International Journal Software Engineering and Computer Science (IJSECS)
5 (3), 2025, 1126-1132
Published Online December 2025 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v5i3.5481.

RESEARCH ARTICLE Open Access

Integrating Zero Trust Architecture with Blockchain Technology to Maintain Data Security in the Cloud

T. Irfan Fajri *
Universitas Islam Kebangsaan Indonesia, Bireuen Regency, Aceh Province, Indonesia.
Corresponding Email: teukuirfanfajri.sister@gmail.com.

Handry Eldo
Universitas Muhammadiyah Mahakarya Aceh, Bireuen Regency, Aceh Province, Indonesia.

Cut Susan Octiva
Universitas Amir Hamzah, Deli Serdang Regency, North Sumatra Province, Indonesia.

Dikky Suryadi
Institut Sains Teknologi Nasional, South Jakarta City, Special Capital Region of Jakarta, Indonesia.

Muhammad Lukman Hakim
Universitas Muhammadiyah Asahan, Asahan Regency, North Sumatra Province, Indonesia.

Received: September 2, 2025; Accepted: November 10, 2025; Published: December 1, 2025.

Abstract: Data security concerns have increasingly become a challenge to cloud computing services due to rising incidents of cyberattacks, identity theft, and data manipulation. The perimeter-based security model is ineffective because of vulnerabilities in authentication and access control, thus necessitating an adaptive layered approach. This paper presents attempts to merge Zero Trust Architecture (ZTA) with Blockchain technology as one possible way to ensure confidentiality, integrity, and availability of data in cloud environments. Research methodology comprises a detailed review of related literature, system architecture analysis, and simulation of the conceptual merger using encryption protocols and smart contracts. Results revealed that ZTA significantly reduces the opportunities for unauthorized access through multi-layered verification and least privilege principles while Blockchain provides a decentralized transparent immutable method for recording transactions on data. The hybrid will enhance security substantially against breaches from external attackers and insiders with an already established verifiable audit trail. This paper concludes that such a merger could create a stronger model—one that is more measurable—and sustainable for securing today's cloud infrastructure.

Keywords: Zero Trust Architecture; Blockchain; Cloud Security; Insider Threats; Data Integrity.

1. Introduction

The quick development of information technology has put cloud computing at the front line of modern data management. Cloud computing provides a scalable, flexible, and cost-effective way to store, process, and share digital information. These features have made it a key player in government, healthcare, education, and finance—industries that deal with large amounts of sensitive data every day. The use of cloud services is increasing as more businesses want to take advantage of a more agile and accessible IT infrastructure. However, even with all its advantages, cloud computing brings major problems for data security. This is still one of the biggest issues for organizations moving to cloud environments. Data breaches, identity thefts, and advanced cyberattacks have raised warnings about the weaknesses in traditional perimeter-based security models. These models are designed to protect the outer edges of a network from outside threats but do not cover increasingly common internal threats and unauthorized access from within. Sensitive data is often spread across many places; internal risks like stolen credentials, bad insiders, and poorly managed access controls become bigger threats in cloud settings. This change in cybersecurity risks has led to reviewing traditional models; it shows that new and stronger frameworks are needed to keep data safe in the cloud [1].

To address these growing security issues effectively, Zero Trust Architecture (ZTA) has surfaced as an applicable model. Unlike traditional architectures that depend on perimeter defenses, ZTA is guided by a core tenet: "never trust, always verify." This means no user or device or application—inside or outside the network—should be trusted by default. All access requests must be authenticated rigorously and authorized with multi-layered validation before being granted access. The architecture ensures that every request is validated based on the least privilege principle; only giving individuals or systems access to specific data they need for their work tasks minimizes risks associated with unauthorized access significantly. It enhances protection against all forms of cyberattacks including those from inside the organization [2]. The ZTA model's adoption has been effective in reducing the probability of data breaches and adding an extra layer of security to cloud environments [3].

Simultaneously, the technology of the blockchain has become an innovative instrument for protecting information and guaranteeing openness in online dealings. Blockchain functions as a distributed record that documents actions over a shared network of machines. Every action is secured through cryptography, making sure that data integrity is kept and preventing any changes. Also, the consensus rules of the blockchain allow transactions to be verified independently, offering a level of accountability and transparency that traditional databases cannot match [4]. These features make the blockchain an ideal partner to ZTA since it offers a secure way for recording and checking data access, making sure only allowed users get access while keeping a permanent unchangeable record of all actions. The use of smart contracts on the blockchain also increases security by automatically running security rules like access controls and policy enforcement which can be changed in real time against new threats [5].

The merger of Zero Trust Architecture with blockchain technology makes an extremely strong security setup for cloud services. By combining ZTA's strict access controls with blockchain's clear and unchangeable transaction records, organizations can reach a better level of safety and responsibility. This combined answer does not just deal with outside attacks—like those using stolen credentials or phishing—but also internal dangers such as insider collusion or data changing. In addition, the unchangeable audit trail given by blockchain lets organizations see data access and check security events after an incident increasing their ability to find and react to threats. This method offers complete protection architecture that is flexible and strong against changing cyber threats [6].This study looks into how Zero Trust Architecture can be combined with blockchain technology to strengthen the security of cloud computing services. It will analyze the integration between these two technologies to come up with practical solutions for cloud service providers and companies on how they can secure their digital assets better. The research aims at not just improving security but also providing actionable insights that organizations could use to maneuver through modern cybersecurity complexities 0[8]. As more people use clouds, knowing and applying mixed security plans like ZTA and blockchain will be key in keeping safe important data and making sure cloud places are correct and trustful.

2. Related Work

Cloud computing has become a major player in how we access, store, and manage data. Its flexibility, scalability, and cost-effectiveness make it an important asset for industries like government, healthcare, education, and finance. But with more organizations moving to the cloud, they are running into big problems when it comes to keeping their data safe [9][10]. Data leaks, threats from insiders, and denial-of-service (DoS) attacks are just some of the dangers that cloud services need to deal with. Old security models based on perimeter defense don't work in cloud environments anymore because they assume threats only come from outside the organization while internal threats like data manipulation and unauthorized access are becoming

more common [12]. To tackle these issues one can use Zero Trust Architecture (ZTA), which was first introduced by Forrester Research and has been further developed by various cybersecurity experts. ZTA is based on the principle of "never trust anyone"—no user or device should be trusted by default whether inside or outside the network perimeter. Every request for access should be verified through authentication, authorization, and validation before any data sharing takes place. This is in line with the least privilege principle where users and devices only get access to what they absolutely need [2]. Studies have indicated that implementing ZTA can significantly lower the number of unauthorized access incidents; some reports indicate a reduction of up to 60% in such occurrences within cloud-based systems [11]. ZTA incorporates continuous identity verification to create a dynamic proactive defense against various cyber threats.

Blockchain technology adds another layer of security through its decentralized ledger system. The cryptographic nature of Blockchain ensures that every transaction is secure and cannot be changed once recorded. Each block in the chain contains information about all transactions that have taken place up until that point; this makes it very hard for anyone else to alter anything without consent from everyone involved making it an extremely reliable method for storing data securely as well as checking its accuracy later on down the line. The features offered by Blockchain—decentralization, transparency, immutability—are very useful when it comes to solving real-world problems related to security in cloud environments. Blockchain can improve both data integrity and transparency while also providing a complete verifiable audit trail [1]. Furthermore, smart contracts used within blockchain ecosystems can automate security policies as well as enforce access control mechanisms which will further enhance cloud data security [4].

Recent studies have looked into the possibility of combining ZTA with Blockchain to form a more solid security structure for cloud settings. This merger takes advantage of the strong points from each tech: ZTA offers strict control over access, while Blockchain provides clear and permanent records of transactions. Bringing these two technologies together improves how users are verified and allowed in, plus it also gives a safe way to record all data accesses and changes without tampering. Moreover, smart contracts in Blockchain networks can automate access controls based on the ZTA framework, making sure that only those who are allowed can get into sensitive information [9]. This mix of technologies has been proven to enhance multi-layered authentication processes while also delivering a transparent and verifiable audit trail for cloud-based systems [14]. The integration of ZTA and Blockchain offers an all-encompassing security answer that tackles both internal and external risks within cloud computing settings. Although external threats such as stolen credentials or malware attacks may be countered by ZTA's stringent access controls, Blockchain guarantees the integrity and transparency of data transactions. These technologies together offer a more dynamic and adaptable security model that can better resist the changing nature of cyber threats [6]. Merging these two strategies develops a more robust security structure, one that can keep data secret and make sure there is responsibility in the cloud. As companies keep using cloud computing, it is very important to think about these integrated answers to shield sensitive data from increasing cyber risks better 0[13].

3. Research Method

This study adopts a qualitative-descriptive approach, supported by conceptual analysis and system simulation [15]. The primary objective is to design, analyze, and evaluate the integration of Zero Trust Architecture (ZTA) with Blockchain technology for improving data security in cloud computing environments. The methodology is structured into several stages, each addressing key components of the research.

3.1 Literature Review

The first stage involves a comprehensive literature review, which aims to explore previous research, international standards, and industry reports related to data security, ZTA, and Blockchain technology. This review draws from a variety of sources, including publications from standards organizations such as NIST, scientific journal articles, and white papers published by cloud service providers. The goal of this phase is to identify key challenges in cloud data security and evaluate the potential and limitations of ZTA and Blockchain when applied independently.

3.2 Needs and Issues Analysis

The next phase focuses on conducting a needs analysis, which covers essential areas such as authentication, authorization, access control, auditing, and data integrity. This analysis maps potential threats (threat modeling) to cloud infrastructure, including data breaches, insider threats, replay attacks, and data manipulation. Based on the results of this analysis, relevant security scenarios are created to assess the effectiveness of integrating ZTA and Blockchain technologies. To measure the security needs and issues in cloud services, a quantitative approach is employed, using Risk Scoring and the Security Effectiveness Index (SEI). The calculations in this stage are carried out as follows:

1) Identification of Assets and Threats
Assets (A) are defined as sensitive data, user identities, access credentials, and transaction logs. Threats (T) include data breaches, insider threats, data manipulation, unauthorized access, and replay attacks.

2) Risk Assessment
Each identified threat is evaluated based on two primary parameters:
Likelihood (L): The probability of the threat occurring, rated on a scale of 1–5.
Impact (I): The severity of the threat's impact on the system, also rated on a scale of 1–5.

The risk score (RS) is calculated using the following formula:

$$\text{Risk Score (RS)} = L \times I$$

The resulting risk score is categorized as follows:
RS 1–5 = Low risk
RS 6–12 = Moderate risk
RS 13–25 = High risk

3) Determining the Level of System Vulnerability
Vulnerability (V) is calculated based on the number of weaknesses identified in areas such as authentication, authorization, encryption, and audit logging. The formula for calculating the vulnerability percentage is:

$$V = \left(\frac{\text{Number of weaknesses identified}}{\text{Total aspects tested}} \right) \times 100$$

3.3 Integration Architecture Design

The third stage focuses on designing the integration architecture for ZTA and Blockchain. In this phase, ZTA is implemented using principles such as least privilege, multi-factor authentication, and network micro-segmentation. Blockchain is integrated as an additional layer for securely recording data transactions and implementing smart contracts. A conceptual model of the architecture is developed, which is illustrated in a diagram that describes the authentication flow, data recording, and validation mechanisms.

3.4 Conceptual Simulation Implementation

The final stage involves testing the proposed architecture through a conceptual simulation. The simulation utilizes cloud-based simulation software and a Blockchain framework to evaluate the integration. The simulation includes the following processes:

1) User authentication procedures.
2) Storage of transaction logs on the Blockchain.
3) Application of smart contracts for automatic access control.

The aim of this simulation is to assess the effectiveness of the integrated system in improving data security compared to traditional security approaches in cloud environments (Nguyen et al., 2020) [7]; (Sultana et al., 2020) [13].

4. Result and Discussion

4.1 Results

A risk assessment was conducted on cloud-based data security systems, identifying several key threats as the study's focus: data breaches, insider threats, data manipulation, and unauthorized access. Each threat was evaluated based on likelihood and impact using a 1–5 scale. Table 1 summarizes the findings.

Table 1. Data Security Risk Analysis Results in Cloud Environment

Types of Threats	Likelihood (L)	Impact (I)	Risk Score (RS)	Risk Category
Data Breach	5	5	25	High Risk
Insider Threat	4	5	20	High Risk
Data Manipulation	3	4	12	Moderate Risk
Unauthorized Access	4	4	16	High Risk
Replay Attack	3	3	9	Moderate Risk

System vulnerability was measured by identifying weaknesses across authentication, authorization, encryption, and audit logging. Out of 6 tested aspects, 3 weaknesses were found, resulting in a vulnerability level calculated as follows:

$$V = \frac{3}{6} \times 100\% = 50\%$$

The Security Effectiveness Index (SEI) was calculated using four parameters: Confidentiality (C), Integrity (I), Availability (A), and Auditability (Au). Table 2 shows the scores obtained for each parameter.

Table 2. SEI Calculation Results

Parameters	Score (0–100)
Confidentiality	85
Integrity	90
Availability	80
Auditability	75

$$SEI = \frac{85 + 90 + 80 + 75}{4} = 82.5$$

Figure 1 displays the security effectiveness values across four main parameters. Integrity scored highest at 90, followed by Confidentiality at 85, Availability at 80, and Auditability at 75. The average SEI value reached 82.5.

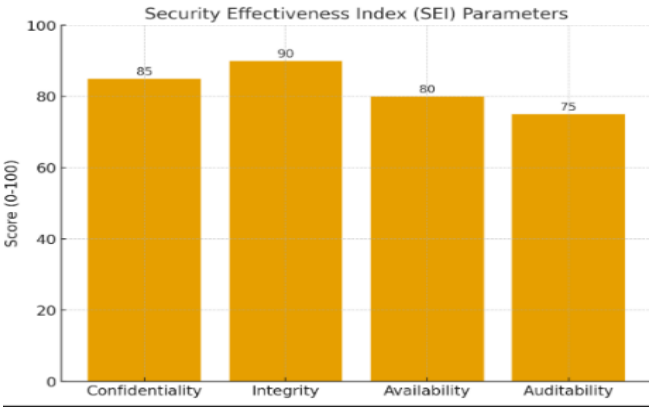

Figure 1. Security Effectiveness Index (SEI)

4.2 Discussion

Data breach emerged as the most critical threat with an RS value of 25, followed by insider threat (RS=20) and unauthorized access (RS=16). These findings align with current global cyberattack patterns, where data leaks and credential abuse by internal actors remain the primary causes of security incidents. The 50% vulnerability score reveals that the system still carries notable security gaps, particularly in opaque audit logging and static access controls that require immediate attention. An SEI score of 82.5 indicates reasonable effectiveness, surpassing the standard threshold of 80%. However, auditability only scored 75, pointing to a clear need for stronger logging mechanisms that are both transparent and tamper-resistant. Among all four parameters measured, auditability stands out as the weakest area that demands priority improvement.

Integrating Zero Trust Architecture (ZTA) with Blockchain offers promising improvements for cloud data security. ZTA addresses unauthorized access and insider threats through multi-factor authentication, least privilege principles, and micro-segmentation—all of which directly target the high-risk threats identified in the risk assessment. Meanwhile, Blockchain technology strengthens integrity and auditability by recording transactions in an immutable and transparent manner. Smart contracts enable automated access control based on predefined security policies, helping reduce data manipulation and replay attack risks. The most notable improvement appears in auditability, where transaction records that cannot be altered make it easier to detect anomalies and prevent malicious insider activities. When ZTA and Blockchain work together, they create a security architecture far more robust than either approach alone. While the current SEI already exceeds the 80% benchmark, adding Blockchain is expected to push auditability scores closer to 90, making the system more transparent and significantly more resistant to both insider threats and data manipulation attempts.

5. Conclusion

The integration of Zero Trust Architecture (ZTA) with Blockchain technology offers a robust approach to strengthening data security in cloud computing services. Risk analysis revealed that data breaches, insider threats, and unauthorized access pose the highest risk levels among all identified threats. The Security Effectiveness Index (SEI) evaluation produced an average score of 82.5, with auditability identified as the weakest area requiring improvement. ZTA implementation has proven effective in strengthening authentication, authorization, and access control mechanisms through the least privilege principle, which directly reduces unauthorized access risks. Blockchain technology, on the other hand, enhances transparency, integrity, and immutability of transaction records through distributed ledger systems and smart contracts. Combining both technologies addresses the individual limitations of each approach while delivering notable improvements in auditability—previously the system's most vulnerable aspect. Based on these findings, the integration of ZTA with Blockchain serves as an adaptive, transparent, and sustainable security architecture model for maintaining data confidentiality, integrity, availability, and accountability in cloud computing environments. The outcomes hold relevance not only for academic discourse but also carry practical implications for cloud service providers and organizations that depend on digital data management systems.

References

[1] Alevizos, L., Ta, V. T., & Eiza, M. H. (2022). Blockchain-enabled intrusion detection and prevention system of APTs within zero trust architecture. *IEEE Access*, *10*, 89270–89288. https://doi.org/10.1109/ACCESS.2022.3200165

[2] Singh, B., & Kaunert, C. (2025). Zero-trust evolution and cloud computing security as multi-mission engineering: Addressing emerging threats, regulations, and modeling solutions via enhancing blockchain consensus algorithm to mitigate data repository breaches. In *Zero-Trust Learning* (pp. 357–385). https://doi.org/10.1201/9781779643575-17

[3] 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

[4] Pooja, S., & Chandrakala, C. B. (2024). Secure reviewing and data sharing in scientific collaboration: Leveraging blockchain and zero trust architecture. *IEEE Access*, *12*, 92386–92399. https://doi.org/10.1109/ACCESS.2024.3423338

[5] Zhang, W., & Chen, L. (2025). Developing a zero-trust security model for cloud migration: Ensuring data integrity and confidentiality in hybrid cloud architectures. *Advances in Theoretical Computation, Algorithmic Foundations, and Emerging Paradigms*, *15*(2), 15–27. https://heilarchive.com/index.php/ATCAEP/article/view/2025-Feb-07

[6] Chen, Z., Yan, L., Lü, Z., Zhang, Y., Guo, Y., Liu, W., & Xuan, J. (2021). Research on zero-trust security protection technology of power IoT based on blockchain. *Journal of Physics: Conference Series*, *1769*(1), 012039. https://doi.org/10.1088/1742-6596/1769/1/012039

[7] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Communications Surveys and Tutorials*, *22*(4), 2521–2549. https://doi.org/10.1109/COMST.2020.3020092

[8] Alevizos, L., Eiza, M. H., Ta, V. T., Shi, Q., & Read, J. (2022). Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Security and Privacy*, *5*(1), e191. https://doi.org/10.1002/SPY2.191

[9] Dhar, S., & Bose, I. (2021). Securing IoT devices using zero trust and blockchain. *Journal of Organizational Computing and Electronic Commerce*, *31*(1), 18–34. https://doi.org/10.1080/10919392.2020.1831870

[10] Potluri, S. (2024). A zero trust-based identity and access management framework for cross-cloud federated networks. *International Journal of Emerging Research in Engineering and Technology*, *5*(2), 28–40. https://doi.org/10.63282/3050-922X.IJERET-V5I2P104

[11] Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. *IEEE Access*, *9*, 69513–69526. https://doi.org/10.1109/ACCESS.2021.3077123

[12] Salim, M. M., Kim, M., Singh, S. K., & Park, J. H. (2026). Zero-trust blockchain-enabled framework for scalable and secure IoT networks. *Future Generation Computer Systems*, *175*, 108093. https://doi.org/10.1016/J.FUTURE.2025.108093

[13] Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, *20*(1), 1–10. https://doi.org/10.1186/S12911-020-01275-Y

[14] Uzoma, E., Enyejo, J. O., & Motilola Olola, T. (2025). A comprehensive review of multi-cloud distributed ledger integration for enhancing data integrity and transactional security. *International Journal of Innovative Science and Research Technology*, 1953–1970. https://doi.org/10.38124/IJISRT/25MAR1970

[15] Chaudhry, U. B., & Hydros, A. K. M. (2023). Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. *IET Blockchain*, *3*(2), 98–115. https://doi.org/10.1049/BLC2.12028