the subject, diversity of industries to reflect different situations of the implementation, pureness of the ZTN solutions and their compliance with security standards.

### 5.1. Case study 1[10]

The paper concerns the problematic effects of the ancient network security architectures when trying to deal with the increased data access demands arisen from the emerging information technologies. This is what it shows that zero trust is a reliable technology that can be imposed on business

functionalities on a dynamic basis of user-based identities to cover the entire end-to-end security perimeter. This strategy provides an alternative mode of improving the capability of enterprise network security facilities. The paper is mainly about authentication and access control management function in connection with further discussion. Access control system is designed to authorize only those users that are authorized and secure so that system stays secure and operates properly and doesn't present a security issue to enterprise networks and servers. The main role of access control system consists of a number of areas: the first is verifying the identity (authenticity) of the user; the second is assessing the attributes (integrity) of the user's devices; and the third is responding with the appropriate response.

### 5.2. Case study 2[11]

The study discusses vulnerabilities of traditional piggy-backing access-control schemes that are built on perimeter principles; once someone breaks into the network they will have full and uninhibited access to all resources. In view of this issue, a Zero Trust Network (ZTN) model is suggested, which is concentrated on user authorization and authentication depending upon the context information related to user and devices they use. Nevertheless, issues arise with control systems which are insufficient in context information for authorization decisions, especially in federated identity systems. The report explores the Zero Trust Nation (ZTN) principles and aims at development of the Zero Trust Federation (ZTF). Thus, this paper proposes introduction of ZTF, fully within identity federations and enabling context sharing among organizational systems. A private information context management system under user consent control is suggested in order to protect the privacy of the user. Furthermore, the project will deploy a ZTF to confirm the concepts of spatial context sharing.

### 5.3. Outcomes for Case Studies of ZTA Implementations

The results and knowledge gained from each case study gives valuable insights as the way of ZTN implementation and adoption, infinity with focus on passwordless authentication technologies, for example FIDO2. In the instance of Case Study 1, it was revealed that the implementation of ZTN and FIDO2 for single-factor authentication was witnessed for the first time, and the users were appreciated for using security keys over traditional passwords, which led to enhanced security posture by minimizing vulnerability with just password-based attacks. This case study showcases the quintessential role of user education and awareness in propagating progress towards the passwordless authentication strategy, as it is also important for devices to be compatible and interfaces to be user-friendly in order to make the transition seamless.

Usability characteristics of using FIDO2 like manual settings and user attitudes towards passwordless authentication were investigated in Case Study 2 and revealed were the barriers to its wide adoption. Learning the results of such a study supports the simplification of authentication process, improvement of user understanding, and creating an interface that moves users without reminding them about the authentication. To make it effective, we have to do it user-friendly way. Overall, the two case studies highlighted the three imperative pillars of user-centric design, education and communication in both avoiding the hindrances of adoption and bettering the overall security posture of organizations as they transition to zero-trust networks facilitated by the zero-trust network authentication technologies.

## 6. Data Analysis and Findings

The synthesis of deep case study findings reaches the conclusion that the associations of the Zero Trust network frameworks and FIDO2 passwordless authentication technologies are of great value in the context of the implementation and impact. From a myriad of the studies emerged a clear spreading positive pattern regarding users' acquiescence and assimilation of security keys instead of the conventional password type. But on the other hand exposure problems were identified like lack of knowledge, device compatibility, and interface usability that emphasize the necessity of user-friendly design and effective communication techniques to facilitate adoption among the users[4].

Shifting from a WTN (Traditional Networking) consideration to FIDO (Fast Identity Online) and deliver a sharp decrease in vulnerability become password-based hacks and also an improvement in the authentication security. Permanent authentication and observance gained prominence as the main aspects of the strong safeguarding pose within these architectures.

The issue of usability was also apparent here, for example, the problem with manual security settings and the transition between authentication tools. It was clear that this knowledge implied the need for more straightforward procedures and comprehensive user education to help avoid adoption deterrents and build a mass adoption mechanism[8].

Key findings demonstrated how user orientation is important in ZTN adoption and that has to be realized through the user experience and understanding as two factors that is vital for successful implementation. Some recommendations contained strategies, such as upgrading device compatibility, creating better user interfaces, and communication improvement techniques to make device familiarization and acceptance easier[3].

From all these aspects, the integration of passwordless authentication options within the ZTN frameworks seems to be a powerful tool at the disposal of the information security team. Studies in which real-world experience can be enriched and used to drive future research and implementation initiate through increased utilization of FIDO2 capabilities, thereby strengthening these organizations' security strategies.

## 7. Discussion and Recommendations

Integrating ZTA in security systems architecture necessitates critical reflections for the organizations striving to improve their security level by adapting to the new wave of cybersecurity threats. Utilizing the ZTA framework for which authentication process is built upon FIDO2 platform can provide organizations with many advantages, such as increased security, higher usability, and improved resilience.

### 7.1. Implications of ZTA Adoption

ZTA represents a paradigm shift followed by a more sophisticated defense strategy that leads the light years ahead in the security model of the long-established perimeter-based approach[2]. ZTA focuses on constant verification and stringent access controls whereas this ensures the misuse of data by the hackers is extremely rare. It also underlines the supremacy of usability in most security strategies which primarily tend to put the purpose of user at the center of such strategies without having to compromise on security.

### 7.2. Benefits for Enhancing Security Posture

Integration ZTA with passwordless authentication technologies will facilitate the process of enhancing your security posture. ZTA does eliminate dependence on outdated passwords and enable MFA (Multi-factor Authentication) with the help of biometrics or security keys, which consequently decreases the odds of theft and unauthorized access considerably[8]. Frequent authentication and tracing as well as the constant monitoring of target processes to detect deviations and determine secure sessions, continue to build up the security of the product.

### 7.3. Challenges and Considerations for Implementation

Along with its advantages, using ZTA with passwordless authentication also has some issues. Organizations need to overcome complications such as devices compatibility and system integration and user education. Making the provision of boring a loose pleasant and interoperable one across various systems platform and devices necessitates careful planning and considered implementation.

### 7.4. Recommendations for Organizations

For the successful implementation of ZTA with passwordless authentication, organizations should focus on the user education and awareness campaigns as a primary measure. It is urgent to put the interfaces user-friendly, provide the necessary training in the field of new authorization methods and to simplify the transition from one to another world. For coupled effort, cooperation with private industry and interfacing of global harmony standards should be used to make communication easier.

### 7.5. Future research directions and areas for improvement

The ZTA implementation research should be devoted to technology improvement in the context of the access control, privacy-preserving systems for the context sharing, as well as to the development of the tools for the automated monitoring and responding to possible security events. Furthermore, allowing space for studying the improved authentication techniques and how they affect the end user experience will lead to a good implementation of the ZTA.

Therefore, ZTA with passwordless authentication is an emphatic shift towards ensuring a more secure and robust cybersecurity posture. Through tackling difficulties, making the most of the strengths as well as developing responsible strategies governmental institutions despite the difficulties of ZTA can succeed against the modern cyber-attacks.

## 8. Conclusion

The study focused on Zero Trust Architecture (ZTA), which is nested with the new passwordless authentication technologies like FIDO2, as a means of alleviating some of the security concerns in the organization. These results highlight the central role of ZTA in the security paradigm, which involves a shift from the classical seat-based borders to a verification protocol in perpetual and very rigorous system of access controls. Herein one of the major findings include the step change security posture realized through the implementation of ZTA and passwordless authentication that eliminates the need for reliance on static passwords and replacing them with multi-factor authentication (MFA) in protecting against credential theft and phishing attacks. Furthermore, one of the ways by which ZTA ensures canonicity is that it provides a user-friendly platform, with which there is an easy identification process that uses biometrics or security keys, and this can guarantee robust security measures. However, they are establishing technical difficulties and difficulties related to user education, device compatibility, and system integration, for ZTA implementation. It is necessary to plan carefully, train people everywhere, and work with industry partners to make them successful. On the part of organizations, the immediate priority is creating awareness among users, simplifying migration processes, and adopting interoperability standards as the right way leading to successful ZTA implementation. Future study must try to perfect the contextual framework by manipulating access rules, strengthening privacy-sensitive approaches for sharing context and exploring advanced authentication techniques. All these are aimed to match user experience and information security from future threats. In sum this might be considered as a strategic being in cybersecurity security to reinforce it and improve all around system security in the dynamic threat environment of our modernity.

## 9. References


1. Talan A. Zero Trust Network Access with Cybersecurity Challenges and Potential Solutions. Masters thesis, National College of Ireland 2022.
2. Tony H, Joseph K, Steve W, Jeffery SC. Zero Trust in a Virtual Cybersecurity World. ProQuest 2021;70: 12-19.
3. Xu Z, Ni J. Research on network security of VPN technology. IEEE Xplore 2020.
4. Ahmed M, Petrova K. A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-based Computing Environments. WISP 2020 Proceedings 2022.
5. Abdullah A, Mengistu T, Che D. ZTIMM: A Zero-Trust-Based Identity Management Model for Volunteer Cloud Computing. Lecture Notes in Computer Science 2020;287-294.
6. Belapurkar R. Zero Trust Architecture - Implementation and Design. RB 2022.
7. Adahman Z, Malik AW, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Computers & Security 2022;122: 102911.
8. Sample C. Shelton C. Loo M, Justice C, Hornung L, Poynter I. ZTA: Never Trust, Always Verify. European Conference on Cyber Warfare and Security 2022;21: 256-262.
9. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. Zero Trust Architecture 2020.
10. Wu YG, Yan WH, Wang JZ. Real identity based access control technology under zero trust architecture. IEEE Xplore 2021.
11. Hatakeyama K, Kotani D, Okabe Y. Zero Trust Federation: Sharing Context under User Control towards Zero Trust in Identity Federation. IEEE Xplore, 2021.