A Comparative Review of Cloud Identity and Access Management Architectures Using Zero-Trust, Decentralized Identity, and AI-Based Techniques

Kishan Vaghela[1], Tushar Desai[2]

Student, Department of CSE, Drs. Kiran & Pallavi Patel Global University, Varnama, Gujarat, India
Email: vaghelakishan301[at]gmail.com

Assistant Professor Department of CSE, Drs. Kiran & Pallavi Patel Global University, Varnama, Gujarat, India
Email: tushardesai.cse.kset[at]kpgu.ac.in

Abstract: ***Cloud Identity and Access Management (IAM) has become a central pillar of cloud security, governing authentication, authorization, and identity lifecycle management across increasingly complex cloud ecosystems. This review provides an in-depth examination of contemporary Cloud IAM architectures, the expanding identity attack surface in multi-cloud and distributed environments, and the operational challenges arising from scale, heterogeneity, and dynamic access requirements. It synthesizes recent research on access control models, Zero-Trust architectures, self-sovereign and decentralized identity frameworks, and AI- assisted IAM mechanisms for anomaly detection, adaptive authentication, and policy enforcement. The review further analyses empirical and conceptual studies addressing cross-cloud interoperability, CIAM–PAM integration, privacy-preserving identity management for IoT and constrained devices, and formal verification of access control policies.***

Keywords: Cloud Identity and Access Management, Cloud Security, Zero-Trust Architecture, Self-Sovereign Identity, Artificial Intelligence, Access Control, Multi-Cloud Environments, Privacy-Preserving IAM.

1. Introduction

The rapid adoption of cloud computing has fundamentally transformed how organizations deploy applications, manage data, and deliver digital services. Modern cloud environments are increasingly characterized by distributed architectures, multi-cloud deployments, and dynamic resource provisioning. While these paradigms offer scalability and flexibility, they also introduce significant security challenges, particularly in the management of identities and access privileges. As a result, Cloud Identity and Access Management (IAM) has become a critical security component for ensuring controlled access to cloud-based resources.

Traditional IAM mechanisms, primarily designed for static and perimeter-based enterprise systems, are often inadequate in cloud environments. Centralized identity stores, static credentials, and coarse-grained access control models struggle to cope with dynamic workloads, cross-domain access requirements, and the growing diversity of identity types, including users, services, applications, and devices. Numerous studies report that identity misconfigurations, excessive privileges, and credential misuse remain leading causes of security breaches in cloud platforms, highlighting the limitations of conventional IAM approaches.

To address these challenges, recent research has proposed a wide range of advanced Cloud IAM architectures. These include Zero-Trust models that eliminate implicit trust and enforce continuous verification, decentralized and self-sovereign identity frameworks that aim to reduce identity fragmentation and enhance user control, and artificial intelligence–assisted IAM systems that leverage behavioral analytics and anomaly detection to enable adaptive access control. In addition, enterprise-focused solutions increasingly explore the integration of Customer Identity and Access Management (CIAM) with Privileged Access Management (PAM) to strengthen governance and reduce insider threats.

2. Literature Study

Jain [1] presented a comprehensive survey on identity and access management in cloud environments, highlighting the role of IAM in authentication, authorization, and identity lifecycle management. The study emphasized the growing complexity of identity governance in multi-cloud systems but lacked comparative evaluation of emerging IAM architectures, limiting its practical guidance for deployment scenarios.

Singh [2] analysed the importance of IAM in securing cloud systems by focusing on access control enforcement and identity governance. While the work provided foundational insights into IAM components, it primarily discussed centralized models and did not address advanced paradigms such as Zero-Trust or decentralized identity.

Ben Haj Salah et al. [3] proposed a cross-cloud identity management framework based on self- sovereign identity principles. Their approach reduced identity fragmentation and improved portability across cloud providers. However, the study highlighted challenges related to governance and large-scale adoption of decentralized identity systems.

Bernabé Murcia et al. [4] introduced a decentralized identity management architecture designed for Zero- Trust multi-domain environments. Their framework eliminated implicit trust and enhanced access control across distributed systems, though it introduced increased policy complexity and operational overhead.

Kyriakidou et al. [5] investigated identity and access management solutions for the computing continuum, covering cloud, edge, and IoT environments. The study emphasized the need for interoperable IAM solutions but did not provide empirical validation across heterogeneous platforms.

Huang et al. [6] proposed a Zero-Trust identity framework tailored for agentic AI systems in cloud environments. Their work demonstrated how continuous verification improves security; however, the framework remained largely conceptual without real-world deployment evaluation.

Aggarwal et al. [7] developed CHEZ, a hyper- extensible Zero-Trust CIAM–PAM architecture for enterprise cloud environments. Their approach strengthened privileged access governance and reduced insider threats, although large-scale performance evaluation was limited.

Sivaraman [8] explored Zero-Trust IAM deployment in multi-cloud environments, highlighting benefits such as reduced lateral movement and fine-grained access control. The study identified challenges in policy management and interoperability across cloud providers.

A systematic review by multiple authors [9] examined IAM requirements and contributions of self-sovereign identity. The review identified privacy and portability advantages of SSI but noted unresolved issues in credential revocation and governance.

Prajapati [10] analysed the role of IAM within Zero- Trust architectures, emphasizing least-privilege enforcement and continuous authentication. While the study reinforced Zero-Trust principles, it lacked comparative analysis with non–Zero-Trust IAM models.

Denzel [11] conducted a survey of security mechanisms in Zero-Trust network architectures, including IAM components. The survey highlighted architectural benefits but did not focus deeply on identity interoperability challenges.

Santucci [12] discussed key security controls required for implementing Zero Trust, including IAM integration. The work provided practical insights but remained high-level without comparative evaluation of IAM techniques.

Wang [13] surveyed IAM solutions for future IoT environments, emphasizing scalability and lightweight authentication. The study identified privacy-preserving IAM as a critical need but highlighted limitations in current IoT–cloud integration mechanisms.

Jadala [14] reviewed IAM practices in cloud security, outlining common challenges such as misconfiguration and excessive privileges. The work focused on best practices rather than architectural comparison.

The WJAETS editorial review [15] presented foundational IAM principles and practices. Although comprehensive, it primarily addressed traditional IAM models and offered limited discussion on advanced architectures.

IRE Journals [16] analyzed recent advances in cloud security practices using IAM, highlighting policy enforcement and monitoring. The study lacked detailed evaluation of decentralized or AI-assisted IAM solutions.

Kovacevic et al. [17] proposed a token-based identity management approach for distributed cloud environments. Their solution enabled lightweight authentication but offered limited governance capabilities.

Ike [18] examined IAM mechanisms in cloud storage systems, emphasizing access control and auditing. The study focused on storage-specific use cases and did not generalize to broader cloud environments.

A federated IAM study by multiple authors [19] analyze identity federation in multi-cloud systems. While federation improved usability, policy inconsistency remained a major limitation.

Chellu [20] presented a case study on integrating Google Cloud IAM with managed file transfer systems. The work demonstrated practical deployment but lacked comparative evaluation with alternative IAM approaches.

Gouglidis et al. [21] applied formal verification techniques to analyze Google Cloud IAM policies. Their approach effectively detected misconfigurations but required specialized expertise and tooling.

Further case studies by Gouglidis et al. [22] evaluated IAM policy verification in real deployments, highlighting the prevalence of policy errors. Scalability remained a concern for large environments.

Vatsa et al. [23] proposed using large language models to synthesize access control policies automatically. Their approach reduced configuration errors but raised concerns regarding explainability and trust.

A survey on AI-assisted IAM by multiple authors [24] examined machine learning techniques for anomaly detection and access control. The study demonstrated improved threat detection but noted robustness challenges.

Madireddy [25] applied graph neural networks for adaptive threat detection using IAM logs. While effective in detecting complex attack patterns, the approach incurred high computational overhead.

Wairagade [26] reviewed AI applications in enterprise IAM systems, emphasizing adaptive authentication and monitoring. The study identified explainability as a key limitation.

Studies on CIAM–PAM integration [27] explored Zero-Trust enterprise architectures that unify customer and privileged identity management. Although governance improved, empirical validation was limited.

Further analysis of CIAM–PAM challenges [28] highlighted operational complexity and lack of standardized evaluation metrics in enterprise deployments.

García-Rodríguez and Skarmeta [29] proposed a privacy-preserving attribute-based IAM framework for IoT environments. Their approach enhanced privacy but faced scalability challenges.

Finally, decentralized IAM solutions for IoT–cloud systems [30] demonstrated improved identity portability and privacy. However, integration with cloud-native IAM services remained an open issue.

3. Proposed Comparative

Methodology

This paper follows a structured comparative analysis framework to examine existing Cloud Identity and Access Management (IAM) approaches. The methodology is designed to enable a systematic comparison of IAM research based on architectural design, access control mechanisms, and security objectives rather than implementation-specific details.

Relevant Cloud IAM research studies are first identified from established academic sources, focusing on works that address identity management, access control, and security in cloud environments. The selected studies are then classified according to their primary architectural and functional focus, including centralized and federated IAM models, Zero-Trust architectures, decentralized and self-sovereign identity frameworks, AI-assisted access control mechanisms, enterprise CIAM–PAM integration, and IAM solutions for IoT and constrained environments.

Each categorized study is subsequently analyze using a common set of comparison criteria. These criteria include the underlying identity model, access control strategy, scalability characteristics, interoperability support, security strengths, and reported limitations. This unified evaluation framework ensures consistency in comparison and enables objective assessment across heterogeneous Cloud IAM approaches.

Based on the comparative evaluation, key strengths and shortcomings of existing solutions are identified, with particular emphasis on challenges related to policy complexity, cross-cloud interoperability, privacy preservation, and the reliability of intelligent access control mechanisms. The synthesized observations are then used to highlight open research challenges and motivate future research directions in Cloud IAM.

4. Comparative Analysis of Cloud Identity and Access Management Approaches

A comparative analysis of representative Cloud Identity and Access Management (IAM) research works to highlight similarities, differences, and limitations across existing approaches. Unlike descriptive surveys, the comparison focuses on how different studies address core IAM challenges such as access control enforcement, scalability, interoperability, and security assurance in cloud environments.

Early studies primarily emphasize **centralized and federated IAM models**, relying on traditional access control mechanisms such as Role-Based Access Control (RBAC). While these approaches simplify identity governance and administrative control, they suffer from coarse-grained permission assignment, limited context awareness, and vulnerability to misconfigurations in dynamic cloud environments. As cloud infrastructures expand across multiple providers, these limitations significantly reduce their effectiveness.

Recent research shifts toward **Zero-Trust IAM architectures**, which eliminate implicit trust and enforce continuous authentication and authorization. Studies adopting Zero-Trust principles demonstrate improved resistance to lateral movement and insider threats. However, the comparison reveals that Zero- Trust IAM solutions often introduce increased policy complexity and operational overhead, particularly in large-scale multi-cloud deployments where consistent enforcement remains challenging.

Another emerging research direction focuses on **decentralized and self-sovereign identity (SSI)** frameworks. These approaches improve identity portability and user control by leveraging decentralized identifiers and cryptographic credentials. While SSI-based IAM reduces identity fragmentation and enhances privacy, existing studies lack mature governance models, efficient revocation mechanisms, and large-scale validation, limiting their adoption in enterprise cloud environments.

Several works explore **AI-assisted IAM mechanisms**, employing machine learning techniques for anomaly detection, policy optimization, and adaptive access control. These approaches demonstrate promising capabilities in identifying abnormal access patterns and reducing human configuration errors. Nevertheless, comparative analysis shows that concerns related to explainability, robustness, and adversarial manipulation remain largely unresolved.

Enterprise-focused studies propose **CIAM–PAM integration frameworks** to unify customer and privileged access management under Zero-Trust principles. Such solutions improve access governance and reduce insider threat risks; however, most evaluations are limited to controlled enterprise settings and lack cross-platform interoperability analysis.

5. Results Analysis

The analysis focuses on evaluating how different IAM approaches address key challenges related to identity models, access control mechanisms, scalability, interoperability, and security assurance in cloud

Paper ID: SR251222161336 DOI: https://dx.doi.org/10.21275/SR251222161336

environments. Unlike experimental studies, the results in this review are derived from a structured comparison of representative research works using a unified evaluation framework.

The analysis reveals a clear evolution in Cloud IAM research from traditional centralized and federated identity models toward more adaptive and security-focused architectures. Early approaches primarily rely on Role-Based Access Control (RBAC) and centralized identity providers, which offer simplicity and ease of administration. However, these solutions exhibit limitations in dynamic cloud environments due to coarse-grained permissions, excessive privilege assignment, and vulnerability to misconfigurations.

Zero-Trust IAM architectures demonstrate improved security by enforcing continuous verification and least-privilege access. The results indicate that Zero-Trust approaches significantly reduce implicit trust and lateral movement risks. Nevertheless, they introduce increased policy complexity and operational overhead, particularly in multi-cloud deployments where consistent enforcement across providers remains challenging.

Decentralized and self-sovereign identity (SSI)- based IAM solutions show strong potential in enhancing identity portability and privacy. The comparative results highlight that while SSI frameworks reduce identity fragmentation, they often lack mature governance models, efficient revocation mechanisms, and large-scale deployment validation. These limitations restrict their adoption in enterprise cloud environments.

AI-assisted IAM solutions improve adaptive decision-making through anomaly detection and policy automation. The analysis shows that such approaches can reduce human configuration errors and enhance threat detection. However, concerns related to explainability, robustness, and susceptibility to adversarial manipulation remain open challenges.

Enterprise-oriented CIAM–PAM integration frameworks provide stronger access governance and improved control over privileged identities. The results indicate that these approaches are effective in reducing insider threats but are typically evaluated in limited enterprise scenarios and lack comprehensive cross-cloud interoperability assessment.

Table 1: Comparative Analysis of Cloud Identity and Access Management Research

Primary Focus	IAM Model	Key Techniques	Limitations
Cloud IAM Survey	Centralized	RBAC, Federation	Lacks comparative and experimental depth
Cross- Cloud IAM	Decentralized	Self- Sovereign Identity, DIDs	Governance and revocation challenges
Zero- Trust IAM	Decentralized	Continuous Verification, Policy Enforcement	Increased policy complexity
Multi- Cloud IAM	Zero-Trust	Context- Aware Access Control	Performance overhead in large deployments
IoT- Oriented IAM	Attribute- Based	ABAC, Lightweight Authentication	Scalability and lifecycle management issues
AI- Assisted IAM	Hybrid	Machine Learning, Policy Automation	Explainability and robustness concerns
Enterprise IAM	CIAM–PAM	Just-in-Time Access, Automation	Limited real- world and cross-cloud validation

Table 2: Summary of Strengths and Challenges Across IAM Approaches

IAM Approach	Key Strengths	Major Challenges
Centralized IAM	Simple administration	Single point of failure
Federated IAM	Improved usability	Policy inconsistency
Zero-Trust IAM	Strong security guarantees	Operational complexity
Decentralized IAM (SSI)	Privacy and portability	Governance and revocation
AI-Assisted IAM	Adaptive access control	Lack of explainability
CIAM–PAM Integration	Enhanced privileged control	Limited cross- cloud support

6. Conclusion

Cloud Identity and Access Management has evolved into a complex and multidimensional security domain, shaped by the rapid adoption of distributed cloud architectures, multi-cloud deployments, and the integration of IoT and intelligent services. The reviewed literature demonstrates that identity- centric threats now exploit weaknesses in access control policies, credential management, and trust assumptions embedded within traditional IAM frameworks. As cloud environments become increasingly dynamic and interconnected, centralized and static IAM models struggle to provide adequate protection against identity misuse, privilege escalation, and insider threats.

The analysis highlights that while advanced approaches- such as Zero-Trust architectures, decentralized and self-sovereign identity models, AI-assisted access control, and CIAM–PAM integration- offer significant improvements in security and adaptability, each approach exhibits inherent limitations when applied in isolation. Zero- Trust models introduce policy complexity and operational overhead, decentralized identity frameworks face governance and scalability challenges, and AI-based IAM solutions raise concerns related to transparency, robustness, and trust in automated decision-making. Similarly, privacy-preserving IAM mechanisms for IoT and constrained devices remain constrained by integration and lifecycle management issues.

Overall, the findings indicate that no single technical solution can effectively address the expanding identity threat landscape in cloud environments. Robust Cloud IAM requires a holistic and integrated strategy that combines adaptive access control, interoperable identity architectures, intelligent monitoring, and strong governance mechanisms. Addressing existing gaps in interoperability, empirical validation, and system resilience will be essential for developing scalable, secure, and trustworthy Cloud IAM frameworks capable of supporting the evolving demands of next-generation cloud ecosystems.

References

[1] P. Jain, “Identity and access management in the cloud,” *Survey Paper*, ResearchGate, 2025.

[2] C. Singh, “Identity and access management: Importance in securing cloud systems,” *Survey Article*, 2023.

[3] A. Ben Haj Salah, M. Ben Ahmed, and H. Yahia, “Identity management in cross-cloud environments: Towards self-sovereign identities using current solutions,” *Journal of Cloud Computing*, vol. 12, no. 1, 2023.

[4] J. M. Bernabé Murcia, R. Ferrús, and J. M. Cabero, “Decentralised identity management for zero-trust multi-domain continuum,” *Computer Networks*, Elsevier, 2024.

[5] A. Kyriakidou et al., “Identity and access management for the computing continuum,” *Preprint*, 2025.

[6] K. Huang, V. S. Narajala, and J. Yeoh, “A zero- trust identity framework for agentic AI,” *Preprint*, 2025.

[7] S. Aggarwal et al., “CHEZ: Hyper-extensible zero-trust CIAM–PAM architecture,” *IEEE IT Professional*, 2025.

[8] H. Sivaraman, “Zero trust identity and access management in multi-cloud environments,” *ESP Journal of Engineering and Technology Advancements*, vol. 3, no. 6, 2023.

[9] Multiple Authors, “IAM requirements and self-sovereign identity contributions: A systematic review,” *Systematic Review*, 2023.

[10] V. Prajapati, “Role of identity and access management in zero trust architecture for cloud security,” *International Journal of Advanced Research in Science and Technology*, 2025.

[11] K. Denzel, “A survey of security in zero trust network architectures,” *GSC Advanced Research and Reviews*, 2025.

[12] F. Santucci, “Implementing zero trust: Expert insights on key security controls,” *Information*, vol. 16, no. 8, MDPI, 2025.

[13] Y. Wang, “A survey on identity and access management for future IoT,” *Computer Networks*, Elsevier, 2025.

[14] A. Jadala, “Identity and access management in cloud security: Best practices and challenges,” *Review Article*, 2025.

[15] Editorial Board, “Identity and access management: Foundations, principles, and practices,” *World Journal of Advanced Engineering and Technology Sciences*, 2025.

[16] IRE Journals, “Advances in cloud security practices using identity and access management,” *IRE Journals*, 2025.

[17] I. Kovacevic, T. Rankovic, and M. Stojkov, “Token-based identity management in the distributed cloud,” *Preprint*, 2024.

[18] J. E. Ike, “Identity and access management in cloud storage: A comprehensive guide,” *Preprint*, 2025.

[19] Multiple Authors, “Federated identity management in multi-cloud systems,” *Journal Article*, 2024.

[20] R. Chellu, “Integrating Google Cloud IAM with managed file transfer,” *Case Study*, ResearchGate, 2025.

[21] D. Gouglidis, M. Kagia, and H. Hu, “Model checking access control policies using Google Cloud IAM,” *Formal Methods Study*, 2023.

[22] D. Gouglidis et al., “Case studies on Google Cloud IAM: Policy verification and misconfiguration detection,” *Empirical Study*, 2023.

[23] A. Vatsa, P. Patel, and W. Eiers, “Synthesizing access control policies using large language models,” *Preprint*, 2025.

[24] Multiple Authors, “AI for identity and access management in the cloud,” *Survey Article*, 2024.

[25] V. T. Madireddy, “Graph neural network-based adaptive threat detection for cloud IAM logs,” *Preprint*, 2025.

[26] A. Wairagade, “Artificial intelligence in identity and access management for enterprise systems,” *Procedia Computer Science*, Elsevier, 2025.

[27] Multiple Authors, “CIAM–PAM related zero- trust architectures for enterprise cloud environments,” *IEEE IT Professional*, 2024.

[28] Multiple Authors, “Operational challenges in CIAM–PAM integration under zero trust,” *Journal of Information Security and Applications*, 2025.

[29] J. García-Rodríguez and A. Skarmeta, “Privacy-preserving attribute-based identity and access management for IoT,” *Computer Networks*, Elsevier, 2023.

[30] Multiple Authors, “Decentralized identity and privacy-preserving access control for IoT–cloud systems,” *Journal of Network and Computer Applications*, 2024.