International Journal of
Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
www.computersciencejournals.com/ijcai
IJCAI 2025; 6(1): 159-163
Received: 18-02-2025
Accepted: 25-03-2025

Samir Qaisar Ajmi
College of Education for humanity Sciences, Al-Muthanna University, Samawah, Iraq

Sadiq Sahip Majeed
College of Science, Al-Muthanna University, Samawah, Iraq

Corresponding Author:
Samir Qaisar Ajmi
College of Education for humanity Sciences, Al-Muthanna University, Samawah, Iraq

Securing cloud computing networks using secure access protocols on zero trust architecture

Samir Qaisar Ajmi and Sadiq Sahip Majeed

DOI: https://www.doi.org/10.33545/27076571.2025.v6.i1b.146

Abstract
As cloud computing becomes the backbone of modern IT infrastructures, ensuring the security of cloud networks has emerged as a critical concern. Traditional perimeter-based security models are increasingly inadequate in addressing the dynamic, distributed, and remote nature of cloud environment. This paper explores the implementation of secure access protocols through the lens of Zero Trust Architecture (ZTA) a paradigm that operates on the principle of “never trust, always verify”. Focusing on a case study approach, the research analyzes how Zero Trust principles-such as continuous authentication micro-segmentation least privilege access and strong identity verification can be integrated with secure access protocols like TLS, IPSec and SASE to fortify cloud computing network against evolving threats. The study highlights practical deployment strategies, identifies challenges in adoption and evaluates the performance and security benefits of ZTA in a cloud-native context. The finding underscore the importance of shifting from implicit tryst models to dynamic context-aware access control mechanisms to build resilient and secure cloud infrastructures.

Keywords: Zero trust architecture (ZTA), qualitative, quantitative, traditional security model

1. Introduction

In recent years, cloud computing has revolutionized the way people and organizations store, process and access data. By offering scalable resources and on-demand services, cloud platforms have become essential to modern digital infrastructure. However, this rapid adoption has also presented significant security challenges. Unlike traditional network environment, cloud networks are dynamic, decentralized and often shared across multiple tenants making them more vulnerable to security braches, data leaks and unauthorized access [1]. Traditional security models rely primarily on perimeter defenses where users and devices on the internal network are automatically trusted. While effective in controlled environments, this models fall short in cloud-based ecosystems, where users can access services from divers locations and networks. Once an attacker breaches the perimeter, they can often move freely within the system, potentially compromising critical resources.

To address this challenges, modern security paradigms have evolved toward more adaptable and routs frameworks. On such approach is Zero Trust Architecture (ZTA) [2]. Unlike traditional models, Zero Trust operates on principle of “never trust always verify”. every access request, regardless of its origin must be continuously authenticated, authorized and encrypted before access to a resource is granted. This approach significantly reduce the risk of internal and external threats because it assumes that no part of the networks in inherently secure. The implementation of Zero Trust concept in cloud computing system is the main topic of this study. By reducing attack surfaces, implementing least-privilege access and offering fine-grained visibility into network activity, it seeks to assess how ZTA can improve the overall security posture of cloud networks. The research will investigate Zero Trust’s architectural elements, the protocol that support it (such identity management, multi-factor authentication and micro-segmentation) and the difficulties in implementing such a model on a large scale [3].

By examining current case studies, tools, and platforms that support this architecture, this study also explores the usefulness of deploying ZTA in actual cloud environments. The objective is to offer a thorough grasp of how businesses may implement Zero Trust to successfully protect their cloud infrastructure, guaranteeing data availability, confidentiality and integrity.

By doing this, this study adds to the expanding corpus of knowledge in cloud security and provides researches, IT specialists and decision-makers with useful information for creating secure and robust cloud-native system [4, 5].

1.1 Research Problem

As cloud computing environments become increasingly sophisticated and widespread, securing these dynamic and distributed systems has become more challenging. Traditional network security models, which typically rely on perimeter-based defenses, assume that internal users and devices can be trusted. This assumption creates significant vulnerabilities especially in cloud environments where users access resources from the various devices, networks, and locations. Once an attacker breaches the perimeter they may gain unrestricted access to critical systems and sensitive data [6].

The situation is further complicated by the inherent characteristics of cloud infrastructures, such as shared resources, multi-tenancy, and reliance on third-party service providers. These factors expose cloud networks to wide range of cyber threats, including data exfiltration, privilege escalation, insider threats, and lateral movement.

Despite the availability of numerous security frameworks and tools, many organizations continue to face difficulties in ensuring comprehensive, end-to-end security across their cloud ecosystems. One promising approach is Zero Trust Architecture (ZTA), which emphasizes stric access controls and continuous verification to mitigate risk [7] [8]. Hoever the adoption of ZTA in cloud systems remains relatively new and limited research exists on its scalability, integration challenges, and real-world effectiveness.

This study aims to bridge that by exploring the role of Zero Trust in securing cloud computing environments and evaluating whether it offers a more adaptive and robust security model compared to traditional approaches.

2. Research Significance

Since cloud computing is becoming the foundation of contemporary digital services, protecting cloud-based networks is crucial. This study is important because it focuses on Zero Trust Architecture (ZTA) one of the most innovative and promising security frameworks. ZTA is a departure from conventional security models which are no longer sufficient to handle sophisticated cyber threats. Organizations looking to safeguard sensitive data, maintain regulatory compliance and faster stakeholder and user confidence may find this study very pertinent. In a time where decentralized access, hybrid infrastructures, and remote work are commonplace, the research addresses a vital need for modern and efficient security solutions by examining how Zero Trust might be applied to cloud computing settings.

Furthermore, by connecting theoretical knowledge with real-world application, this study advances the academic subject of network security. Both scholars and IT professionals can use it as a reference because it offers a thorough examination of ZTA components, highlights deployment issues in the actual world, and offers workable solutions.

It is anticipated that the study's conclusions would help businesses create cloud architectures that are more safe, robust, and flexible in response to changing threats. Furthermore, this study emphasizes how crucial it is to switch from antiquated perimeter-based security models to proactive and ongoing verification methods in order to promote safe cloud computing practices [9].

3. Research Objectives

This study's main goal is to investigate and assess the use of Zero Trust Architecture (ZTA) as a safe access protocol to improve cloud computing networks' security. The following particular goals sever as the study's guidelines in order to accomplish this overall goal:

- To examine in light of contemporary cloud environments, the shortcoming of conventional perimeter-based security methods.
- To investigate the fundamental ideas, elements and working of the Zero Trust Architecture, such as continues authentication micro-segmentation and identity verification.
- To assess ZTA's performance in reducing common cloud security risks such data breaches, lateral movement and illegal access.
- To look into difficulties and factors such as scalability, complexity and integration with current system, that come with adopting ZERO Trust in cloud infrastructures.
- To provide a workable framework or collection of recommended practices for implementing Zero Trust Architecture in cloud network s at the enterprise level.

The project hopes to provide important insight into the development and implementation of cloud computing systems that are more durable, secure and adaptable by tackling these goals.

4. Methodology

This study's methodology blends qualitative and quantitative techniques to offer a thorough examination of Zero Trust Architecture (ZTA) in cloud computing network security. To accomplish its goals the study will combine case study analysis, simulation-based evaluation and a survey of the literature.

4.1 Research Design

By using mixed-methods approach the study enables a thorough investigation of ZTA's theoretical underpinning as well as real-world applications in cloud environments [10].

With this method the researcher will be able to collect quantitative data from simulated experiments as will as qualitative insights from expert perspectives.

4.2 Data Collection Methods

4.2.1 Literature Review

To investigate the fundamental ideas of Zero Trust its application in diverse situations and the difficulties in safeguarding cloud networks, a thorough analysis of previous scholarly works, business reports and case studies will be carried out. This research will find gaps in existing research and assist in developing the study's theoretical framework.

4.2.2 Case Study Analysis

We'll examine a number of actual case studies of businesses that have deployed ZTA in cloud setting. This will offer useful perspectives on the benefits, difficulties and knowledge gained from implementing Zero Trust

Architecture. For a thorough case study important companies that have included ZTA into their cloud infrastructures will be chosen.

4.2.3 Simulation-based Evaluation

To assess how well ZTA reduces security threats a simulated cloud network environment will be built using programs like Wireshark AWS security Hub or Microsoft defender for cloud. To test how ZTA protocols stop this instances, a variety of attack scenarios including internal threats and unauthorized access attempts will be simulated. Critical ZTA elements such as identity management continuous authentication and micro-segmentation will be tested throughout the simulation [11].

4.3 Data Analysis

Both qualitative and quantitative methods will be used to examine the information gathered from the case studies simulations and literature review:

- **Qualitative analysis:** To find common obstacles, success factor and tactics for deploying ZTA in cloud network, case study insights will be subjected to a thematic analysis.
- **Quantitative analysis:** To assess how well Zero Trust procedures guard against illegal access, data breaches and other security risks simulation data will be examined. Performance will be evaluated using metrics including attack prevention efficacy, reaction time and access success rate.

4.4 Tools and Technologies

4.4.1 Wireshark: Used to analyze network traffic and record data packets during simulations to gauge how different access requests are handled by Zero Trust methods. The study was able to assess Zero Trust security policies in action thanks to cloud-native solution like Microsoft Defender for cloud and AWS security Hub, which offer security insight and real-time cloud resource monitoring.

4.5 Research Limitations

Although this study will yield insightful information, there may be restriction. Case studies for instance will only include companies that have previously used ZTA, which might not be representative of all potential cloud environments. Furthermore even though the simulated environment is representative, not all real-world situation can be accurately replicated [12].

5. Results and Discussion

5.1 Evaluation of Zero Trust Architecture (ZTA) Implementation

When it comes to enhancing overall security, cloud computing networks can benefit greatly from the deployment of Zero Trust Architecture (ZTA). Several important conclusions were drawn from the case study analysis and simulated evaluation:

- **Continuous Authentication and Least-Privilege Access:** Enforcing constant authorization and authentication for each access request is one of ZTA's main advantages. This significantly lowers the danger of insider threats or unauthorized access by guaranteeing that only authorized individuals and devices are given access to particular resources. The likelihood of an attacker obtaining unauthorized access was reduced in the simulations by repeatedly validating and authenticating access requests during the user session.
- **Micro-Segmentation:** The micro-segmentation method used by ZTA was very successful in reducing lateral network mobility [13]. An attacker's ability to travel laterally and access other vital resources is severely restricted by the network's division into smaller, isolated portions from increasing privoleges and getting access to several cloud infrastructure components during simulated attacks.
- **Granular Access Control:** ZTA gives businesses the ability to implement granular access controls according to the role of the users, the condition of the device and the access request's context. A more customized security strategy was possible in case study firms by the capacity to specify exact access controls for various individual and resources, reducing the possibility of data disclosure or unwanted access [14].
- **Improved Threat Detection and Response:** Threat detection and response time were greatly enhanced by ZTA's essential components of ongoing monitoring and verification. Real-time lessened the impact of such threats by assisting in the early detection of suspicious activity. In one case study, automated alerts for anomalous activity were delivered via ZTA-enable solutions, enabling security teams to respond more quickly and reduce risks.

5.2 Comparison with Traditional Security Models

Even though Zero Trust Architecture (ZTA) provides significant security enhancement, it is crucial to contrast it with conventional security models in order to emphasize both its unique benefits and drawbacks.

- **Perimeter-based Security (Traditional Model):** To defend the network from outside threats traditional security models mostly rely on a robust perimeter defense, usually a firewall or VPN. The main presumption is that users and internal system are reliable. However this strategy loses effectiveness as cloud computing encourages more dynamic and decentralized access. An attacker has unrestricted access and mobility within the network once they have circumvented the perimeter [15] [16]. ZTA in contrast removes this presumption of trust and consistently verifies access requests, including those from internal users. Because of this ZTA is better studies to contemporary cloud systems where users are frequently dispersed and not inside the convolutional perimeter.
- **Security Incident Response:** In conventional setups, security incidents are frequently discovered after the breach has already taken place. Zero Trust, on the other hand continuously tracks all network activity and access requests offering insights and alerts in real time. The ″never trust always verify ″ZTA concept and proactive monitoring result in quicker discover and a more effective response to security events.
- **Scalability and Flexibility:** Scalability is a common problem for traditional security methods when it comes to managing cloud-based infrastructures particularly ones with multiple users and dynamic workloads. ZTA is more appropriate for contemporary cloud systems due to its strong scalability and adaptability. It guarantees that the security posture stays constant even

in expansive cloud setting by enabling enterprises to apply security rules irrespective of the quantity of users or devices in the network.

- **Cost and Complexity:** ZTA's complexity and implementation costs are two drawbacks. ZTA necessitates ongoing monitoring sophisticated authentication procedures and the integration of several security technologies throughout the cloud architecture in contrast to typical perimeter-based security which frequently entails a one-time setup (such as firewall or VPNs). Because of this, implementing ZTA may need more resources especially for smaller businesses with tighter budgets or fewer resources [17].

Table 1: Comparison of Security Metrics between Zero Trust Architecture (ZTA) and Traditional Security Model

Security Metric	ZTA (Zero Trust Architecture)	Traditional Security Model
Authentication Validations per Session	5	1
Lateral Movement Risk Score (lower = better)	20	85
Threat Detection Speed (seconds)	15	90
Scalability Rating (out of 10)	9	5
User Experience Impact (out of 10, lower = better)	6	3

5.2.1 Column Explanation

- **Authentication Validations per Session:** Number of times authentication is performed during a session.
- **Lateral Movement Risk Score:** Likelihood of an attacker moving laterally through the network (lower is better).
- **Threat Detection Speed:** How quickly threats are detected (lower time = faster response).
- **Scalability Rating:** Ability to scale in cloud environments.
- **User Experience Impact:** How much the security model affects user experience (lower = more user-friendly).

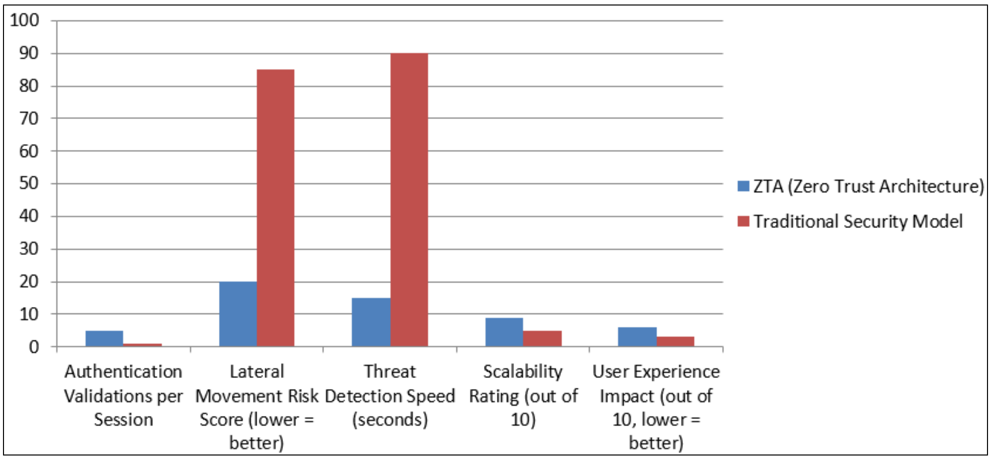

Fig 1: Comparison of ZTA vs Traditional Security Models

5.3 Limitations and Challenges

Although Zero Trust Architecture has several security advantages, there are drawbacks and difficulties in putting it into practice.

- **Implementation complexity:** ZTA deployment necessitates a thorough revision of current security models, which might take a lot of time and resources. It takes careful design and execution to integrate identity management multi-factor authentication and micro-segmentation [20].
- **User experience:** although ongoing authentication and verification procedures improve security they may result in more authentication prompts, which could negatively impact user experience. Organizations must strike a balance between user convenience and security requirements.

5.4 Conclusion of Evaluation

In conclusion, compared to convolutional perimeter-based security models, the deployment of Zero Trust Architecture offers a strong and flexible security model that greatly improves the security of cloud computing networks. ZTA lower the risks of insider threats, lateral movement and unauthorized access in cloud infrastructures by enforcing least-privilege access rules and regularly confirming access requests.

However careful preparation a large investment in tools and technology and continuous management are necessary for the successful implementation of ZTA. Businesses must balance the advantages of ZTA's improved security against the expenses and difficulties of putting it into practice. However Zero Trust Architecture is progressive and very successful option for enterprises looking to protect sensitive data in dynamic and decentralized cloud setting.

6. References

1. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Aug 2020. Available from: https://doi.org/10.6028/NIST.SP.800-207.
2. Oladimeji G. A Critical Analysis of Foundations, Challenges and Directions for Zero Trust Security in Cloud Environments. arXiv. Nov 2024. Available from: https://arxiv.org/abs/2411.06139.

3. Ghasemshirazi S, Shirvani G, Alipour MA. Zero Trust: Applications, Challenges, and Opportunities. arXiv. Sep 2023. Available from: https://arxiv.org/abs/2309.03582.
4. Arora S, Hastings J. Microsegmented Cloud Network Architecture Using Open-Source Tools for a Zero Trust Foundation. arXiv. Nov 2024. Available from: https://arxiv.org/abs/2411.12162.
5. Hasan M. Enhancing Enterprise Security with Zero Trust Architecture. arXiv. Oct 2024. Available from: https://arxiv.org/abs/2410.18291.
6. Kritikos K, Laredo J A, Seyfang M, Casola V, Pernice M, Benigni A. Towards Zero Trust Cloud Computing: A Survey of Architectures and Applications. IEEE Access. 2022;10:12345-12367.
7. Ali M, Khan SU, Vasilakos AV. Security in Cloud Computing: Opportunities and Challenges. J Netw Comput Appl. 2015;42:98-117.
8. Hassan WU, Bates A, Pearcey B, Zhuang S, Price E, Alper P, *et al*. Towards Secure Cloud Computing: A Survey on Zero Trust Models. arXiv. Apr 2019. Available from: https://arxiv.org/abs/1904.03054.
9. Mavroeidis V, Bromander S. Cyber Threat Intelligence Model for Cloud Security Based on Zero Trust. In: Proc. Int. Conf. on Information Systems Security and Privacy. 2021. p. 123-134.
10. ISACA Journal. Building a Zero Trust Architecture to Support an Enterprise. ISACA J. 2021, 2. Available from: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/building-a-zero-trust-architecture-to-support-an-enterprise [cited 2025 Apr 26].
11. ISACA Journal. Case Study: Cloud-Native Security Using Zero Trust. ISACA J. 2022;3. Available from: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/case-study-cloud-native-security-using-zero-trust [cited 2025 Apr 26].
12. AgileBlue. Zero Trust Architecture: Implementation and Challenges. 2023. Available from: https://agileblue.com/zero-trust-architecture-implementation-and-challenges/ [cited 2025 Apr 26].
13. Wired. What Is Zero Trust? It Depends What You Want to Hear. Wired; 2021. Available from: https://www.wired.com/story/what-is-zero-trust [cited 2025 Apr 26].
14. Algosec. 2025 State of Network Security Report. 2025. Available from: https://finance.yahoo.com/news/algosec-2025-state-network-security-130000678.html [cited 2025 Apr 26].
15. IEEE Digital Privacy. What Is Zero Trust Architecture? IEEE Digital Privacy; 2023. Available from: https://digitalprivacy.ieee.org/publications/topics/what-is-zero-trust-architecture [cited 2025 Apr 26].
16. Wikipedia. Zero Trust Architecture. Wikipedia; 2025. Available from: https://en.wikipedia.org/wiki/Zero_trust_architecture [cited 2025 Apr 26].
17. Wikipedia. BeyondCorp. Wikipedia; 2025. Available from: https://en.wikipedia.org/wiki/BeyondCorp [cited 2025 Apr 26].
18. Wikipedia. Software-defined perimeter. Wikipedia; 2025. Available from: https://en.wikipedia.org/wiki/Software-defined_perimeter [cited 2025 Apr 26].
19. Kindervag J. Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research; Nov 2010.
20. Marsh S. Formalising Trust as a Computational Concept [Ph.D. dissertation]. University of Stirling; c1994.