

Robust IAM Solution for Enterprise Cloud Services

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |



**Institute of Technical Education and Research SIKSHA ‘O’ ANUSANDHAN DEEMED TO BE UNIVERSITY**

**Bhubaneswar, Odisha, India**

# Abstract

In the field of Cloud Identity and Access Management (IAM), blockchain technology offers a strong solution for overseeing user identities and safeguarding access to resources. The utilization of hashed encryption in blockchains guarantees the secure storage of IAM data, safeguarding it from unauthorized entry and offering a dependable system of record for historical data and access modifications. This encryption method not just protects the integrity of data but also simplifies verification.

The existing database security measures have successfully prevented unauthorized entry, but there are still obstacles to maintaining the integrity of access privileges. The utilization of advanced methods such as machine learning and behavioural analysis is being researched in order to identify and stop unauthorized alterations to access permissions, ultimately improving security. Selecting the right consensus mechanisms, such as proof of authority or practical Byzantine fault tolerance, is vital in IAM infrastructure to guarantee security and reliability in blockchain deployments.

Government and regulatory agencies are increasingly acknowledging the benefits of blockchain-powered IAM systems, providing transparency, enhanced data security, and a visible audit trail. These systems allow individuals to securely and efficiently handle their personal information, with uses across different industries such as healthcare and finance.

In conclusion, incorporating blockchain technology into IAM systems marks a major step forward in data security, providing improved protection and compliance features to meet the changing requirements of contemporary businesses.

# Contents

1. Introduction 4
2. Problem 12
3. Existing solutions on IAM 13
4. Proposed Solutions 17
5. Conclusion 21
6. References 22

**Introduction**

With the rising adoption of cloud solutions in businesses for their flexibility, cost savings, and scalability, handling user identities and access within this environment becomes more intricate and demanding. Cloud Identity and Access Management (IAM) is essential for managing access to corporate resources, protecting data, and meeting regulatory standards. Conventional approaches like single sign-on and password management may result in multiple identities and inadequate access controls, increasing security vulnerabilities. The increasing risk of identity theft emphasizes the importance of strong IAM solutions. Blockchain technology offers a hopeful strategy, providing trust, accountability, and transparency. Optimal strategies for cloud IAM involve centralized management of identities and utilizing robust authentication techniques for improved security.

### Understanding Cloud Identity and Access Management What is IAM?

Cloud IAM consists of the policies, procedures, and technologies that are utilized to oversee digital identities and control access to cloud resources. It guarantees that the correct people are given the right access to technology assets, reducing the dangers linked with unauthorized entry and data breaches.

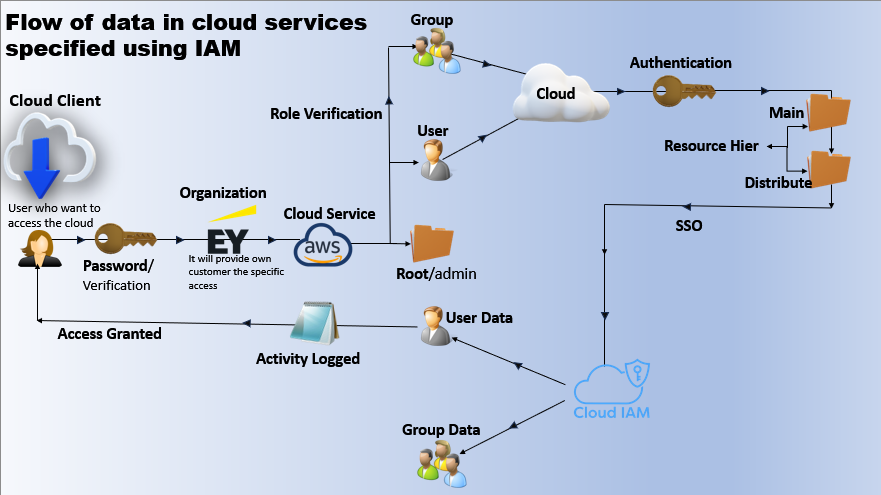
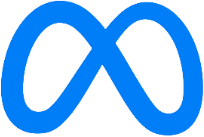




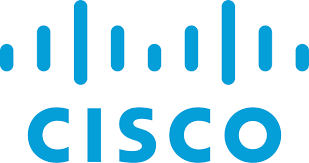
Fig 1: Pictorial Representation IAM

**Platforms that use IAM**

IAM







## Loopholes in Cloud Network

Cloud networks, while offering numerous advantages such as scalability, cost- efficiency, and accessibility, are also susceptible to various security vulnerabilities and loopholes. Understanding these potential pitfalls is crucial for organizations leveraging cloud services. Here are some of the key loopholes in cloud networks:

### Data Breaches and Leaks

One of the most significant risks in cloud networks is the possibility of data breaches. Cloud environments are accessible over the internet, which makes them a target for cyberattacks. Sensitive data stored in the cloud, if not properly protected, can be accessed by unauthorized parties, leading to data leaks. Misconfigured cloud storage settings, weak encryption, and inadequate access controls can exacerbate this risk.

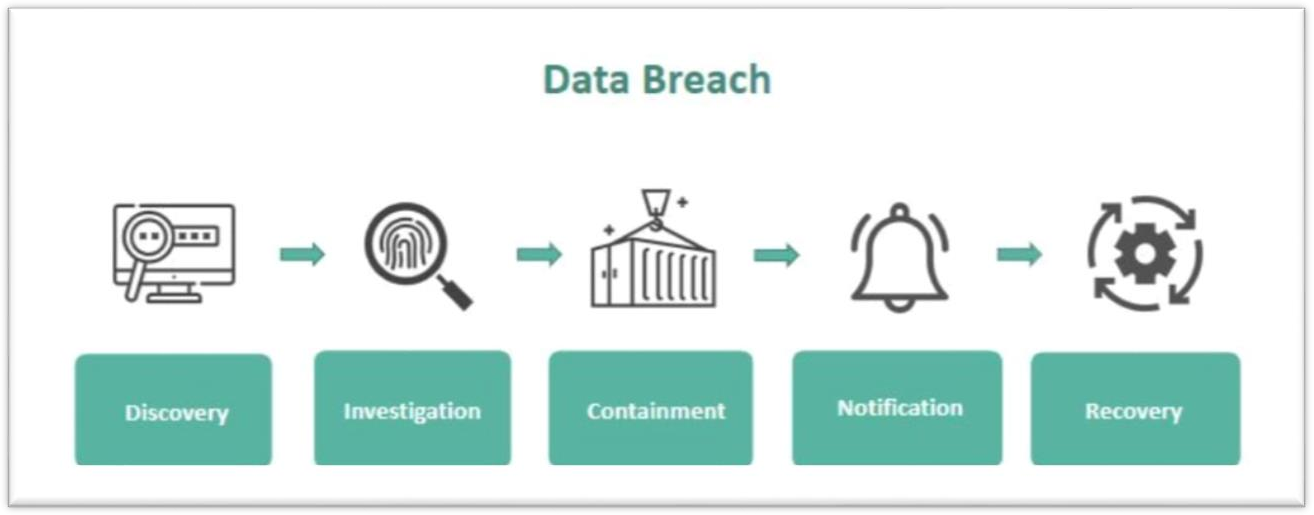




Fig 2: Data Breach

### Insider Threats

Insider threats are another major concern in cloud security. Employees or contractors with access to sensitive information can misuse their privileges, either maliciously or accidentally. This risk is heightened in cloud environments due to the broader range of users who may have access to the data and services. Effective identity and access management (IAM) strategies are essential to mitigate this risk.

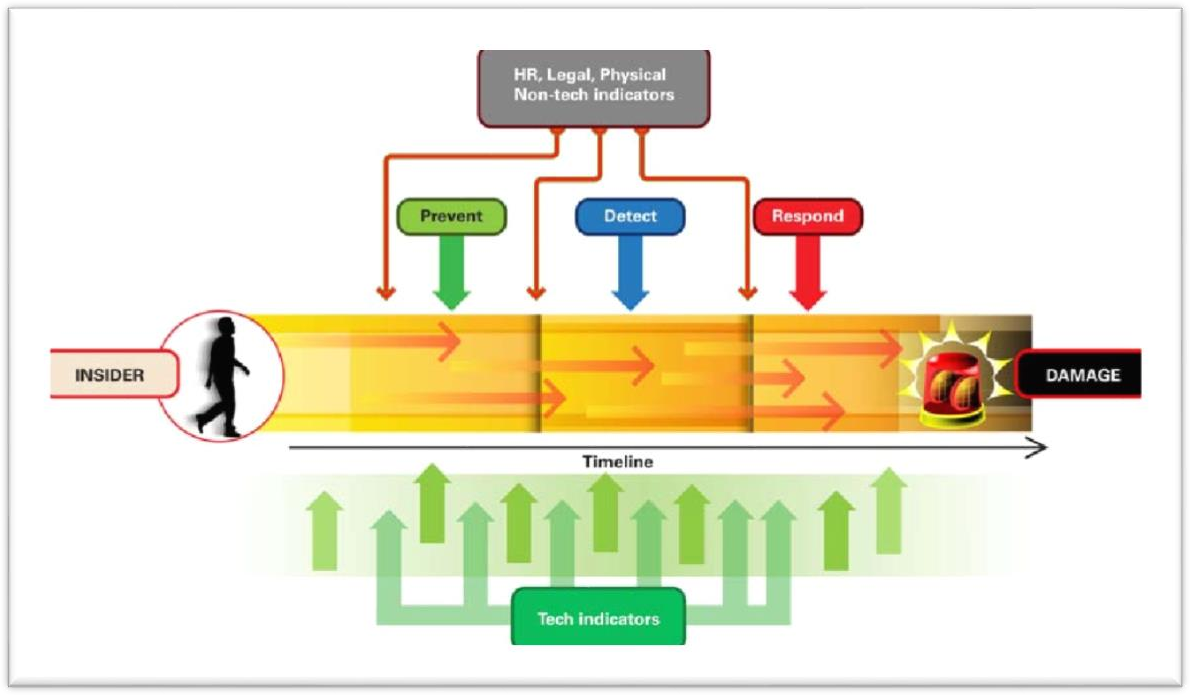




Fig 3: Insider Threats

### Denial of Service (DoS) Attacks

Cloud services are susceptible to DoS attacks, which can disrupt service availability by overwhelming the system with excessive traffic. While cloud providers offer scalability to handle increased loads, a large-scale attack can still degrade performance or incur significant costs. Properly configured network security measures, such as rate limiting and traffic filtering, are necessary to defend against these attacks.

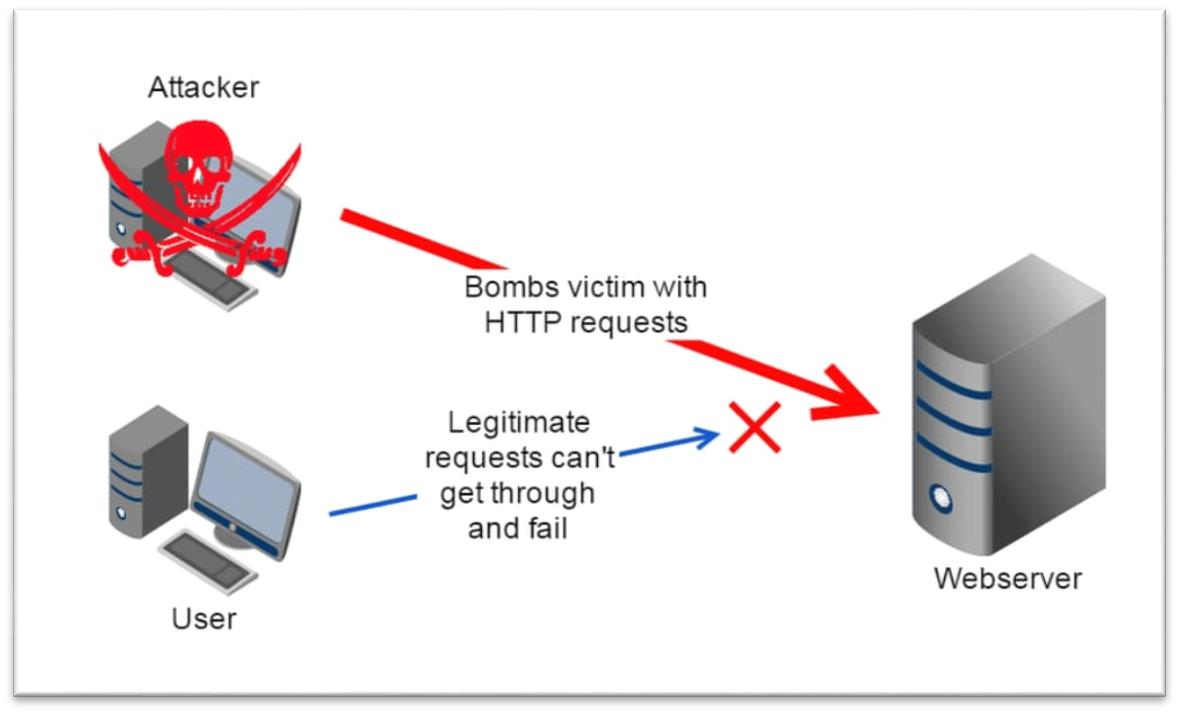


Fig 4: Denial Of Service (DOS) Attacks

### Compliance and Legal Risks

Compliance with regulations such as GDPR, HIPAA, or PCI DSS is a significant concern in cloud environments. Misunderstandings regarding data ownership, data residency, and compliance responsibilities can lead to legal and financial penalties. Organizations must clearly define and understand the roles and responsibilities of both the cloud provider and the client.





Fig 5: Compliance

## Different IAM Policies

Identity and Access Management (IAM), policies are critical for defining permissions for users, groups, and roles. These policies determine who can access specific resources and what actions they can perform. Here are the different types of IAM policies along with examples:

### Identity-Based Policies:

* + **User Policies:** Policies attached directly to IAM users.
  + **Group Policies**: Policies attached to IAM groups, which apply to all users in the group.
  + **Role Policies:** Policies attached to IAM roles, often used by services or applications.
  + **Example:** A policy allowing read-only access to a specific S3 bucket.

### Managed Policies:

* + **AWS Managed Policies:** Predefined policies created and maintained by AWS, available for all accounts.
  + **Customer Managed Policies:** Policies created and managed by users in their own AWS accounts.
  + **Example:** AWS managed policy for administrative access.
  + Policy name: AdministratorAccess

### Session Policies:

* + Session policies are a type of policy that you pass to an AWS Security Token Service (STS) session when creating temporary credentials. These policies control the permissions for the session and can be used to enforce specific security requirements during the session's duration.
  + **Policy Description:** This session policy grants read-only access to the specified S3 bucket and its objects.

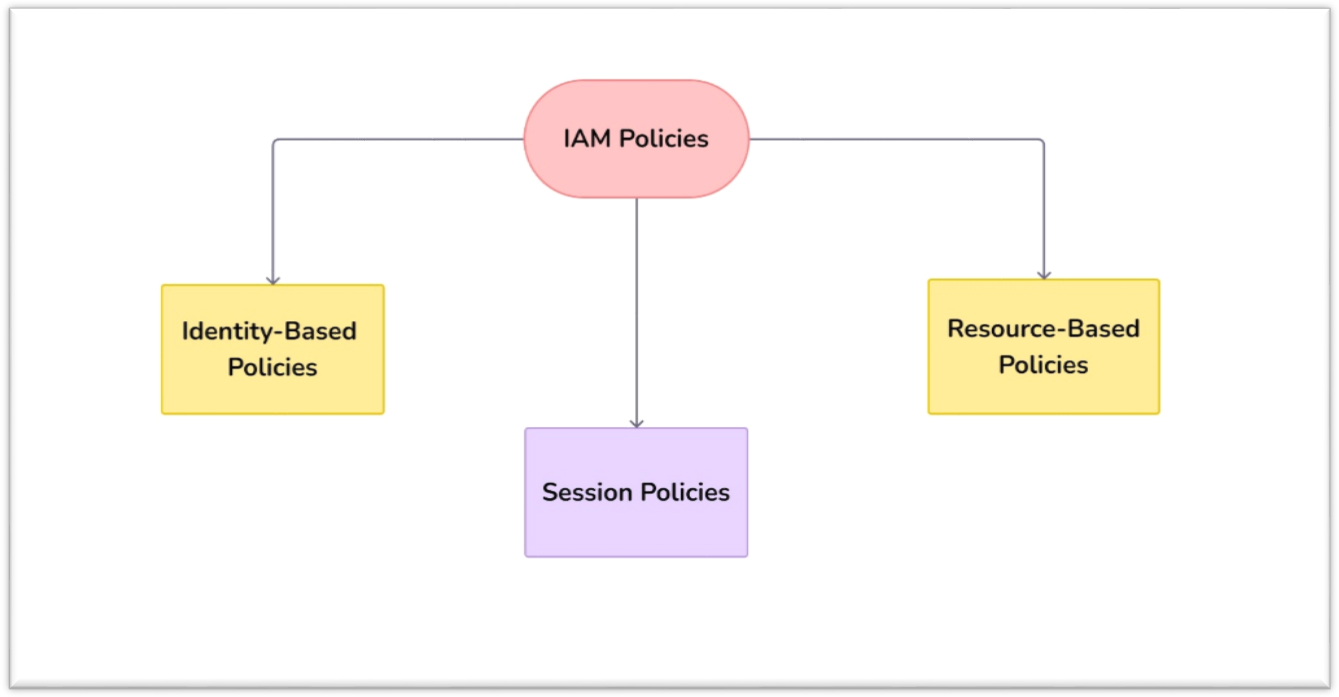


Fig 6: IAM Policies

### Importance of Cloud IAM

1. **Security**: Protects against unauthorized access, data breaches, and potential cyber threats.
2. **Compliance**: Helps meet regulatory requirements by enforcing stringent access controls.
3. **Efficiency**: Streamlines the process of managing user identities and access permissions.
4. **Scalability**: Adapts to the growing needs of enterprises, managing a large number of users and devices.

### Key Components of Cloud IAM

* 1. **Authentication**: Verifying the identity of users attempting to access resources.
  2. **Authorization**: Determining the level of access granted to authenticated users.
  3. **User Management**: Handling the lifecycle of user identities within the organization.
  4. **Access Policies**: Defining rules and conditions under which access is granted.

### Benefits of IAM in Enterprises.

* + 1. **Enhanced Security:** IAM (Identity and Access Management) enhances security by ensuring that only authorized individuals can access sensitive information and systems. This reduces the risk of data breaches and unauthorized access.
    2. **Enhanced User Experience:** Functions such as single sign-on (SSO) make the login procedure easier, giving users smooth entry to various systems and applications.
    3. **Risk Reduction:** IAM reduces security risks by monitoring user actions and identifying irregularities. This proactive approach helps detect and mitigate potential threats, ensuring the safety and integrity of systems and data.
    4. **Cost Efficiency:** IAM enhances cost efficiency by automating user management processes and reducing administrative tasks. This leads to lower operational costs and minimizes the financial impact of security breaches and compliance issues.

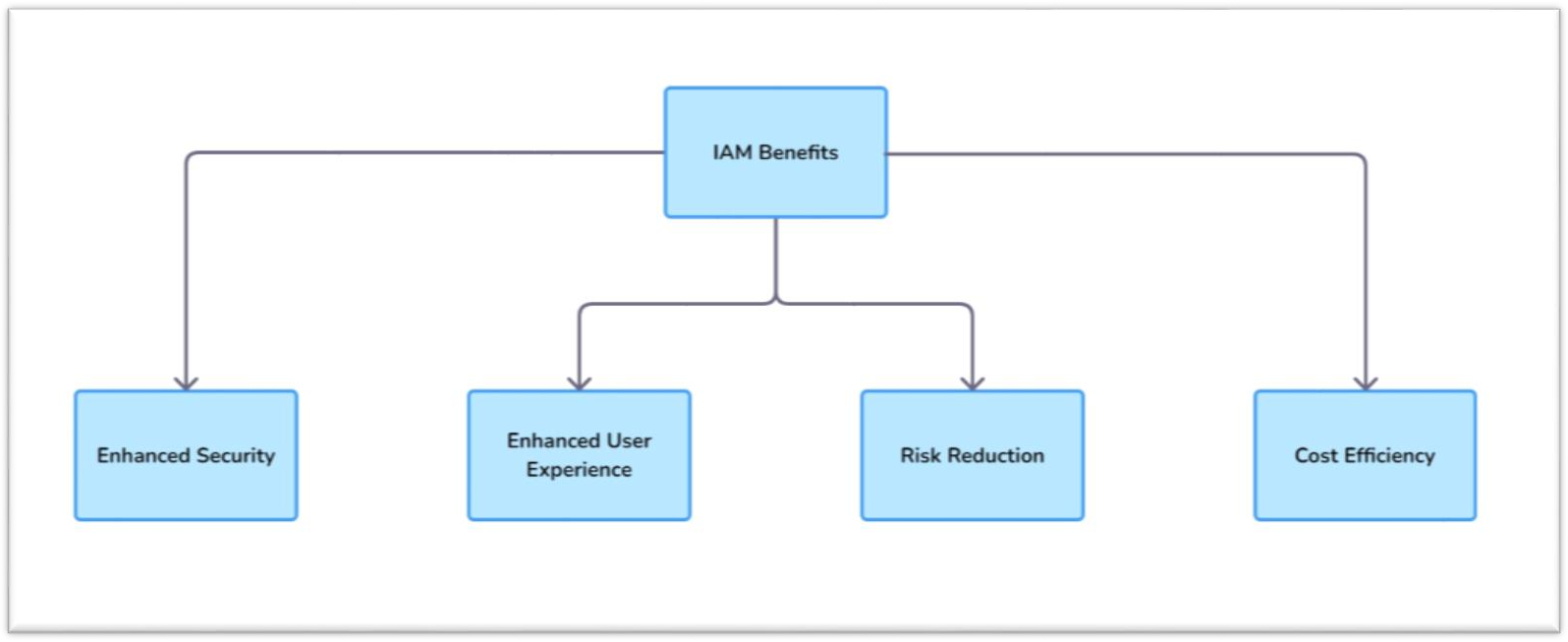




Fig 7: Benefits of IAM

# Problems

1. **Protocols and standards:** The TCP/IP model, which is the basic communication model on the Internet, is made up of different protocols and standards. Cloud services that function within this framework must comply with global standards in order to facilitate compatibility across different platforms. Cloud service providers need to develop, set up, run, carry out, evaluate, oversee, and enhance their services in line with a thorough service management system. This system guarantees that service needs, such as design, delivery, transition, and continuous enhancement, are consistently fulfilled. Because cloud services are IT-focused by nature, they are strongly connected to IT management systems, highlighting the importance of solid protocols and standards for ensuring both quality and security.
2. **Misuse of Privileges:** Insiders exploit their access to sensitive resources, compromising the organization's integrity, confidentiality, or availability.
   * **PIM Solutions**: Use Privileged Identity Management (PIM) solutions to protect cloud servers.
3. **Cloud Network Risks:** In cloud environments, third-party vendors or cloud administrators may misuse resources to attack the organization's infrastructure.

### Denial of Service (DoS) & Distributed Denial of Service (DDoS)

**Attacks**

* + 1. **DoS Attack:** Overloading a server with fake requests to prevent it from serving legitimate ones.
    2. **DDoS Attack:** Similar to DoS but initiated by multiple sources, typically bots or malware from infected hosts.
    3. **Cloud Vulnerability:** Cloud servers, supporting IaaS and SaaS models, are particularly vulnerable.

### Mitigation:

* + - * Use firewalls to control access to ports, protocols, and IP addresses.
      * Limit and regulate network bandwidth programmatically (e.g., using DataPower Gateway) to prevent service overload.

1. **Access Governance:** Properly defined access governance policies can significantly reduce the risk of Insider attacks.

# Existing solutions on IAM

1. **Integration of Identity Access Models:** Recent advancements in identity access models, such as smart gates, have improved security and efficiency, especially in airports and border control.

### Biometric Technology Advancements:

* 1. **Colombia:** Gemalto's biometric authentication at Bogota International Airport has enhanced border control using iris recognition.
  2. **Saudi Arabia:** Implementation of biometric borders has improved national security.
  3. **European Union:** The Eurodac system has unified biometric authentication across EU member states.

### Impact of AI on Biometric Systems:

* 1. **Processing Power:** High computational resources enhance the accuracy and speed of AI algorithms in biometric systems; limited resources can cause delays.
  2. **Memory Resources:** Adequate memory is crucial for handling large datasets required for biometric authentication.
  3. **Challenges in Cloud Environments:** Biometric systems must adapt to varying computational resources across cloud platforms. Solutions like adaptive algorithms are being developed to optimize performance.

### Future Directions:

* 1. **Resource Management:** Focus on AI-driven resource allocation, predictive analysis, and data compression to improve efficiency.
  2. **Scalability and Reliability:** Innovations in these areas aim to enhance the scalability and reliability of biometric systems in cloud environments.

1. **Hypothesis (H4):** Enhancements in AI-powered biometric authentication systems will lead to improved user acceptance, reliability, and accuracy in cloud environments.

# Differences in IAM for different cloud enterprises

## Google's Cloud Platform (GCP) Key Ideas:

* **Identity**: Refers to users, groups, or service accounts. GCP utilizes Google accounts or identities managed by Google for users.
* **Functions**: Predetermined functions and personalized functions determine the activities that identities are able to carry out. Roles can be detailed and are given to users, group, or service accounts.
* **Regulations**: IAM policies are utilized to connect roles with identities. JSON is used to write policies that are linked to resources for access control.

### Important characteristics:

* **Types of IAM Roles:** Consist of preset roles, standard roles (Owner, Editor, Viewer), and personalized roles.
* **Service Accounts**: Unique accounts utilized by applications or virtual machines to engage with GCP services.
* **Control**: IAM policies are implemented on the resource level and can be hierarchical to enable inheritance.

## Microsoft Azure

### Key Ideas:

* **Identity:** Azure Active Directory (AAD) is utilized for managing identity, encompassing individuals, groups, and service principals.
* **Responsibilities:** Azure employs role-based access control (RBAC) with pre-defined roles and user-defined roles that determine authorization levels.
* **Procedures**: In Azure, Role Assignments are utilized to link roles with identities at various levels such as subscription, resource group, or resource.

### Main Characteristics:

* **Roles in RBAC**: Comprise of predefined roles such as Owner, Contributor, Reader, as well as roles that are customizable.
* Service Principals are employed to authorize applications or services to access Azure resources.
* **Access Control:** Roles are passed down the resource hierarchy, enabling adaptable and expandable access control.

## Amazon Web Services (AWS) Key Ideas:

* **Identification**: AWS makes use of IAM users, groups, and roles. IAM users are single accounts, IAM groups consist of users, and IAM roles are utilized to provide temporary access to AWS services.
* **Regulations**: IAM policies are defined using JSON and dictate authorization. Policies are connected to individuals, groups, or roles.
* **Functions**: Functions are utilized to assign access with specific permissions. They are often utilized for AWS services, granting access across accounts, and federating users.

### Main characteristics:

* **IAM Roles**: Consist of roles for AWS services, accessing multiple accounts, and temporary credentials.
* **IAM Policies:** Managed policies and inline policies allow for precise control over access permissions.
* **Access Control:** IAM policies are linked to identities (users, groups, roles) and resources, and permissions are determined according to policy evaluation logic.

|  |  |  |  |
| --- | --- | --- | --- |
| Aspect | Google Cloud Platform (GCP) | Microsoft Azure | Amazon Web Service (AWS) |
| Identity Management | * Google accounts * service accounts | * Azure Active Directory (AAD) * Users * Groups * Service Principals | * IAM users * IAM groups * IAM roles |
| Roles and Policies | * Roles define permissions * Hierarchical resource management * IAM policies (JSON) | * Roles define permissions * Hierarchical resource management * Role Assignments | * Roles define permissions * Flat structure * IAM policies |
| Service Accounts/ Service Principals/ IAM Roles | * Service accounts used for applications and VMs. | * Service principals used for applications and services. | * IAM roles used for applications and cross-   accounts access. |



Table 1: Differences between Google Cloud Platform (GCP), Microsoft Azure, Amazon Web Service (AWS)

# Proposed Solutions

### Ensuring Consensus Mechanisms and Security Protocols

* Blockchains provide a safe way to store IAM data through encrypted hashing, ensuring a secure system of record.
* Hashed encryption secures data by converting it into a cryptographic form, thus safeguarding it from unauthorized access and maintaining data integrity.
* This method makes it easier to securely store and verify historical access data and access change transactions.
* Even with progress in modern database security, difficulties remain in stopping unauthorized alterations to data access permissions.
* Novel techniques like machine learning and behavioural analysis are being created to identify and address unauthorized alterations.
* Blockchains, especially in the IAM sector, offer major security benefits compared to unencrypted storage for user and access information.
* Choosing the correct consensus mechanism, like proof of authority or practical Byzantine fault tolerance, is essential for the security and dependability of blockchain implementations in IAM infrastructure.
* Giving top priority to security and reliability is crucial for optimizing the efficiency of blockchain implementations in IAM systems.

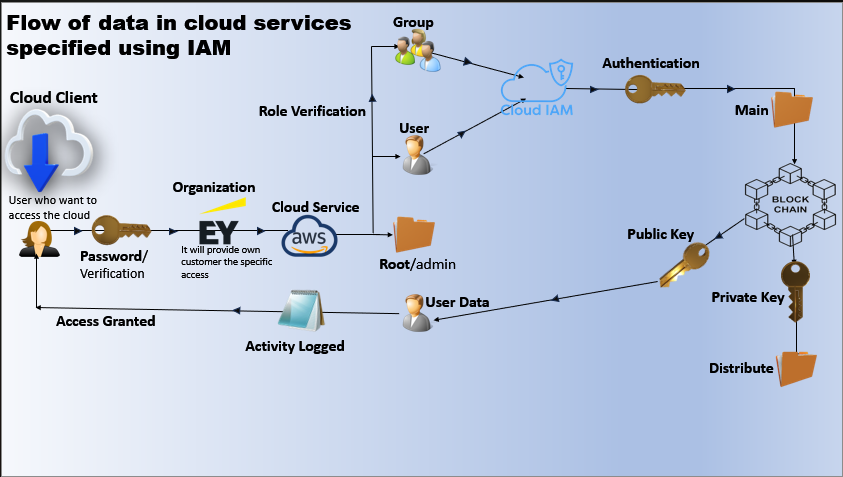




Fig 8: Blockchain

### Multi-Factor Authentication (MFA)

MFA stands for Multi-Factor Authentication. It's a security process that requires users to provide more than one way to verify their identity before they can access an account or system. This adds an extra layer of protection beyond just a password.

### Implementation of MFA

1. **Something You Know:** This is usually a password or PIN.
2. **Something You Have:** This could be a smartphone, security token, or smart card. For example, you might receive a code on your phone that you need to enter after your password.
3. **Something You Are:** This involves biometrics like fingerprints, facial recognition, or voice recognition.

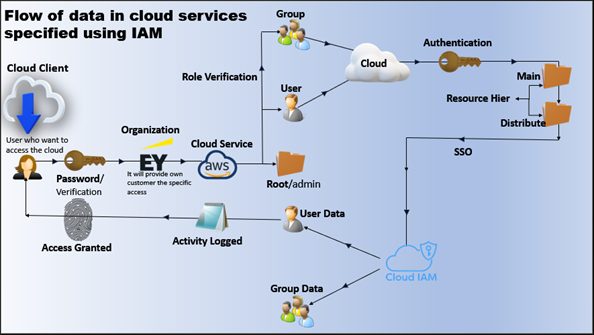
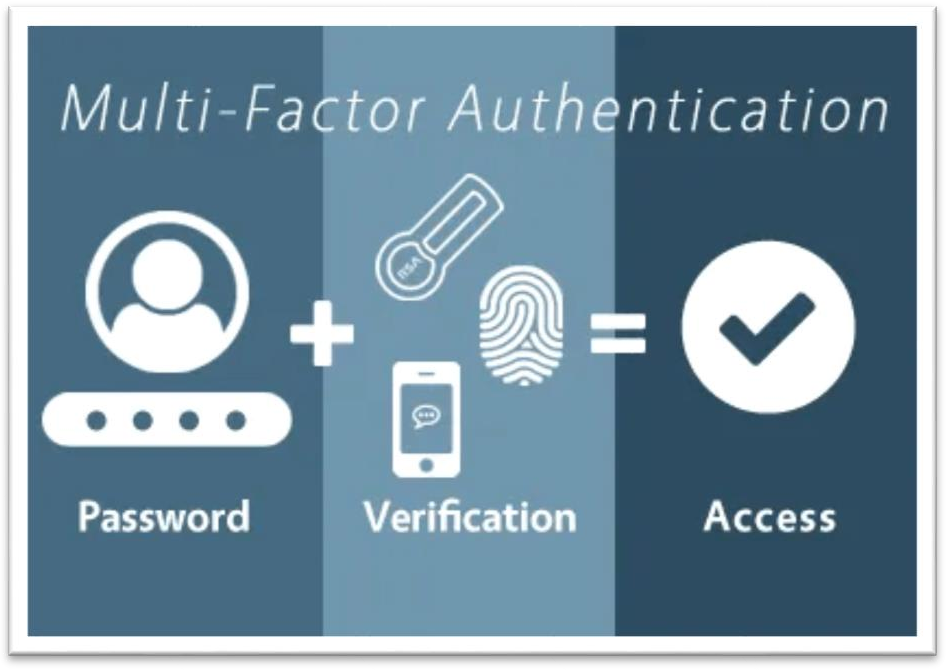




Fig 9: Multi Factor Authentication (MFA)

### To implement MFA, you would typically:

1. Set up an MFA system on the platform or application.
2. Configure the methods you want to use (like SMS codes or an authenticator app).
3. Instruct users on how to set up their devices and follow the steps to verify their identities when logging in.

### Session Timer

A session timer in AWS refers to the duration for which temporary security credentials are valid. These temporary credentials are typically obtained using AWS Security Token Service (STS) and are used to create short-term sessions that grant limited permissions.

### Key Characteristics of Session Timers:

1. Temporary Credentials:
   * Temporary credentials include an access key ID, a secret access key, and a session token.
   * These credentials are used to sign requests to AWS services.
2. Duration:
   * The duration of a session can ranges from a few minutes to several hours, depending on the use case and the service's limits.
   * You can specify the duration when you request the session. If not specified, the default duration is applied.

### Configurable Session Duration:

* + Different AWS services and API calls may have different maximum session durations.
  + For example, the ‘AssumeRole’ API allows specifying a session duration from 15 minutes (900 seconds) to a maximum of 12 hours (43,200 seconds).
  + Service-specific roles might have different maximum durations, like roles for AWS IAM Identity Center, which default to a one-hour maximum.

### Expiration:

* + Once the session expires, the temporary credentials are no longer valid, and any subsequent API requests signed with these credentials will be denied.
  + You need to request new temporary credentials if access is still required.

### Example Scenarios:

1. **Short-Term Access:**
   * If you need to provide access for a short-term task, such as accessing an S3 bucket for a specific operation, you can create a session with a limited duration.

### Temporary Elevated Permissions:

* + For performing a time-bound administrative task that requires elevated permissions, you might create a session with a duration just long enough to complete the task (e.g., 2 hours).

### How to Specify Session Duration:

When using the ‘AssumeRole’ API to create a session, you can specify the session duration using the ‘DurationSeconds’ parameter.

### Setting Session Timers for Various Services:

1. AWS Management Console:
2. AWS CLI and SDKs:

### Benefits of Using Session Timers:

1. Enhanced Security:
2. Controlled Access:
3. Flexibility:

By effectively using session timers, you can balance the need for access with the necessity of maintaining a secure AWS environment.

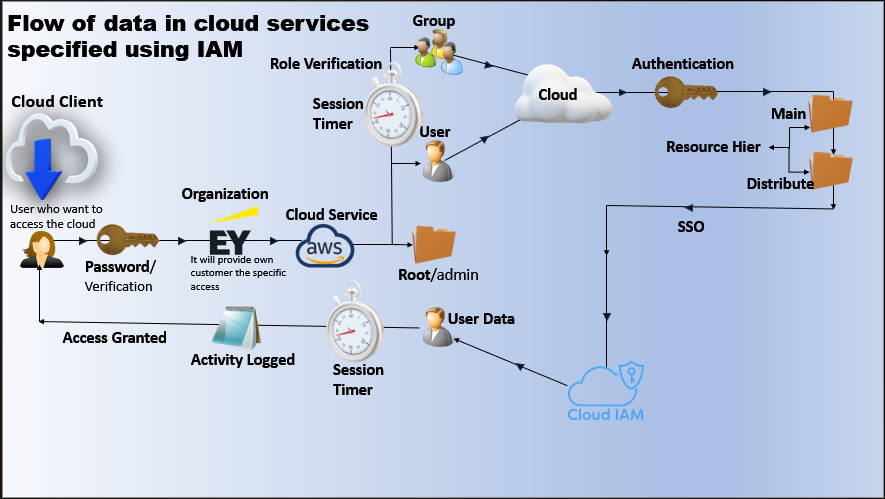




Fig 10: Session Timer

# Conclusion

The incorporation of blockchain technology into Cloud IAM systems shows potential for improving data security and integrity. Blockchain uses hashed encryption to securely store IAM data, preventing unauthorized access and creating a reliable access management record. This method tackles current database security issues and also brings in new features for ensuring data accuracy and stopping unauthorized access rights changes.

Careful consensus mechanism selection is essential in ensuring security and reliability when implementing blockchain in IAM systems. With the advancement of regulatory frameworks and technological innovations, blockchain-based IAM systems are in a position to have a significant impact on protecting sensitive data across different sectors. The ongoing growth and acceptance of these systems underscore the significance of strong security measures in the digital era, ultimately enhancing the security and reliability of the digital environment for both users and organizations.

# References

1. Google Scholar- https://scholar.google.com/
2. Scopus- https://[www.scopus.com/home.uri](http://www.scopus.com/home.uri)
3. I. A. Mohammed, "IDENTITY & ACCESS MANAGEMENT SYSTEM BASED ON BLOCKCHAIN," IDENTITY, 2021.
4. Asian Journal of Research in Computer Science Volume 17, Issue 3, Page 38- 56, 2024; Article no.AJRCOS.112496 ISSN: 2581-8260
5. H. Guo and X. Yu, "A survey on blockchain technology and its security," Blockchain: research and applications, 2022.
6. A. Khalil, M. Khreishah Azeem, Consolidated Identity Management System for secure mobile cloud computing, Comput. Networks. 65 (2014) 99–110, https://doi.org/10.1016/j.comnet.2014.03.015.
7. O’Gorman L: Comparing passwords, tokens, and biometrics for user authentication. In Proceedings of the IEEE. Volume 91(12). Piscataway, New Jersey, United States: IEEE; 2003:2021–2040.
8. Eucalyptus Systems Inc.: Eucalyptus Identity and Access Management (IAM). 2012. [https://[www.eucalyptus.com/](http://www.eucalyptus.com/) docs/eucalyptus/4.0/security- guide/security\_bp\_access.html], [Online accessed August-2014]
9. Google Cloud, “Quotas and limits, Cloud IAM Documentation,” Google Cloud, 2022. https://cloud.google.com/iam/quotas. (Accessed: 01-Feb2022)
10. R. Housley and B. Aboba, “Guidance for Authentication, Authorization, and Accounting (AAA) Key Management,” Jul. 2007, doi: 10.17487/rfc4962.