International Journal of Applied Mathematics, Sciences, and Technology for National Defense
Volume 3, Issue 1, 35-44
e_ISSN: 2985-9352, p_ISSN: 2986-0776
https://www.journal.foundae.com/index.php/JAS-ND
DOI : https://doi.org/10.58524/app.sci.def.v3i1.669

Zero trust framework for protecting federal networks and cloud services

Sudheer Kotilingala
IBM Corporation,
USA

Article Info

Article history:

Received: February 2, 2025
Revised: March 26, 2025
Accepted: April 17, 2025
Published: April 30, 2025

Keywords:

Cloud computing
FedRAMP
Network Security
Zero Trust Architecture

Abstract

There has been a rapid uptake of cloud technologies in public sectors due to increased efficiency across operations while increasing the complexity of cyber threats. This paper analyses the original Zero Trust Architecture (ZTA) concept as a security concept applicable to federal networks and cloud services protection. It mainly involves linking ZTA principles with FedRAMP regulations and insists on constant validation, minimisation of rights, and breach presumption. The study outlines guidelines for ZTA implementations for compliance and readiness in the cloud environments.

To cite this article: Kotilingala, S. (2025). Zero trust framework for protecting federal networks and cloud services. *International Journal of Applied Mathematics, Sciences, and Technology for National Defense,* 3(1), 35-44

INTRODUCTION

Cloud computing has become a popular option in the advanced adoption of digital modernisation solutions, offering flexibility, scalability, and operations (Kolawole, 2025). However, these advancements have also increased the risk of hacking, data leakage, misconfigurations, and interim access. Cloud environments in government and critical infrastructure sectors face complex cyber threats, particularly in areas such as IAM weaknesses, misconfigurations, and third-party dependencies (Veeramachaneni, 2024). Zero Trust Architecture (ZTA) is a strong and stable model that has been established to respond to these challenges. Unlike traditional perimeter-based models, ZTA adopts a "never trust, always verify" approach, enforcing additional authentication and strict access control measures. This study examines improvement strategies for ZTA within the context of FedRAMP security, focusing on architecture, design, implementation, challenges, and benefits (Stafford, 2020).

Challenges in Federal Networks and Cloud Services

Because they are substantial platform structures, security issues in federal networks and cloud services are high. Lack of proper security control implementations, inadequate identity and access management mechanisms, third-party dependencies, and the dynamic nature of compliance all form the basis of these environments (Vang & Lind, 2023). Adhering to strict frameworks such as FedRAMP is challenging; coupled with emerging cyber threats, it is even more difficult. To counter these problems, a sound security solution involves adopting sophisticated mechanisms, cyclic evaluation, and compliance with security measures in frontline protection and defence of government data from cybercriminals (CISA, 2021; NSA, 2021).

***Corresponding Author:**
Sudheer Kotilingala, IBM Corporation, USA, Email: reachsudheer.kotilingala@gmail.com

Misconfigured Security Controls

Inadequate security control settings are among the most critical aspects of today's federal cloud solutions. Misconfigurations result from human factors, implementation issues, or lack of proper supervision. For instance, a cloud storage bucket might be wrongly set up and expose the wrong information to the public, causing considerable company security compromises. To overcome this challenge, there should be standard audits, configuration management with the assistance of automatic systems, and strict compliance checks. Another challenge persists in Identity and Access Management (IAM). Intake IAM practices include poor password policies or lack of scheduled and routine user access review; these can result in unauthorised access and data leakage. Public sector infrastructures are potentially at risk if they have inadequate IAM systems due to identity-based attacks that use users' credentials to access public sector systems. IAM policies must be bolstered using tools like MFA and rigorous access reviews (Paul & Rao, 2023).

Third-Party Risks and Dependencies

Third parties and dependence are also issues for federal networks and cloud services. Many public sectors acquire cloud solutions, software, and services from a third-party provider. However, one can single out another drawback: the attackers, or the loopholes in the third party, may spread as far as federal systems, yet with an emphasis on secure data. Third-party risk management must be effective, and security controls must be carried out periodically to ensure legal compliance with contracts, holding to the security provisions from third-party agreements.

Compliance Challenges with FedRAMP Frameworks

Other challenges related to FedRAMP frameworks are also easily encountered. While FedRAMP offers a unified standard for the security assessment and authorisation process, achieving and maintaining compliance in large-scale, distributed, and complex cloud systems can be pretty costly. Agencies must solve encryption, data localisation, and access management issues while always complying with changing requirements. Real-life security events and documented incidents demonstrate network vulnerabilities which demands the implementation of a rigorous defense mechanism like Zero Trust. Several recent successful cyberattacks on federal cloud computing have originated from incorrect configurations, insufficient IAM, or third-party issues. Such events bring the understanding that the government requires a robust security model like Zero Trust to provide protection and meet compliance requirements to safeguard federal data (Kopparthi, 2024).

Zero Trust Architecture Alignment with FedRAMP

ZTA is in union with the FedRAMP framework due to more centralised access policies and continuous check & control and is governed by the 'never trust, always check' postulate. All users and devices must be constantly vetted under ZTA, apply for the least privileged access, and always presume breach. These tenets align with key FedRAMP security priorities, including identity management, encryption, authorisation, and risk-based access control (Taylor, 2014). When adopted, ZTA will help public sectors improve FedRAMP's security controls compliance to update threat identification, secure data handling, and cloud protection from cyber threats .

Figure 1 highlights how ZTA's fundamental components are systematically connected to FedRAMP control requirements. First and foremost, ZTA insists on the proactive checking of users and devices, the grant of the bare minimum level of access, and the postulate of business breach, all relevant to the question of safe access and danger mitigation (Shepherd, 2022). These principles are implemented using activities such as authentication and authorisation, access rights control, and preemptive threat management, which correspond to the FedRAMP recommended security measures. These are then linked to FedRAMP controls using technologies like IAM for effective client and identity management, MFA for enhanced authentication, Micro-Segmentation to contain threats, SIEM for continuous monitoring as well as Vulnerability Management for risk prevention, Threat Intelligence and Response for proactive threat handling (Kim et al., 2024; Sweeny, 2021).

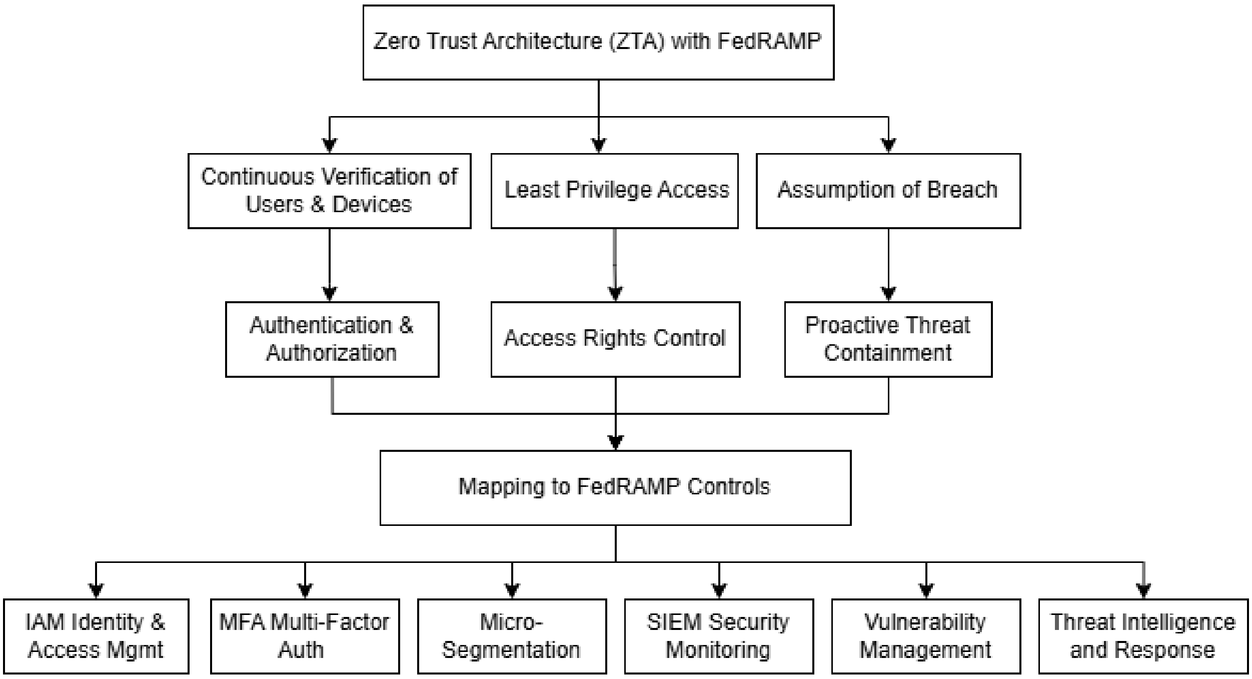
Zero Trust Architecture (ZTA) with FedRAMP
Continuous Verification of Users & Devices
Least Privilege Access
Assumption of Breach
Authentication & Authorization
Access Rights Control
Proactive Threat Containment
Mapping to FedRAMP Controls
IAM Identity & Access Mgmt
MFA Multi-Factor Auth
Micro-Segmentation
SIEM Security Monitoring
Vulnerability Management
Threat Intelligence and Response

Figure 1. Zero Trust Architecture Alignment with FedRAMP

Mechanism of Zero Trust

The model underlies the Zero Trust Architecture (ZTA) is "never trust and always verify", meaning that no user, device or system is granted initial trust whether they are within the network boundaries. It is about the constant identification of users and portable devices, their minimal access rights, and the given utility working based on the probabilistic approach that presupposes the existence of the breach (Syrotynskyi et al., 2024). Such an approach helps to maintain the uniformity of putting into practice security controls for decreasing attack vectors for cyber threats. In this approach, every user and device trying to access the system must regularly complete an authentication and authorisation process. This removes blind trust and complicates any access attempt that is repeatedly checked. Simply put, least privilege access only grants each user's requested access rights, the level of privileges required to do the job. This helps lower the risk of compromised accounts inflicting maximum attacks on the organisation's identity. Next, the assumption of a breach mindset involves the constant anticipation of infiltrations so that systems do not lose much when the worst happens. The proactive approach highlighted in this plan is based on containment and fast reaction.

Mapping Zero Trust Principles to FedRAMP Security Controls

These principles translate to most FedRAMP security controls through rigid policies in IAM, where users and devices are always authenticated. In MFA, the user is presented with multiple ways of proving that the right person requires several steps before being granted access. Micro-segmentation breaks down a network into separate sections to minimise the movement of threats within the network. Security Information and Event Management (SIEM) monitors the event's security in real time and detects threats in real-real terminating the threat (CISA, 2021). The alignment of these principles to FedRAMP controls improves durability, comprehensibility, and conformance in federal cloud networks.

Key Enabling Technologies

Zero Trust Architecture (ZTA) fundamental components are Identity and Access Management (IAM) for accurate authentication, Multi-Factor Authentication (MFA) to compact the layers of the threats, Network Micro-Segmentation to reduce the coverage area of the threats, and Security Information and Event Management (SIEM) for continuous threat identification response. Collective, these technologies provide strong protection, constant vigilance and near real-time response to incidents in the federal cloud environments (Ajish, 2024; Tanque & Foxwell, 2023).

Identity and Access Management

IAM stands for Identity and Access Management, which provides strong protection to organisations by allowing only those employees to access those systems that the management enables. It assists in controlling the access and the authentication process used to control the access to the system resources. Multi-factor authentication (MFA) enhances the traditional single factor to another to discourage access to the wrong individuals. This provides the system access after the client has provided several forms of identification.

Network Micro-Segmentation

Micro-segmentation cuts a network into different isolated areas to minimise the mobility of attackers. It reduces the susceptibility of the user's information to compromise on a larger scale. SIEM enforces real-time monitoring and threat intelligence, increasing quick response time to security threats. They collect and parse security logs coming from different sources.

Vulnerability Management

Vulnerability management is essential in protecting federal networks and cloud services. This is a process of discovering, evaluating and implementing measures against system, application or configuration risks. Regular scans, timely patching, and automation are crucial to identifying the hazardous openings in the organisation and rectifying them before adversaries utilise them. A proactive VM program enables public sectors to be ready to protect their essential systems' integrity, confidentiality and availability. Enhanced constant vigilance and reporting of security processes going on in organisations working on the internet will reduce the magnitude of the impact of cyber threats and data breaches that may feature now and then.

Threat Intelligence and Response

Threat intelligence and response plans are essential to prepare federal clouds against new threats that might arise in the future. Agencies can get a live feed of the related destructive events by incorporating threat intelligence feeds, behavioural analysis, and other enhanced threat detection methods. Containing and recovering from cyber incidents can be easily implemented by threat response strategies such as incident response plans & automated mitigation workflows. Cooperation between government agencies and information exchange services increases threat awareness and improves aggregate protection.

METHOD

ZTA, or Zero Trust Architecture, is a security approach where no trust is granted to any underlying system or network, regardless of the user's location or device. Given the stringent requirements of FedRAMP, designing a scalable ZTA model necessitates a holistic approach incorporating advanced security practices (Colomb et al., 2023). The following is the content of the research categorised by components.

Architecture Design

ZTA for FedRAMP entails the development of a security architecture in which trust is not accorded to any origin or level. It also notes that architecture continually performs authentication, authorising, and monitoring. These are identity and access management (IAM) systems, segmentation, and robust encryption. The solutions built natively for the cloud allow growth while remaining fully compliant with FedRAMP. Moreover, putting in place endpoint security checks guarantees that any device seeking connection to the network will be scanned as frequently (Phiayura & Teerakanok, 2023).

Figure 2 illustrates key components of a Zero Trust model designed for FedRAMP compliance. The core argument around which all the model components revolve is ‘never trust, always verify.’ This safe processes principle is implemented using Authentication & Access Control measures such as Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and Privileged Access Management (PAM). These components work with Endpoint Security, which checks the devices that connect to the system and scans them to ensure the system’s safety. Realizing both the authentication and endpoint security is backed by solid Data Protection measures like encryption and Data Loss Prevention (DLP) for maintaining the data secrecy during storage plus transfer. Further, the model contains API Security to protect the application interfaces by real-time verification and constant traffic. Last but not least, Logging & Monitoring, utilising the use of SIEM as well as UEBA, puts all the components together and provides the desired means of perceiving, tracking, and handling anomalous activities, compliance, and acute threats actively – thus setting the ground for the implementation of ZTA across the FedRAMP environments (Ahmadi, 2024).

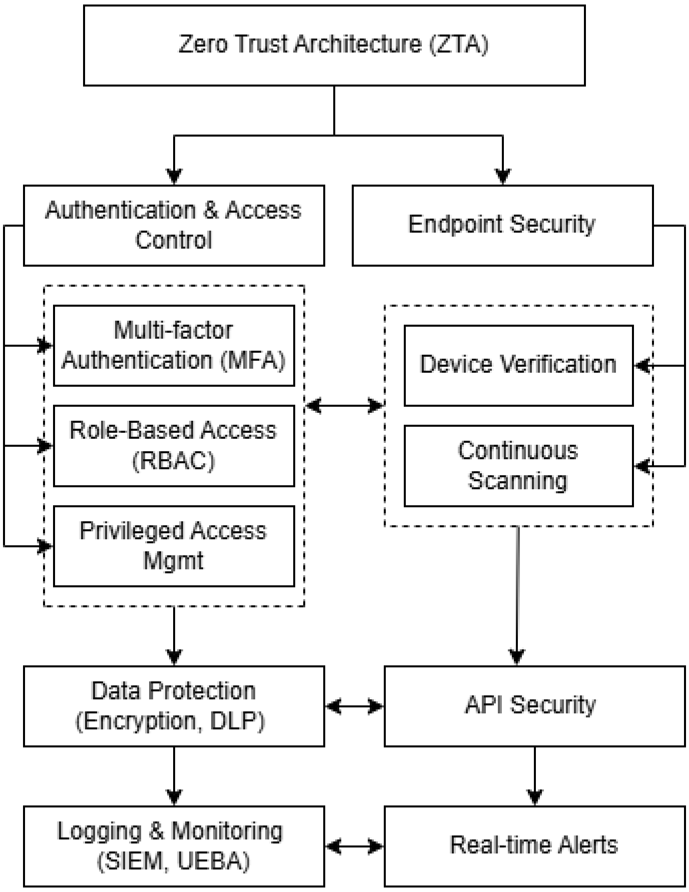
Zero Trust Architecture (ZTA)
Authentication & Access Control
Endpoint Security
Multi-factor Authentication (MFA)
Role-Based Access (RBAC)
Privileged Access Mgmt
Device Verification
Continuous Scanning
Data Protection (Encryption, DLP)
API Security
Logging & Monitoring (SIEM, UEBA)
Real-time Alerts

Figure 2. ZTA Model for FedRAMP Compliance

Authentication and Access Control

The matters based on traditional access control include authentication and should guarantee that not every user can have access to the resources. RBAC, for instance, remains a firm IAM policy that grants access based on the roles an individual assumes at a given company. Multi-factor authentication is crucial for tying an additional layer of protection into accounts by using a password and possessing a mobile token. Moreover, privileged access management also minimises and controls the level of access to inner systems, improving security.

Data Protection

Data protection in zero-trust models is the key to guaranteeing data confidentiality in storage and transfer. Database and file encryption stabilises data in storage facilities using methods like AES-256 and protects data during transmission with methods like TLS. Data Loss Prevention (DLP) strategies are also essential. They identify sensitive information to prevent it from being accessed or transferred insecurely, preserving data clarity.

API Security

In a Zero Trust Architecture, protection against the abuse of application interfaces is essential for API security. Implementations of real-time validation facilitate restricted acceptance of API calls so that only correct calls are accomplished. API gateways ensure this practice by making a sieve of all the requests made and rate-limiting mechanisms placed on it. Moreover, constant observation of API traffic allows early identification of signs of attacks or unauthorised utilisation of the API, such as increased traffic.

Logging and Monitoring

Constant checks are central to the security and operation of a Zero Trust system. UEBA and other similar tools identify patterns of users and system performance and may discover that they have been compromised. Using SIEM systems means the possibility of collecting and analysing separate information about security incidents each second, as well as a guaranteed immediate response to any violations.

Implementation of ZTA in FedRAMP Environments

Implementing a flattened network within Zero Trust Architecture (ZTA) for FedRAMP compliance requires strategic adjustments to security frameworks. This includes the IM-IT implementation process, integration factors, and approaches to addressing the interoperability issues(Kopparthi, 2024; Ren et al., 2025).

Method for Adoption of Zero Trust Principles to Support Federal Cloud Systems

The initial phase involves a security risk audit to identify gaps and assess the current security environment. After that, a robust IAM system incorporating MFA and RBAC will be defined, and network segmentation will be used to minimise attack vectors. SIEM and UEBA should ideally be used to monitor the network for threats to combat them perpetually. Last, the security should be reviewed at least once yearly, and a FedRAMP compliance assessment should be applied for updates and enhancements.

Table 1. The correlation between FedRAMP controls, the Zero Trust focus area, and the use case

Requirement Area	FedRAMP Controls	Zero Trust Focus	Use Cases
Logging and Monitoring	• AU-11 (Audit Record Retention) • SI-4 (System Monitoring)	Continuous monitoring and anomaly detection	• Monitor unauthorized access attempts in real time. • Investigate incidents using audit logs.
Identity and Access Management	• AC-4 (Information Flow Enforcement) • IA-2 (Identification and Authentication)	Least privilege access and continuous verification	• Enforce multi-factor authentication (MFA). • Automate user access reviews and compliance checks.
Vulnerability Management	• RA-5 (Vulnerability Scanning) • CA-2 (Security Assessments)	Proactive vulnerability discovery and mitigation	• Detect misconfigurations in cloud resources. • Patch vulnerabilities based on prioritization.
Network Segmentation	• SC-7 (Boundary Protection) • SC-12 (Cryptographic Protection)	Isolate workloads and encrypt communications	• Implement micro-segmentation in hybrid cloud. • Secure sensitive data using encryption.
Data Protection	• SC-12 (Encryption) • SC-28 (Protection of Information at Rest)	Encrypt data at rest and in transit	• Encrypt sensitive files stored in cloud environments. • Apply tokenization and data masking.
Threat Intelligence and Response	• IR-4 (Incident Handling) • SI-3 (Malicious Code Protection)	Automated incident response and mitigation	• Detect and respond to DDoS attacks. • Block malicious activities using AI-based threat detection.
Zero Trust Architecture	• NIST 800-207 Alignment • SA-9 (External System Services)	Adopt Zero Trust principles (assume breach)	• Implement Zero Trust for remote workforce. • Secure access to SaaS applications with adaptive controls.

Table 1 illustrates how FedRAMP controls align with Zero Trust focus areas and use cases, guiding ZTA deployment in FedRAMP environments. Every requirement area describes FedRAMP controls and related Zero Trust frameworks and identifies how the controls solve significant security issues such as unauthorised access, vulnerability, and data protection.

Key Considerations to Ensure a Seamless Integration

Integrating ZTA systems into current FedRAMP-compliant systems hinges on the significance of ZTA components about FedRAMP security requirements, particularly IAM, encryption, and access. Control. Cloud-native solutions require integration into FedRAMP, and the ZTA Framework must not diminish efficiency. FedRAMP requires constant monitoring, and therefore, for any integration to be successful, the two must monitor and follow FedRAMP's continuous tracking in real-time.

Overcoming Interoperability Barriers between US Governing Bodies

The most significant issues when implementing ZTA involve interoperability problems across different cloud ecosystems and agencies. Agencies must establish best practices regarding the ZTA implementation to provide unity across cloud providers and technologies. Third-party integration requires strong access and secure application program interfaces, or APIs. Further, training and clear documentation are critical in muscle memory regarding security for public sectors.

The Difficulties of Adopting Zero Trust for FedRAMP Compliance

Zero Trust Architecture (ZTA) is not easily implementable in FedRAMP-compliant environments. These challenges arise from technical approaches, operational processes, and system organisation that call for practical evaluation and design to achieve a transition to the advanced security model of zero trust (Azad et al., 2024).

Integrating Computerisation with Pre-existing Federal Systems

Most public sectors use outdated systems that are not built to support the zero-trust model. Implementing ZTA in some of these legacy systems can be quite a nightmare because current systems may not be compatible with modern security standards. There is no support for new authentication modes, and monitoring security anomalies without interrupting essential services is challenging. To overcome this challenge properly, there's a need to begin by prioritising such systems to address first, and depending on their nature, there may be a need to reinvent or replace some of the underlying infrastructures to comply with ZTA.

The Balance of Security Needs with Organisational Functioning

Zero Trust frameworks seek to apply demanding security protocols, which adds tension in achieving velocity and accessibility in operational practices. For instance, never-ending authentication, daily/weekly access control reviews, and fine-grain access will cause operational latency and affect organisational efficiency. The agencies must find the perfect working balance for ZTA, especially regarding their security needs and working processes. One of the most important things to accomplish regarding deployment is ensuring that users are given access at appropriate levels while having a strong security solution.

Main Limitations in ZTA Deployment within Federal Environments

ZTA deployment within environments demands a considerable investment in monetary and human resources. In many cases, agencies may be unable to provide adequate funds for the required technologies, instruments, and training that support ZTA. Also, there can be a lack of internal knowledge of the organisation to provide the necessary high level of security and to use innovative cloud-based solutions for a zero-trust strategy. Such gaps may be filled outside through contracting or acquiring new products and services for federal cybersecurity personnel. At the same time, continuous training may also be needed to improve the teams.

Reducing Cultural Resistance to Implementing Zero Trust

The implementation of Zero Trust security faces significant resistance because organisations maintain an established perimeter-based security philosophy. People in organisations who work in more relaxing environments will resist continuous authentication, stricter access privileges, and other measures associated with the Zero Trust strategy. This resistance might be addressed through effective presentation of the values of ZTA, constant familiarisation of the agency faculty with the ZTA policies, and the support of leadership in creating a security-minded agency culture. Furthermore, when a good change management plan is developed, the following can be pointed out and concerns addressed, thus ensuring that a smooth transition to these systems is made due to the potential of giving long-term security advantages.

RESULTS AND DISCUSSION

Adopting ZTA across FedRAMP-compliant cloud platforms has benefits for security and ease of compliance with emerging requirements (Chandramoulu & Butcher, 2023; Sarkar et al., 2022).

Improved Protection Against Cybersecurity Risk

As it eliminates the centralisation of authority and decentralises security measures like authentication, access control, and monitoring, Zero Trust improves the robustness of the federal cloud networks. (These layers have proven beneficial in safeguarding against the potential for a cyber threat such as data leakage, insider threat, and advanced persistent threats (APTs).) ZTA assumes threats are active inside and outside the network and minimises the risk any attacker can pose by reducing their mobility once inside the network.

Enhance Alignment to FedRAMP Controls and Guidelines

It must be noted that Zero Trust's strict access controls, MFA, and data protection fully correspond to the FedRAMP security control and provide recommendations. ZTA's focus on constant checking and validation guarantees that FedRAMP's tight security and privacy standards are met. The ability to automate and continuously scan for threats in the context of a Zero Trust perspective makes compliance easier and assists with achieving the rigorous FedRAMP certification status.

Increased Visibility of Cloud Computing and Related Systems

In ZTA, public sectors obtain enhanced insights into their cloud environment because monitoring user actions, device connectivity, and network flow is required in real-time. SIEM systems backed up with further Zero Trust platforms offer real-time security monitoring and generate reports that can save agencies time detecting security threats. This increases general security and provides a way through which Any threat or policy breach that may pose a significant problem may be spotted early.

Changes to Federal Cybersecurity Restrictions

Due to its flexibility, Zero Trust is easily actionable and can be adjusted to the flowing federal cybersecurity mandates, such as the changes in FedRAMP controls or new legislation. This framework can be altered easily to respond to dynamically changing risks so that the agencies stay current with the standards. Furthermore, due to its support for scalability, ZTA can be implemented more quickly as public sectors increase the overall scale of cloud environments or incorporate new technologies into them (Akinsanya, 2024).

Trends for Behavioural Analysis Through ZTA for Increasing Federal Cloud Security

As the use of ZTA advances, several emerging trends are believed to define the future of cloud security in the federal environment. Both of these trends are aimed at using innovative technologies and evolving with newly introduced changes in regulations to enhance the security of public sectors (Bobbert & Timmermans, 2024; Kim et al., 2024).

The Blending of AI and Machine Learning in the Approaches to Zero Trust Threat Identification

AI and ML are the primary features of the Zero Trust technology advancements, which enhance the performance of the existing solutions. These technologies may help the threat detection process and divide significant volumes of comprehensive extraneous information in real time. AI and ML algorithms present a possibility to quickly analyse network traffic, user actions, and device interactions and correctly recognise hazardous patterns. As these programs continuously learn from information, they can also prevent new security threats from arising and developing, making federal cloud networks even more secure.

Cloud-Native ZTA Solutions Shift Enabled for FedRAMP

Zero Trust solution offerings are emerging as more organisations adopt cloud-native cloud solutions, including those meeting FedRAMP requirements. Emerging cloud-native ZTA solutions offer scalability, flexibility, and compatibility with diverse cloud environments. These solutions can potentially provide a more flexible and economically viable approach to the Zero Trust principles in a comprehensive federal cloud toward that vision by using containerisation, microservices, and serverless computing. Moreover, such solutions must integrate well with FedRAMP controls to uphold public sector compliance while implementing state-of-the-art security approaches.

Policy achieved and shifting requirements for related policies enabling ZTA

With proliferated types of cyber threats, developing regulatory requirements and policies that govern the implementation of zero-trust concepts in public sectors remains relevant. Future policies will likely emphasise ongoing validation, least privilege access, and continuous monitoring to counter evolving threats. New regs will probably offer further direction on using Zero Trust across different cloud environments and affirm agencies' FedRAMP compliance with general Federal cybersecurity requirements. The fact that there is an evolution of policy and regulation will make more agencies embrace ZTA as a standard security model and guarantee long-term defence for such burgeoning threats.

CONCLUSION

Zero Trust Architecture (ZTA) contributes significantly to improving the security of FedRAMP-compliant cloud applications by adopting principles that always validate users and devices, control access, and assume breaches. These principles coincide with the security tenets used by FedRAMP to provide a sound solution to the cybersecurity issues encountered by public sectors. In addition to protecting federal networks from misconfiguration of security controls and poor identity management, ZTA also enhances protection against advanced threats.

The adoption of Zero Trust in public sectors is expected to grow, driven by advancements in AI and ML and evolving regulatory requirements. Since AI and ML are cloud-native solutions, their development and improvement will contribute to ZTA's threat identification and counteraction efficacy. As modern regulatory requirements gradually enable the Zero Trust concept, public sectors will expand the implementation of this model, thus providing better protection to the prioritised government information and computing facilities.

AUTHOR CONTRIBUTIONS

Author of this article played an important role in the process of method conceptualization, simulation, and article writing.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

CISA. (2021). *Cybersecurity and Infrastructure Security Agency - Zero Trust Maturity Model*. Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security division.

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

Kopparthi, V. J. R. (2024). Federal cloud security: A strategic approacj to FedRAMP compliance and governance. *International Journal of Research in Computer Applications and Information Technology (IJRCAIT)*, 7(2), 2288–2296. https://doi.org/10.5281/zenodo.14500455

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. https://doi.org/10.3390/su141811213

NSA. (2021). *Zero trust: A guide for implementation.* National Security Agency, U.S.

Taylor, L. (2014). FedRAMP: History and future direction. *IEEE Cloud Computing,* 1(3), 10-14. https://doi.org/10.1109/MCC.2014.54

Kolawole, I. (2025). Leveraging Cloud-based ai and zero trust architecture to enhance U. S. cybersecurity and counteract foreign threats. *World Journal of Advanced Research and Reviews*, 2025, 25(03), 006-025. https://doi.org/10.30574/wjarr.2025.25.3.0635

Veeramachaneni, V. (2024). Integrating Zero Trust Principles into IAM for Enhanced Cloud Security. *Recent Trends in Cloud Computing and Web Engineering*, 7(1), 78–92. https://doi.org/10.5281/zenodo.14162091

Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. *Journal of Engineering Research and Reports*, 26(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083

Chandramouli, R., & Butcher, Z. (2023). *A zero-trust architecture model for access control in cloud-native applications in multi-location environments*. US Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207A

Paul, B., & Rao, M. (2023). Zero-trust model for smart manufacturing industry. *Applied Sciences*, 13(1), 221. https://doi.org/10.3390/app13010221

Shepherd, C. (2022). *Zero trust architecture: Framework and case study* (Graduate Student Project). Boise State University.

Akinsanya, A. (2024). Securing the Future: Implementing a Zero-Trust Framework in U.S. Critical Infrastructure Cybersecurity. *International Journal of Advance Research, Ideas and Innovations in Technology*, 10(3) V1013-1221.www.IJARIIT.com

Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. *IEEE Access*, 11, 19487-19511. https://doi.org/10.1109/ACCESS.2023.3248622

Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, 27, 101227. https://doi.org/10.1016/j.iot.2024.101227

Kim, H., Kim, Y., & Kim, S. (2024). *A study on the security requirements analysis to build a zero trust-based remote work environment*. Retreived from arXiv preprint arXiv:2401.03675.

Ajish, D. The significance of artificial intelligence in zero trust technologies: a comprehensive review. *Journal of Electrical Systems and Information Technology,* 11(30), 1-23. https://doi.org/10.1186/s43067-024-00155-z

Syrotynskyi, R., Tyshyk, I., Kochan, O., Sokolov, V., & Skladannyi, P. (2024). Methodology of network infrastructure analysis as part of migration to zero-trust architecture. *CSDP* 2024, (3800), 97-105.

Tanque, M., & Foxwell, H. J. (2023). Cyber risks on IoT platforms and zero trust solutions. *In Advances in Computers*, 131(2023), 79-148. https://doi.org/10.1016/bs.adcom.2023.04.003

Kim, Y., Sohn, S. G., Jeon, H. S., Lee, S. M., Lee, Y., & Kim, J. (2024). Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. *KSII Transactions on Internet and Information Systems (TIIS)*, 18(9), 2665-2691.

Sweeney, C. (2021). *A Zero-Knowledge Multi-Factor Authentication Framework for Actualizing the Federal Zero-Trust Enterprise* (Master's thesis), Utica College.

Bobbert, Y., & Timmermans, T. (2024). Zero Trust and Compliance with Industry Frameworks and Regulations. *In: Arai, K. (eds) Advances in Information and Communication. FICC 2024. Lecture Notes in Networks and Systems*, vol 921. Springer, Cham. https://doi.org/10.1007/978-3-031-54053-0_43

Colomb, Y., White, P., Islam, R., & Alsadoon, A. (2023). Applying Zero Trust Architecture and Probability-Based Authentication to Preserve Security and Privacy of Data in the Cloud. *In: Daimi, K., Alsadoon, A., Peoples, C., El Madhoun, N. (eds) Emerging Trends in Cybersecurity Applications*. Springer, Cham. https://doi.org/10.1007/978-3-031-09640-2_7

Vang, T., & Lind, M. L. (2023). Factors Influencing Cloud Computing Adoption in a Zero-Trust Environment. https://doi.org/10.21203/rs.3.rs-3152878/v1

Ren, Y., Wang, Z., Sharma, P. K., Alqahtani, F., Tolba, A., & Wang, J. (2025). Zero Trust Networks: Evolution and Application from Concept to Practice. *Computers, Materials & Continua*, 82(2), 1593-1613. https://doi.org/10.32604/cmc.2025.059170