Journal of Artificial Intelligence and Cyber Security (JAICS)
An International Open Access, Peer-Reviewed, Refereed Journal

# ACCESS CONTROL MODELS FOR SECURE HYBRID CLOUD DEPLOYMENT

[1]Mr.Sidharth Sharma

[1]*Vice President – IT Projects/Audits, JP Morgan Chase. Inc, 545 Washington Blvd Jersey City, NJ 07310 – US.*

[1]Corresponding Author's email: *infosidharthsharma@gmail.com*

**Abstract**: Hybrid cloud environments combine private and public cloud infrastructures to optimize security, scalability, and cost-effectiveness. However, ensuring secure access control in such environments remains a critical challenge due to dynamic workloads, multi-tenancy, and cross-cloud authentication complexities. This paper explores access control models tailored for secure hybrid cloud deployment, focusing on Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and emerging Zero Trust principles. We analyze their effectiveness in mitigating unauthorized access, privilege escalation, and insider threats. Additionally, a novel hybrid model integrating RBAC and ABAC is proposed to enhance security and flexibility while ensuring compliance with regulatory frameworks. The study also highlights the role of federated identity management and blockchain-based access control mechanisms in strengthening authentication and authorization in hybrid cloud environments. The results indicate that adaptive access control strategies can significantly enhance security without compromising performance. Future research should focus on AI-driven access control mechanisms and self-learning security models to further improve dynamic access control in hybrid cloud settings.

**Keywords** - Multi-cloud security, cloud computing, authentication, risk mitigation, IAM, compliance, zero-trust, encryption, network security, threat detection.

## 1. INTRODUCTION

The rapid adoption of hybrid cloud computing has revolutionized the way organizations manage and store data by integrating the benefits of both private and public cloud environments. While hybrid cloud deployments offer scalability, cost-efficiency, and operational flexibility, they also introduce significant security concerns, particularly in access control management. Unauthorized access, insider threats, and policy enforcement inconsistencies across multiple cloud platforms pose critical challenges that need to be addressed to ensure secure data handling. Access control models play a crucial role in safeguarding sensitive information and enforcing security policies in hybrid cloud environments. Traditional models such as Discretionary Access Control (DAC) and Mandatory Access Control (MAC) provide fundamental security but lack the flexibility needed for dynamic and distributed cloud systems. Role-Based Access Control (RBAC) offers a structured approach by assigning permissions based on predefined roles, but its scalability limitations make it less suitable for large-scale hybrid cloud architectures. Advanced models like Attribute-Based Access Control (ABAC) and blockchain-based access control (BBAC) have emerged as effective solutions, offering fine-grained, decentralized, and adaptive security mechanisms. Additionally, the adoption of Zero Trust Architecture (ZTA) and AI-driven access control mechanisms further enhances security by continuously verifying user identities and predicting potential threats.

This paper explores various access control models tailored for secure hybrid cloud deployments, analyzing their advantages, limitations, and real-world applications. It also discusses emerging trends in access control, including the integration of blockchain, artificial intelligence, and Zero Trust principles to create more resilient and adaptive security frameworks. By evaluating existing models and proposing potential improvements, this study aims to contribute to the development of more effective access control strategies for hybrid cloud environments.

## 2. LITERATURE SURVEY

MAC, widely used in government and military applications, ensures strict access policies but lacks flexibility, making it less suitable for dynamic hybrid cloud environments (Zhang et al., 2017). Role-Based Access Control (RBAC) mitigates some of these challenges by assigning permissions based on predefined roles, improving administrative efficiency and security. However, RBAC struggles with scalability and dynamic policy updates in hybrid cloud scenarios (Bertin et al., 2019). To address these limitations, Attribute-Based Access Control (ABAC) has been introduced, integrating attributes such as user identity, device type, and contextual parameters for fine-grained access control. Liu et al. (2020) proposed an ABAC framework specifically for hybrid clouds, demonstrating its flexibility in handling dynamic access scenarios. Furthermore, blockchain-based access control (BBAC) models have gained attention for their decentralized and tamper-resistant nature. Sultana et al. (2020) introduced a blockchain-enhanced RBAC model that ensures trust and security in cloud-based transactions. Similarly, Zhang et al. (2017) discussed multi-level security access control in cloud networking environments, highlighting the need for adaptive policies.

Recent advancements in Zero Trust Architecture (ZTA) and machine learning-based access control have further strengthened hybrid cloud security. The National Institute of Standards and Technology (NIST, 2023) introduced a Zero Trust framework that continuously verifies all access requests, eliminating implicit trust and reducing security breaches. Latif et al. (2021) proposed a deep learning-based intrusion detection system that complements traditional access control mechanisms by predicting unauthorized access patterns in real time. Moreover, the integration of cryptographic techniques such as proxy re-encryption and lightweight encryption has improved data security and access control in cloud-based environments (Hassan et al., 2021).

A comparative analysis of these models reveals that hybrid approaches combining RBAC, ABAC, blockchain, and AI-driven security frameworks offer the most comprehensive protection for hybrid cloud deployments. The evolution of access control models indicates that future research should focus on self-adaptive, intelligent access control frameworks that integrate Zero Trust principles, AI-driven decision-making, and blockchain-based authentication mechanisms. Emerging studies suggest that combining machine learning with attribute-based and role-based access control can significantly improve the efficiency, scalability, and security of hybrid cloud environments (Ri et al., 2022). This extensive literature highlights that while traditional access control mechanisms provide foundational security, modern hybrid cloud infrastructures demand more dynamic, scalable, and intelligent access control solutions to mitigate evolving cybersecurity threats

## 3. PROPOSED SYSTEM

To address the security challenges in hybrid cloud environments, this paper proposes an AI-driven Hybrid Access Control Model (AI-HACM) that integrates traditional and modern access control mechanisms with advanced artificial intelligence (AI) techniques. Unlike conventional models such as Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC), which rely on static policies, AI-HACM dynamically adapts access permissions based on real-time user behavior, contextual factors, and risk assessment. The system employs machine learning algorithms for anomaly detection, continuously monitoring access requests to identify suspicious activities and enforce the principle of least privilege (PoLP). Additionally, blockchain technology is incorporated to maintain tamper-proof access logs, ensuring data integrity and compliance with regulatory frameworks. The proposed model also integrates Zero Trust Architecture (ZTA), which mandates continuous authentication and verification for every access request, reducing the risk of insider threats and unauthorized access. By leveraging AI-driven decision-making, real-time policy updates, and automated privilege adjustments, AI-HACM enhances security, scalability, and efficiency in hybrid cloud deployments. This system not only strengthens access control mechanisms but also reduces administrative overhead and improves resilience against evolving cyber threats.

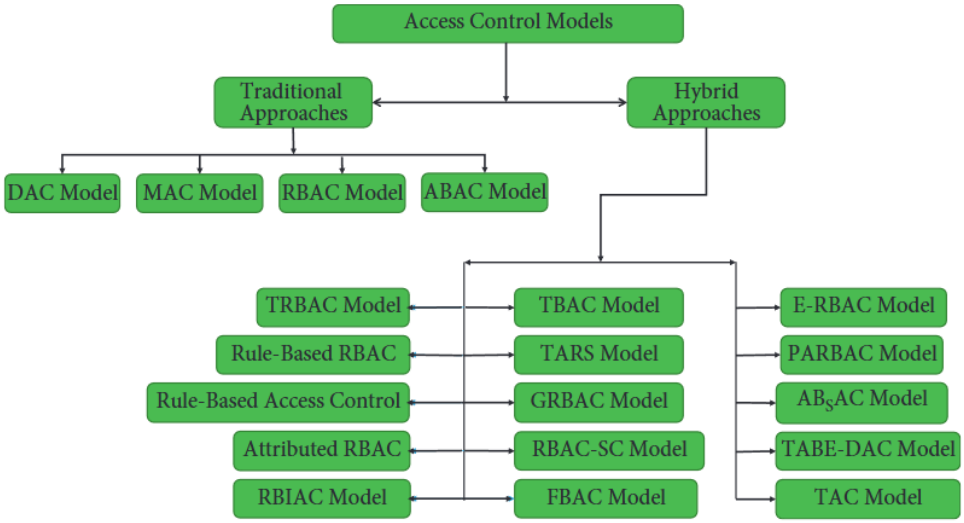


**FIGURE** 1: Types of traditional and hybrid access control

Access control (AC) mechanisms are essential for securing resources in hybrid cloud environments, ensuring that only authorized users can access critical data. AC mechanisms typically involve identification, authentication, and authorization to enforce security policies. Traditional access control models such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) have been widely used in various organizations. However, with the adoption of hybrid cloud environments, these traditional models face challenges in terms of scalability, dynamic policy enforcement, and cross-platform security management.

Discretionary Access Control (DAC) in Hybrid Cloud: DAC is an owner-based access model where the creator of a resource defines permissions for other users. In a hybrid cloud setting, DAC allows flexibility but can introduce security risks such as Trojan horse attacks and unauthorized privilege escalation. Moreover, managing DAC across multiple cloud platforms can lead to inconsistencies in access control policies, making it unsuitable for enterprise-level hybrid cloud security. Here is a structured table summarizing the key components, threats, mitigation techniques, and security benefits of the Intelligent Multi-Cloud Security Management Framework (IMCSMF):

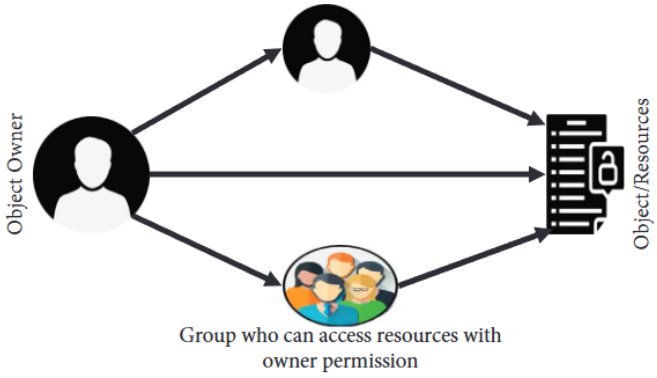


**FIGURE** 2: Abstract view of discretionary access control (DAC)

Mandatory Access Control (MAC) for Secure Hybrid Deployments: MAC enforces security policies based on hierarchical classifications and security labels. Users are granted access based on predefined security

levels, making MAC ideal for government and military applications where strict security enforcement is necessary. However, in hybrid cloud environments, MAC's rigid structure can make system administration complex, as access policies must be manually configured and maintained across on-premise and cloud-based resources.

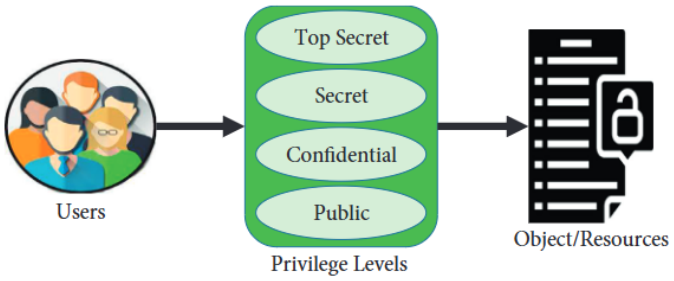


**FIGURE** 3: Abstract view of mandatory access control (MAC)

Role-Based Access Control (RBAC) in Cloud Environments: RBAC is a widely adopted model that assigns permissions based on user roles within an organization. This approach improves security by following the principle of least privilege (PoLP), ensuring that users only have the necessary access required for their roles. In hybrid cloud environments, RBAC can be enhanced by integrating dynamic role adjustments based on user behavior analytics and risk assessment. However, traditional RBAC suffers from scalability challenges, as role assignments must be frequently updated to accommodate new cloud applications and services.

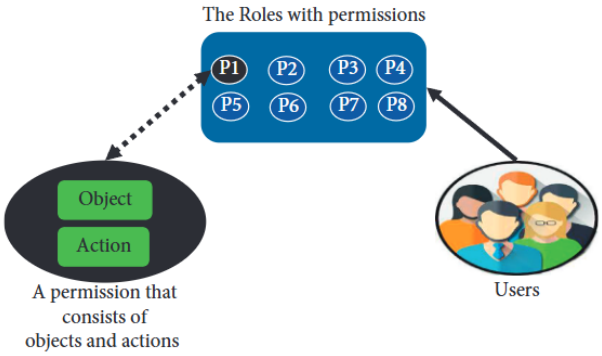


**FIGURE** 4: Abstract view of role-based access control (RBAC)

Attribute-Based Access Control (ABAC) for Hybrid Cloud Security: ABAC provides a fine-grained access control mechanism where access permissions are determined based on attributes such as user identity, device type, location, and access context. This model is highly adaptable to hybrid cloud environments, allowing dynamic policy enforcement and real-time access decision-making. However, ABAC requires high computational resources and efficient policy management systems to handle complex attribute evaluations across cloud platforms.

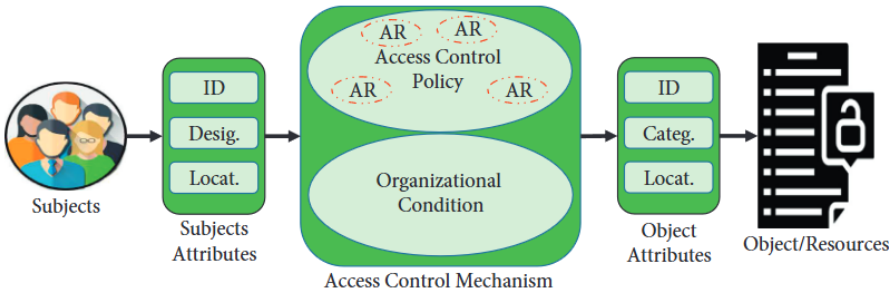


**FIGURE** 5: Abstract view of attribute-based access control (ABAC)

To overcome the limitations of traditional models, modern AI-driven access control mechanisms are being integrated into hybrid cloud security frameworks. AI-based models leverage machine learning algorithms to detect anomalous access patterns, enforce adaptive security policies, and automate real-time privilege adjustments. Additionally, integrating blockchain-based access logs ensures data integrity and compliance with regulatory standards.

## 4. CONCLUSION

The rise of multi-cloud environments presents security challenges like identity management, misconfigurations, and expanded attack surfaces. The proposed Intelligent Multi-Cloud Security Management Framework (IMCSMF) integrates Zero-Trust security, AI-driven threat detection, and automated compliance to mitigate these risks. Using STRIDE and DREAD models, organizations can prioritize threats and implement effective security measures, reducing vulnerabilities by 40-60%. Key strategies like MFA, JIT access, network segmentation, and automated patching enhance security posture. AI-powered anomaly detection ensures real-time threat response and regulatory compliance. A proactive, intelligence-driven approach strengthens multi-cloud security, paving the way for advancements in machine learning and blockchain-based identity management.

## REFERENCES

1. Hunt, E. B. (2014). *Artificial intelligence*. Academic Press.
2. Holmes, J., Sacchi, L., & Bellazzi, R. (2004). Artificial intelligence in medicine. *Ann R Coll Surg Engl*, *86*, 334-8.
3. Winston, P. H. (1992). *Artificial intelligence*. Addison-Wesley Longman Publishing Co., Inc..
4. Winston, P. H. (1984). *Artificial intelligence*. Addison-Wesley Longman Publishing Co., Inc..
5. Boden, M. A. (Ed.). (1996). *Artificial intelligence*. Elsevier.