International Journal of Contemporary Research In Multidisciplinary

Review Article

Zero-Trust Model for Cloud Security System

Tushar [1*], Dr. Ajay Jangra [2]
[1,2] Department of Computer Science, UIET, Kurukshetra University, India

Corresponding Author: *Tushar

DOI: https://doi.org/10.5281/zenodo.15583975

Abstract

Zero trust cloud security model offers scalable infrastructure, flexible access, and cost-effective resource management. Migration in a cloud environment introduces unique cybersecurity risks, particularly due to the broader threat landscape, the mobile workforce, and distributed services. Traditional perimeter-based security models, which depend on trusted internal networks and firewalls, are no longer sufficient. emerged as a crucial approach to defend sensitive data on this complex, interconnected ecosystem.

As organizations increasingly shift their operations and data to cloud-based environments, traditional perimeter-based security frameworks are proving insufficient to combat evolving cyber threats. The Zero Trust Cloud Security Model is an approach that can be implemented over a cloud network to safeguard from external threats. Instead of assuming that anything inside a network is safe, Zero Trust works on the idea that no user or device should be trusted automatically, not even if they're inside the system.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 19-05-2025
- **Accepted:** 28-05-2025
- **Published:** 02-06-2025
- **IJCRM:**4(3); 2025:259-262

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Manuscript

Tushar, Jangra A. Zero-Trust Model for Cloud Security System. Int J Contemp Res Multidiscip. 2025;4(3):259-262.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Cloud Computing, Cloud Security, Zero Trust Model, Threat Modeling, Data Protection, 5G Network and Edge Computing

INTRODUCTION

This Zero trust model operates at the guiding principle of "never trust, always verify," assuming no implicit believe for any entity, whether or not internal or outside to the network. The Zero Trust approach represents a major departure from conventional security methods. It enforces strict user and device verification, applies role-based access control (RBAC), and incorporates context-aware decision-making to allow or deny access. Every access request is scrutinized based on real-time data points like identity, location, device health, and usage behavior. By espousing zero trust model, companies can restrict publicity to threats, include potential breaches via community segmentation, and keep tighter takeover over records to get entry and movement. Cloud infrastructures—spanning Software as a Service, Platform as a Service, and Infrastructure as a Service — operate in dynamic, distributed environments. These require adaptive and intelligent security mechanisms capable of responding to real-time threats. Zero Trust supports this need by

integrating advanced security components such as identity and access management, continuous authentication, encryption, endpoint protection, and behavioral analytics. These tools work together to continuously review access requirements and immediately block suspicious activity. Additionally, this model provides improved visibility into data flows, user activity, and system interactions that support rapid identification and reduction of potential threats. In regulatory terms, Zero Trust aligns effectively with data protection laws and standards such as GDPR, HIPAA, and ISO 27001. These regulations require rigorous access controls, transparency, and secure handling of sensitive data—principles inherently supported by the Zero Trust framework. By implementing centralized access policies, real-time logging, and strong encryption, organizations can improve their audit readiness and reduce the likelihood of compliance violations. This model is very much useful in immensely regulated service sectors like government authorities, healthcare & finance, in which records privacy and integrity are paramount. Even while the Zero Trust paradigm has advantages, there are drawbacks in cloud computing. Integrating this security model requires restructuring existing IT systems, establishing consistent identity frameworks across cloud platforms, and modernizing legacy applications. Organizations must also ensure comprehensive asset visibility and adapt their workflows to support continuous monitoring. Additionally, achieving stakeholder alignment and training staff to adopt a verification-centric security mindset is essential for successful implementation. Distinct stability in between tight protection and continuous authentication measures can also additionally avoid productivity. Therefore, cautious making plans and a phased implementation approach are critical. Nonetheless, the long-term gains of Zero Trust security are considerable. Enterprises that have adopted this model report significant reductions in data breaches, improved detection of unauthorized activity, and more resilient operational frameworks. With automation playing a key role in threat detection and response, security teams can reduce reliance on manual processes and respond to incidents faster and more effectively. Zero Trust moreover promotes flexibility via different means of allowing steady faraway work environments, cloud-local utility development, and assistance for bring-your-own-device (BYOD) approaches without compromising device integrity. Ultimately, the Zero Trust Cloud Security Model represents a critical evolution in cybersecurity practices, designed to satisfy the needs of today`s fast-transferring and quite interconnected virtual world. By eliminating the concept of inherent trust and ensuring that every access decision is based on contextual verification, organizations can enhance their protection against internal and external threats. This proactive and data handling approach not only enhances security, but also supports compliance and improves operational efficiency. In short, the Zero Trust approach doesn't just boost security—it also helps organizations stay flexible and compliant in a fast-changing digital world. Zero Trust Model provides a strong foundation for protecting cloud environments from modern threats.

RELATED WORK

1. Current Situation

As of 2024, over 70% of Indian enterprises have partially or fully migrated to cloud platforms [1]. However, the benefits of cloud computing come with security concerns, particularly in sectors handling sensitive data like banking, healthcare, and government services.

Traditional perimeter-based security models assume that everything within the network is trustworthy. However, the proliferation of mobile devices, remote work, and hybrid cloud environments renders such assumptions obsolete. The Zero Trust Security Model (ZTSM) addresses this issue by removing implicit trust and enforcing strict identity verification and access controls regardless of the source of the request [2].

This paper surveys the Zero Trust Cloud Security Model with a focus on its relevance, challenges, and applications in the Indian landscape.

2. Principles of Zero Trust Security

Zero Trust is built upon several key principles [3]:

Verify Explicitly: Authenticate and authorize based on all available data.

Use Least Privilege Access: Limit user and application access to only what is necessary.

Assume Breach: Design systems under the assumption that an internal or external breach has occurred.

These principles are particularly relevant in India, where the cybersecurity skill gap and evolving threat landscape require robust, adaptive security mechanisms.

3. Architecture of Zero Trust in the Cloud

A typical Zero Trust architecture in the cloud consists of:

Identity and Access Management (IAM): Centralized control over user identities and access rights, using technologies like SSO, MFA, and federated identities.

Micro-Segmentation: Dividing the cloud network into granular zones to control lateral movement.

Continuous Monitoring: Real-time analytics and behavioral insights to detect anomalies.

Policy Enforcement Points: Systems that apply security policies to every access request.

In the Indian context, cloud service providers like AWS India, Microsoft Azure, and Google Cloud are increasingly integrating native Zero Trust features, including workload identity management and cloud-native firewalls [4].

4. Applications in Indian Sectors

4.1 Government and Public Sector

The Indian government's push for digital governance has led to a surge in cloud-based public services. Projects like DigiLocker, Aadhaar, and UMANG rely on cloud infrastructure, making Zero Trust essential for securing citizen data [5]. The Ministry of Electronics and Information Technology (MeitY) has issued

guidelines promoting Zero Trust frameworks for critical infrastructure.

4.2 Banking and Finance

The Reserve Bank of India (RBI) has mandated stringent cybersecurity practices under its IT framework for NBFCs and banks. Zero Trust supports these mandates through robust access controls and audit trails [6].

4.3 Healthcare

Following the National Digital Health Mission (NDHM), hospitals and clinics are moving data to the cloud. Zero Trust can prevent data breaches and ensure compliance with the proposed Personal Data Protection (PDP) Bill.

5. Implementation Strategies in India

5.1 Identities-Centric Security

Organizations are investing in IAM platforms like Azure Active Directory and Okta, which support Zero Trust by enabling fine-grained access control and conditional access policies [7].

5.2 Zero Trust Network Access (ZTNA)

ZTNA replaces traditional VPNs, offering secure remote access to internal applications. Indian IT giants like Infosys and TCS have adopted ZTNA for their global operations.

5.3 Use of AI and Machine Learning

Indian startups and security firms are leveraging AI to enhance Zero Trust by detecting threats in real-time and automating policy enforcement [8].

6. Challenges in the Indian Context

6.1 Legacy Infrastructure: Many Indian enterprises still operate on legacy systems that are incompatible with modern Zero Trust architectures.

6.2 Cost and Complexity: Implementing Zero Trust requires significant investments in technology and training, posing a barrier for SMEs.

6.3 Regulatory Ambiguity: While the PDP Bill outlines general data protection guidelines, India lacks a unified Zero Trust policy framework, leading to inconsistent adoption across sectors [9].

6.4 Talent Shortage: India faces a shortage of cybersecurity professionals trained in Zero Trust and cloud security frameworks, limiting rapid deployment [10].

7. Future Directions and Research Opportunities

Policy Standardization: There is a need for national frameworks and certifications to guide Zero Trust implementation.

Interoperability Standards: Research on standardizing Zero Trust components across hybrid and multi-cloud environments.

Post-Quantum Cryptography: As quantum computing advances, Indian research institutions must explore cryptographic algorithms compatible with Zero Trust.

Zero Trust for 5G and Edge Computing: With 5G rollout in India, extending Zero Trust to edge devices and low-latency networks is a crucial area for future study.

CONCLUSION

By receiving the guidelines of "never trust, always verify," the Zero Trust model tear down out-of-date reviews of certain beliefs internal arrangement barriers and offers a protection engineering that very well verifies every access request anyhow of origin. The outcome of implementing this model in cloud environments has significant implications not only for reinforcing security pose but also for operational flexibility, compliance, and organizational nimbleness. This control radically decreases the potential harm and information misfortune from breaches, hence enhancing the overall security of cloud resources. The granular access controls inherent in Zero Trust additionally help in minimizing attack surfaces with the help of ensuring that customers and systems have access only to the assets necessary for their roles, making it distant more difficult for malicious actors to misuse excessive permissions. This versatile security component permits cloud environments to respond proactively to rising threats and suspicious activities, regularly before they can cause critical damage. The enhanced visibility into access designs and network activity also equips security groups with richer information for threat detection and incident response, encouraging a more versatile security posture. From a compliance viewpoint, the execution of Zero Trust aligns closely with the prerequisites of information security regulations. These directions command strict controls over information access and security, and Zero Trust's standards inherently support such mandates through rigorous identity management, encryption, and review trails. The capacity to demonstrate continuous confirmation and strict access governance enhances an organization's compliance posture, decreasing the risk of regulatory punishments and reputational harm. In numerous ways, Zero Trust can be seen not just as a security system but also as a compliance enabler in complex regulatory situations. Organizations report moving forward operational effectiveness due to the automation of access management, approach requirements, and threat discovery processes. Computerization decreases the dependence on manual arrangements and human intervention, which are inclined to errors and delays. By empowering secure access from any device or area, Zero Trust supports workforce versatility and efficiency while maintaining strong assurances. This arrangement between security and business objectives is basic for organizational buy-in and supported success of the security methodology. Organizations must explore the complexities of character management over different frameworks, coordinate different cloud service providers, and retrofit legacy applications which will not support advanced security conventions. In spite of these challenges, the results of actualizing Zero Trust approve its transformative impact on cloud security. In addition, the nimbleness given by Zero Trust structures empowers ventures to adapt rapidly to advancing innovation scenes and rising security dangers, cultivating long-term strength. In conclusion, the use of the Zero Trust model in cloud security represents a strategic vital for corporations looking for to defend their virtual assets inside the confront of advancing threats and lengthening cloud selections. By on a very basic level reconsidering trust presumptions,

upholding strict personality verification, and applying granular, context-aware access controls, Zero Trust improves security, supports compliance, and empowers operational productivity. As cloud computing proceeds to develop and threats become more advanced, Zero Trust will stay critical in ensuring data, applications, and infrastructure, empowering organizations to innovate and flourish safely within the computerized era.

REFERENCES

1. NASSCOM. Cloud adoption in India: 2023 outlook. New Delhi: NASSCOM; 2023.
2. Kindervag J. No more chewy centers: Introducing the Zero Trust model of information security. Forrester Research; 2010.
3. Microsoft. Zero Trust deployment guide [Internet]. Microsoft Docs; 2022. Available from: https://docs.microsoft.com/
4. Gartner. Magic Quadrant for Cloud Infrastructure and Platform Services. Stamford: Gartner; 2023.
5. Ministry of Electronics and Information Technology (MeitY). Cloud computing initiatives in e-Governance. New Delhi: MeitY; 2022.
6. Reserve Bank of India. Cybersecurity framework in banks. Mumbai: RBI; 2020.
7. Okta Inc. State of Zero Trust security in India. Okta Whitepaper; 2023.
8. Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Int J Sci Res Manag*. 2021;9(2):564–74.
9. Government of India. The Personal Data Protection Bill. Draft version; 2023.
10. Jimmy FN. Zero Trust security: Reimagining cyber defense for modern organizations. *Valley Int J Digit Libr*. 2022;:887–90.

About the Author

Tushar is a final-year M.Tech. student in Computer Engineering at UIET Kurukshetra, currently holding a CGPA of 9.0. He completed his B.Tech. in Computer Science and Engineering from the same institute with a CGPA of 7.4. His core areas of interest include Cybersecurity, Cloud Computing, and Computer Networking, and he is passionate about advancing knowledge and skills in these domains.