Frontiers in Computer Science and Artificial Intelligence
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Zero-Trust Architectures for Securing U.S. Critical Infrastructure

Md Fahim Ahammed
Department of Information Assurance and Cybersecurity, Gannon University, Erie, Pennsylvania, USA
Corresponding Author: Md Fahim Ahammed, **Email:** mdfahimahammed7773@gmail.com

| ABSTRACT

Zero Trust Architecture is an emerging trend in cybersecurity in the USA, changing the tact of cybersecurity strategies in groundbreaking ways. Whereas traditional models of security depend on a depth defense strategy, assuming implicit trust within internal networks, Zero Trust is designed on the principle of "never trust, always verify." This takes into consideration stringent verification processes for identities, irrespective of the location or network environment. ZTA, through the use of multifactor authentication, micro-segmentation, and behavioral analytics, among other advanced technologies, enables an organization's capability to defend itself against insider attacks, ransomware, and advanced persistent threats. The main principles of Zero Trust Architecture, challenges related to the implementation of this approach, and tangible benefits provided to modern enterprises are discussed in this paper. In this paper, through an in-depth case study analysis and empirical evidence, we try to demonstrate how the adoption of the Zero Trust framework advances security, reduces the attack surface, and enables organizations to respond effectively against emerging threats. The findings underpin that moving to a Zero Trust model is not only a tactical shift but also a strategic one for organizations in the USA in light of the current threat landscape, which aims at the protection of their key digital assets.

| KEYWORDS

Zero-Trust Architectures; Securing Critical Infrastructure; Multifactor authentication; Cybersecurity; Cyber-Attack Mitigation

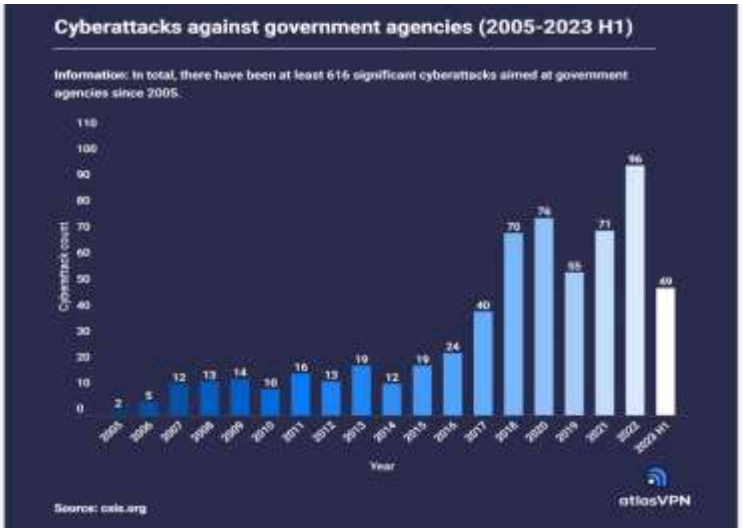
| ARTICLE INFORMATION

ACCEPTED: 15 November 2025 **PUBLISHED:** 30 November 2025 **DOI:** 10.32996/fcsai.2025.4.2.7

Introduction

Fernandez & Brazhuk, A. (2024), posited that in the recent two decades discourses of the Zero Trust Architecture (ZTA) have been championed as a transformative approach to bolstering organizational security in the USA. The need for ZTA can be understood from the ever-growing intricacy and diversity in modern IT environments. An organization may keep several internal networks and connect to multiple external ones that may include remote offices and partner systems. Enterprise applications may sit on-premise or run dynamically off the cloud platforms and storage services. Besides, IT system integration with IoT and cyber-physical systems further increases this complexity. Green-Ortiz et al. (2023), postulated that operational models such as BYOD and WFH further increase the diversity of these environments. The aftermath of the pandemic further exacerbated this fragmentation by making it necessary for users to access an extensive range of applications and resources over a highly distributed infrastructure. It is now increasingly going to happen from a wider range of diverse devices and locations. All these factors have contributed towards an expanded attack surface, where very often several mismatched systems in terms of their security models are knitted together, making system management so complex. On the contrary, cyberattacks have also grown more sophisticated and frequent, hence underlining the dire need for solid security frameworks such as ZTA.

Background to the Study



Cyberattacks against government agencies (2005-2023 H1)

Information: In total, there have been at least 616 significant cyberattacks aimed at government agencies since 2005.

Source: csis.org

Figure 1: Depicts Cyberattacks Against Government Agencies in the USA

As can be observed from the chart above, from 2005 to the first half of 2023, major cyberattacks on government agencies drastically increased, further evidence of the increasing challenges of cybersecurity in such organizations. From just 2 attacks in 2005, the number has grown steadily to a high of 96 attacks in 2022. There is a particularly steep rise after 2016, with incidents jumping from 19 in 2015 to 40 in 2016, reflecting the growing sophistication of cyber threats and increased digitization of government operations. Of these, 49 were already reported by mid-2023, an indication that this year could be worse than 2022 if the trends persist (Seaman, 2023). An uptick that underlines the increasing geopolitical friction, ever-expanding attack surfaces from technological adoptions, and continuous evolvement of cyberattack methods. Results have underlined the need for further steps to be taken by governments with more proactive cybersecurity measures to secure their infrastructures and services (Khan, 2023).

According to Muhammad et al. (2022), the face of cybersecurity has entirely flipped due to rapid technological development and, at the same time, increasingly complex cyber threats. For this reason, traditional security models, whose basis is mainly on perimeter defense, are no longer valid to deal with the subtleties of today's digital environment. Moore (2022), indicated that the shift from on-premise infrastructure to cloud-based services, coupled with remote work and an increased reliance on mobile devices, expands the attack surface and brings a host of vulnerabilities to organizations at every turn. Given this shift, there has had to be a reevaluation of strategies undertaken toward security and focus attention on Zero Trust Architecture, or ZTA, as the rising alternative to traditional approaches.

As per Macaulay & Bhasker (2024), the central tenet of the ZTA architecture is the principle of "never trust, always verify," which revolves around identity verification and continuous monitoring, rather than the implicit trust delivered within network boundaries. It enforces key concepts such as least privilege access, micro-segmentation, and multi-factor authentication, not only to reduce the attack surface area but also to grant access in a tightly controlled and continuously monitored manner to highly treasured resources. For instance, least privilege access restricts user access to resources, granting access only to what users need to fulfill their jobs. This operation is done so that the resultant damage from any breaches is as minimal as possible. Similarly, Oladimeji (2024), asserted that micro-segmentation splits the network into small, isolated sections; this automatically limits the ability of an attacker to move laterally. Even more advanced, Zero Trust strategies are powered by artificial intelligence and machine learning that will eventually support proactive threat detection and response.

Research Objectives

The Prime objective of this research project is to examine the deployment of Zero-Trust Architecture (ZTA) as a cybersecurity framework for safeguarding critical infrastructure in the United States. This paper examines the effectiveness of Zero-Trust principles in minimizing security risks, enhancing resiliency, and inhibiting unauthorized access in interdependent systems at the heart of national security. The presented study aims to provide recommendations for integrating Zero--Trust models necessary to protect against cyber threats in evolution and further enhance the general security posture of such critical systems by examining the ZTA architecture and implementation of ZTA in critical infrastructure sectors.

Understanding the Zero-Trust Architecture

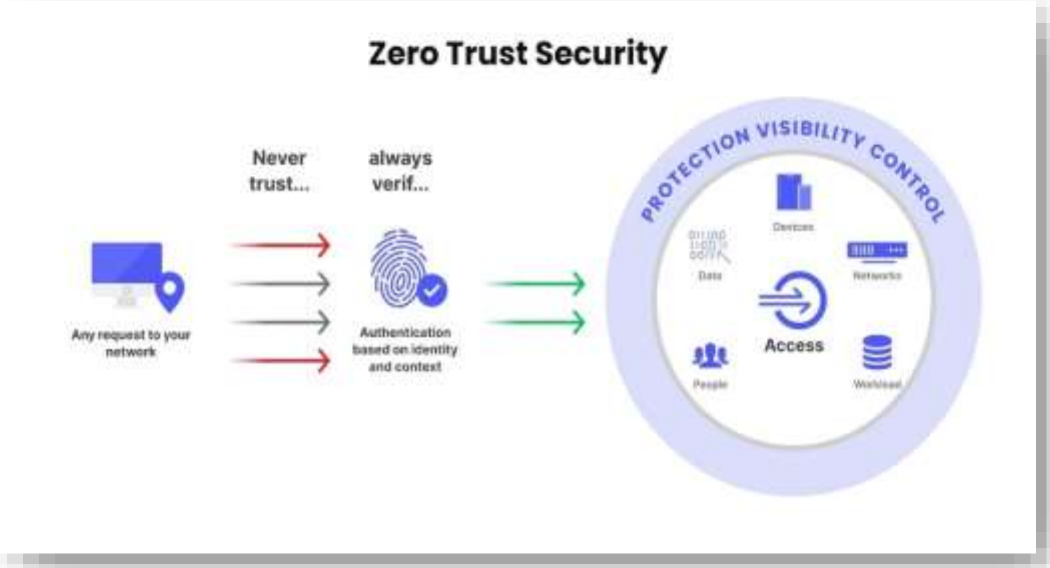

Zero Trust Security
Never trust...
always verif...
Any request to your network
Authentication based on identity and context
PROTECTION VISIBILITY CONTROL
Devices
Data
Networks
Access
People
Workload

Figure 2:Exhibits the Zero-Trust Architecture

The operational definition of zero trust and zero trust architecture can be described as follows:

- **Zero Trust**: Is defined as a framework of concepts and strategies aimed at reducing uncertainty in making precise, least-privilege access decisions for each request within information systems and services, through an organization's entire lifecycle, with the assumption that the network is compromised (Stafford, 2022).
- **Zero Trust Architecture:** Refers to an organization's cybersecurity strategy that integrates zero-trust principles across people, workflows, and component interactions along with access control policies. Therefore, a Zero Trust enterprise is defined as the totality of network infrastructure physical and virtual- along with their operational policies created based on the implementation of a Zero Trust Architecture plan (Syed, 2022).

Akinsanya (2024), reported that Zero Trust security models center on resource protection, governed by the principle that trust can never be implied, only explicitly verified. Zero Trust Architecture provides a comprehensive approach to enterprise resource and data security through measures dealing with human and non-human identities, credentials, access control, operations, endpoints, hosting environments, and the infrastructure beneath it. Its main objective is to restrict access to the barest minimum of subjects who have a need-to-know, using the principles of least privilege that give access permission to only what shall be used to perform certain tasks, write, and delete. Traditionally, organizations, including federal agencies, have used a perimeter-based approach to security wherein users from within gain authorization to access a plethora of internal resources. This approach, however, has continued to pose challenges relative to unauthorized lateral movement within the network, among others (Edo et al., 2022). Whereas TIC and perimeter firewalls are a number of the stronger gateways in terms of blocking external internet-based threats, they tend to be less effective when it comes to identifying and stopping internal attacks or securing users and devices outside the traditional enterprise perimeter, like remote workers, cloud services, and edge devices.

As portrayed in Figure 1 Conceptual model of access: A subject needs to get access to an enterprise resource. This is authorized through a PDP and enforced via the corresponding PEP.

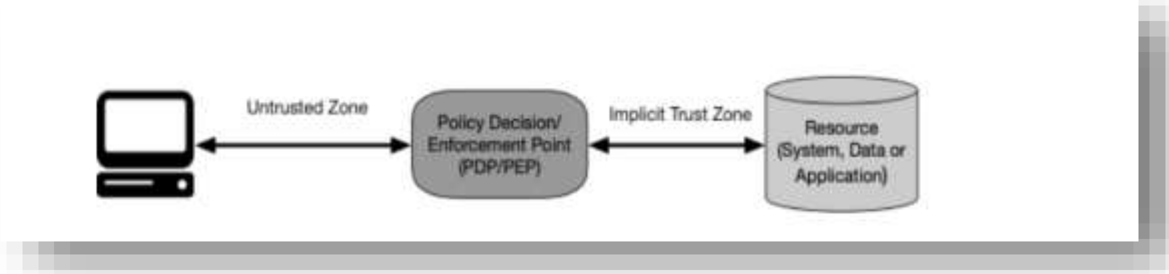

Untrusted Zone
Policy Decision/ Enforcement Point (PDP/PEP)
Implicit Trust Zone
Resource (System, Data or Application)

Figure 3: Visualizes the Zero-Trust Access

As showcased above, the system must first verify the authenticity of the subject and whether the request is valid. The PDP and PEP work together to evaluate and decide whether the subject should be granted access to the resource. As such, it is quite evident that among other concepts, zero trust concentrates heavily on two major areas: authentication and authorization. It appraises the confidence level specifically the subject's identity for each request, whether that level of confidence is sufficient to permit access; whether the device used to make the request meets the security standards requirements relevant for representing and protecting that subject's identity, and whether other contextual factors impact that confidence level (Fernandez & Brazhuk, 2024). Organizations shall implement dynamic, risk-based policies regarding resource access and shall ensure such policies are effectively and correctly enforced with every access request. This approach is based on the principle of no implied trust, meaning that success in an initial authentication requirement (logging into a system, for example) cannot grant implicit validity to all further resource request accesses (Federici et al., 2022).

Muhammad et al. (2022), articulated that the implicit trust zone refers to that area where all entities are trusted to an equal extent as they were during their last verification by a PDP or PEP. A possible analogy might be the passenger screening process in most modern airports: once one has passed through the security checkpoint representing the PDP/PEP, all passengers, employees, and crew in the terminal are trusted. Here, the implicit trust zone would be the boarding area. While the PDP/PEP will enforce controls to ensure that all activity within that zone has mutual trust levels, once traffic has passed the PEP, no policies can be enforced anymore. The implicit trust zone should be minimized for maximum security. Zero Trust introduces concepts related to the location of the PDP/PEP closer to the resource for explicit authentication and authorization of all subjects, devices, and workflows within the enterprise (Green-Ortiz et al., 2023).

Tenets of the Zero Trust Architecture

A significant volume of studies by Akinsanya (2022), on Zero Trust underscore the concept of eliminating wide-area perimeter defenses-e.g., enterprise firewalls a factor. However, most of these definitions continue to define themselves concerning perimeters in some way as a part of the functional capabilities of a ZTA. The following is an attempt at defining ZT and ZTA in terms of basic tenets that ought to be involved rather than what is excluded. These are the ideal tenets, although it is fair to say that not all tenets may be fully implemented in their purest form for a given strategy (Edo et al., 2022). A zero-trust architecture is designed and implemented with adherence to the following zero-trust principles:

- **All computing services and data sources are treated as resources**: The networks will be composed of diverse ranges of devices from small-footprint senders publishing data to aggregators or storage, to SaaS systems to devices sending actions to actuators. Enterprises will also consider personal devices to be resources if they are accessing enterprise-owned assets (Moore, 2022).
- **All communications are secured regardless of their network location:** Since placing a device on a network does not imply trust. Access requests from inside the enterprise network infrastructure-in other words, from within a traditional network perimeter- are subjected to the same security standards as requests from devices on external or non-enterprise networks. One cannot rely on trust based on the devices' location inside the enterprise's network. These communications shall be affected using the best possible security measures available, with the assurance of confidentiality, integrity, and authenticity of the source (Sarkar et al., 2022).
- **Enterprise resources would be per-session available:** Access would be permitted only after the trust in the requester is evaluated. The access would be granted based on the principle of least privilege, which provides only the permissions needed to carry out certain tasks. Authentication and authorization for one resource do not necessarily propagate to another resource, and trust may be validated only at the time of a specific transaction or session, rather than only at the point of access (Syed et al., 2022).
- **Access to resources is regulated by distinct policies that assess various components, such as the detectable state of the user's identity, the application or service being accessed, and the features of the requesting asset:** Other behavioral and environmental attributes may play into this as well. Organizations protect resources by identifying their assets, and defining who their members are-which also includes how to authenticate users from federated communities and identifying what level of access those members should have. In the context of a zero-trust framework, client identity is taken to mean user accounts or service identities and any attributes or artifacts an organization provides to authenticate automated processes (Seaman, 2023). The requestor asset's state might include the software versions in use, the network address, the time of day and date of request, prior behaviors, and even installed credentials. Behavioral attributes are the automated analytics of both users and devices and their deviations from normal behavior. Policies are the access rules that are based on the attributes assigned by an organization for users, devices, data, or applications. Other environmental attributes can relate to contextual aspects, such as place or circumstances regarding the requestor (Oladimejie 2024).

- **Asset Integrity and Security Posture:** According to Khan (2023), the enterprise is in a constant state of being aware and monitoring the integrity and security posture of all owned and associated assets, trust no asset by default. The security posture of the asset is a factor in determining whether to authorize resource requests. Enterprises should implement a continuous diagnostics and mitigation (CDM) system or an equivalent in support of a Zero Trust Architecture (ZTA), monitoring device and application posture by applying patches and fixes when needed. The assets known to be compromised, vulnerable, or not managed by the enterprise would fall into an alternate category, and perhaps be denied all access to the enterprise resources, as compared to the devices owned or associated with the enterprise that are kept in a known good state. This may extend to associated devices, where limited access to certain resources could be granted. Accordingly, there is a huge demand for an efficient monitoring and reporting system to achieve credible insights into the existing status of enterprise assets.

Logical Elements of Zero-Trust Architecture

Several logical components compose a typical ZTA deployment in an enterprise. These Components can be operated either on-premise as a service or as a cloud-based service. Figure 4 presents the model of the conceptual framework showing the basic relationship of the components. This is an ideal model showing logical components and their respective Interactions (Edo et al., 2022). From Figure 4, the policy decision point (PDP) is divided into two logical components: the policy engine and the policy administrator (defined below). The different components use the control plane to communicate, while the application data is communicated on a data plane.

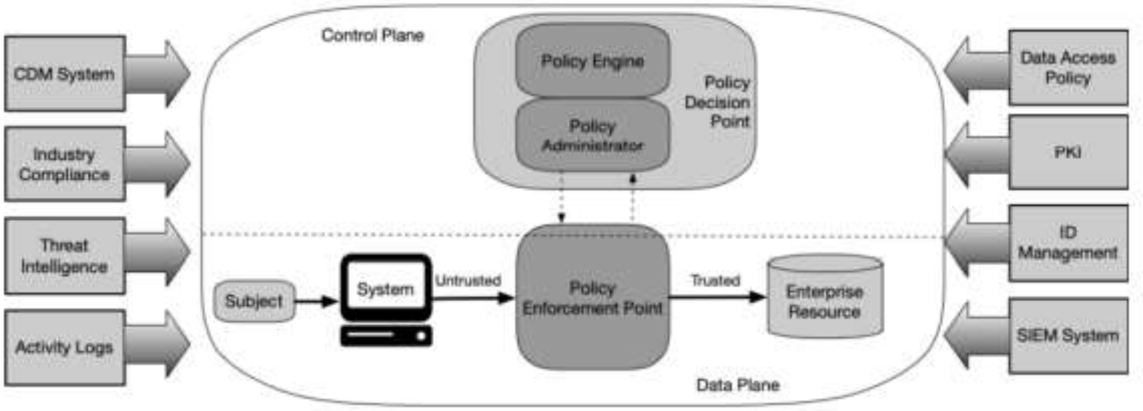


Figure 4: Portrays the Key Components of a ZFT

The Policy Engine (PE). This component is responsible for the final decision regarding access from a certain subject to some resource. It makes this decision based on enterprise policies as well as on inputs from external sources, e.g., CDM systems or threat intelligence services, feeding into a trust algorithm; see Section 3.3 below. The PE works in conjunction with the policy administrator component. It makes and logs the decision - approved or denied, while the policy administrator carries out the decision (Macaulay & Bhasker, 2024).

Policy Administrator (PA). The function is responsible for creating or deleting the communication channel between the subject and resource, usually by issuing instructions to the responsible Policy Enforcement Points. The latter generates any session-specific authentication tokens or credentials needed by the client to access enterprise resources. A PA is closely related to the PE and relies on its decision to either allow a session or deny it. When the session is authorized and authenticated, the PA configures the PEP to initiate the session (Edo et al., 2022). In case of an access denial or revocation of any previous approval, the PA sends a message to the PEP for connection termination.

Policy Enforcement Point (PEP). As per Green-Ortiz et al. (2023), this component manages the establishment, monitoring, and termination of connections between a subject and an enterprise resource. It interacts with the Policy Administrator (PA) to forward access requests and receive policy updates. While conceptually a single component within Zero Trust Architecture, the PEP can be segregated into two parts: the client-side portion-for example, an agent on a laptop-and the resource-side portion, such as a gateway controlling access to the resource or it can be a single portal acting as a gatekeeper for the communication paths. Beyond the PEP is the trust zone, in which resides the enterprise resource.

Continuous Diagnostics and Mitigation System. The system provides near real-time data regarding enterprise asset status and configuration and applies updates to configuration and software components. The CDM shall provide the policy engine information on the status of the asset seeking access to enterprise resources such as whether the operating system is the most current patched version, whether approved software components are installed and free of corruption, whether unauthorized components have been added, and whether any exploits for known vulnerabilities are detected (Akisanya, 2024). CDM systems are also supposed to identify and, when relevant, apply a subset of policy to non-enterprise devices that attach to the enterprise network.

Industry Compliance System. This is the system that ensures an enterprise stays in compliance with any relevant regulatory requirements for instance, FISMA, or industry-specific standards on healthcare or financial systems. It captures all policy rules an organization sets up to stay compliant with such regulations (Khan, 2023).

Threat Intelligence Feed(s). This component provides information from internal and external feeds to the policy engine to make decisions on access. These feeds could be from various services that draw data from diverse sources about newly identified attacks, vulnerabilities, flaws in software, new malware, and attacks against other assets. By availing this information, the policy engine will deny access to the enterprise assets.

Log network and system activity. The enterprise system will capture logs from the assets, network traffic, resource access actions, and other occurrences in real or near-real time, providing insight into the security posture of enterprise information systems(Moore, 2022).

Data Access Policies. These are the properties, rules, and policies defining access to enterprise resources. These rules may be created manually in a management interface, or they may be generated automatically in a policy engine. These policies provide the basis for access to resources and define the basic access rights for accounts and applications within the enterprise. They must be reflective of the mission roles and requirements of the organization as established in the data classification policy (Seaman, 2023).

Enterprise public key infrastructure PKI: This component is the system responsible for generating and logging the various issued certificates to resources, subjects, services, and applications. This also includes a global certificate authority ecosystem and Federal PKI,4 of which may or may not be integrated with the enterprise PKI. This could also be a PKI not based on X.509 certificates (Sarkar et al. 2022) .

Identity management system. This engineering artifact creates, stores, and manages enterprise user accounts and identity records (e.g., lightweight directory access protocol (LDAP) server). This system contains the necessary subject information (e.g., name, email address, certificates) and other enterprise characteristics such as role, access attributes, and assigned assets. This system often leverages other systems, such as a PKI, for artifacts associated with user accounts. This system may be a component of broader federated target communities and may include non-enterprise employees or links to non-enterprise assets for collaboration to be enabled (Muhammad et al., 2022).

Security information and event management (SIEM) system. This component collects security-centric information for later analysis. This data is then used to refine policies and warn of possible attacks against enterprise assets.

Trust Algorithm

According to Seaman (2023), the policy engine acts as the "brain" in a Zero Trust Architecture (ZTA) deployment, and the trust algorithm (TA) provides the main decision-making process thereof. The trust algorithm renders a decision to grant or deny access to a resource. The policy engine takes input from various sources, such as a policy database that may include observable data on subjects, their attributes and roles, historical behavior patterns, threat intelligence feeds, and other metadata. Such a decision-making process can be grouped into broad areas, as illustrated in Figure 5.

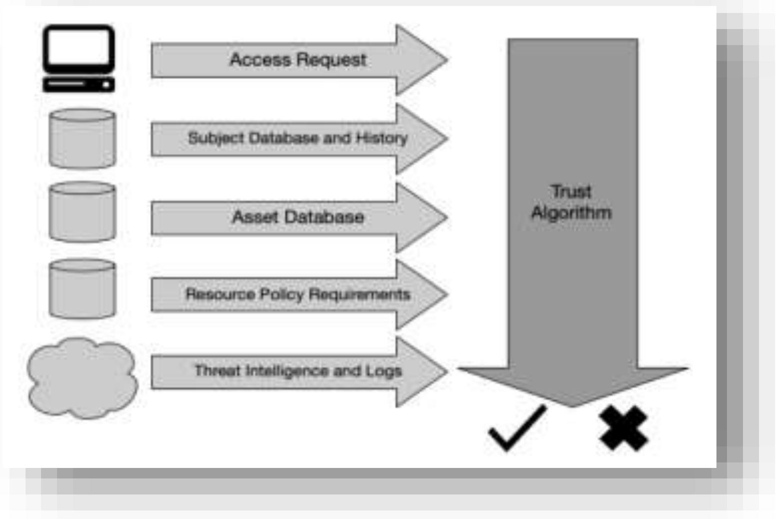

Access Request
Subject Database and History
Asset Database
Resource Policy Requirements
Threat Intelligence and Logs
Trust Algorithm

Figure 5: Displays the Trust Algorithm Input

- **Access Request:** This is a subject's specific request for access to some resource. The major factor in the decision is the resource being requested, but aspects of the requester are considered as well. This can include the version of the operating system, the software being used in making the request, such as is the application on an approved list, and the patch level. All of these factors, in addition to the security posture of the asset, may lead to restriction or denial of access (Oladimeji, 2024).
- **Subject Database & History:** This database identifies "who" is accessing the resources. Subjects can include human users and other processes on behalf of the enterprise or partners. It contains subject attributes and privilege assignments, which provide the basis for policies. User identities can also include logical identifiers such as account IDs, created by authentication test results returned by the PEPs. Other attributes, like current time and geolocation, may be applied to establish confidence levels in the identity being checked (Sarkar et al., 2022). While multiple subjects' privileges can form a role, access must be granted on an individual basis for specific identified needs rather than simply because the individual fits into a named organizational role. This information is encoded and stored in some form within an identity management system and policy database, and may also include records of past subject behavior in the form of some trust algorithm (TA) (Moore, 2022).
- **Asset Database:** This domain contains the known status of all the assets owned by the enterprise insofar as it is possible, this even includes BYOD. It is utilized to not only compare the observable status of the requesting asset, such as OS versioning installed software and the integrity of said software (Khan, 2022).
- **Resource Requirements:** This set of policies complements the user ID and attributes database with the minimum requirements that must be met to access a resource. Among such minimum requirements might be things like authenticator assurance levels- hence, as an example, this would include MFA-network restrictions, such as overseas IP address blocking-data sensitivity considerations, and asset configuration standards. It is here that these policies should be collaboratively developed by the data custodians who have major responsibility for safeguarding the data with business process owners who have major responsibility for the mission or tasks relying on the data (Syed et al., 2022).
- **Threat Intelligence and Logs:** This domain is the information feeds from general threats and active malware on the internet. This operation can also involve specific insights related to suspicious communication by a device, such as communications to potential malware command-and-control nodes. Threat intelligence may be provided by external services or from internal scans and discoveries. It provides attack signatures data and their mitigation strategies. This generally is an externally operated service rather than one managed directly by the enterprise (Edo, 2022).

Conclusion

In summation, the deployment of Zero-Trust Architecture represents an important step toward better cybersecurity for U.S. critical infrastructure. The paper also found that the principles of Zero-Trust, such as continuous authentication, least-privilege access, and strict monitoring, would go a long way in reducing vulnerabilities and mitigating the risks associated with both external and internal threats. On the other hand, major complexities associated with legacy systems, the need for robust policy enforcement, and the use of advanced technologies are some of the key challenges that must be overcome for successful implementation. This research underlines that while ZTA is a very promising concept, its real implementation needs to be tailored to the specific needs of each critical infrastructure sector and must represent continuous coordination among government agencies, industry stakeholders, and cybersecurity experts if it will succeed.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Akinsanya, A. (2024). Securing the Future: Implementing a Zero-Trust Framework in US Critical Infrastructure Cybersecurity.

[2] Edo, O. C., Tenebe, T., Etu, E. E., Ayuwu, A., Emakhu, J., & Adebiyi, S. (2022). Zero Trust Architecture: Trend and Impact on Information Security. International Journal of Emerging Technology and Advanced Engineering, 12(7), 140.

[3] Federici, F., Martintoni, D., & Senni, V. (2023). A zero-trust architecture for remote access in industrial IoT infrastructures. *Electronics*, *12*(3), 566.

[4] Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces, 89, 103832.

[5] Green-Ortiz, C., Fowler, B., Houck, D., Hensel, H., Lloyd, P., McDonald, A., & Frazier, J. (2023). *Zero Trust Architecture*. Cisco Press.

[6] Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116.

[7] Macaulay, T., & Bhasker, D. (2024). High Performance Computing Infrastructure and Zero Trust Architecture. *Pulse & Praxis: The Journal for Critical Infrastructure Protection, Security and Resilience*.

[8] Moore, C. (2022). A Zero Trust Approach to Fundamentally Redesign Network Architecture within Federal Agencies (Doctoral dissertation, Capella University).

[9] Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. *International Journal of Computer Science and Technology*, *6*(4), 99-135.

[10] Oladimeji, G. (2024). A Critical Analysis of Foundations, Challenges and Directions for Zero Trust Security in Cloud Environments. *arXiv preprint arXiv:2411.06139*.

[11] Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. *Sustainability*, *14*(18), 11213.

[12] Seaman, J. (2023). Zero trust security strategies and guideline. In *Digital Transformation in Policing: The Promise, Perils and Solutions* (pp. 149-168). Cham: Springer International Publishing.

[13] Stafford, V. (2020). Zero trust architecture. *NIST special publication*, *800*, 207.

[14] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, 57143-57179.