International Journal of Multidisciplinary Research and Growth Evaluation.

Identity and Access Management in Cloud Storage: A Comprehensive Guide

Joy Ezinwanneamaka Ike [1*], Joseph Darko Kessie [2], Henry Emenike Okaro [3], Enuma Ezeife [4], Tolulope Onibokun [5]
[1] Ahmadu Bello University, Nigeria
[2] Eastern Illinois University, USA
[3] University at Buffalo State University of New York, USA
[4] Ernst & Young, USA
[5] University of Ibadan, Nigeria

* Corresponding Author: **Joy Ezinwanneamaka Ike**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 02
March-April 2025
Received: 13-01-2025
Accepted: 14-02-2025
Page No: 245-252

Abstract
With the growing adoption of cloud storage, ensuring data security and regulatory compliance has become a critical challenge for organizations. Identity and Access Management (IAM) plays a fundamental role in protecting cloud-based resources by providing authentication, authorization, and monitoring capabilities. This comprehensive guide explores the key principles, technologies, and best practices of IAM in cloud storage environments, addressing modern security threats and compliance requirements. The review outlines core IAM components, including Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Multi-Factor Authentication (MFA), which enhance access security. Additionally, it discusses identity federation mechanisms such as OAuth, OpenID Connect, and SAML, which facilitate secure authentication across multiple cloud platforms. Given the increasing sophistication of cyber threats, we highlight the integration of Artificial Intelligence (AI) and Machine Learning (ML) into IAM systems for adaptive authentication, anomaly detection, and automated policy management. A comparative analysis of leading cloud IAM solutions from providers such as AWS, Microsoft Azure, and Google Cloud is presented, focusing on their security features and implementation strategies. Moreover, the review addresses compliance challenges, including GDPR, HIPAA, and ISO 27001, and offers best practices for maintaining IAM governance in multi-cloud environments. This emphasizes the importance of Zero Trust Architecture (ZTA), a security model that ensures continuous verification and least-privilege access to minimize risks. Future directions in IAM development, including blockchain-based identity management and AI-driven risk assessments, are also explored. By providing a structured approach to implementing IAM in cloud storage, this guide aims to help organizations strengthen security, mitigate unauthorized access risks, and enhance operational efficiency in cloud environments.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.2.245-252

Keywords: Identity and Access Management, Cloud Security, Authentication, Authorization, Zero Trust Architecture, Multi-Factor Authentication, AI-driven IAM

1. Introduction

Cloud storage has revolutionized how organizations and individuals store, manage, and access data (Nidamanuri, 2022) [33]. Unlike traditional on-premises storage solutions, cloud storage offers scalability, flexibility, and cost-effectiveness, allowing users to store vast amounts of data while accessing it from any location. With the rise of big data, Internet of Things (IoT), and artificial intelligence (AI), cloud storage has become a critical infrastructure for modern computing (Belgaum *et al*., 2021) [7]. Major cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud offer cloud storage

Solutions that enable enterprises to efficiently manage workloads, ensure data availability, and optimize operational costs. However, while cloud storage provides numerous advantages, it also introduces significant security challenges (Tabrizchi and Kuchaki, 2020) [47]. Data stored in the cloud is often shared across multiple users and accessed remotely, increasing the risk of unauthorized access, data breaches, and cyberattacks. Therefore, implementing robust security mechanisms is essential to safeguard sensitive data and ensure compliance with regulatory frameworks such as GDPR, HIPAA, and ISO 27001.

One of the most critical components of cloud security is Identity and Access Management (IAM). IAM ensures that only authorized users and devices have access to cloud-stored data, enforcing security policies through authentication, authorization, and role-based access control (RBAC) (Dhanalakshmi and George, 2023) [13]. Effective IAM solutions incorporate multi-factor authentication (MFA), least privilege access, and continuous monitoring to detect anomalies and prevent unauthorized data access. Cloud service providers offer IAM frameworks to enhance security. Integrating IAM with AI-driven anomaly detection further strengthens security by identifying unusual login behaviors, privilege escalation attempts, and insider threats. Despite advancements in IAM and encryption technologies, securing cloud storage presents several challenges. Cybercriminals exploit weak authentication mechanisms and misconfigured cloud settings to gain unauthorized access to sensitive data. Compromised credentials and insider threats pose additional risks. While encryption protects stored data, managing encryption keys securely remains a challenge. Poor key management practices, such as storing keys alongside encrypted data, can lead to security vulnerabilities. Organizations must comply with data protection laws that impose strict requirements on data storage, access control, and audit logging (Labadie and Legner, 2023) [24]. Meeting compliance standards while maintaining operational efficiency is a complex task. As organizations grow, managing IAM policies for thousands of users and devices becomes challenging. Manual access control updates lead to misconfigurations, creating potential security loopholes. Attackers use sophisticated techniques such as phishing, credential stuffing, and privilege escalation to bypass traditional security measures (Kaur *et al*., 2023) [21]. Insiders with legitimate access can also pose security risks by misusing privileges.

This review aims to explore modern approaches to securing cloud storage, focusing on IAM, AI-driven security mechanisms, and encryption strategies. Examine IAM frameworks used by major cloud providers and their role in enhancing access control. Analyze AI-driven security models, including anomaly detection, behavior analytics, and automated policy enforcement. Evaluate encryption methodologies, such as homomorphic encryption and attribute-based encryption (ABE), in protecting cloud-stored data (Alemami *et al*., 2023) [3]. Identify challenges and future directions in securing large-scale cloud environments. By addressing these aspects, this review will provide insights into best practices, security frameworks, and emerging technologies that can strengthen cloud storage security while ensuring data privacy, compliance, and operational efficiency.

2. Methodology

The PRISMA methodology was applied to systematically review Identity and Access Management (IAM) in cloud storage, ensuring a transparent and reproducible research process. The study followed four main phases: identification, screening, eligibility, and inclusion.

During the identification phase, an extensive search was conducted using databases such as IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar. Keywords and phrases such as "Identity and Access Management in Cloud Storage," "Cloud Security and IAM," "Multi-Factor Authentication in Cloud Environments," and "AI-driven IAM Solutions" were used to retrieve relevant studies. Boolean operators (AND, OR) were employed to refine searches, and filters were applied to limit results to peer-reviewed journal articles, conference papers, and authoritative reports published between 2015 and 2024.

In the screening phase, duplicate studies were removed, and titles and abstracts were reviewed for relevance. Studies focusing on IAM in non-cloud environments or general cybersecurity without IAM-specific insights were excluded. Full-text reviews were performed on shortlisted papers to assess their alignment with the research objectives.

The eligibility assessment was based on predefined inclusion and exclusion criteria. Studies were included if they provided empirical data, security frameworks, case studies, or comparative analyses on IAM in cloud storage. Exclusion criteria involved studies lacking technical depth, opinion-based articles without validation, or those focusing on outdated IAM models.

The final inclusion phase resulted in a selection of high-quality sources that contributed to understanding IAM frameworks, authentication mechanisms, AI-driven enhancements, and security challenges in cloud storage. The systematic approach ensured a comprehensive review, allowing for an evidence-based discussion on IAM best practices and emerging trends.

2.1 Fundamentals of Identity and Access Management (IAM)

Identity and Access Management (IAM) is a framework of policies, technologies, and processes used to ensure that the right individuals have appropriate access to resources in an organization or cloud environment. IAM systems are crucial for enforcing security, reducing unauthorized access risks, and managing user identities effectively (Atiewi *et al*., 2020) [6]. The core components of IAM include identity governance, authentication, authorization, and auditing. Identity Governance refers to the policies and procedures that regulate user identities, ensuring compliance with security standards and regulatory requirements. Authentication is the process of verifying user identities using credentials such as passwords, biometrics, or multi-factor authentication (MFA). Authorization determines the level of access a verified user has, enforcing permissions based on predefined policies. Auditing and Monitoring track access and user activities, ensuring compliance and detecting potential security threats. The IAM framework is built upon the AAA security model, which consists of Authentication, Authorization, and Accounting. Authentication verifies a user's identity before granting access. This can be achieved using various authentication mechanisms, including single-factor authentication (SFA), multi-factor authentication (MFA), and passwordless authentication techniques such as biometrics and smart cards (Suleski *et al*., 2023) [46]. Authorization ensures that authenticated users can only access resources for which they have permission. Authorization methods include role-based access control (RBAC), attribute-based access control (ABAC), and policy-based access control (PBAC). Accounting involves tracking and logging user activities to maintain security, compliance,

and accountability. It ensures that security incidents can be investigated effectively by providing a record of actions performed by users within an IAM system.

Fig 1: IAM framework

IAM frameworks commonly use Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) to enforce access permissions. RBAC assigns permissions based on predefined roles within an organization. The simplicity and scalability of RBAC make it a widely adopted model in enterprise environments. ABAC extends RBAC by incorporating attributes such as user location, device type, or security clearance level (Ameer *et al*., 2022) [5]. Access decisions in ABAC are made dynamically based on conditions and policies rather than static roles. ABAC offers greater flexibility and granularity in access control compared to RBAC, making it well-suited for complex cloud environments with dynamic access requirements. The Principle of Least Privilege (PoLP) is a fundamental IAM concept that ensures users are granted only the minimal access required to perform their tasks. This reduces security risks associated with excessive privileges, mitigating the impact of potential insider threats or compromised accounts. Zero-Trust Security Model takes PoLP a step further by enforcing a "never trust, always verify" approach to access control. Unlike traditional security models that rely on network perimeters, Zero Trust assumes that all users, devices, and applications are potential threats. It requires continuous authentication, least privilege enforcement, and strict access controls based on real-time risk assessment. Identity and Access Management is a critical component of cybersecurity, ensuring that user identities and access privileges are managed securely. The implementation of AAA principles, RBAC and ABAC models, and security frameworks like PoLP and Zero Trust helps organizations strengthen their access control mechanisms. As cloud environments evolve, IAM frameworks must integrate advanced technologies, such as AI-driven authentication and real-time anomaly detection, to enhance security and adaptability in dynamic digital ecosystems (Julakanti *et al*., 2022) [19].

2.2 IAM technologies and standards for cloud storage

Identity and access management (IAM) technologies and standards play a critical role in securing cloud storage by ensuring that only authorized users and applications can access sensitive data. As cloud environments become more complex and widely adopted, standardized. IAM protocols and technologies are essential to managing authentication, authorization, and identity federation efficiently (Mostafa *et al*., 2023) [4]. Several key IAM technologies, including OAuth, OpenID Connect, Security Assertion Markup Language (SAML), Multi-Factor Authentication (MFA), and Single Sign-On (SSO), contribute to robust cloud security. Additionally, major cloud providers such as AWS, Microsoft Azure, and Google Cloud offer IAM solutions tailored to cloud environments. Furthermore, IAM systems are increasingly integrated with Cloud Access Security Brokers (CASBs) to enhance security, visibility, and compliance in cloud storage environments (Ahmad *et al*., 2022) [2].

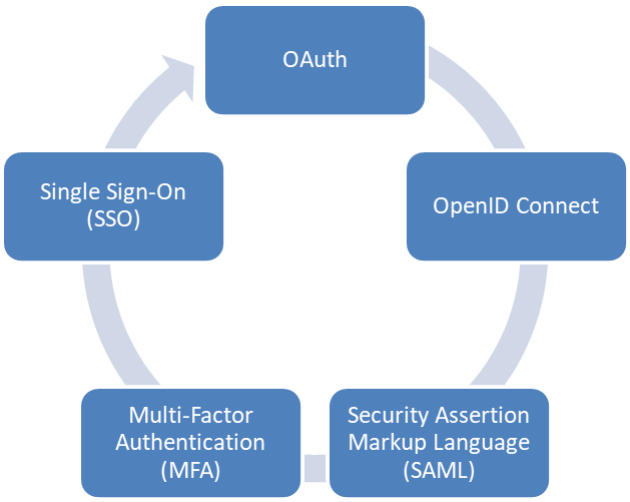

Fig 2: Several key IAM technologies

Identity federation enables users to authenticate across multiple applications and services without maintaining separate credentials for each platform. Three widely used standards for identity federation in cloud IAM are OAuth, OpenID Connect, and SAML. OAuth (Open Authorization) is an open standard that provides secure delegated access to resources without exposing user credentials. OAuth 2.0, the most widely used version, enables users to grant third-party applications limited access to their cloud storage without sharing passwords. This is commonly used in cloud services for authorizing API access. OpenID Connect (OIDC) is an authentication layer built on top of OAuth 2.0. It enables identity verification by issuing JSON Web Tokens (JWTs) that contain user authentication data. OpenID Connect is widely adopted in cloud storage services for securing user logins and access management. SAML (Security Assertion Markup Language) is an XML-based standard that facilitates Single Sign-On (SSO) by exchanging authentication and authorization data between identity providers and cloud service providers (Subbarao *et al*., 2023) [45]. SAML is often used by enterprises for federated identity management, ensuring seamless user authentication across multiple cloud applications.

Multi-Factor Authentication (MFA) enhances IAM security by requiring users to verify their identity using multiple authentication factors. These factors typically include. Something You Know – Passwords or security questions. Something You Have – Hardware tokens, smart cards, or mobile authentication apps. Something You Are – Biometric authentication, such as fingerprint or facial recognition. MFA reduces the risk of unauthorized access, even if user credentials are compromised, making it a fundamental security requirement for cloud storage environments. Single Sign-On (SSO) streamlines authentication by allowing users to log in once and gain access to multiple cloud applications

without re-authenticating. By reducing password fatigue and login redundancies, SSO enhances both security and user experience (Liu *et al*., 2021) [25]. Many cloud service providers integrate SSO with federated identity solutions such as SAML and OpenID Connect to enable seamless access across platforms.

Cloud service providers offer dedicated IAM solutions to enforce access control and security policies. AWS IAM (Identity and Access Management) provides fine-grained access control over AWS resources using policies, roles, and user permissions. It supports MFA, role-based access control (RBAC), and identity federation using SAML and OpenID Connect (Singh *et al*., 2023) [44]. AWS IAM also integrates with AWS Security Token Service (STS) to provide temporary credentials for secure access. Microsoft Azure Active Directory (Azure AD) is a cloud-based IAM solution offering identity federation, SSO, and access management across Microsoft 365, Azure, and third-party applications. It supports conditional access policies, risk-based authentication, and integration with on-premises Active Directory. Google Cloud IAM allows organizations to define and enforce access controls for Google Cloud resources. It supports role-based access management, service accounts for automated workflows, and integration with Google Workspace for identity federation. Google Cloud IAM also offers IAM Conditions, enabling attribute-based access control (ABAC) policies (El Sibai *et al*., 2020) [14].

Cloud Access Security Brokers (CASBs) serve as intermediaries between cloud users and cloud service providers, offering visibility, data protection, and threat prevention. Integrating IAM with CASBs enhances security by enforcing identity-aware access policies, detecting anomalous login activities, and preventing unauthorized access to cloud storage. CASBs leverage IAM capabilities to implement adaptive access controls, such as enforcing MFA when suspicious login attempts are detected (Tayouri *et al*., 2022) [49]. Additionally, CASBs provide real-time monitoring and compliance reporting, helping organizations meet regulatory requirements for cloud data security. IAM technologies and standards are essential for securing cloud storage environments, ensuring that users and applications access data securely and efficiently. OAuth, OpenID Connect, and SAML enable identity federation, while MFA and SSO enhance authentication security and usability. Major cloud providers offer IAM solutions tailored to cloud environments, and the integration of IAM with CASBs further strengthens access control and compliance. As cloud adoption continues to grow, IAM technologies will play a critical role in mitigating security risks, preventing data breaches, and ensuring regulatory compliance in cloud storage security.

2.3 Implementing IAM in cloud storage

Implementing Identity and Access Management (IAM) in cloud storage is essential for ensuring data security, access control, and regulatory compliance. IAM frameworks help organizations manage users, roles, and permissions, preventing unauthorized access and reducing security risks (Devlekar and Ramteke, 2022) [12]. Key aspects of IAM implementation include defining access policies, managing identities through users and service accounts, enforcing access control mechanisms, and securing credentials and encryption keys.

IAM policies define the access rules governing who can access cloud storage resources and what actions they can perform. Cloud service providers, such as AWS, Microsoft Azure, and Google Cloud, use policy-based access control to enforce security restrictions. IAM policies should grant the minimum necessary permissions to users and applications, reducing the risk of unauthorized access (Talluri and Makani, 2023) [48]. Users are assigned roles with predefined permissions, simplifying access management and reducing administrative overhead. Policies enforce access decisions based on user attributes such as department, job role, or security clearance. Organizations can implement conditions such as location, device type, or authentication strength to enforce additional security measures. IAM policies should be regularly reviewed and updated to align with organizational changes and security best practices (Muhammad *et al*., 2022) [31].

Identity management is a core component of IAM, involving the administration of users, groups, and service accounts to ensure secure access to cloud storage. Individual users are assigned unique credentials and permissions based on their role within the organization (Mishra *et al*., 2021) [27]. Users should be required to authenticate using strong passwords and multi-factor authentication (MFA). Grouping users with similar responsibilities simplifies access control. Instead of assigning permissions to each user individually, administrators can grant access at the group level (Paci *et al*., 2018) [36]. Non-human identities, such as applications and automated workflows, use service accounts to authenticate and interact with cloud storage resources securely. Service accounts should be assigned specific roles with limited privileges to minimize security risks. Identity federation, using protocols such as SAML and OpenID Connect, allows organizations to integrate IAM with existing enterprise identity providers, enabling seamless authentication across cloud and on-premises environments.

Implementing strict access control mechanisms ensures that only authorized users and applications can access cloud storage resources. Cloud platforms allow administrators to define roles with specific permissions for accessing storage services such as Amazon S3, Azure Blob Storage, and Google Cloud Storage. Access Control Lists (ACLs), specify granular access permissions at the file or folder level, enabling more precise control over data sharing. Cloud storage providers allow organizations to enforce access restrictions at both the storage bucket and object levels, ensuring that sensitive data is protected from unauthorized access. Organizations can issue temporary access tokens for short-term data access, reducing the risk of credential exposure. By implementing a combination of IAM roles, ACLs, and encryption policies, organizations can effectively secure cloud storage environments while maintaining flexibility in data access (Ovabor and Atkison, 2023) [35].

Protecting authentication credentials, API keys, and encryption keys is critical to preventing unauthorized access and data breaches. Cloud providers offer dedicated key management services (e.g., AWS Secrets Manager, Azure Key Vault, Google Cloud KMS) for storing and managing encryption keys securely. Regularly rotating encryption keys and credentials minimizes the risk of exposure and ensures compliance with security best practices. Organizations should implement logging and monitoring solutions to detect unauthorized access attempts, compromised credentials, or security misconfigurations. Continuous verification of users and devices accessing cloud storage ensures that compromised credentials alone are not sufficient to gain unauthorized access. Effective IAM implementation in cloud storage environments enhances security, minimizes unauthorized access risks, and ensures compliance with data protection regulations (Cinar, 2023) [10]. By setting up well-defined IAM policies, managing identities effectively,

enforcing access control mechanisms, and securing credentials, organizations can safeguard sensitive data in cloud storage. As cloud security threats continue to evolve, IAM strategies must be continuously improved to address emerging challenges and maintain robust protection against unauthorized access (Indu *et al*., 2018; Mohammed, 2019) [17, 19].

2.4 AI and Automation in IAM for cloud security

Identity and Access Management (IAM) is a critical component of cloud security, ensuring that only authorized users and systems can access cloud resources. Traditional IAM systems rely on static rules and predefined access policies, which are often inadequate in detecting sophisticated cyber threats and unauthorized access attempts (Khambam and Kaluvakuri, 2023) [23]. Artificial Intelligence (AI) and automation enhance IAM by providing real-time anomaly detection, risk-based authentication, and automated policy enforcement. Machine learning (ML) techniques enable identity risk scoring, adaptive authentication, and continuous access reviews, strengthening overall cloud security. This explores the role of AI and automation in IAM, highlighting their impact on cloud security.

AI-driven IAM solutions play a crucial role in identifying unauthorized access attempts and security anomalies in cloud environments. Traditional rule-based security mechanisms struggle to detect sophisticated threats, such as credential theft, insider attacks, and account takeovers. AI enhances IAM by continuously monitoring user behaviors and network activity, identifying deviations from normal patterns. Machine learning algorithms analyze vast amounts of authentication and access log data to establish baseline behavior for each user. When an access request deviates from this baseline such as logging in from an unusual location, using an unfamiliar device, or attempting to access sensitive data at abnormal times AI-driven IAM systems trigger alerts or enforce additional authentication steps. Credential stuffing attacks, where attackers use stolen credentials from data breaches to gain unauthorized access (Zhang, 2021) [50]. Insider threats, where employees attempt to access or modify sensitive data beyond their permissions. Privilege escalation attempts, where users try to gain higher access rights without authorization. By leveraging AI for anomaly detection, organizations can identify security threats in real time, reducing the risk of data breaches and unauthorized access (Aggarwal *et al*., 2023) [1].

AI enhances IAM by implementing identity risk scoring, a method that assesses the likelihood of an access request being malicious based on multiple risk factors. Machine learning models evaluate various parameters, such as. User behavior patterns, frequency, location, and timing of access requests. Device reputation, whether the device used for authentication has a history of suspicious activity (Sikder *et al*., 2021) [43]. Network and IP address, assessing if login attempts originate from high-risk geolocations or anonymized networks (e.g., VPNs, TOR). Historical attack patterns, correlating authentication attempts with known attack signatures. Each access attempt is assigned a risk score, which determines the required authentication actions. Low-risk requests allow seamless access, while high-risk attempts trigger step-up authentication (e.g., Multi-Factor Authentication) or are blocked outright. However, if the same credentials are used to log in from a foreign country minutes later, the risk score increases significantly, prompting additional authentication checks or denying access (Conners *et al*., 2022) [11].

Traditional IAM systems require manual policy configuration and periodic access reviews, which are labor-intensive and prone to errors. AI and automation streamline these processes by enabling dynamic policy enforcement and automated access reviews. IAM compliance requires regular access reviews to ensure that users only have necessary permissions (Schrimpf *et al*., 2021) [40]. AI-driven automation simplifies this by. Generating automated reports on access rights and privilege changes. Identifying and revoking dormant accounts to minimize attack surfaces. Cross-referencing access patterns with organizational policies to detect unauthorized privilege escalations (Boi *et al*., 2023) [8]. This proactive approach reduces the burden on IT administrators, ensures compliance with regulatory frameworks, and minimizes security gaps.

Traditional authentication methods rely on static credentials, which can be easily compromised. AI-driven adaptive authentication enhances IAM by dynamically adjusting authentication requirements based on real-time risk assessments. Behavioral analytics uses AI to continuously learn and analyze user behaviors, detecting subtle anomalies that might indicate unauthorized access (Shaik *et al*., 2023) [41]. AI and automation have transformed IAM for cloud security by enhancing unauthorized access detection, implementing machine learning-based identity risk scoring, automating policy enforcement, and enabling adaptive authentication. AI-driven IAM systems proactively identify security threats, dynamically adjust access controls, and reduce the administrative burden associated with traditional IAM management. As cloud environments continue to grow in complexity, AI-powered IAM solutions will play an increasingly vital role in securing sensitive data and ensuring regulatory compliance. Future advancements in AI-driven IAM will further improve cloud security, providing real-time threat mitigation and seamless user experiences.

2.5 Compliance and regulatory considerations

In today's digital landscape, organizations must adhere to stringent regulatory frameworks to ensure data protection, privacy, and security. Three key compliance frameworks that significantly impact Identity and Access Management (IAM) are the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and ISO 27001. The GDPR, enacted by the European Union, establishes strict guidelines for the collection, storage, and processing of personal data. Organizations handling EU citizens' data must implement IAM controls, such as role-based access control (RBAC), multi-factor authentication (MFA), and data minimization techniques (Katari and Ankam, 2022) [20]. Compliance with GDPR requires maintaining user consent records and providing mechanisms for data subject rights, such as the right to erasure and data portability. HIPAA is a U.S. regulation that protects the privacy and security of healthcare information. Covered entities and business associates must implement IAM solutions that include access control, authentication, and audit trails to prevent unauthorized access to Protected Health Information (PHI). IAM systems must also support automatic logoff, encryption, and secure authentication to ensure compliance. This international standard outlines best practices for Information Security Management Systems (ISMS). Organizations seeking ISO 27001 certification must implement strong IAM policies, ensuring that user access is granted based on the principle of least privilege (PoLP). IAM solutions should support continuous monitoring, access reviews, and authentication measures to maintain compliance with ISO 27001 (Podugu *et al*., 2023) [37].

Auditability and accountability are crucial components of

IAM, ensuring that organizations can track and verify all access-related activities. A well-structured IAM system enables organizations to log, monitor, and review user access to sensitive information. Effective IAM solutions generate detailed audit logs that capture access attempts, failed logins, and privilege escalations. These logs should be stored securely and analyzed using Security Information and Event Management (SIEM) tools to detect anomalies and unauthorized access attempts. Periodic access reviews ensure that users have appropriate permissions and that unauthorized accounts are promptly revoked. Organizations should implement automated certification processes to streamline access validation. IAM systems should enforce stringent identity lifecycle policies, including user provisioning, de-provisioning, and role modifications (Jasper *et al*., 2023) [18]. Organizations must maintain accountability by assigning ownership to access permissions and implementing segregation of duties (SoD) policies.

Organizations can enhance IAM governance and compliance by adopting best practices that align with regulatory requirements and industry standards. Users should only have the minimum necessary permissions to perform their job functions. Implementing role-based access control (RBAC) and attribute-based access control (ABAC) helps enforce this principle. Multi-Factor Authentication (MFA), adds an extra layer of security by requiring users to verify their identity using multiple authentication factors, such as passwords, biometrics, or hardware tokens (Mohammed *et al*., 2023) [28]. This practice reduces the risk of unauthorized access. Organizations should conduct periodic penetration testing and vulnerability assessments to identify IAM weaknesses. Compliance audits should be performed to ensure adherence to regulatory frameworks. Automating user provisioning and de-provisioning minimizes human errors and ensures timely access revocation for departing employees or role changes. Organizations must establish a well-defined incident response plan to address IAM-related security breaches (Nahar and Gill, 2022) [32]. This includes prompt identification, containment, investigation, and remediation of access-related threats. By implementing these best practices, organizations can achieve robust IAM governance while maintaining compliance with regulatory standards, ensuring data security, accountability, and effective access control (Nookala, 2020) [34].

2.6 Challenges and best practices in IAM for cloud storage

Introduction identity and access management (IAM) plays a critical role in securing cloud storage by regulating user permissions, authentication, and access control mechanisms (Alsirhani *et al*., 2022) [4]. As organizations increasingly adopt multi-cloud environments, IAM complexities grow, presenting challenges in security, compliance, and operational efficiency. This explores common IAM misconfigurations, best practices for implementation in multi-cloud environments, strategies for IAM lifecycle management, and future trends in IAM for cloud security. Common IAM Misconfigurations and Security Risks Several misconfigurations in IAM can expose cloud storage to significant security risks. Some of the most common issues include. Assigning excessive permissions to users and applications increases the attack surface and risks unauthorized data exposure (Hammi *et al*., 2022) [16]. Failure to implement multi-factor authentication (MFA) makes it easier for attackers to exploit compromised credentials. Improperly defined roles result in users having more privileges than necessary, increasing the potential for insider threats. Misconfigured IAM policies may unintentionally allow public access to sensitive cloud storage resources. Without proper logging, security teams lack visibility into access patterns, making it difficult to detect unauthorized activities (Sharma, 2021) [42]. Failure to rotate API keys and credentials regularly heightens the risk of credential theft and misuse. Best Practices for IAM Implementation in Multi-Cloud Environments. To ensure robust IAM security across multi-cloud environments, organizations should adopt the following best practices. Restrict user and application permissions to the minimum necessary for their tasks. Enable MFA and use modern authentication protocols such as OAuth 2.0 and SAML. Utilize centralized IAM solutions such as AWS IAM, Google Cloud IAM, or Azure AD to streamline identity management across cloud platforms. Conduct frequent access reviews and enforce compliance with security policies. Implement conditional access rules based on device health, location, and risk levels to enhance security (Michael and Sarah, 2019) [26]. Deploy identity governance solutions to automate provisioning, deprovisioning, and access reviews.

Strategies for IAM lifecycle management and periodic reviews a well-defined IAM lifecycle management strategy is essential to maintain security and compliance in cloud environments. Key strategies include; Automate user onboarding and offboarding to prevent orphaned accounts. Conduct regular reviews to ensure that users retain only the permissions necessary for their roles. Enforce periodic password and API key rotations to mitigate credential theft risks. Utilize cloud-native logging tools such as AWS CloudTrail and Azure Monitor to track access patterns and detect anomalies (Saad *et al*., 2020) [39]. Implement fine-grained access controls to enhance security posture.

Future Trends in IAM for Cloud Security IAM continues to evolve as cloud security challenges intensify. Emerging trends shaping the future of IAM include, Zero trust architecture (ZTA), a shift towards continuous verification of identities, ensuring no implicit trust. AI-driven anomaly detection and automated identity governance enhance IAM security. Blockchain-based identity solutions provide enhanced privacy and security. Adoption of biometric and hardware-based authentication methods to reduce reliance on passwords (Khalil *et al*., 2022) [22]. Advanced IAM frameworks designed to seamlessly integrate across hybrid and multi-cloud environments.

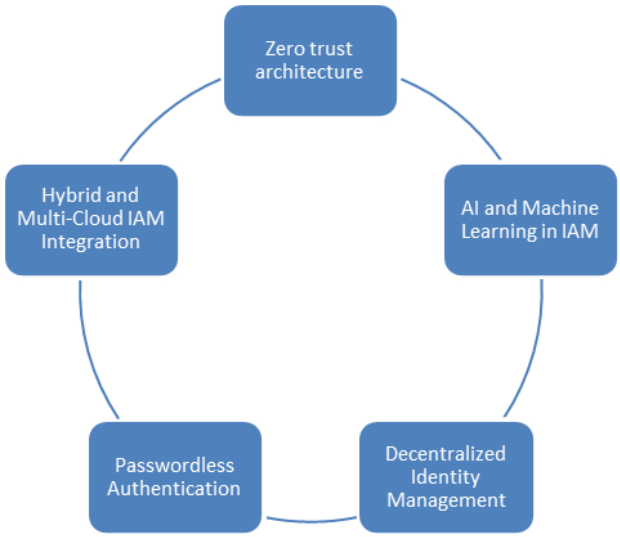

Fig 3: Future Trends in IAM for Cloud Security

IAM is a fundamental component of cloud security, and its effective implementation is critical for protecting sensitive data. Organizations must address common IAM misconfigurations, enforce best practices in multi-cloud environments, and adopt robust lifecycle management strategies (Gade, 2022; Reece *et al*., 2023) [15, 38]. With the emergence of AI, Zero Trust, and decentralized identity solutions, the future of IAM in cloud security promises enhanced protection and efficiency. A proactive approach to IAM governance will be key to mitigating risks and ensuring resilient cloud security in the evolving digital landscape (Chisty *et al*., 2022) [9].

3. Conclusion

Identity and access management (IAM) plays a crucial role in securing cloud storage by ensuring that only authorized users and systems can access sensitive data. IAM frameworks provide organizations with centralized authentication, authorization, and access control mechanisms, mitigating risks associated with unauthorized access, data breaches, and insider threats. By implementing robust IAM policies, enterprises can enforce least privilege principles, monitor user activities, and respond to security incidents effectively.

For organizations adopting IAM for cloud security, several key takeaways emerge. First, a well-structured IAM strategy should incorporate multi-factor authentication (MFA), role-based access control (RBAC), and continuous monitoring to enhance security posture. Second, automated identity lifecycle management ensures timely access provisioning and deprovisioning, reducing the risk of stale or orphaned accounts. Third, organizations must integrate IAM with compliance frameworks to meet regulatory requirements and industry best practices. Lastly, fostering a security-first culture and conducting regular access audits are essential for maintaining IAM effectiveness.

Looking ahead, IAM will continue evolving to address emerging challenges in cloud security. Advancements in artificial intelligence (AI) and machine learning (ML) will enable adaptive authentication, detecting and mitigating anomalies in real time. The rise of decentralized identity management, based on blockchain technology, could enhance security and privacy by reducing reliance on central authorities. Additionally, the adoption of passwordless authentication and zero-trust architectures will further strengthen cloud security by minimizing credential-based attacks. As cloud environments become more complex, organizations must stay proactive in integrating IAM innovations to safeguard their data and infrastructure effectively.

IAM remains a foundational component of cloud security, offering comprehensive protection against access-related threats. By embracing emerging IAM technologies and best practices, organizations can enhance their resilience against evolving cyber risks in the digital era.

4. Reference

1. Aggarwal D, Sharma D, Saxena AB. Role of AI in cyber security through anomaly detection and predictive analysis. Journal of Informatics Education and Research. 2023;3(2).
2. Ahmad S, Mehfuz S, Mebarek-Oudina F, Beg J. RSM analysis-based cloud access security broker: A systematic literature review. Cluster Computing. 2022;25(5):3733–63.
3. Alemami Y, Al-Ghonmein AM, Al-Moghrabi KG, Mohamed MA. Cloud data security and various cryptographic algorithms. International Journal of Electrical and Computer Engineering. 2023;13(2):1867.
4. Alsirhani A, Ezz M, Mostafa AM. Advanced authentication mechanisms for identity and access management in cloud computing. Computer Systems Science & Engineering. 2022;43(3).
5. Ameer S, Benson J, Sandhu R. Hybrid approaches (ABAC and RBAC) toward secure access control in smart home IoT. IEEE Transactions on Dependable and Secure Computing. 2022;20(5):4032–51.
6. Atiewi S, Al-Rahayfeh A, Almiani M, Yussof S, Alfandi O, Abugabah A, Jararweh Y. Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography. IEEE Access. 2020;8:113498–511.
7. Belgaum MR, Alansari Z, Musa S, Alam MM, Mazliham MS. Role of artificial intelligence in cloud computing, IoT, and SDN: Reliability and scalability issues. International Journal of Electrical and Computer Engineering. 2021;11(5):4458.
8. Boi B, Gupta T, Rinhel M, Jubea I, Khondoker R, Esposito C, Sousa BM. Strengthening automotive cybersecurity: A comparative analysis of ISO/SAE 21434-compliant automatic collision notification (ACN) systems. Vehicles. 2023;5(4):1760–802.
9. Chisty NMA, Baddam PR, Amin R. Strategic approaches to safeguarding the digital future: Insights into next-generation cybersecurity. Engineering International. 2022;10(2):69–84.
10. Cinar B. The role of cloud service brokers: Enhancing security and compliance in multi-cloud environments. Journal of Engineering Research and Reports. 2023;25(10):1–11.
11. Conners J, Devenport C, Derbidge S, Farnsworth N, Gates K, Lambert S, McClain C, Nichols P, Zappala D. Let's authenticate: Automated certificates for user authentication. In: Network and Distributed Systems Security Symposium (NDSS). 2022 Jan.
12. Devlekar S, Ramteke V. Identity and access management: High-level conceptual framework. Cardiometry. 2022;(24):393–9.
13. Dhanalakshmi G, George GVS. Secure and privacy-preserving storage of e-healthcare data in the cloud: Advanced data integrity measures and privacy assurance. International Journal of Engineering Trends and Technology. 2023;71(10):238–53.
14. El Sibai R, Gemayel N, Bou Abdo J, Demerjian J. A survey on access control mechanisms for cloud computing. Transactions on Emerging Telecommunications Technologies. 2020;31(2):e3720.
15. Gade KR. Cloud-native architecture: Security challenges and best practices in cloud-native environments. Journal of Computing and Information Technology. 2022;2(1).
16. Hammi B, Zeadally S, Khatoun R, Nebhen J. Survey on smart homes: Vulnerabilities, risks, and countermeasures. Computers & Security. 2022;117:102677.
17. Indu I, Anand PR, Bhaskar V. Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal. 2018;21(4):574–88.
18. Jasper KD, Raja AV, Neha R, Rajest SS, Regin R, Senapati B. FMDB transactions on sustainable computing systems. Journal title incomplete in original entry; clarification needed.
19. Julakanti SR, Sattiraju NSK, Julakanti R. Securing the cloud: Strategies for data and application protection. NeuroQuantology. 2022;20(9):8062–73.

20. Katari A, Ankam M. Data governance in multi-cloud environments for financial services: Challenges and solutions. Educational Research (IJMCER). 2022;4(1):339–53.
21. Kaur P, Alam A, Kaur S, Sahota RS. Access control application prevention and mitigation of cyber-attacks. International Journal of Research and Innovation in Applied Science. 2023;8(10):91–105.
22. Khalil U, Malik OA, Uddin M, Chen CL. A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: A comprehensive review, recent advances, and future research directions. Sensors. 2022;22(14):5168.
23. Khambam SKR, Kaluvakuri VPK. Multi-cloud IAM strategies for fleet management: Ensuring data security across platforms. Unspecified source; journal name required.
24. Labadie C, Legner C. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. Journal of Information Technology. 2023;38(1):16–44.
25. Liu G, Gao X, Wang H. An investigation of identity-account inconsistency in single sign-on. In: Proceedings of the Web Conference 2021. 2021 Apr. p. 105–17.
26. Michael R, Sarah J. Unlocking the power of Azure AD: best practices for enterprise identity control. International Journal of Trend in Scientific Research and Development. 2019;3(6):1447–55.
27. Mishra RA, Kalla A, Braeken A, Liyanage M. Privacy-protected blockchain-based architecture and implementation for sharing of students' credentials. Information Processing & Management. 2021;58(3):102512.
28. Mohammed AHY, Dziyauddin RA, Latiff LA. Current multi-factor authentication: approaches, requirements, attacks, and challenges. International Journal of Advanced Computer Science and Applications. 2023;14(1).
29. Mohammed IA. Cloud identity and access management–a model proposal. International Journal of Innovations in Engineering Research and Technology. 2019;6(10):1–8.
30. Mostafa AM, Rushdy E, Medhat R, Hanafy A. An identity management scheme for cloud computing: review, challenges, and future directions. Journal of Intelligent & Fuzzy Systems. 2023;Preprint:1–23.
31. Muhammad T, Munir MT, Munir MZ, Zafar MW. Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. International Journal of Computer Science and Technology. 2022;6(4):99–135.
32. Nahar K, Gill AQ. Integrated identity and access management metamodel and pattern system for secure enterprise architecture. Data & Knowledge Engineering. 2022;140:102038.
33. Nidamanuri NDS. Optimizing library data handling with cloud and big data technologies. European Journal of Advances in Engineering and Technology. 2022;9(8):75–81.
34. Nookala G. Automation of privileged access control as part of enterprise control procedure. Journal of Big Data and Smart Systems. 2020;1(1).
35. Ovabor K, Atkison T. User-centric privacy control in identity management and access control within cloud-based systems. International Journal on Cybernetics & Informatics (IJCI). 2023;12(12):59.
36. Paci F, Squicciarini A, Zannone N. Survey on access control for community-centered collaborative systems. ACM Computing Surveys (CSUR). 2018;51(1):1–38.
37. Podugu S, Rayapureddi VK, Gupta M. Auditing customer identity and access management. In: Modernizing Enterprise IT Audit Governance and Management Practices. IGI Global; 2023. p. 181–210.
38. Reece M, Lander TE Jr, Stoffolano M, Sampson A, Dykstra J, Mittal S, *et al*. Systemic risk and vulnerability analysis of multi-cloud environments. arXiv preprint arXiv:2306.01862. 2023.
39. Saad M, Spaulding J, Njilla L, Kamhoua C, Shetty S, Nyang D, *et al*. Exploring the attack surface of blockchain: a comprehensive survey. IEEE Communications Surveys & Tutorials. 2020;22(3):1977–2008.
40. Schrimpf A, Drechsler A, Dagianis K. Assessing identity and access management process maturity: first insights from the German financial sector. Information Systems Management. 2021;38(2):94–115.
41. Shaik M, Gudala L, Sadhu AKR. Leveraging artificial intelligence for enhanced identity and access management within zero trust security architectures: a focus on user behavior analytics and adaptive authentication. Australian Journal of Machine Learning Research & Applications. 2023;3(2):1–31.
42. Sharma H. Impact of DSPM on insider threat detection: exploring how DSPM can enhance the detection and prevention of insider threats by monitoring data access patterns and flagging anomalous behavior. International Journal of Computer Science and Engineering Research and Development (IJCSERD). 2021;11(1):1–15.
43. Sikder AK, Petracca G, Aksu H, Jaeger T, Uluagac AS. A survey on sensor-based threats and attacks to smart devices and applications. IEEE Communications Surveys & Tutorials. 2021;23(2):1125–59.
44. Singh C, Thakkar R, Warraich J. IAM identity access management—importance in maintaining security systems within organizations. European Journal of Engineering and Technology Research. 2023;8(4):30–8.
45. Subbarao D, Raju B, Anjum F, Rao CV, Reddy BM. Microsoft Azure active directory for next-level authentication to provide a seamless single sign-on experience. Applied Nanoscience. 2023;13(2):1655–64.
46. Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the internet of healthcare things. Digital Health. 2023;9:20552076231177144.
47. Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing. 2020;76(12):9493–532.
48. Talluri S, Makani ST. Managing identity and access management (IAM) in Amazon Web Services (AWS). Journal of Artificial Intelligence & Cloud Computing. 2023;SRC/JAICC-159:147(2):2–5.
49. Tayouri D, Hassidim S, Smirnov A, Shabtai A. White paper-cybersecurity in agile cloud computing--cybersecurity guidelines for cloud access. Cybersecurity in Agile Cloud Computing--Cybersecurity Guidelines for Cloud Access. 2022;1–36.
50. Zhang Q. Detecting credential stuffing between servers. In: Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2020 International Workshops. Nanjing, China: Springer International Publishing; 2021. p. 454–64.