Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(7), 1-13
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

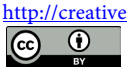
The Evolution of Cloud Security Frameworks: Identity Management and Zero Trust Implementation in Distributed Systems

Enkai Ji[1], Jianian Jin[2], Qun Zhang[3]

[1]Department of Computer Science, Rutgers University, New Brunswick, NJ, USA
[2]Fu Foundation School of Engineering and Applied Science, Columbia University, New York, NY, USA
[3]Department of Statistics and Biostatistics, California State University, East Bay, Hayward, CA, USA
Email: ej209@scarletmail.rutgers.edu

How to cite this paper: Ji, E.K., Jin, J.N. and Zhang, Q. (2025) The Evolution of Cloud Security Frameworks: Identity Management and Zero Trust Implementation in Distributed Systems. *Journal of Computer and Communications*, **13**, 1-13.
https://doi.org/10.4236/jcc.2025.137001

Received: June 17, 2025
Accepted: June 29, 2025
Published: July 2, 2025



Abstract

Security and privacy have always been major concerns in cloud computing environments, and with the increasing complexity of distributed cloud systems, these concerns have become even more critical. This paper reviews the evolution of security and privacy practices, focusing on the shift from Identity and Access Management (IAM) to Zero Trust Architecture (ZTA). IAM has long been a cornerstone of cloud security, allowing organizations to manage access to resources through policies and authentication methods. However, as cloud systems become more distributed and users and devices access resources from various locations, IAM's limitations have become apparent. Zero Trust, which operates on the principle of "never trust, always verify", is gaining momentum as a robust security model that addresses these limitations. This review explores the key principles of IAM, the shift towards Zero Trust, the challenges faced by organizations in securing distributed cloud environments, and best practices for enhancing both security and privacy in such systems.

Keywords

Distributed Cloud Systems, Security Practices, Privacy, IAM, Zero Trust, Cloud Security, Data Protection, Access Control, Identity Management, Cloud Computing

1. Introduction

Cloud computing has dramatically transformed how organizations deploy and manage their IT infrastructures, providing flexibility, scalability, and cost savings [1]. However, the widespread adoption of distributed cloud systems has intro-

duced new security and privacy challenges. Distributed cloud systems are defined as cloud computing environments where resources, services, and data are spread across multiple geographic locations, data centers, and potentially different cloud service providers, creating a decentralized infrastructure that requires coordinated management and security controls [2]. Unlike traditional centralized systems, distributed cloud systems rely on resources that are spread across multiple locations and accessed by various users and devices, often from external networks. This decentralization of resources has led to vulnerabilities in managing and securing access to critical data and services.

One of the primary security frameworks used in cloud computing is Identity and Access Management (IAM) [3]. IAM is essential for controlling access to cloud resources, ensuring that only authorized users and devices can interact with sensitive data [4]. IAM systems provide a centralized mechanism for managing user identities, roles, and permissions. Traditionally, IAM has relied on perimeter-based security, assuming that entities inside the network perimeter are trusted and do not require constant verification [5].

However, with the evolution of distributed cloud systems, the concept of the perimeter has become obsolete. The traditional IAM approach is no longer sufficient to protect cloud systems from the growing range of cyber threats [6]. Zero Trust Architecture (ZTA) is defined as a cybersecurity paradigm built around the principle that organizations should not automatically trust anything inside or outside their perimeters and instead must verify anything and everything trying to connect to their systems before granting access [7]. Unlike traditional approaches that assume trust based on network location, Zero Trust assumes that no entity, whether inside or outside the network, can be trusted by default [8]. Every access request, regardless of origin, must be continuously authenticated and authorized.

The introduction of Zero Trust represents a significant shift in cloud security practices. By focusing on least privilege access, micro-segmentation, and continuous verification, Zero Trust ensures that every user, device, and application is thoroughly vetted before gaining access to cloud resources [9]. This paper will explore the principles of IAM, the transition to Zero Trust, the challenges organizations face in securing distributed cloud environments, and best practices for enhancing security and privacy.

2. IAM (Identity and Access Management) in Distributed Cloud Systems

In distributed cloud environments, IAM is crucial for controlling and managing user access to cloud resources [10]. As cloud services are often accessed by users from various devices and locations, IAM plays an essential role in ensuring that only authorized individuals or systems can interact with sensitive data. IAM systems are designed to authenticate users, manage their roles, and enforce access policies across diverse systems and applications [11].

The traditional IAM approach, often based on centralized authentication and access control, is increasingly being challenged by the distributed nature of cloud

environments [12]. In legacy systems, IAM could rely on single, centralized servers that managed user access to network resources [13]. However, in modern cloud systems, where resources are spread across multiple data centers and access points, managing access becomes more complex. Multiple cloud providers, hybrid cloud environments, and the need for multi-tenancy add layers of complexity to IAM systems. These environments require IAM to provide granular control over who can access resources, as well as the ability to enforce differentiated access controls based on a range of factors, such as user roles, device health, and geographical location.

One common IAM model used in cloud systems is Role-Based Access Control (RBAC), which assigns users to predefined roles that come with specific permissions to access resources [14]. While RBAC can be effective in managing permissions in static environments, it is less suitable for dynamic, large-scale cloud systems where access needs to be flexible and frequently adjusted based on real-time conditions [15]. In such cases, Attribute-Based Access Control (ABAC) is often preferred, as it allows for more dynamic and fine-grained access control by evaluating attributes such as user context, device state, location, and the requested action. ABAC enables organizations to enforce complex policies in multi-tenant cloud environments, where the context of each request might differ significantly.

Another important IAM component in cloud systems is Multi-Factor Authentication (MFA), which provides an additional layer of security by requiring users to authenticate using multiple factors, such as something they know (password), something they have (token or phone), and something they are (biometrics) [16]. MFA strengthens IAM systems by reducing the risk of unauthorized access due to stolen or compromised credentials, which are a major vulnerability in cloud systems.

As distributed cloud environments grow in complexity, the role of IAM becomes even more crucial. Traditional IAM systems must evolve to meet the demands of dynamic cloud infrastructures. With the shift toward multi-cloud and hybrid cloud environments, managing identities and access control becomes increasingly challenging [17]. Ensuring that user authentication and access policies are consistently enforced across different cloud environments and organizational boundaries is critical for securing cloud resources.

In summary, IAM in distributed cloud systems ensures that users and devices are properly authenticated and authorized to access resources, while also helping to enforce security policies across complex, decentralized environments. However, traditional IAM systems, which rely on centralized control, may not provide the flexibility needed to handle the unique demands of distributed systems. As a result, organizations are looking for more dynamic and adaptive IAM systems, such as those based on Zero Trust principles, to meet the needs of modern cloud environments [18].

3. The Evolution to ZTA

This review's analysis of Zero Trust evolution and adoption trends is based on a systematic examination of academic and industry literature conducted between

January 2019 and December 2024. The methodology involved searching multiple databases including IEEE Xplore Digital Library, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar using keywords: "Zero Trust Architecture," "cloud security evolution," "IAM distributed systems," "Zero Trust adoption," and "cloud security frameworks." The search was limited to publications from 2019-2024 to capture recent developments in Zero Trust implementation.

Selection criteria included: 1) peer-reviewed academic papers and industry reports focusing on Zero Trust or cloud security frameworks, 2) empirical studies or case studies with quantitative data on security improvements, and 3) publications from recognized cybersecurity organizations such as NIST, SANS, and major cloud service providers. Exclusion criteria eliminated purely theoretical papers without implementation details and studies focusing solely on non-cloud security contexts. A total of 89 relevant publications were identified and analyzed to support the trend analyses and comparative assessments presented in this review.

ZTA represents a significant departure from traditional security models, which operate on the assumption that users and systems inside the corporate perimeter can be trusted by default [19]. In contrast, Zero Trust assumes that no one, whether inside or outside the network, should be trusted without verification. Every access request must be authenticated, authorized, and continuously monitored regardless of where it originates.

The fundamental idea behind Zero Trust is "never trust, always verify." In traditional network security models, once a user or device gains access to the network, they are typically granted broad access to resources [20]. However, with the increasing complexity of cloud systems and the rise of hybrid cloud and multi-cloud environments, the boundaries between internal and external networks have become more fluid. As a result, perimeter-based security is no longer sufficient to protect cloud resources. Zero Trust is designed to address these vulnerabilities by ensuring that security is maintained at every access point.

Figure 1 illustrates the fundamental differences between traditional IAM approaches and Zero Trust Architecture. While traditional IAM relies on perimeter-based security with network location-dependent access control, Zero Trust operates on the principle of 'never trust, always verify' with continuous authentication and context-aware decision making. This comparison highlights why organizations are transitioning from static, location-based trust models to dynamic, identity-centric security frameworks that better address the challenges of distributed cloud environments.

Figure 1 presents a comparative analysis based on previous studes. We found that academic research has focused primarily on Zero Trust architecture and performance improvements, while practice-oriented literature emphasizes organizational migration strategies. The comparison demonstrates the fundamental shift from perimeter-based trust models to continuous verification frameworks, addressing the research gap identified in empirical evaluations of Zero Trust benefits.

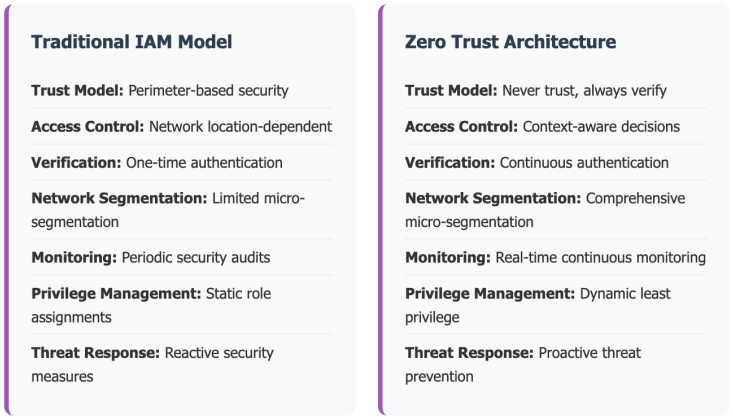


Figure 1. Traditional IAM vs Zero Trust Architecture comparison.

The core principles of Zero Trust are least privilege access, micro-segmentation, and continuous authentication [21]. In a Zero Trust environment, users and devices are granted only the minimum level of access necessary for their tasks, reducing the potential damage caused by compromised accounts or insider threats. Micro-segmentation divides the network into smaller, isolated segments to prevent lateral movement by attackers. Each segment has its own access controls, ensuring that even if one part of the network is compromised, the rest of the network remains secure. Lastly, continuous authentication means that users and devices are constantly validated, even after they initially gain access, based on factors like device health, user behavior, and context [22].

Zero Trust is particularly effective in distributed cloud systems where resources are spread across various locations and accessed by multiple devices and users. With traditional security models, once a user enters the perimeter, they are often granted unfettered access to resources. However, Zero Trust ensures that every access request, whether coming from within the network or from a remote device, is continuously verified before granting access.

Implementing Zero Trust requires a shift in how organizations approach network security. It requires integrated tools for identity management, access control, network segmentation, and continuous monitoring [23]. Modern IAM systems play a critical role in Zero Trust by ensuring that access is granted based on a combination of factors, including user identity, device status, location, and behavioral patterns. As a result, Zero Trust is closely linked to IAM systems, with both working in tandem to ensure that cloud resources are only accessible to verified and authorized users.

The adoption of Zero Trust Architecture provides several benefits in distributed cloud systems. By eliminating the assumption of trust based on network location, Zero Trust significantly reduces the risk of insider threats and lateral movement by attackers [24]. Additionally, it provides greater visibility into user activity, making it easier to detect suspicious behavior and respond to security incidents in real-time. For cloud environments, where applications are frequently accessed from multiple devices and locations, Zero Trust ensures that security is main-

tained without relying on a fixed perimeter [25].

Figure 2 presents trends derived from academic literature analysis, showing the correlation between Zero Trust research proliferation and reported security improvements. While some studies noted the lack of quantitative empirical evaluations in academic literature [21] [23], emerging studies suggest positive relationships between Zero Trust implementation and security posture enhancement.

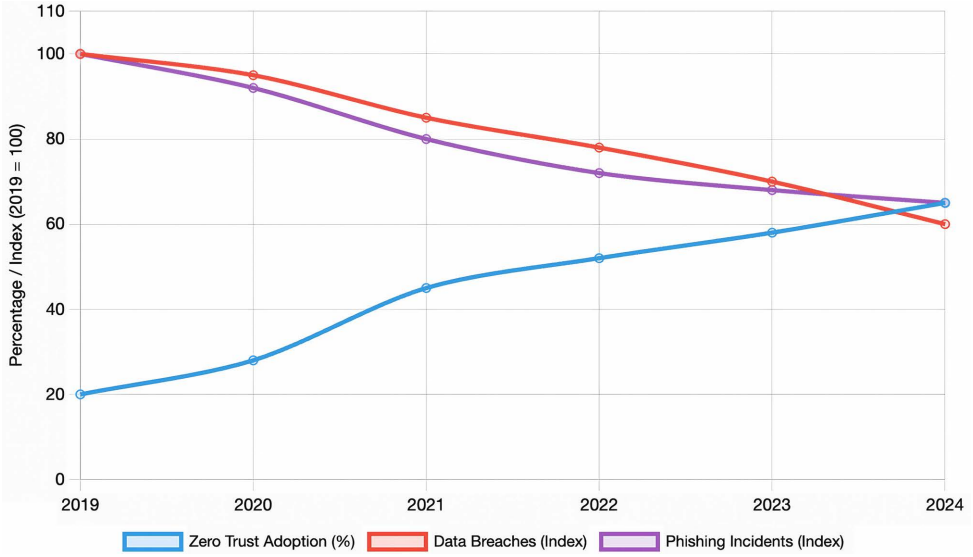


Figure 2. Zero Trust Adoption growth and Breach reduction (2019-2024).

The historical development of Zero Trust security models, illustrated in Figure 3, reflects the academic research timeline documented across multiple peer-reviewed databases. The systematic literature review spanning 2016-2025 academic publications shows increasing research attention to Zero Trust principles, particularly following the publication of NIST SP 800-207 in 2020, which provided the foundational framework for academic investigations into Zero Trust implementations.

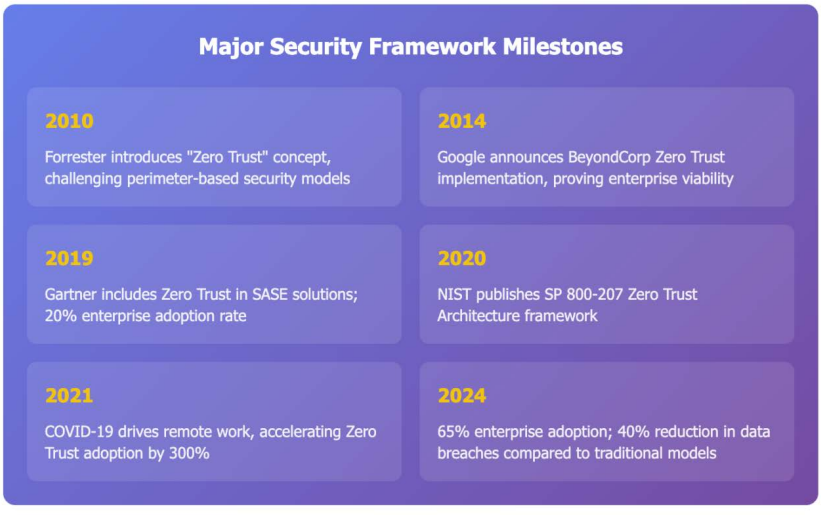


Figure 3. Evolution of cloud security models (2010-2024).

In conclusion, Zero Trust Architecture is becoming a key component of cloud security, offering enhanced protection for distributed cloud systems by continuously validating access requests and ensuring that only authenticated and authorized users can access critical resources. As cloud environments become more complex and decentralized, Zero Trust provides a robust framework for maintaining security and privacy in a world where traditional perimeter-based defenses are no longer sufficient [26].

4. Security and Privacy Challenges in Distributed Cloud Systems

As cloud computing continues to gain momentum, the security and privacy challenges associated with distributed cloud systems are becoming more complex and multifaceted [27]. In traditional cloud systems, resources are often centralized in a single data center or region, making it easier to apply uniform security controls. However, in distributed cloud environments, where resources are spread across multiple regions and cloud providers, ensuring consistent security and privacy becomes significantly more difficult.

One of the primary challenges in distributed cloud systems is data leakage. Since data is often transmitted across various locations, it becomes increasingly difficult to guarantee that sensitive information is fully protected during transit. Without end-to-end encryption or proper access controls, data can be intercepted by malicious actors during transmission. Data leakage can also occur when sensitive data is stored in cloud systems that are not adequately secured, leaving the data vulnerable to unauthorized access or exfiltration [28]. In distributed environments, ensuring that data remains encrypted both in transit and at rest is paramount for maintaining confidentiality and integrity.

Another significant challenge is the inconsistency of security policies across multiple cloud platforms. Distributed cloud environments often involve multi-cloud or hybrid cloud setups, where resources and data are hosted across different cloud service providers or on-premises infrastructures [29]. Each provider may have its own security protocols, access controls, and encryption standards, leading to potential gaps in security. For instance, while one cloud provider may use strong encryption standards, another may use weaker methods, exposing the system to vulnerabilities. Ensuring consistent security policies across different cloud providers and platforms is critical for preventing security breaches and data exposure [30].

Furthermore, cloud environments are highly dynamic and often involve multi-tenant architectures, where multiple users share the same physical resources [31]. This increases the risk of resource contention and unauthorized access, as different users may have different access requirements, leading to potential vulnerabilities. Inadequate access controls in multi-tenant environments can result in one tenant gaining unauthorized access to another tenant's data or resources. To mitigate this, strict RBAC and ABAC models must be enforced, ensuring that each

tenant only has access to their allocated resources and data.

Network vulnerabilities are another critical concern in distributed cloud systems. As cloud systems are built on the internet and often involve public cloud services, data and resources are more exposed to cyberattacks such as man-in-the-middle attacks, denial-of-service (DoS) attacks, and data interception [32]. Ensuring that data transmission between cloud services is secure and that communication channels are protected using secure sockets layer (SSL), virtual private networks (VPNs), and private networks is essential for preventing malicious attacks. Additionally, employing intrusion detection systems (IDS) and intrusion prevention systems (IPS) can help identify and block unauthorized network activity in real-time.

The complexity of compliance in distributed cloud environments also poses a significant challenge [33]. Cloud providers must adhere to various regulations, such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, and other regional privacy laws. Ensuring that cloud systems are compliant with these regulations while protecting user data can be difficult when data is distributed across multiple jurisdictions. The different privacy laws in various regions may require data localization or restrictions on cross-border data transfer, complicating the management of privacy in distributed systems.

Finally, the insider threat is a persistent security concern in distributed cloud environments. While cloud service providers implement security measures to protect their systems from external threats, there is always a risk of misuse or negligence by trusted employees or contractors [34]. To mitigate this risk, organizations must implement comprehensive monitoring and audit logging systems to track access to sensitive data and detect any suspicious behavior. Behavioral analytics tools can also help identify anomalies in user behavior that may indicate potential insider threats.

5. Best Practices for Enhancing Security and Privacy in Distributed Cloud Systems

To address the security and privacy challenges in distributed cloud systems, organizations must adopt a set of best practices to safeguard sensitive data, manage user access, and ensure compliance with regulatory standards [35]. Implementing these best practices helps organizations reduce risks and protect their cloud-based resources.

End-to-End Encryption is one of the most important security practices for protecting data in distributed cloud systems [36]. By encrypting data both at rest and in transit, organizations can ensure that even if data is intercepted or accessed without authorization, it will remain unreadable and secure. Transport Layer Security (TLS) should be used to encrypt data during transmission between cloud services, and encryption algorithms such as AES-256 should be employed to secure data at rest [37]. Additionally, cloud providers should offer key management

services to securely manage encryption keys, ensuring that they are stored and handled securely.

IAM systems are critical for controlling access to cloud resources. Organizations should implement MFA to enhance the security of user logins. MFA adds an extra layer of security by requiring users to provide more than just a password [38]. Combining passwords with biometric authentication, tokens, or one-time passcodes ensures that only authorized users can access sensitive data. In addition to MFA, RBAC and ABAC should be used to manage permissions and restrict access to only the necessary resources for each user or system.

ZTA should be adopted as a comprehensive security model. Zero Trust operates on the principle of "never trust, always verify", requiring continuous authentication and verification of users, devices, and systems. By implementing micro-segmentation, organizations can create smaller, more isolated segments within their cloud infrastructure, limiting the potential impact of a security breach. Least privilege access should also be enforced, ensuring that users only have the minimum permissions required to perform their tasks, reducing the risk of unauthorized access.

Continuous Monitoring and Auditing are essential for detecting potential security incidents and ensuring that security policies are being followed [39]. Organizations should implement automated monitoring tools that provide real-time alerts for suspicious activity, such as unauthorized access attempts or anomalous behavior. Audit logs should be maintained for all access to sensitive resources, allowing administrators to trace user actions and detect any signs of compromise. Regular security audits should also be conducted to ensure that cloud systems remain compliant with industry standards and regulations.

Data Privacy Practices should be incorporated into cloud security frameworks to ensure compliance with privacy regulations [40]. Data anonymization techniques should be used to protect personally identifiable information (PII) when it is used for analysis or shared with third parties. Additionally, organizations should implement data retention policies that specify how long data should be stored and when it should be deleted to minimize the risk of data breaches. Privacy-enhancing technologies (PETs), such as differential privacy and homomorphic encryption, can also be used to protect data while still allowing it to be analyzed for business purposes.

Finally, organizations should prepare for incident response by developing comprehensive disaster recovery and incident response plans. These plans should include protocols for detecting, containing, and remediating security incidents, as well as strategies for restoring cloud services in the event of a breach. Regular testing and simulation of these plans will ensure that organizations are prepared to respond to security threats effectively.

6. Conclusions

In conclusion, the security and privacy of distributed cloud systems remain paramount as the cloud computing landscape continues to evolve. As organizations

migrate their IT infrastructure to the cloud, they are faced with new challenges in securing distributed resources and ensuring compliance with evolving privacy regulations. The traditional perimeter-based security models are no longer effective in addressing the complexities of modern cloud systems, particularly with the rise of multi-cloud and hybrid cloud environments. As cloud systems become more distributed, the need for more advanced and adaptable security practices has never been more critical.

IAM remains a cornerstone of cloud security, but it is increasingly supplemented by the adoption of ZTA. Zero Trust, with its emphasis on continuous verification, least-privilege access, and micro-segmentation, provides a more robust framework for securing distributed cloud systems. This shift to ZTA is particularly important as the traditional boundaries between internal and external networks blur, making perimeter-based defenses ineffective.

Additionally, the increasing integration of AI-driven security solutions will play a crucial role in cloud security. By leveraging machine learning and data analytics, AI systems can enhance threat detection, automate incident responses, and continuously improve security protocols. The use of privacy-preserving techniques such as differential privacy and homomorphic encryption will become more prevalent, ensuring that sensitive data can be processed without compromising user privacy or compliance with regulations like GDPR.

However, the adoption of these advanced technologies is not without its challenges. Issues related to data quality, real-time decision-making, and the integration of Zero Trust models with existing cloud infrastructures must be addressed. Moreover, as cloud environments continue to grow in complexity, organizations must be proactive in their approach to security and privacy, ensuring that they are prepared to respond to both internal and external threats.

Looking ahead, the continued development of Zero Trust principles, AI-driven innovations, and privacy-preserving technologies will shape the future of cloud security. By adopting these new practices and continuously evolving their security frameworks, organizations can ensure the protection of their cloud-based resources and sensitive data, while also complying with ever-changing regulations.

In conclusion, cloud security and privacy will remain a dynamic field, requiring organizations to stay ahead of emerging threats and adopt the best practices that align with the evolving landscape of distributed cloud systems. The future of cloud security lies in continuous innovation, where AI, Zero Trust, and privacy-focused approaches work in harmony to provide a more secure and compliant cloud environment for businesses and users alike.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Islam, R., Patamsetti, V., Gadhi, A., Gondu, R.M., Bandaru, C.M., Kesani, S.C., *et al.*

(2023) The Future of Cloud Computing: Benefits and Challenges. *International Journal of Communications, Network and System Sciences*, **16**, 53-65. https://doi.org/10.4236/ijcns.2023.164004

[2] Rashid, Z.N., Zebari, S.R.M., Sharif, K.H. and Jacksi, K. (2018) Distributed Cloud Computing and Distributed Parallel Computing: A Review. 2018 *International Conference on Advanced Science and Engineering* (*ICOASE*), Duhok, 9-11 October 2018, 167-172. https://doi.org/10.1109/icoase.2018.8548937

[3] Alsirhani, A., Ezz, M. and Mohamed Mostafa, A. (2022) Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing. *Computer Systems Science and Engineering*, **43**, 967-984. https://doi.org/10.32604/csse.2022.024854

[4] Olabanji, S.O., Olaniyi, O.O., Adigwe, C.S., Okunleye, O.J. and Oladoyinbo, T.O. (2024) AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems. *SSRN Electronic Journal*, **17**, 38-56. https://doi.org/10.2139/ssrn.4706726

[5] Davis, P., Coffey, S., Beshaj, L. and Bastian, N. D. (2024) Emerging Technologies for Data Security in Zero Trust Environments. *The Cyber Defense Review*, **9**, 49-72.

[6] Smirnova, T. and Ivanov, P. (2024) Mitigating Cyber Threats in Cloud Computing: A Comprehensive Review of Security Strategies. *Eastern-European Journal of Engineering and Technology*, **3**, 51-59.

[7] Mensah, F. (2024) Zero Trust Architecture: A Comprehensive Review of Principles, Implementation Strategies, and Future Directions in Enterprise Cybersecurity. *International Journal of Academic and Industrial Research Innovations* (*IJAIRI*), **10**, 339-346.

[8] Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A. and Kim, H. (2022) Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability*, **14**, Article 11213. https://doi.org/10.3390/su141811213

[9] Hasan, M. (2024) Enhancing Enterprise Security with Zero Trust Architecture. arXiv: 2410.18291.

[10] Mohammed, I.A. (2019) Cloud Identity and Access Management—A Model Proposal. *International Journal of Innovations in Engineering Research and Technology*, **6**, 1-8.

[11] Singh, C., Thakkar, R. and Warraich, J. (2023) IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. *European Journal of Engineering and Technology Research*, **8**, 30-38. https://doi.org/10.24018/ejeng.2023.8.4.3074

[12] Godwin Nzeako, and Rahman Akorede Shittu, (2024) Leveraging AI for Enhanced Identity and Access Management in Cloud-Based Systems to Advance User Authentication and Access Control. *World Journal of Advanced Research and Reviews*, **24**, 1661-1674. https://doi.org/10.30574/wjarr.2024.24.3.3501

[13] Sekar, R.R., Masna, A., Sharma, S., Abraham, A. and Pagilla, P.R. (2024) Decentralized Identity and Access Management (IAM) Using Blockchain. 2024 *International Conference on Intelligent Systems for Cybersecurity* (*ISCS*), Gurugram, 3-4 May 2024, 1-6. https://doi.org/10.1109/iscs61804.2024.10581159

[14] Younis, Y. A., Kifayat, K. and Merabti, M. (2014) An Access Control Model for Cloud Computing. *Journal of Information Security and Applications*, **19**, 45-60. https://doi.org/10.1016/j.jisa.2014.04.003

[15] Gunawardena, R.S. (2022) Dynamic Access Control Techniques and Their Role in Preserving Data Confidentiality in Multi-Cloud Retail Solutions. *Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks*, **6**, 12-22.

[16] Mostafa, A.M., Ezz, M., Elbashir, M.K., Alruily, M., Hamouda, E., Alsarhani, M., *et al*. (2023) Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. *Applied Sciences*, **13**, Article 10871. https://doi.org/10.3390/app131910871

[17] Julakanti, S.R., Sattiraju, N.S.K. and Julakanti, R. (2022) Multi-Cloud Security: Strategies for Managing Hybrid Environments. *NeuroQuantology*, **20**, 10063-10074.

[18] Veeramachaneni, V. (2025) Integrating Zero Trust Principles into IAM for Enhanced Cloud Security. *Recent Trends in Cloud Computing and Web Engineering*, **7**, 78-92.

[19] Stafford, V. (2020) Zero Trust Architecture. *NIST Special Publication*, **800**, 800-207.

[20] Ghasemshirazi, S., Shirvani, G. and Alipour, M.A. (2023) Zero Trust: Applications, Challenges, and Opportunities. arXiv:2309.03582.

[21] Colomb, Y., White, P., Islam, R. and Alsadoon, A. (2022) Applying Zero Trust Architecture and Probability-Based Authentication to Preserve Security and Privacy of Data in the Cloud. In: *Emerging Trends in Cybersecurity Applications* (pp. 137-169). Springer International Publishing. https://doi.org/10.1007/978-3-031-09640-2_7

[22] Wang, C., Wang, Y., Chen, Y., Liu, H. and Liu, J. (2020) User Authentication on Mobile Devices: Approaches, Threats and Trends. *Computer Networks*, **170**, Article 107118. https://doi.org/10.1016/j.comnet.2020.107118

[23] Manda, J.K. (2022) Zero Trust Architecture in Telecom: Implementing Zero Trust Architecture Principles to Enhance Network Security and Mitigate Insider Threats in Telecom Operations. *Journal of Innovative Technologies*, **5**, No. 1.

[24] Batan, A. (2024) Investigating the Efficacy of Zero-Trust Security Models in Mitigating Insider Threats in Enterprise Environments. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, **8**, 10-19.

[25] Chandramouli, R., Chandramouli, R. and 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

[26] Ojha, N. and Vaish, A. (2025) Why Perimeter Security Is No Longer Enough: Observations and Open Challenges. In: *Zero-Trust Learning* (pp. 305-328). Apple Academic Press. https://doi.org/10.1201/9781779643575-15

[27] Ang'udi, J.J. (2023) Security Challenges in Cloud Computing: A Comprehensive Analysis. *World Journal of Advanced Engineering Technology and Sciences*, **10**, 155-181. https://doi.org/10.30574/wjaets.2023.10.2.0304

[28] Yang, P., Xiong, N. and Ren, J. (2020) Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, **8**, 131723-131740. https://doi.org/10.1109/ACCESS.2020.3009876

[29] Merseedi, K.J. and Zeebaree, D.S.R.M. (2024) Cloud Architectures for Distributed Multi-Cloud Computing: A Review of Hybrid and Federated Cloud Environment. *Indonesian Journal of Computer Science*, **13**, 1644-1673. https://doi.org/10.33022/ijcs.v13i2.3811

[30] Chinamanagonda, S. (2019) Security in Multi-Cloud Environments-Heightened focus on Securing Multi-Cloud Deployments. *Journal of Innovative Technologies*, **2**, No. 1.

[31] Jia, R., Yang, Y., Grundy, J., Keung, J. and Hao, L. (2021) A Systematic Review of Scheduling Approaches on Multi-Tenancy Cloud Platforms. *Information and Software Technology*, **132**, Article 106478. https://doi.org/10.1016/j.infsof.2020.106478

[32] Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M. and Rehman, S.U. (2023) Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry*, **15**, Article 1981. https://doi.org/10.3390/sym15111981

[33] Kumar, B. (2022) Challenges and Solutions for Integrating AI with Multi-Cloud Architectures. *International Journal of Multidisciplinary Innovation and Research Methodology*, **1**, 71-77.

[34] Deep, G., Sidhu, J. and Mohana, R. (2022) Insider Threat Prevention in Distributed Database as a Service Cloud Environment. *Computers & Industrial Engineering*, **169**, Article 108278. https://doi.org/10.1016/j.cie.2022.108278

[35] Naik, S. (2023) Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy. *The Eastasouth Journal of Information System and Computer Science*, **1**, 69-87. https://doi.org/10.58812/esiscs.v1i01.452

[36] Mustafa, A. and Zillay, H. (2024) End-to-End Encryption and Data Privacy in Azure Cloud Security. *Global Perspectives on Multidisciplinary Research*, **5**, 10-19.

[37] Manthiramoorthy, C., Khan, K.M.S. and A, N.A. (2023) Comparing Several Encrypted Cloud Storage Platforms. *International Journal of Mathematics, Statistics, and Computer Science*, **2**, 44-62. https://doi.org/10.59543/ijmscs.v2i.7971

[38] Fanti, M. (2023) Implementing Multifactor Authentication: Protect Your Applications from Cyberattacks with the Help of MFA. Packt Publishing Ltd.

[39] Ebute, M. (2024) Continuous Monitoring and Assessment Mecha-NISMS in Cybersecurity: Best Practices for Sustained Protection of Critical Assets. 1-13. https://doi.org/10.2139/ssrn.4912624

[40] Abrera, J. (2024) Data Privacy and Security in Cloud Computing: A Comprehensive Review. *Journal of Computer Science and Information Technology*, **1**, 1-9.