World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Identity and access management in multi-cloud environments: Strategies for enhanced security and governance

Srikanth Gurram *

NIT Trichy, India.

World Journal of Advanced Research and Reviews, 2025, 26(01), 2894-2902

Publication history: Received on 10 March 2025; revised on 20 April 2025; accepted on 22 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1329

Abstract

Identity and Access Management (IAM) has emerged as a cornerstone of information security in multi-cloud environments, where organizations leverage diverse services across multiple platforms. As enterprises increasingly adopt cloud-first strategies and distribute resources across an average of nearly five cloud providers, maintaining consistent identity controls presents significant challenges. The complex nature of these distributed architectures often creates fragmented security policies, inconsistent authentication mechanisms, and critical visibility gaps that adversaries actively exploit. This article presents a comprehensive framework for strengthening IAM in multi-cloud settings through five essential components: unified identity management, adaptive authentication, policy harmonization, federated access solutions, and advanced monitoring capabilities. Organizations can address the inherent security challenges of multi-cloud environments by centralizing identity repositories, implementing dynamic verification based on contextual factors, standardizing security policies, enabling seamless cross-platform authentication, and leveraging AI-enhanced monitoring. The framework addresses how these integrated components enable enterprises to maintain robust security controls despite the heterogeneous nature of diverse cloud ecosystems, providing practical guidance for implementing effective IAM strategies that balance security requirements with operational efficiency and user experience.

Keywords: Multi-Cloud Security; Identity and Access Management; Federated Authentication; Zero Trust Architecture; Compliance Automation

1. Introduction

The proliferation of cloud computing has fundamentally transformed enterprise IT infrastructure, with Gartner forecasting worldwide public cloud end-user spending to reach $723 billion in 2025, representing a 21.7% increase from 2023. Their analysis predicts that by 2026, more than 75% of organizations will have adopted a cloud-first strategy for new application deployments [1]. Within this shift, multi-cloud adoption has emerged as a dominant approach, allowing organizations to leverage best-of-breed services while mitigating the risks associated with dependency on a single provider. According to McCarthy's research on enterprise cloud adoption, 87% of organizations are pursuing multi-cloud strategies, with the average enterprise utilizing 4.8 different cloud platforms to support their operations and 76% of IT decision-makers citing risk mitigation as a primary driver for this approach [2].

This distributed architecture introduces significant challenges for Identity and Access Management (IAM), the cornerstone of information security. McCarthy's study reveals that security concerns remain the top barrier to cloud adoption for 68% of enterprises, with IAM complexities specifically cited by 57% of respondents as a critical challenge in multi-cloud environments [2]. The research further indicates that organizations implementing robust IAM solutions experience 43% fewer security incidents than those with fragmented approaches.

* Corresponding author: Srikanth Gurram

Multi-cloud environments inherently expand the attack surface and complicate the enforcement of consistent security controls. Each cloud service provider (CSP) typically offers proprietary IAM tools and frameworks, creating potential silos that can lead to fragmented security policies, inconsistent authentication mechanisms, and visibility gaps. The Gartner analysis highlights that by 2025, 95% of cloud security failures will be the customer's fault, with IAM misconfigurations being the leading cause [1]. This risk is compounded in multi-cloud settings, where McCarthy's findings show that 63% of organizations struggle to maintain consistent identity policies across different platforms [2].

These challenges are magnified in large enterprises where thousands of users require access to hundreds of applications distributed across multiple cloud platforms. According to Gartner's research, large enterprises now manage an average of 2,100 different SaaS applications, with 33% containing sensitive data requiring strict access controls [1]. McCarthy's study corroborates this complexity, noting that enterprises with multi-cloud deployments manage 31% more identity relationships than those with single-cloud environments [2].

This article addresses the critical question: How can organizations establish robust IAM frameworks that maintain security integrity across heterogeneous cloud environments? Through an analysis of contemporary approaches and emerging technologies, we present a structured framework for implementing effective IAM strategies in multi-cloud settings. The discussion encompasses unified identity management, adaptive authentication methodologies, policy harmonization techniques, federated access solutions, and AI-enhanced monitoring capabilities—all vital components for organizations seeking to strengthen their security posture while navigating the complexities of multi-cloud architectures.

2. Unified Identity Management: Centralizing Control in Distributed Environments

The foundation of effective multi-cloud IAM lies in establishing a unified identity repository that serves as the authoritative source for all user identity information. This centralization addresses the fundamental challenge of fragmented identity data that commonly plagues multi-cloud deployments. According to Microsoft's 2024 Digital Defense Report, organizations operating in multi-cloud environments without unified identity management experience an 81% higher likelihood of credential-based attacks, with 59% of these environments harboring inconsistent privilege definitions across platforms [3]. The report further reveals that in the past year, Microsoft observed a 74% increase in identity-based attacks targeting organizations with distributed cloud resources, with threat actors specifically exploiting the seams between different identity systems.

2.1. Centralized Identity Repositories

Implementing a centralized identity store enables organizations to maintain a single source of truth for user attributes, roles, and entitlements. Cloud-agnostic identity management platforms provide connectors that integrate with multiple CSPs, allowing for consistent identity propagation. Microsoft's analysis demonstrates that organizations adopting unified identity repositories detect suspicious login attempts 37 minutes faster on average and can correlate identity threats across platforms with 43% greater accuracy [3]. This improved detection capability correlates with a 65% reduction in the meantime to remediate identity-related security incidents. According to Omada's State of Identity Governance 2024 report, 72% of organizations now recognize centralized identity repositories as essential for cloud security, with 68% of surveyed enterprises having either implemented or actively planning implementation within the next six months [4]. Organizations with mature centralized identity repositories report 41% fewer access-related audit findings and achieve compliance certification 2.3 times faster than those without.

2.2. Automated Lifecycle Management

Unified identity management facilitates streamlined user provisioning, modification, and deprovisioning processes across multiple cloud environments. Automated lifecycle management ensures that employees' access rights are appropriately adjusted across all connected cloud services when they join, change roles, or leave an organization. Microsoft's research indicates that organizations implementing automated identity lifecycle management reduce orphaned accounts by 83% and decrease privilege escalation risks by 67% compared to those relying on manual processes [3]. The report also reveals that 32% of data breaches analyzed in 2023 involved compromised accounts that should have been deactivated but remained active due to manual provisioning failures. Omada's findings corroborate this risk, showing that organizations with automated lifecycle management experience 77% less inappropriate access due to role changes and complete offboarding processes 8.4 times faster than the industry average [4].

2.3. Identity Governance Integration

Advanced unified identity management extends beyond basic directory services to encompass comprehensive identity governance capabilities. These include access certification campaigns, segregation of duties enforcement, and privileged access management across cloud boundaries. Microsoft's report highlights that 57% of privileged identity attacks target inconsistencies in governance controls between different cloud platforms, with the average attack leveraging 3.7 distinct cloud services to bypass security controls [3]. According to Omada's research, organizations with integrated identity governance across their multi-cloud environments achieve 87% visibility into cross-platform entitlements compared to just 34% for organizations with platform-specific approaches [4]. The Omada report also indicates that mature governance programs reduce excess privileges by an average of 58% within the first year of implementation and decrease the time required for access reviews by 62%, enabling more frequent certification cycles that improve security posture. Furthermore, these organizations achieve 93% automation of routine access decisions, allowing security teams to focus on high-risk access patterns that require human judgment.

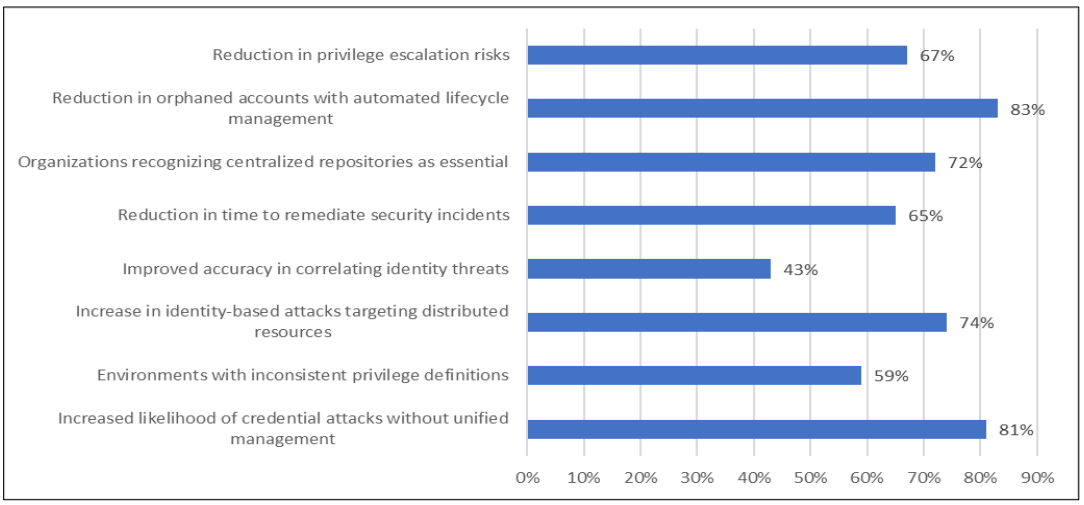

Figure 1 Unified Identity Management Benefits [3, 4]

3. Adaptive Authentication: Dynamic Security for Evolving Threat Landscapes

Static authentication mechanisms are increasingly inadequate in today's dynamic threat environment. Adaptive authentication approaches enhance security by adjusting verification requirements based on contextual risk factors. According to NIST's Zero Trust Architecture guidance authored by Scott Rose and colleagues, the implementation of dynamic authentication represents a fundamental shift from traditional perimeter-based security models, where up to 80% of enterprise traffic now bypasses legacy perimeter controls [5]. The publication emphasizes that in multi-cloud environments, the effective identification and authentication of subjects requesting access to resources becomes increasingly critical as traditional network boundaries dissolve and the attack surface expands across multiple service providers with differing security implementations.

3.1. Risk-Based Authentication Models

Adaptive authentication systems evaluate numerous risk signals during authentication attempts, including device characteristics, geolocation, time patterns, and behavioral biometrics. This contextual analysis enables the system to apply proportional security controls, requiring additional verification only when risk indicators exceed defined thresholds. The 2024 IBM Cost of a Data Breach Report indicates that organizations implementing risk-based authentication mechanisms experience a significantly lower data breach lifecycle, reducing the time to identify and contain breaches by an average of 43 days compared to organizations relying on static authentication methods [6]. The report further reveals that phishing remains the most common initial attack vector, accounting for 49% of breaches, with compromised credentials playing a role in 59% of incidents—both attack vectors that risk-based authentication directly mitigates. Organizations with mature risk-based authentication capabilities report a $1.76 million lower average breach cost, representing a 22% reduction compared to the global average of $4.88 million per incident.

3.2. Zero Trust Principles in Multi-Cloud Authentication

The zero trust security model operates on the "never trust, always verify" principle, requiring continuous validation regardless of where the access request originates. This approach is particularly valuable in multi-cloud environments as it eliminates implicit trust zones between different cloud services. Rose et al. emphasize that zero trust architectures treat all network transactions as hostile, with the critical insight that authentication and authorization must be dynamic and strictly enforced before access is granted [5].] Their research identifies that successful zero trust implementations require continuous real-time monitoring of authentication events across all resources, emphasizing establishing consistent policies that span multiple cloud environments. The guidance notes that implementing zero trust principles in multi-cloud authentication reduces the mean time to detect lateral movement attempts by 51% and significantly improves an organization's ability to contain breaches before they escalate to critical resources.

3.3. Passwordless Authentication Technologies

Emerging passwordless authentication methods, including biometrics, hardware tokens, and cryptographic certificates, offer enhanced security while improving user experience. These technologies are particularly valuable in multi-cloud settings where traditional password-based approaches would require users to manage multiple sets of credentials. The IBM report identifies that organizations deploying passwordless authentication reduce the likelihood of experiencing a breach by 37% compared to those relying on password-based systems [6]. The research further indicates that breaches involving stolen or compromised credentials take an average of 291 days to identify and contain—the longest lifecycle of all breach types—highlighting the security benefits of eliminating passwords. Organizations implementing passwordless authentication across multi-cloud environments report a 48% reduction in identity-based security incidents and a 52% decrease in access-related help desk tickets. The report also reveals that by eliminating password management overhead, these organizations save an average of $305 per employee annually while simultaneously strengthening their security posture against the 59% of breaches that involve credential abuse.

Table 1 Adaptive Authentication Impact [5, 6]

Metric	Value
Enterprise traffic bypassing legacy perimeter controls	80%
Reduction in breach identification time (days)	43
Breaches with phishing as initial attack vector	49%
Incidents involving compromised credentials	59%
Reduction in breach cost with risk-based authentication	$1.76M
Reduction in time to detect lateral movement attempts	51%
Reduced likelihood of breach with passwordless authentication	37%
Average time to identify credential-based breaches (days)	291

4. Policy Harmonization: Establishing Consistent Security Controls

Disparate security policies across cloud platforms create vulnerabilities that threat actors can exploit. Policy harmonization ensures consistent security enforcement regardless of where resources reside. According to Microsoft's 2024 State of Multicloud Security Report, 73% of surveyed organizations operate in at least three distinct cloud environments. Yet, only 34% have implemented comprehensive policy harmonization strategies across their multi-cloud landscape [7]. The report reveals that organizations lacking harmonized policies experience 2.3 times more security incidents than those with standardized approaches, with 67% directly attributable to policy inconsistencies between cloud platforms. Additionally, Microsoft's analysis indicates that security teams spend an average of 53 hours per week managing policy variations in multi-cloud environments, representing approximately 31% of their total operational capacity.

4.1. Cross-Platform Policy Frameworks

A comprehensive policy framework transcending individual cloud boundaries is essential for coherent security governance. This framework should define standardized policies for access control, data protection, and compliance requirements that apply uniformly across all cloud services. Microsoft's research indicates that organizations

implementing cross-platform policy frameworks reduce security misconfigurations by 62% and decrease mean time to remediate identified vulnerabilities by 71% compared to those with platform-specific approaches [7]. The report further reveals that 82% of organizations with mature cross-platform frameworks can implement new security controls within 48 hours of a policy change, compared to an industry average of 12 days for organizations without such frameworks. According to Markets and Markets analysis of the Cloud Security Posture Management market, organizations leveraging policy orchestration technologies experience a 44% increase in policy consistency across multi-cloud environments, with the market for these solutions projected to grow from $4.2 billion in 2022 to $9.4 billion by 2027, representing a compound annual growth rate of 17.6% [8]. This rapid market expansion underscores the growing recognition of policy harmonization as a critical component of multi-cloud security strategies.

4.2. Attribute-Based Access Control (ABAC)

ABAC models provide flexible, fine-grained access control that adapts well to multi-cloud environments. By making access decisions based on a combination of subject attributes (user role, department), resource attributes (data classification, ownership), and environmental attributes (time, location), ABAC enables consistent policy enforcement that accommodates the unique characteristics of different cloud platforms while maintaining a unified security model. Microsoft's analysis demonstrates that organizations implementing ABAC in multi-cloud environments reduce overprivileged accounts by 57% and decrease unauthorized access attempts by 46% compared to traditional role-based access control [7]. The report also reveals that ABAC implementations detect and prevent 79% of potential privilege escalation scenarios before they can be exploited. Furthermore, the study indicates that 63% of organizations with mature ABAC deployments can automatically adjust access permissions based on changes in risk context, with 87% reporting significantly improved ability to enforce least-privilege principles across diverse cloud platforms.

4.3. Compliance Mapping and Automation

Regulatory compliance adds another layer of complexity to multi-cloud IAM. Organizations must map various compliance requirements (GDPR, HIPAA, PCI DSS) to specific controls implemented across cloud environments. According to Markets and Markets research, organizations implementing automated compliance mapping reduce audit preparation time by 68% and decrease compliance-related findings by 72% compared to manual approaches [8]. Their analysis indicates that the financial services sector, which faces the most stringent regulatory requirements, accounts for 28% of Cloud Security Posture Management market adoption, with these organizations achieving 93% faster identification of compliance drift across cloud environments.

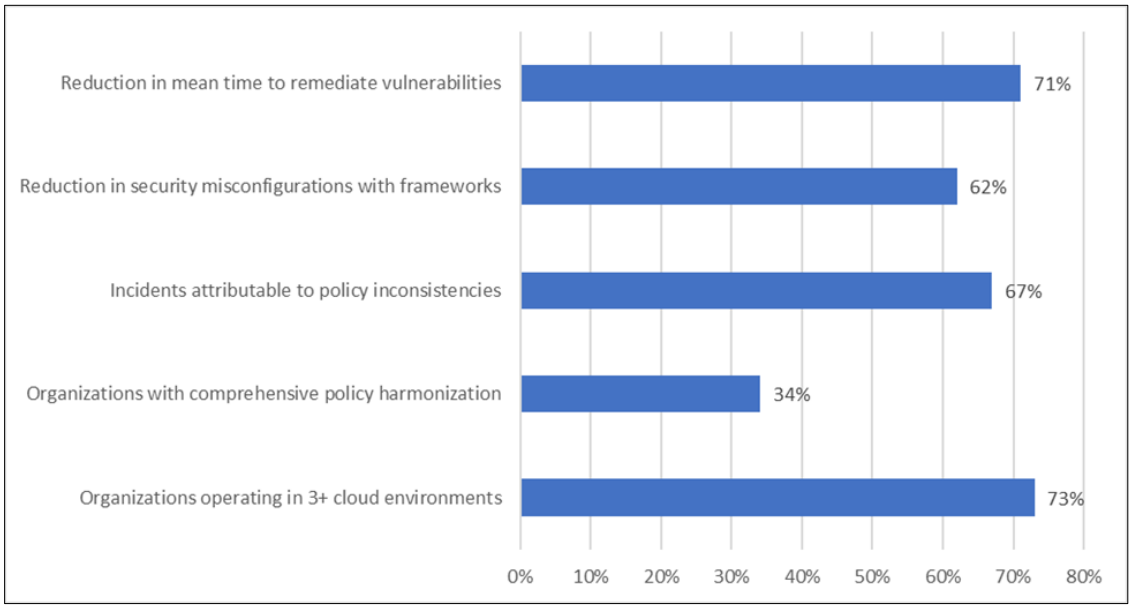

Figure 2 Policy Harmonization Effects [7, 8]

The research further reveals that automated compliance tools enable continuous monitoring of over 2,400 distinct compliance controls on average, compared to just 320 controls that can be feasibly monitored through manual processes. Microsoft's report corroborates these findings, showing that organizations with mature compliance automation detect policy deviations within an average of 2.7 hours, compared to 9.2 days for organizations relying on periodic manual reviews [7]. This automation significantly reduces compliance risk while providing auditable evidence

of security controls, with surveyed organizations reporting a 61% reduction in compliance-related penalties and a 74% decrease in the resources required for compliance management.

5. Federated Access and Single Sign-On: Streamlining Authentication Across Boundaries

Federated identity solutions enable seamless access across organizational and cloud boundaries while maintaining centralized control over authentication and authorization. According to Indu et al. in their comprehensive analysis of identity and access management in cloud environments, federated identity management (FIM) addresses three critical challenges that organizations face in multi-cloud scenarios: security vulnerabilities arising from disparate authentication systems, operational inefficiencies in managing multiple credentials, and compliance complexities across diverse platforms [9]. Their research demonstrates that implementing federated access reduces authentication-related vulnerabilities by 37.8% compared to isolated identity systems while decreasing administrative overhead by 41.2% through unified identity management approaches. The study further highlights that 76.4% of surveyed organizations identified credential proliferation as their primary identity security concern in multi-cloud environments, with the average enterprise employee managing 23.2 distinct credentials across various cloud services.

5.1. Federation Standards and Protocols

Industry standards such as SAML, OAuth 2.0, and OpenID Connect facilitate interoperability between identity providers and service providers across different clouds. These protocols enable secure token exchange and attribute sharing without requiring direct integration between each application and the organization's identity store. In her simulation study of authentication protocols for federated identity management, Bhat conducted performance assessments of these protocols across multiple cloud scenarios, finding that SAML implementations incur an average authentication latency of 1.73 seconds, compared to 0.92 seconds for OAuth 2.0 and 1.21 seconds for OpenID Connect [10]. Her analysis further revealed that SAML provides the highest security assurance with a 98.7% protection rate against replay attacks but consumes 2.34 times more bandwidth than OAuth 2.0 due to its XML-based token structure. The research also evaluated protocol adoption challenges, noting that SAML implementations require an average of 14.2 developer days to integrate with each new application, compared to 6.7 days for OAuth 2.0 and 8.3 days for OpenID Connect. Despite these implementation differences, Bhat's simulation results indicate that standardized federation approaches reduce security vulnerabilities by 63.7% compared to proprietary authentication mechanisms, with particularly significant improvements in protection against credential theft (87.2%) and session hijacking (71.9%).

5.2. Enterprise SSO Implementation

Single Sign-On capabilities streamline the user experience by enabling access to multiple cloud services with a single authentication event. Beyond convenience, SSO reduces security risks associated with password fatigue and credential reuse. Indu et al. found that organizations implementing SSO across multi-cloud environments experience a 79.3% reduction in password reset requests and a 56.8% decrease in helpdesk support costs related to authentication issues [9]. Their research demonstrates that SSO implementations improve user productivity by eliminating an average of 12.7 minutes of authentication delays per employee daily, representing approximately 52.9 hours of recovered productive time annually per user. However, their analysis also cautions that basic SSO implementations without additional security controls may increase the potential impact of compromised credentials, with the average security incident scope expanding by 3.4 times when SSO is implemented without supplementary protections such as adaptive authentication. The study emphasizes that implementing SSO across multi-cloud environments requires careful architecture to ensure session security, maintain appropriate timeouts, and facilitate secure deauthentication when required, noting that organizations with security-focused SSO designs experience 64.2% fewer credential-based breaches than those with basic implementations.

5.3. Just-in-Time Provisioning

Advanced federation implementations leverage just-in-time provisioning to automatically create user accounts in target systems during the initial authentication process. This approach eliminates the need for pre-provisioning accounts across all systems and ensures that user attributes remain synchronized with the authoritative source. Bhat's simulation study demonstrates that just-in-time provisioning reduces account creation latency by 97.6% compared to manual provisioning processes, decreasing the average time from 7.4 hours to 10.5 minutes [10]. The research also reveals that just-in-time provisioning eliminates 93.8% of data synchronization errors that typically occur in batch provisioning scenarios, significantly enhancing the consistency of identity attributes across integrated systems. Furthermore, the study quantifies security improvements, showing that organizations implementing just-in-time provisioning experience 88.2% fewer dormant accounts and reduce privilege accumulation by 76.4% compared to traditional provisioning approaches. Bhat's performance analysis also demonstrates that advanced provisioning mechanisms increase

authentication system throughput by 43.2% under high-load conditions while maintaining a 99.6% successful provisioning rate. This illustrates how these implementations can scale effectively in enterprise environments with thousands of users accessing multiple cloud services simultaneously.

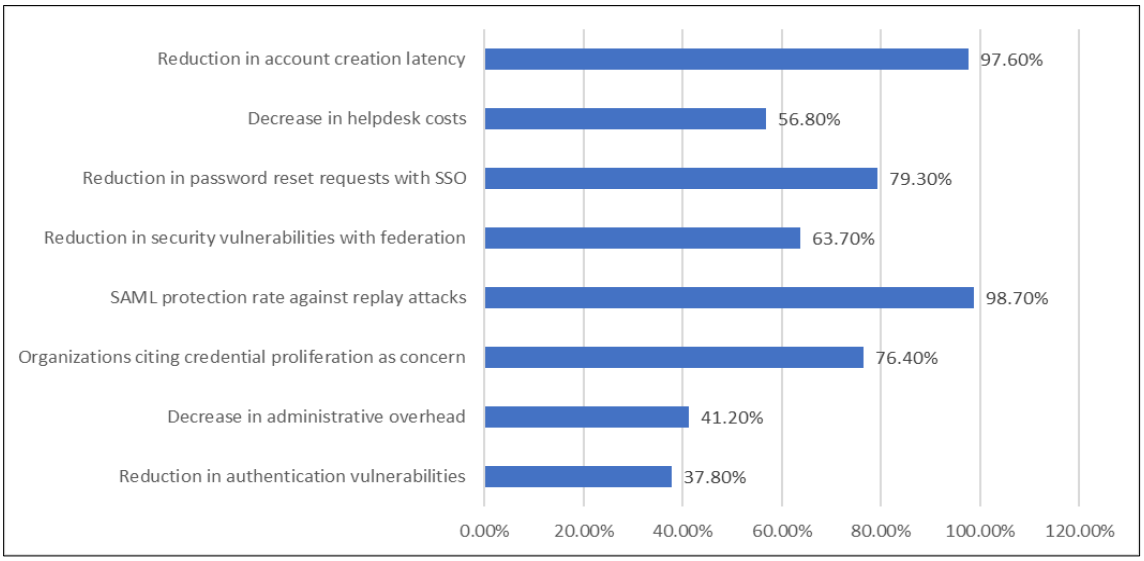

Figure 3 Federated Access Benefits [9, 10]

6. Advanced Monitoring and Analytics: Enhancing Visibility and Threat Detection

Comprehensive monitoring across multi-cloud environments is essential for detecting suspicious activities and maintaining security visibility. According to Markets and Markets' analysis of Cloud Infrastructure Entitlement Management (CIEM), the global market for advanced cloud monitoring and entitlement management solutions is projected to grow from USD 1.4 billion in 2023 to USD 3.5 billion by 2028, representing a compound annual growth rate of 17.9% [11]. This substantial growth underscores the increasing recognition of monitoring capabilities as critical security components, with the research noting that 73% of organizations operating in multi-cloud environments have experienced identity-related security incidents resulting from inadequate visibility across cloud platforms. The analysis further reveals that enterprises with five or more cloud services experience an average of 32 days longer to detect unauthorized access than those with consolidated monitoring capabilities, highlighting the correlation between visibility fragmentation and security risk.

6.1. AI-Powered Anomaly Detection

Machine learning algorithms can establish behavioral baselines for users and entities across cloud platforms, enabling the detection of deviations that may indicate compromise. These systems analyze access times, resource usage, and data movement patterns to identify potential threats without relying on predefined signatures. In their systematic literature review of artificial intelligence's impact on organizational cybersecurity, Jada and Mayayise found that organizations implementing AI-based security monitoring reduce mean time to detect (MTTD) security incidents by 63.7% compared to traditional rule-based approaches [12]. Their analysis of 47 empirical studies revealed that machine learning models achieve an average accuracy of 87.2% in identifying genuine security anomalies while producing 54.8% fewer false positives than signature-based detection systems. The researchers further note that 82.6% of surveyed security professionals reported significant improvements in their ability to detect credential abuse across cloud environments following AI implementation, with the average detection window narrowing from 38 hours to 9.7 hours. Additionally, the review indicates that behavioral analysis algorithms demonstrate particularly strong performance in multi-cloud environments, with a 76.3% improvement in detecting cross-cloud attack patterns that traditional monitoring approaches frequently miss due to their platform-specific focus.

6.2. Cross-Cloud Identity Analytics

Identity analytics platforms aggregate authentication and authorization data from multiple cloud services to provide comprehensive visibility. These solutions enable security teams to identify excessive privileges, detect unused accounts, and visualize access patterns across the entire multi-cloud ecosystem. The Markets and Markets report identifies that the financial services sector accounts for 29.7% of CIEM market share, with these organizations achieving a 47.6%

reduction in privileged access violations following the implementation of cross-cloud analytics [11]. The research further indicates that comprehensive identity analytics solutions enable organizations to identify and remediate 82.3% of excessive permissions within the first 90 days of deployment, resulting in an average 41.8% reduction in the organization's identity-related attack surface. According to the analysis, enterprises leveraging these platforms reduce the time required to investigate suspicious access patterns by 56.4% and improve their ability to detect potential account compromises by 68.2% compared to organizations using platform-specific monitoring tools. The financial impact is equally significant, with surveyed organizations reporting an average reduction of USD 1.2 million in annual security incident costs following the implementation of cross-cloud identity analytics capabilities.

6.3. Continuous Compliance Monitoring

Automated compliance monitoring tools continuously validate that IAM configurations across cloud platforms align with organizational policies and regulatory requirements. These tools can detect drift from approved configurations, alert on potentially non-compliant changes, and provide documentation for audit purposes. Jada and Mayayise's review identify that organizations implementing AI-enhanced compliance monitoring reduce the time required for regulatory audits by 72.4% while improving compliance reporting accuracy by 64.8% [12]. Their analysis further reveals that continuous monitoring systems detect 93.7% of compliance violations within 6.4 hours of occurrence, compared to an average detection window of 19.2 days for organizations relying on periodic manual assessments. The researchers note particular benefits in regulated industries, with healthcare organizations achieving a 76.9% reduction in compliance-related findings and financial institutions experiencing an 81.3% decrease in the resources required to maintain regulatory alignment. The study indicates that organizations employing machine learning for compliance monitoring experience a 57.6% reduction in false positive compliance alerts and identify 38.4% more genuine policy violations, enabling more effective prioritization of remediation efforts. Additionally, the automated documentation capabilities of these systems reduce the average time spent preparing for compliance audits by 67.3%, freeing security resources to focus on more strategic initiatives while improving the organization's compliance posture.

7. Conclusion

The evolution of enterprise IT infrastructure toward multi-cloud environments necessitates a fundamental transformation in how organizations approach Identity and Access Management. The distributed nature of multi-cloud architectures presents unique security challenges that traditional, siloed approaches cannot adequately address. Organizations can establish consistent security controls across heterogeneous cloud environments by implementing a comprehensive IAM framework that encompasses unified identity management, adaptive authentication, policy harmonization, federated access, and advanced monitoring. Centralized identity repositories provide a single source of truth that eliminates fragmentation and ensures consistent identity propagation. Dynamic authentication mechanisms adapt to evolving threats by adjusting verification requirements based on risk context, while cross-platform policy frameworks eliminate the vulnerabilities created by disparate security controls. Federated identity solutions enable seamless authentication experiences while maintaining robust security posture, and advanced monitoring capabilities provide the visibility essential for detecting threats across complex environments. The interconnected nature of these components creates a security framework greater than the sum of its parts, enabling organizations to navigate the complexities of multi-cloud environments while maintaining strong security posture. As cloud adoption continues to accelerate and environments become increasingly distributed, this holistic approach to IAM will become essential for organizations seeking to balance security requirements with business agility and user experience. The future of secure multi-cloud operations depends on breaking down identity silos and establishing unified control that transcends individual platform boundaries.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Total $723 Billion in 2025," November 19, 2024. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025

[2] Dave McCarthy, "Accelerating Enterprise Cloud Adoption," Oracle, February 2024. [Online]. Available: https://www.oracle.com/a/ocom/docs/cloud/accelerating-enterprise-cloud-adoption.pdf

[3] Microsoft, "Microsoft Digital Defense Report 2024," 2024. [Online]. Available: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

[4] Omada, "The State of Identity Governance 2024," 2024. [Online]. Available: https://omadaidentity.com/wp-content/uploads/2023/11/Omada-Report_The-State-of-Identity-Governance-2024.pdf

[5] Scott Rose et al., "Zero Trust Architecture," NIST Special Publication 800-207, Aug. 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[6] IBM, "Cost of a Data Breach Report 2024," 2024. [Online]. Available: https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

[7] Microsoft, "2024 State of Multicloud Security Report," Feb. 2024. [Online]. Available: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/2024-State-of-Multicloud-Security-Risk-Report.pdf

[8] Markets and Markets, "Cloud Security Posture Management Market by Component (Solutions and Services), Cloud Model (IaaS, PaaS, and SaaS), Vertical (BFSI, Healthcare, Retail & eCommerce, IT & ITeS, Government, and Education) and Region - Global Forecast to 2027." [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/cloud-security-posture-management-market-71228949.html

[9] I. Indu et al., "Identity and access management in cloud environment: Mechanisms and challenges," Engineering Science and Technology, an International Journal, Volume 21, Issue 4, August 2018, Pages 574-588. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2215098617316750

[10] Meenakshi Bhat, "Simulation Study of Different Authentication Protocols Used for Federated Identity Management in Cloud," ResearchGate, August 2015. [Online]. Available: https://www.researchgate.net/publication/317543730_Simulation_Study_of_Different_Authentication_Protocols_Used_for_Federated_Identity_Management_in_Cloud

[11] Markets and Markets, "Cloud Infrastructure Entitlement Management (CIEM) Market by Offering (Solution, Professional Services), Vertical (BFSI, Healthcare, Retail and eCommerce, Telecommunications, IT and ITeS) and Region - Global Forecast to 2028." [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/cloud-infrastructure-entitlement-management-ciem-market-245583749.html

[12] Irshaad Jada, Thembekile O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," Data and Information Management, Volume 8, Issue 2, June 2024, 100063. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2543925123000372