STM JOURNALS

International Journal of
Mobile Computing Technology

Volume 1, Issue 2, 2023
July—December
DOI (Journal): 10.37591/IJMCT

https://journals.stmjournals.com/ijmct

Review IJMCT

Zero Trust Security Governance by Utilizing Identity and Access Management

Sampath Talluri*

Abstract

The Zero Trust Paradigm, a more stringent approach to network security, operates on the fundamental concept of "Never Assume, Always Authenticate." It is currently being implemented in different countries to align with their national cybersecurity and access management governance policies. The differentiation of these Zero Trust systems is contingent upon factors such as awareness, infrastructure, expenses, and security demand. Additionally, the identity-based access management models within the Zero Trust system exhibit variations depending on factors such as user profiles, resource allocations, application domains, the specific Zero Trust rules in place, and the role of the Zero Trust administrator. The aforementioned disparities contribute to the phenomenon of security fragmentation, resulting in the proliferation of risk and vulnerability to attacks in various network zones. This study conducts deductive research on the standard frameworks of identity-based zero-trust system, as implemented in the United States and India, both at an industrial level and in other domains. The research substantiates their soundness based on the available factual data regarding the updates and advancements made in addressing evolving security and user-access management concerns. In the subsequent section, the conclusion highlights potential areas for enhancement and notable characteristics observed in the respective models that can be integrated to develop a zone-neutral Zero Trust model. This result showed that India's Zero Trust infrastructure lacks the scalability and innovation scope of the USA's Zero Trust system. Thus, to develop a zone-neutral model operational in both areas, India's model should be integrated with advanced classification, detection, and user management systems and better areas of application.

Keywords: zero trust, user identity, authentication, regional ZT, ZT systems

INTRODUCTION

The Zero Trust (ZT) Paradigm is a strategic framework that eliminates inherent trust within a network infrastructure. Authentication, authorization, and periodical validation are necessary prerequisites for granting access to all users and devices, irrespective of their location within or outside an organization's network. The program's primary objective was to establish a system that ensures access to resources following identity and context, departing from the conventional security model centered around perimeters [1]. The technique was implemented as part of the "BeyondCorp" effort, which was devised by Google in 2010.

*Author for Correspondence
Sampath Talluri
E-mail: tsampatht1@gmail.com

AM Lead Engineer, Department of Computer Science, Western Michigan University, United States

Received Date: June 24, 2023
Accepted Date: July 07, 2023
Published Date: July 20, 2023

Citation: Sampath Talluri. Zero Trust Security Governance by Utilizing Identity and Access Management. International Journal of Mobile Computing Technology. 2023; 1(2): 6–17p.

By implementing this approach, Google was able to facilitate secure employee access to company apps and data regardless of their location or device, eliminating the necessity for a virtual private network. The core notion of zero trust was introduced by Forrester Research analyst John Kindervag in 2014 in a paper titled "The Zero Trust Model of Information Security" [2]. The individual put out a novel security framework predicated on the notion that all individuals, regardless of their

affiliation with the organization or their position within its network, should only be deemed trustworthy if they undergo a verification process. The paper delineated the ZT approach, grounded on two fundamental principles: "Never trust, always verify."

On the other hand, in a perimeter-based traditional system, the network is partitioned into an internal and external network using a firewall, intrusion detection system, or intrusion prevention system as the boundary. Determining an object's location inside the physical network is used to assess whether it is within the internal network. Objects residing within the internal network are inherently considered to be trusted. In contrast, external objects necessitate authentication before establishing confidence. In a perimeter-based security architecture, the confidence granted to an authorized item persists over an extended duration.

The proliferation of cloud computing and Internet of Things technology and the widespread adoption of telecommuting have made remote work an essential mode of employment, particularly in light of the COVID-19 pandemic. Hence, considering the object's physical placement, it becomes increasingly challenging to ascertain its presence within the internal network and assign it an appropriate level of confidence. The conventional security approach must be revised to safeguard organizational assets and resources due to the rise in mobility, cloud usage, remote work, bring your own device rules, and sophisticated cyberattacks [3].

The National Institute of Standards and Technology (NIST) has introduced the notion of zero trust architecture (ZTA) as a potential solution to tackle the emerging challenge and problem at hand [4]. The architecture in question diverges from perimeter-based security approaches since it operates on the principle that an object's trustworthiness is not contingent upon its physical placement.

As mentioned earlier, taking every network component as untrusted and establishing confidence in an object is contingent upon the processes of identity identification and trust appraisal. Once the system has allocated the appropriate permissions to the object, the object is able to execute operations that are relevant to its assigned permissions. At that point, there are specific questions that need to be confirmed:

- Parameters on which the ZT system evaluates identity and sets accessibility score for a subject.
- Parameters on which the ZT system evaluates and sets accessibility score for a subject's resources.
- Parameter selection criteria in the ZT access management
- Rule of *conditional parameters* set for the subject or subject's resources.
- Criteria of ZT Admin Role

This study makes deductive research on the standard frameworks of identity based ZT systems as adopted at the industrial level and above in the United States and India. Based on the current information gathered on the updates and progress to tackle emerging security and user-access management issues, the research justifies their validity. Thereafter, in the concluding part, it suggests the areas to improve, and distinctive features as observed in the respective models that can be incorporated into the other.

Contributions made by this research are as follows:

- Identification and exploration of identity based ZT security governance systems as currently adopted in specific regions (The United States and India, as studied in this research) and evaluation of their vitality and sustainability.
- Gather the distinctive demands and user-based access management criteria that the analyzed ZT systems aim to serve and assess their feasibility and potentiality.
- Extend the research scope to recommend a region neutral ZT model based on amalgamating the usable features of the studied models.

This article is composed of sections that include the latest related scholarly articles, methods, and tools used to develop and fulfill the objective of this research, findings, and deductions made on them, and lastly, the conclusion of the research comprised of suitable recommendations on improvements and possible amalgamation options that can be implemented to develop a region neutral ZT system workable and effective in diverse zone and cater authentic user demands (this research is limited to industrial segments where ZT models are currently utilized).

RELATED PAPER

In this section, a precise discussion of the currently done scholarly works on the ZT system, its role and importance in industry, and the current identity-authentication-based ZT system models are implemented or analyzed. From the inferences and deductions gathered from the discussion presented here, the proposed research scheme of this work is conceptualized and implemented.

Paul and Rao [5] made a comprehensive examination and documentation of the currently evolving zero-trust strategy. The authors made a thorough elucidation of its fundamental principles, architectural framework, and procedural guidelines for implementation. Their study presented an overview of the smart manufacturing sector, an evaluation of current cyber security measures, and a presentation of a zero-trust model design. Additionally, the report discussed the necessary components for implementing this model in both on-premises and cloud-based infrastructure.

Fernandez and Brazhuk [6] employed the possible security patterns that are usable in the creation and assessment of security architectures. In this context, the authors applied the methodology to scrutinize the anticipated outcomes of the ZT model. In this study, the researchers established a connection between the concepts behind ZT and the existing insights into security issues on which ZT technology is working. Their study attempted to answer the potentiality and significance of this technological approach.

Adahman et al. (2022) [7, 8] examined potential strategies for implementing ZTA within an organizational context. The cost analysis of ZTA tools and resources was performed using a data-driven and quantitative approach. This study aimed to analyze the reduction in data breach risk through the implementation of ZTA, using recent events as a basis for modeling. This involved determining the annual budget allocation for each tool, considering the organization's personnel headcounts and their specific business requirements.

He et al. [9] presented documentation of the prevailing ZTA while concurrently undertaking an analysis of its fundamental technologies, namely identity authentication, access control, and trust assessment. The present study attempted a comprehensive examination of the primary solutions within each technological domain, with the aim of juxtaposing and scrutinizing their respective merits and demerits.

Zhang (2023) [10] put forth a groundbreaking proposition for a novel hybrid system that combined computational intelligence with privacy-preserving and zero-trust principles. Expanding upon the foundational principles of the zero-trust architecture, the present system endeavored to establish a secure and safeguarded environment, all the while upholding the paramount importance of preserving individual privacy. The aforementioned objective was accomplished through the utilization of multi-tiered trust mechanisms within the confines of a corporate network, wherein each solicitation for access was subjected to a thorough process of authentication, authorization, and encryption prior to being bestowed with the privilege of entry.

Tang et al. [11] made an exploration and analysis of authentication technology within the context of the zero trust network paradigms. Their scholarly manuscript employed a Traceable Universal Designated Verifier Signature to establish a privacy-preserving authentication framework within the

context of ZTA. The study inferred that in the context of client–server interactions, it was imperative to prioritize the safeguarding of client access privacy. The study entailed ensuring that the server administrator refrained from divulging any details pertaining to the client's access behavior to external entities or third parties.

Liu et al. [12], on the other hand, focused their work on developing a novel protocol for local identity authentication and roaming identity authentication, which was founded upon a ZTA. In the proposition, they presented a group signature scheme that is revocable, wherein the expiration time was intricately linked to the key possessed by each individual edge terminal device. Based on the proposed resolution, the researchers agreed that it was evident that the inclusion of the identity authentication token, which was rendered invalid by the expired key, within the revocation list is unnecessary. This omission served to enhance the efficacy of the revocation-checking process, thereby optimizing its efficiency.

Then, Feng et al. [13], in their scholarly manuscript, presented a proposition for a security model known as the zero-trust paradigm. Subsequently, they proceeded to incorporate the concepts of blockchain and Merkle tree into the construction of a decentralized identity storage framework, thereby ensuring the utmost dependability, confidentiality, and efficacy in data modifications while concurrently enhancing the efficiency of authentication processes. Moreover, the implementation of the proxy was initiated to facilitate bilateral authentication between cloud servers, thereby mitigating both internal and external vulnerabilities. Furthermore, a reputation assessment mechanism has been employed in order to mitigate the likelihood of nodes gaining access to malevolent cloud services.

METHODS AND TOOLS

The research is conceptualized based on the geography-specific access management need of network systems incorporated where different ZT models are currently utilized. Particularly, this study focuses on the industrial demands and security governance on which ZT systems are being implemented. A theoretical and operational analysis of two standard ZT architectures is done—(a) one is NIST and (b) the other conceived by India's CERT in its security and resource management system to be applicable in Government Organizations and connected units ONLY. These systems are compared and evaluated in terms of the purpose they are planned to meet, and then, based on the results, their usability, sustainability, and possibility of amalgamation to build a zone-neutral ZT model are discussed.

In this way, this analysis tries to interpret an optimization strategy that can be implemented to scale up the ZT systems as zone-neutral models compatible with the security governance of any region wherever to be implemented. First, the current ZT technology incorporation in global industrial segments and their prospects are given below to boost for better understanding:

The Figures 1 and 2 shows the spread and incorporation of ZT technology systems in global industrial segments. The graph below shows the global industrial segments where the ZT system is currently incorporated.

There are certain criteria on which ZT system frameworks are developed, and vary from region to region [14]. These criteria are as follows:

Criteria 1: The employee seeks convenient and reliable means of accessing business resources, regardless of their physical work environment. This access is attempted using either an enterprise-managed device or a personally owned device. The provided ZTA solution can effectively enforce the corresponding access request dynamically and with little delay.

Criteria 2: An employee is endeavoring to gain access to the publicly accessible internet in order to do several jobs. Although the web-based service is not under the ownership and management of the company, the corresponding access request for that resource will still be effectively enforced in a

dynamic and real-time manner through the implementation of a ZTA solution where it effectively administers employee access, irrespective of their geographical location.

Criteria 3: The stakeholder is attempting to gain access to specific business resources and the Internet. This scenario will illustrate a particular user experience in which a stakeholder endeavors to gain access to specific corporate resources and the Internet to carry out the intended service for the company. The ZTA solution is to be developed to effectively and promptly enforce access requests for resources made by the contractor, with dynamic and near real-time capabilities.

Criteria 4: In the realm of corporate services, it is common for multiple servers to engage in intercommunication. An instance can be observed where a web server establishes communication with an application server. The proposed ZTA solution should be capable of facilitating the enforcement of network connections between specified servers in a dynamic and near real-time manner.

Criteria 5: Two firms, namely Company X and Company B, have the potential to engage in a collaborative initiative that involves the sharing of resources. In this particular context, the ZTA solution can let authorized users belonging to one organization safely access designated resources from the other enterprise reciprocally.

Criteria 6: Organizations possess various tools such as monitoring systems, security information and event management systems, and other resources that can supply data for the purpose of supporting security analytics. In the given context, the integration of monitoring and security information and event management systems with the policy engine within a ZTA solution would result in enhanced accuracy in the computation of trust scores or confidence levels in near real-time [15].

Based on these above-stated criteria, the ZT model that is generally implemented is shown in Figure 3 [16]:

Based on industrial and network location demands, the components' features are particularly important to be enhanced, assessed, and updated [16].

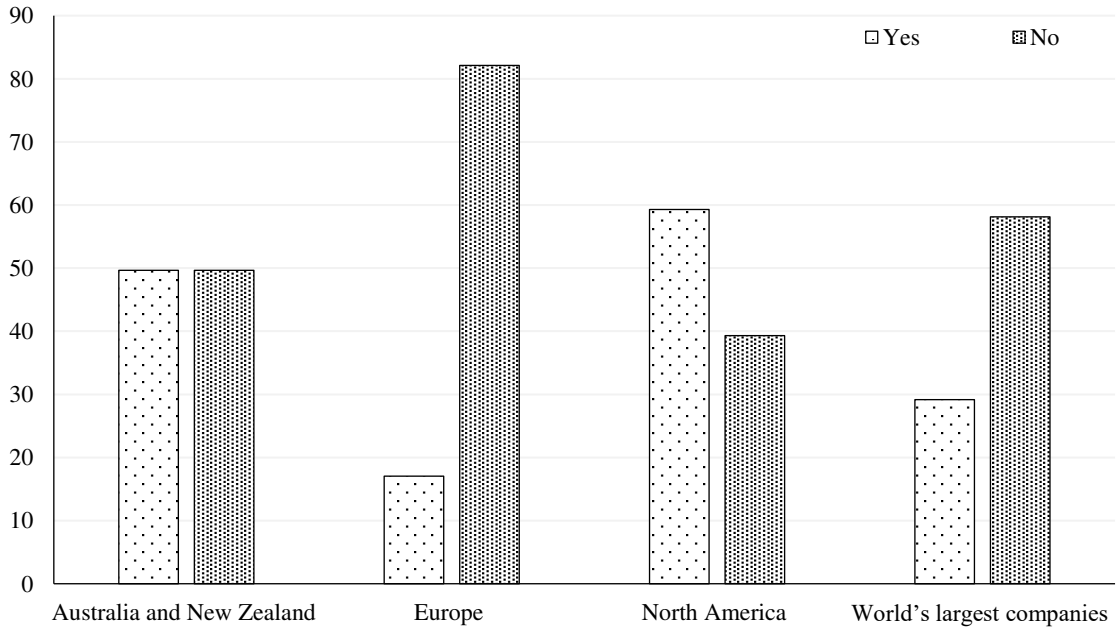

Figure 1. ZT technology incorporates country-based industrial segments.

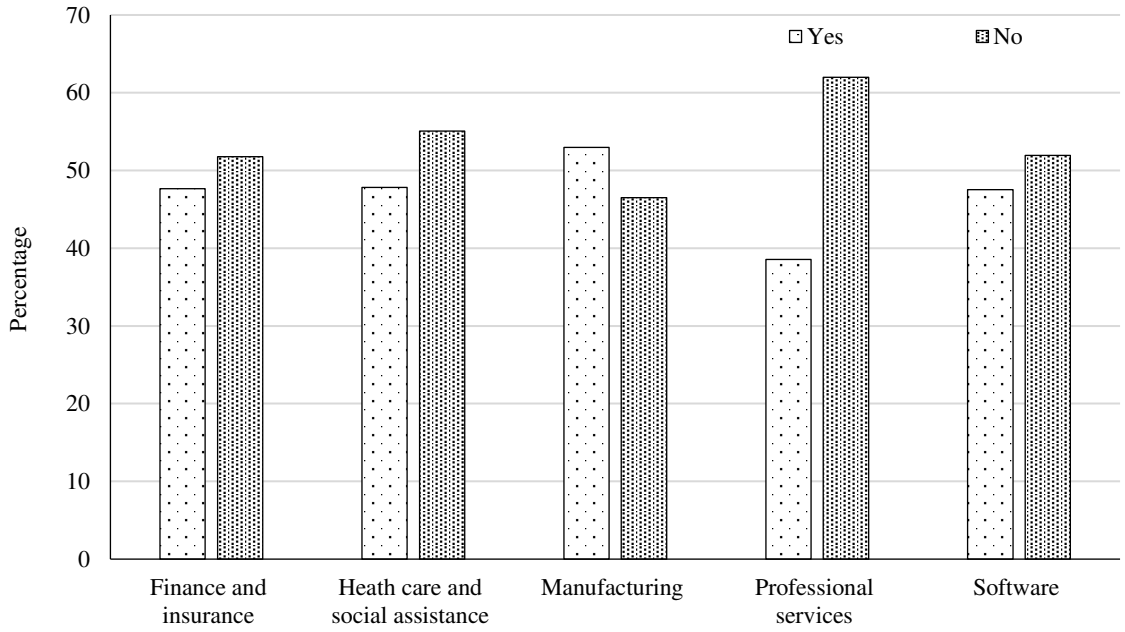

Figure 2. Worldwide industry specific ZT technology incorporation.

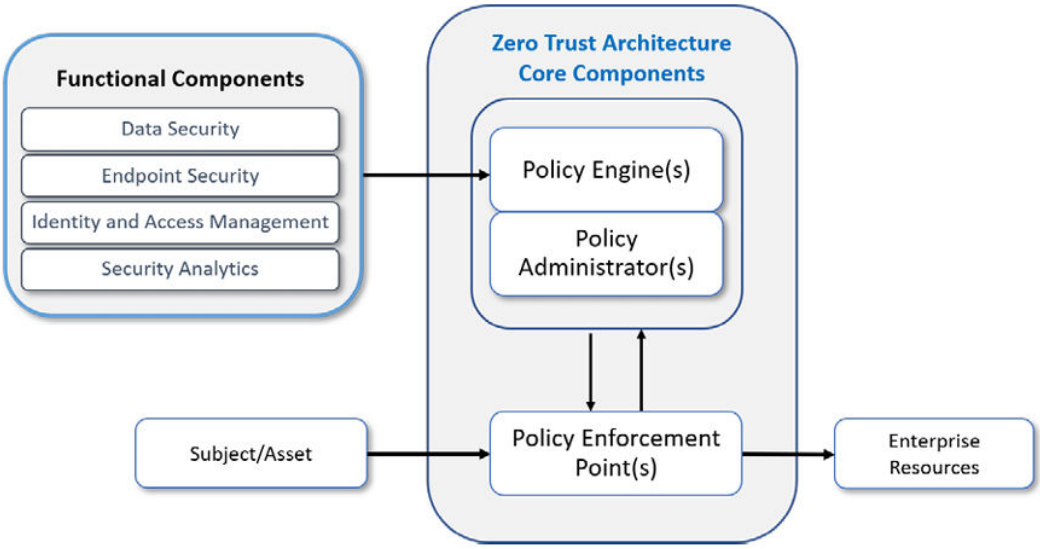

Figure 3. ZT Architecture.

RESULTS AND FINDINGS

Factual deductive analysis is done in this research, selecting two currently recognized and utilized (in the industrial segment in particular and other user-driven networking areas as well)—NIST and the latest CERT's ZTA as proposed based on IT Act of India 2000.

The factual data gathered and analyzed is given below.

NIST Architecture

Current Zonal Needs of ZT Technology where NIST is Utilized

The current level of voluntary adherence to the CSF as implemented in the USA, needs to be improved in achieving robust cybersecurity measures for critical infrastructure. The realization of this fact was underscored by the occurrence of the ransomware assault on Colonial Pipeline in the year

2021, which prompted the Biden administration to subsequently enforce obligatory cybersecurity prerequisites in pivotal critical infrastructure domains, encompassing oil and natural gas pipelines, aviation, rail, and water [17].

In light of the escalating frequency of prominent security breaches, the Biden administration took action in May 2021 by issuing an executive order that necessitates U.S. Federal Agencies to strictly comply with NIST 800-207 as an obligatory measure for the implementation of Zero Trust [18]. The standard has undergone rigorous validation and received extensive input from various stakeholders, including commercial customers, vendors, and government agencies. Consequently, numerous private organizations consider it to be the de facto standard for private enterprises.

Features

The NIST ZT Architecture is built with these three fundamental logical conceptualizations [19]:

- The concept of continuous verification is a fundamental principle in NIST ZT Architecture. It refers to the ongoing process of validating and ensuring the accuracy, reliability, and rigorous authentication process to access every resource without exception.
- Minimize the potential impact radius. Implement measures to mitigate the potential consequences in the event of an external or internal breach.
- Develop a system to enable the automated acquisition and processing of contextual information, as well as the generation of corresponding responses. Utilize behavioral data and extract contextual information from the entirety of the IT stack, encompassing identity, endpoint, workload, and other relevant components, to obtain the most precise and reliable response.

The NIST's latest update is Cybersecurity Framework (CSF) 2.0 Reference Tool. This resource provides users with the opportunity to examine the Draft CSF 2.0 Core, which includes Functions, Categories, Subcategories, and Implementation Examples. Additionally, it gives versions of the draft Core that are compatible with both human and machine reading, available in JSON and Excel forms.

Now, the tool enables users to access and extract certain sections of the Core by employing relevant search phrases. This tool will ultimately empower users to generate their personalized iteration of the CSF 2.0 Core by selecting specific Informative References. Additionally, it will offer a user-friendly and efficient means for users to delve into many facets of the CSF Core (CSF 2.0, 2023).

Industrial Purpose

The xFramework has been extensively employed for the purpose of mitigating cybersecurity threats since its initial release in 2014. There is a prevailing consensus that modifications are necessary to tackle existing and forthcoming cybersecurity obstacles effectively and to enhance the accessibility of the Framework for organizational utilization. The NIST is collaborating with the community to maintain the efficacy of the CSF 2.0 in the future while simultaneously upholding the original aims and objectives of the CSF.

The CSF 2.0 has been designed to address and adapt effectively to the notable transformations of cybersecurity capabilities [17].

- This encompasses various aspects such as zero-trust capabilities, automation for countering cyberattacks, and secure software development.
- Technologies such as the progressive development of cloud service and deployment models, along with the corresponding cloud security risks, as well as the advancements in AI, machine learning, quantum computing, and encryption.
- The availability of resources for enhancing organizational cybersecurity risk management capabilities.

Figure 4. NIST CSF 2.0 updated ZT Architecture.

Framework Structure

The NIST CSF (Cybersecurity Framework) works like a wheel due to the interconnectedness of its framework functions as shown in Figure 4. As an illustration, an entity will classify its resources within the IDENTIFY phase and thereafter implement measures to safeguard such resources during the PROTECT phase. Investments made in the planning and testing of the GOVERN and IDENTIFY.

Functions are crucial for facilitating prompt incident response and recovery measures in the context of cybersecurity incidents within the RESPOND and RECOVER Functions. The function of GOVERN holds a central position within the organizational framework since it serves as a guiding principle for the implementation of the remaining five functions [20].

CERT's Zero Trust Architecture: India

Current Zonal Needs of ZT Technology where Zero Trust Architecture is Utilized

According to Ripu Bajwa, the Director and General Manager of Data Protection Solutions at Dell Technologies India, India is expected to continue being highly susceptible to cyber threats and data-loss incidents in the year 2023 [21]. In order to address the issue at hand, the concept of zero trust is put forth as a security framework that necessitates conducting security checks, authentication, authorization, and validation for all users, both internal and external to the organization's network, prior to granting them physical or virtual access to the enterprise, its systems, applications, and data repository [20].

In practice, based on the findings of Cloudflare's 2021 report titled "Data security in the Age of Zero Trust," it has been observed that there exists a significant level of awareness regarding the concept of Zero Trust in various countries, including Australia, Japan, Singapore, Malaysia, and India. Notably, Australia and Malaysia exhibit an almost ubiquitous level of awareness in this regard. India has been identified as having the lowest level of awareness, necessitating the need for immediate attention and resolution [22].

Features

The objectives of the government are focused on establishing an internet that is open, safe, trusted, and accountable for its users. Subsequently, the technological advancements and the rapid evolution of the internet in contemporary times have been noteworthy. The Indian Computer Emergency Response Team (CERT-In), established and designated as the national agency for addressing cyber incidents and cyber security incidents, as per the stipulations outlined in section 70B of the Information Technology (IT) Act, 2000 has proposed Zero Trust system framework [23] that is currently being applicable within the realm of governmental entities and their affiliated counterparts ONLY.

In their security monitoring and incident management guidelines, the agency has incorporated Zero Trust, which is currently applicable ONLY in government organizations and connected units (CERT-In) [24].

- The Zero Trust approach encompasses a comprehensive framework consisting of eight fundamental pillars. These pillars are as follows: User, Device, Network, Infrastructure, Application, Data, Visibility and Analytics, and Orchestration and Automation.
- A ZTA ought to be seamlessly integrated as an enterprise cybersecurity architecture that is fundamentally rooted in the principles of zero trust. ZTA necessitates the authentication and authorization of all users and devices prior to their acquisition of access privileges to resources.
- ZTA can be implemented utilizing diverse methodologies, albeit commonly encompassing the amalgamation of technologies, including identity and access management, micro-segmentation, cloud security, continuous monitoring, and advanced authentication mechanisms.
- The incorporation of the Defense-in-Depth strategy, in conjunction with the zero trust approach, is deemed crucial for organizations to effectively establish a multitude of security mechanisms and controls across their computer network. This comprehensive implementation aims to safeguard the confidentiality, integrity, and availability of both the network itself and the valuable data it contains.

Industrial Purpose

The IT industry currently needs help pertaining to the trustworthiness of technology and data. Consequently, implementing the "Zero Trust Model" allows organizations to adopt a stance of initial skepticism towards any entity or information, thereby addressing this challenge. India's adoption of the New IT Act signifies a method targeted at prompting the necessity to modernize the longstanding perimeter-based network security model.

The perimeter method was based on the assumption that users located within the confines of a corporate or enterprise network were considered "trusted" users, hence granting them access to network data without the requirement of multi-factor authentication [25]. Individuals who were not part of the network were classified as "untrusted" users. The New IT Act is expected to incorporate the principle of "Zero Trust" in its regulations for "Implementation Organizations" and "Compliant Organizations" to implement solutions that facilitate Zero Trust Strategies.

Framework Structure

CERT's ZTA follows the framework structure as mentioned below [23]:

- The Zero Trust approach takes into account the absence of a conventional network perimeter, wherein networks can exist locally, in the cloud, or in a combination or hybrid form, with IT resources dispersed across various locations.
- Additionally, employees and users can be situated at any given location.
- Zero trust is a concept that entails the reduction of access to resources, including data, compute resources, applications, and services. This reduction is limited to only those end users, systems, and assets that have been identified as requiring access.
- Additionally, it involves the continuous authentication and authorization of each access request, ensuring the verification of identity and security posture.

The two region-centric ZT systems—(a) USA's NIST and (b) India's CERT's ZT Architecture (Compliant with IT Act 2000) that we discussed above present their development strategies discretely attached to the current demands and user access management concerns as shown in Figure 5.

We can see that the USA, being a world power, is very concerned about its wealth and defense against external enemy attacks. Also, considering the growing number of cybercrimes and illicit/suspicious network penetration/system access attempt cases, the country's ZT framework incorporated in NIST has enhanced its cybersecurity infrastructure (updated to 2.0 version).

On the other hand, India, being an economically progressing country that is making significant progress in IT and digital networking technologies, is inclining towards adopting the ZT system. The factual analysis presented here shows a visible picture of the infrastructure behind the USA's ZT infrastructure. It is not much extended to cover the wider commercial zones, including private and regional units. CERT-In's ZT model is developed based on the fundamental ZT architecture rather than including advanced innovative elements.

Table 1 summarizes the main features of the two ZT architectures under consideration.

Comparing the aspects incorporated in NIST and CERT-In's ZT architecture, we can ascertain that the USA's NIST is much more innovative and inclusive in terms of access and resource management, while India's CERT-In ZT architecture is included with ZT's general fundamental features that lack automation, faster classification, advanced detection, and analytical features. These features, as they are being incorporated through AI-powered Deep Learning/Machine Learning in NIST's framework, make the system much more expansive, scalable, fast, and accurate.

Figure 5. IT Act 2000 compatible ZT architecture.

Table 1. Two ZT architectures.

NIST ZT Architecture (updated with CSF 2.0)	CERT-In ZT Architecture
• Safety in Automated Access Management System • Incorporation of AI (Deep Learning and Machine Learning) in Access Management, User Recognition, Demand Management and Security Control • Compliant with National Cybersecurity Governance Policies • Enhancing ZT usability in Enterprise segments • Enhanced compatibility in diverse user access management • Continuous User Authentication • User-Friendliness • Resource Access Control • Response and Recovery Management • Integration to Cloud environment	• Ensuring ZT usability in Government sector and connected units ONLY. • Improvement from traditional perimeter-based Network Access Management System • Compliant with IT Act 2000 • Scalable in terms of its usability in Network Access Management (Extended to cloud and hybrid networking platforms) • Compatible with Enterprise Cybersecurity Governance Policies • Zone independent User Access Control • Continual User Authentication • Resource Access Control

CONCLUSION

Under the current scenario of growing risk in cybersecurity, robust access management is a mandatory aspect to be taken care of. In our deductive research as presented above, we have done factual analysis on two recognized ZT models—the USA's NIST (updated by CSF 2.0) and India's CERT-In's ZT Architecture. The comparative assessment of the two ZT systems highlights distinctive differences between the two architectures. Such differences are certainly the result of a number of conditions. In this research, the conditions are found as follows:

- Infrastructural constraints
- Awareness
- Skillset
- Cost
- Innovation scope
- Areas of application
- Network architecture
- Security and access management need
- Cybersecurity policies

Today, because of rapid digital advancement in networking and internet usage, countries all over the world are somehow interconnected with one another. Cyber laws are also made with similar perspectives. Therefore, India and the USA, although their needs, infrastructure, access demand, and security management are far different from one another, can implement similar ZT systems. Hence, India's ZT architecture needs improvement in the following areas:

- Scalable for application areas
- Infrastructural improvements
- Scope of Innovation (integration of AI in terms of achieving accuracy, fastness, and automation)
- Scalable in user access management
- Cyberlaw updates including advanced and global cyber risks (This is important to include in India's cyber law policies in terms of the country's global accessibility provisions and user resource usage)
- Awareness and Skill in ZT technology

These improvements not only optimize the two architectures, but the architecture can also gain wider usage areas and meet Access Management's purpose at a higher level than only being confined within regional boundaries.

REFERENCES

1. Chaudhry UB, Hydros AKM. Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. IET Blockchain. 2023; 3 (2): 98–115. doi: 10.1049/blc2.12028.
2. Heath D. (2023). The evolution of zero trust and the frameworks that guide it. [Online] IBM Blog. Available at https://www.ibm.com/blog/the-evolution-of-zero-trust-and-the-frameworks-that-guide-it/
3. AD360. (2023). Zero trust. [Online] ManageEngine. Available at https://www.manageengine.com/active-directory-360/manage-and-protect-identities/zero-trust-security.html [
4. Rose S, Borchert O, Mitchell S, Connelly S. (2020). Zero Trust Architecture. [Online] Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
5. Paul B, Rao M. Zero-trust model for Smart Manufacturing Industry. Appl Sci. 2022; 13 (1): 221. doi: 10.3390/app13010221.
6. Fernandez EB, Brazhuk A. A critical analysis of zero trust architecture (ZTA). SSRN Electron J. 2022. doi: 10.2139/ssrn.4210104.
7. Adahman Z, Malik AW, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Comput Sec. 2022; 122: 102911. doi: 10.1016/j.cose.2022.102911.

8. Adahman Z. Zero-trust architecture and its cost-effectiveness on network security. Ndsuedu. 2022. Available from: https://library.ndsu.edu/ir/handle/10365/32683.
9. He Y, Huang D, Chen L, Ni Y, Ma X. A survey on Zero Trust Architecture: challenges and future trends. Wirel Commun Mob Comput. 2022; 2022: 1–13. doi: 10.1155/2022/6476274.
10. Zhang Y. Privacy-preserving with Zero trust computational intelligent hybrid technique to English education model. Appl Artif Intell. 2023; 37 (1). doi: 10.1080/08839514.2023.2219560.
11. Razavian M, Paech B, Tang A. The vision of on-demand architectural knowledge systems as a decision-making companion. J Syst Softw. 2023; 198: 111560. doi: 10.1016/j.jss.2022.111560.
12. Liu H, Ai M, Huang R, Qiu R, Li Y. Identity authentication for edge devices based on zero-trust architecture. Concurrency Comput Pract Experience. 2022; 34 (23). doi: 10.1002/cpe.7198.
13. Feng Y, Zhong Z, Sun X, Wang L, Lu Y, Zhu Y. Blockchain enabled Zero trust based authentication scheme for Railway Communication Networks. J Cloud Comput. 2023; 12 (1). doi: 10.1186/s13677-023-00411-z.
14. Deloitte. (2021). Zero Trust: 2021 A revolutionary approach to Cyber or just another buzz word? [Online] Available at https://dokumen.tips/documents/zero-trust-deloitte-2021-7-18-zero-trust-is-a-framework-for-looking-at-cyber.html?page=1
15. Okta. (2023). The state of zero trust security in global organizations. [Online] Available at https://www.okta.com/resources/reports/state-of-zero-trust-security-in-global-organizations/
16. Kerman A, Borchert O, Rose S. (2020). Implementing a zero trust architecture. [Online] Available at https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
17. Teplinsky MJ. (2023). A review of NIST's draft Cybersecurity Framework 2.0. [Online] Available at https://www.lawfaremedia.org/article/a-review-of-nist-s-draft-cybersecurity-framework-2.0
18. Talluri S, Anne VP. Active directory implementation: resolving provisioning/deprovisioning access and ensuring accurate user identity and access across the organization using IAM. Int J Inf Technol. 2023; 4 (02): 29–37.
19. Raina, K. (2023). Zero trust security explained: principles of the zero trust model. [Online] Available at https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/
20. NIST. (2023). Public draft: The NIST Cybersecurity Framework 2.0 National Institute of Standards and Technology. Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf
21. Tejaswi M. (2023). Zero trust to become cornerstone of data security this year in India: Dell's Ripu Bajwa. [Online] The Hindu. Available at https://www.thehindu.com/business/zero-trust-to-become-cornerstone-of-data-security-this-year-in-india-dells-ripu-bajwa/article66793069.ece
22. Sathyajith S. (2022). Role of zero trust in India's digital transformation journey. [Online] Entrepreneur. Available at https://www.entrepreneur.com/en-in/growth-strategies/role-of-zero-trust-in-indias-digital-transformation-journey/433648
23. Guru S. (2022). The new standard for cyber security of organisations and enterprises: zero trust architecture. [Online] Cyber Secure India. Available at https://cybersecureindia.in/new-standard-for-cyber-security-organisations-and-enterprises-zero-trust-architecture/
24. CERT. (2021). Safe & Trusted Internet: Guidelines on Information Security Practices for Government Entities. [Online] Available at https://www.cyberyodha.org/2023/06/safe-trusted-internet-guidelines-on.html
25. Alappat MR. (2023). Multifactor authentication using zero trust. Thesis. [Online] Rochester Institute of Technology. Available at https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=12639&context=theses#:~:text=The%20concept%20of%20Zero%20Trust,authentication%20before%20being%20granted%20access

