IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306102|

In-Depth Evaluation of Access Control Strategies during Cloud Migration

Dr. S. Arulselvarani, Ms. J. Jayasudha

Assistant Professor, Department of Computer Science, UDC College, Trichy, Tamilnadu, India

Assistant Professor, Department of Computer Science, Research Scholar, Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

ABSTRACT: This paper aims to provide a comprehensive analysis of various access control mechanisms relevant to cloud migration. Through an in-depth examination of each mechanism's strengths, weaknesses, and applicability, organizations can make informed decisions to tailor their access control strategies to meet their unique security requirements. By exploring the intricacies of Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Multi-Factor Authentication (MFA), Just-In-Time Access (JIT), Network Access Control (NAC), Policy-Based Access Control, Attribute-Based Encryption (ABE), this paper seeks with the knowledge needed to design robust access control frameworks for their cloud migration. Enhance their security posture and mitigate risks associated with cloud migration, ultimately enabling them to realize the full benefits of cloud computing while safeguarding their valuable assets and sensitive data.

KEYWORDS: Access control techniques, RBAC, ABAC, PBAC and Block Chain Technology.

I. INTRODUCTION

Assess the effectiveness of various access control mechanisms in mitigating security risks associated with cloud migration, considering factors such as authentication, authorization, and auditability. Identify the strengths and weaknesses of each access control mechanism, including scalability, complexity, interoperability, and adaptability to diverse cloud environments. Determine the suitability and applicability of access control mechanisms across different cloud service models (IaaS, PaaS, and SaaS) and deployment models (public, private, hybrid). This comprehensive analysis of access control mechanisms provides valuable insights into the intricate landscape of securing cloud environments during migration. Cloud computing for its scalability, flexibility, and cost-effectiveness, the need to ensure robust security measures become paramount. Among the critical components of cloud security, access control mechanisms play a pivotal role in safeguarding sensitive data, applications, and resources from unauthorized access and malicious activities. In the dynamic landscape of cloud migration, where traditional security boundaries dissolve and new challenges emerge, a comprehensive understanding of access control mechanisms is essential for mitigating risks and maintaining compliance.

II. ROLE-BASED ACCESS CONTROL (RBAC)

Role-Based Access Control (RBAC) plays a crucial role in user authentication during cloud migration, ensuring that the right individuals have access to the appropriate resources and services in the cloud environment.

Benefits of RBAC

- Granular Access Control: RBAC allows administrators to define roles that correspond to specific job functions or responsibilities within the organization.
- Simplified User Management: RBAC simplifies user management by grouping users into roles and assigning permissions to these roles.
- Scalability: RBAC scales effectively as organizations grow and evolve. This scalability ensures that access control remains manageable and efficient, even as the organization expands.
- Enhanced Security: RBAC promotes the principle of least privilege, ensuring that users only have access to the resources necessary to fulfill their roles.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306102|

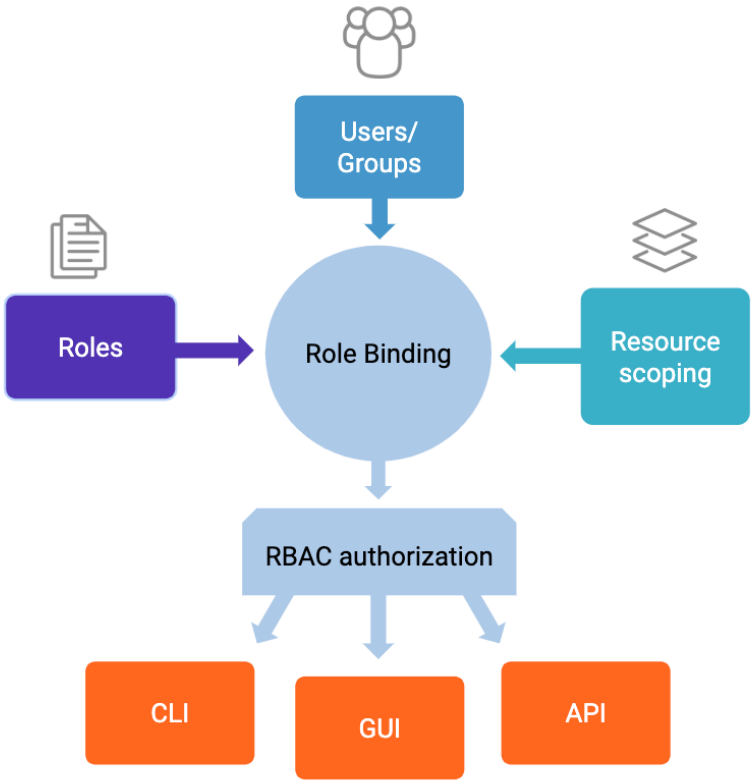

Figure -1 Attribute-Based Access Control (ABAC)

The ABAC mechanism refers to Attribute-Based Access Control, which is a method of restricting access to resources based on attributes associated with users and resources. ABAC evaluates a wide range of attributes to make access decisions. These attributes can include user roles, department, location, time of access, device used, and any other relevant characteristics.

Benefits of ABAC

Fine Grained Access Control

ABAC enables organizations to define access policies based on a wide range of attributes, such as user roles, department, location, time of access, device type, and more.

Integration with Identity Providers

During cloud migration, organizations may leverage identity providers (IdPs) such as Active Directory, LDAP, or SAML for authentication and user attribute management.

Compliance and Governance

ABAC facilitates compliance with regulatory requirements and internal governance policies during cloud migration.

Adoption of Zero Trust Architecture

ABAC, organizations can implement a Zero Trust approach to access control, verifying each access request based on the attributes of the user, device, and context before granting access to cloud resources.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306102|

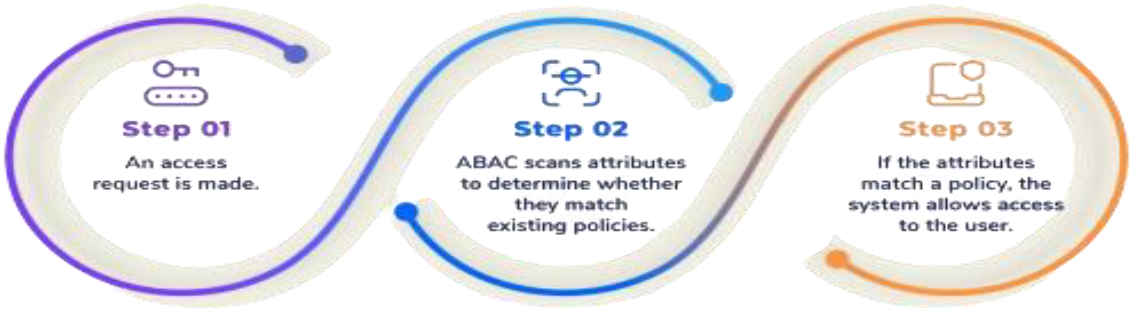

Figure -2 Zero Trust Architecture

Policy-Based Access Control (PBAC)

PBAC stands for Policy-Based Access Control, which is a method of access control that focuses on defining and enforcing access policies centrally rather than hard coding access rules into individual systems or applications.

Policy Definition:

PBAC, access control policies are defined based on the organization's requirements, regulatory compliance needs, and business rules. These policies specify who can access what resources under which conditions.

Policy Evaluation:

When a user attempts to access a resource, the access request is evaluated against the predefined access control policies.

Policy Enforcement:

The enforcement of access control request satisfies the conditions specified in the access control policies, access is granted, otherwise, access is denied.

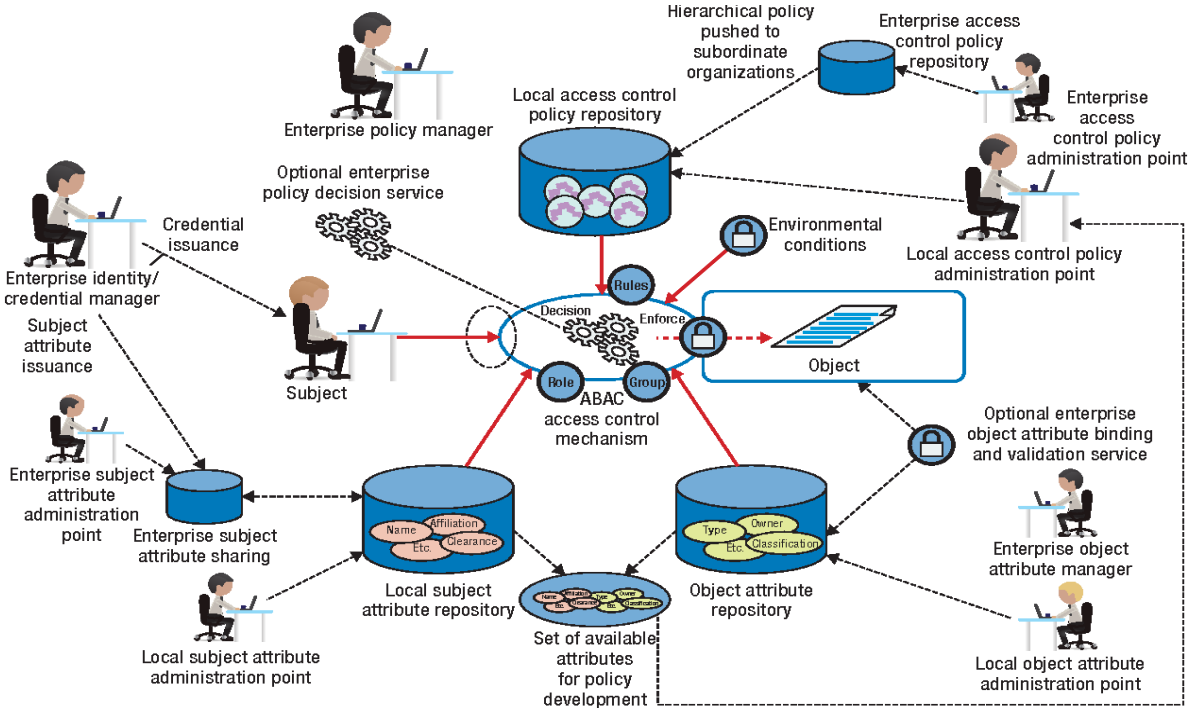

Figure -3 ABAC Access Control Mechanism

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306102|

Comparison of RBAC,ABAC and PBAC

	RBAC	ABAC	PBAC
Permissions depend on	Predefined roles with the same set of permissions across each role.	Sets of specific attributes for each request to determine relevant permissions.	Sets of specific policies that determine relevant attributes and permissions.
Type of access control	Coarse-grained	Fine-grained	Fine-grained
Real-time parameters	No	Yes	Yes
Context specificity	New roles can be defined for each new context of permissions needed.	Sets of attributes can be defined for each new context of permissions needed.	Policies can be defined to adjust the attributes for each new context.
Cost to implement and maintain	Relatively cheap because it can be maintained by a small IT department.	Costly because it requires a large experienced IT team to maintain.	Implementation is costly, but maintenance is not.
Ease of compliance	Assignment of a role may give certain employees unwanted access to sensitive information. Compliance is difficult to ensure. Fairly easy to define new roles or revoke certain permissions for a particular role, but the risk of role explosion is high.	Highly-specific permissions can be granted, but the translation of company policies from the business to the IT end can cause errors and weaken compliance.	Easy-to-use GUI and reliance on policies allow business managers to set permissions directly, ensuring high compliance.

III. BLOCK CHAIN TECHNOLOGY

Using block chain technology to secure DNA cryptography represents an innovative approach to enhancing the security and privacy of genetic data. DNA cryptography involves encoding sensitive information into DNA sequences, which are then stored or transmitted securely. Block chain can complement this process by providing a decentralized, tamper-proof ledger for managing access, ensuring data integrity, and facilitating secure transactions. Block chain enables fine-grained access control mechanisms, allowing users to specify who can access their genetic data and under what conditions. Smart contracts can be utilized to enforce access permissions and privacy preferences, ensuring that only authorized parties can decrypt and access the encoded DNA information. Block chain operates on a decentralized network of nodes, eliminating single points of failure and reducing the risk of data breaches or cyber attacks. Unlike traditional centralized cloud environments, where a breach in one central location can compromise the entire system, block chain-based cloud solutions distribute data across multiple nodes, making it more resilient to attacks and unauthorized access.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306102|

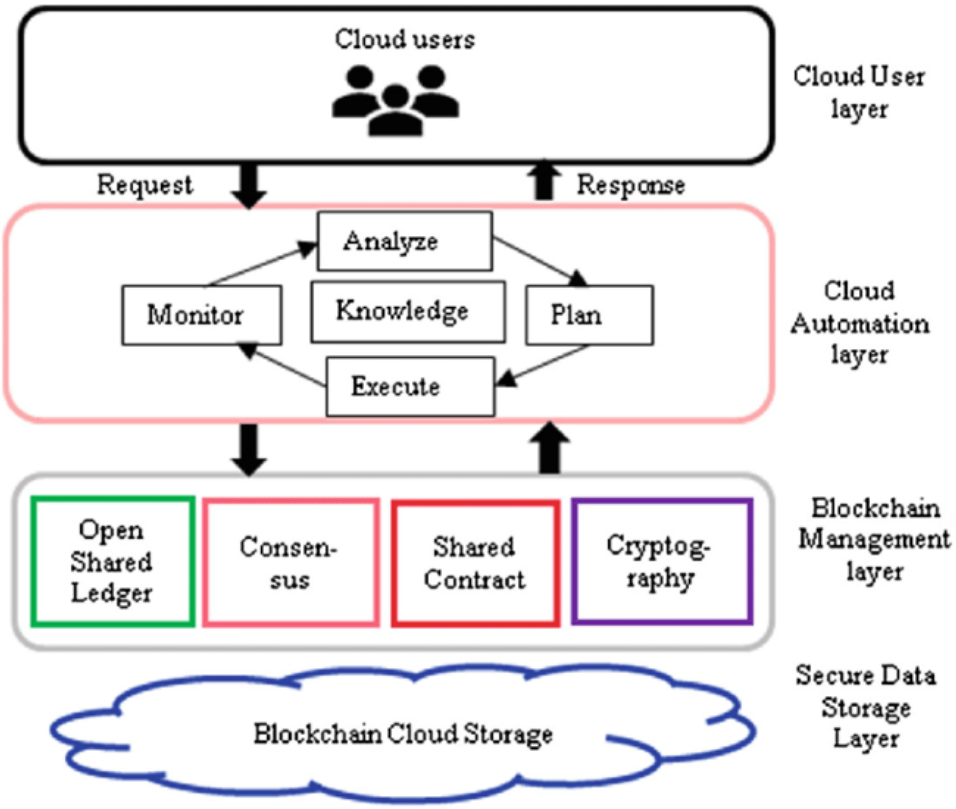

Figure – 4 Block chain Technology

IV. CONCLUSION

Effective access control strategies are indispensable for ensuring the security, compliance, and performance of cloud deployments. By adopting a comprehensive approach that incorporates role-based access control, automation, continuous monitoring, and organizations can successfully navigate the complexities of cloud migration and achieve their strategic objectives while safeguarding their assets and data. Aiming to provide insights into the challenges and best practices associated with managing access controls in cloud environments. The importance of identity and authentication mechanisms cannot be overstated. Implementing strong authentication methods such as multi-factor authentication and robust identity management solutions is essential to prevent unauthorized access and protect sensitive data.

REFERENCES

1. An Effective Approach to Cloud Migration for Small and Medium Enterprises IEEEXplore-2020, Awatef Balobaid, Debatosh Debnath.
2. Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments IEEE Access 2020, Rubina Ghazal,Ahmad Karman Malik,NAuman Qadeer.
3. "Security Techniques For Protecting Data In cloud Computing" IEEE Access 2021- Choragudi Sasidhar and Dr. Sunita Gond.
4. "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments" IEEE Access 2022-Ishu Gupta
5. "Efficient and Secure Attribute-Based Access Control with Identical Sub-Policies Frequently Used in Cloud Storage". IEEE Access 2022-KaipingXue.
6. "A systematic literature review for authorization and access control: definitions, strategies and models" Web Information system,2022-Aya Khaled Yousef Sayed Mohamed, Josef Kung.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306102|

7. "Access control scheme based on block chain and attribute -based searchable encryption in cloud environment", Springer Journal of Cloud Computing, 202- Liang Yan
8. "Block chain Based Cloud Computing: Architecture and Research Challenges" IEEE Access 2020 VNUBharathi Murty,Lawanya Shri M,SEifedine kadry.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details