International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 2, Mar-Apr 2025

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Securing Cloud Infrastructure Using Policy-Based Access Control in Cybersecurity

R Krubagaran*, K Padmavathi**, M Gopi Vinayagam***
*(Computer Technology, PSG College Of Arts & Science, Coimbatore
Email: srarunes@gmail.com)
** (Computer Technology, PSG College Of Arts & Science, Coimbatore
Email : padmasakthivel@gmail.com)
*** (Computer Technology, PSG College Of Arts & Science, Coimbatore
Email : gopivinayagam28@gmail.com)

----------**********----------

Abstract:

This abstract explores the integration of PBAC in cloud environments as a cybersecurity framework that ensures only authorized users and devices access critical resources. By using context-aware policies, PBAC enhances the granularity of access control, minimizes the risks associated with privilege escalation, and mitigates potential threats like unauthorized data access, insider attacks, and external breaches. The paper highlights how PBAC can complement traditional security mechanisms, such as identity and access management (IAM), to provide a more adaptive and scalable approach to cloud security, improving compliance with industry regulations while safeguarding against emerging cyber threats.

Keywords — ***Cloud Security, Policy-Based Access Control (PBAC), Cybersecurity, Access Control, IAM, RBAC.***

----------**********----------

I. INTRODUCTION

Cloud computing has revolutionized business operations, but its dynamic nature introduces security challenges. Traditional access control mechanisms like RBAC and IAM lack contextual awareness, leading to over-privileged users and insider threats. Policy-Based Access Control (PBAC) addresses these limitations by dynamically enforcing access policies based on user roles, attributes, and environmental factors. This paper proposes a PBAC framework for cloud security, emphasizing fine-grained access control, scalability, and threat mitigation.

II. RELATED WORK

Existing cloud security relies on static RBAC and IAM systems, which suffer from:

- Limited Context Awareness: Inability to adapt to dynamic access scenarios.
- Scalability Issues: Struggles with growing cloud architectures.
- Insider Threats: Fails to detect malicious actions by authenticated users. Recent advancements in PBAC demonstrate improved flexibility and security.

III. SYSTEM ANALYSIS

Traditional cloud security relies on mechanisms like Role-Based Access Control (RBAC) and Identity and Access Management (IAM) to regulate resource access. While these systems provide foundational security, they often lack the flexibility required to address the dynamic nature of modern cloud environments. Static role assignments grant predefined access rights, which may not account for changing contextual factors, leading to over-privileged users and potential security gaps. Moreover, these systems operate with limited context awareness, failing to consider critical factors like device security, user location, or network status. As cloud infrastructures grow in complexity, scalability becomes a challenge, leaving traditional systems unable to adapt effectively. These limitations, combined with insufficient granularity and vulnerability to insider threats, expose sensitive resources to risks such as privilege escalation and unauthorized data access.

IV. DRAWBACKS OF EXISTING SYSTEM

- Static Role Assignments: Access rights are predefined based on user roles, which may not account for contextual or situational changes, leading to potential over-privileged users.
- Limited Context Awareness: Existing systems lack the ability to consider contextual factors such as device type, geographic location, or time of access, which are critical for mitigating sophisticated cyber threats.
- Scalability Challenges: As organizations grow and adopt complex cloud architectures, the static nature of RBAC systems makes it difficult to scale effectively while maintaining security.
- Susceptibility to Insider Threats: Traditional systems often fail to detect malicious actions performed by authenticated users, leaving sensitive resources vulnerable to insider attacks.

V. PROPOSED SYSTEM

The proposed system uses Policy-Based Access Control (PBAC) to address the limitations of traditional access control in cloud environments. PBAC dynamically enforces access policies based on user groups, enhancing security and adaptability. Context-aware policies, such as time of access, ensure that users can only access files within their designated group, preventing outsiders from viewing or downloading them. If any changes are made within the group, the group key is updated, improving defense against cyber threats. PBAC offers fine-grained policy enforcement, ensuring users access only necessary resources, reducing the risk of privilege escalation. It integrates seamlessly with IAM and RBAC systems, providing a multi-layered security framework.

VI. ADVANTAGES OF PROPOSED SYSTEM

- Context-Aware Policies: Access decisions are based on dynamic factors such as time of access, providing a more robust defense against external and insider threats.
- Granular Access Control: PBAC allows for fine-grained policy definition and enforcement, ensuring that users access only the specific resources necessary for their roles and tasks.
- Dynamic Privilege Management: User privileges are dynamically adjusted based on context, significantly reducing the risk of privilege escalation and over-provisioning.
- Integration with Traditional Mechanisms: PBAC complements existing IAM and RBAC systems, creating a layered

security approach that combines static and dynamic policy enforcement.

VII. SCOPE FOR FUTURE ENHANCEMENT

Policy-Based Access Control (PBAC) is evolving as a dynamic and adaptive security model, especially in cloud and distributed environments. As cyber threats grow more sophisticated, PBAC offers a flexible framework to enhance security. Below are key future directions for PBAC in cybersecurity:

- Integration with Artificial Intelligence (AI) and Machine Learning (ML).
- Zero Trust Architecture (ZTA) Enhancement.
- Blockchain for Decentralized Policy Management.
- Context-Aware and Risk-Adaptive Policies.
- Quantum-Resistant Cryptography for Policy Enforcement.

VIII. CONCLUSION

The increasing adoption of cloud computing has introduced complex security challenges, necessitating advanced access control mechanisms to protect sensitive data and resources. Traditional models like Role-Based Access Control (RBAC) and Identity and Access Management (IAM) often lack the flexibility to adapt to dynamic cloud environments, leading to security gaps such as over-privileged users and insider threats. Policy-Based Access Control (PBAC) emerges as a robust solution, offering fine-grained, context-aware security policies that dynamically adjust based on user roles, environmental factors, and real-time risk assessments. As cyber threats grow more sophisticated, PBAC provides the agility needed to stay ahead, making it an indispensable component of next-generation cloud defense strategies.

ACKNOWLEDGMENT

We are very grateful to Prof. Dr. K Padmavathi (Guide and Associate Professor, Department of Computer Technology, PSG College of Arts & Science, Coimbatore) For her expert guidance and continuous encouragement throughout the project. At last, we must express our sincere, heartfelt gratitude to all staff members and students of the Department of Computer Technology who helped us directly or indirectly during this course of work.

REFERENCES

[1] R. Sandhu and P. Samarati, "Access Control: Principles and Practice," IEEE Communications Magazine, vol. 32, no. 9, pp. 40–48, 1994.
[2] M. A. Alshehri and R. Sandhu, "Access Control Models for Cloud Computing: A Survey," IEEE Access, vol. 8, pp. 177 090–177 118, 2020.
[3] J. Park and R. Sandhu, "Towards Usage Control Models: Beyond Traditional Access Control," ACM Symposium on Access Control Models and Technologies (SACMAT), 2002.
[4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, 2011.
[5] D. Ferraiolo et al., "Role-Based Access Control (RBAC): Features and Motivations," IEEE Computer Society Applications Conference, 1995.
[6] L. Kagal et al., "A Policy Language for Pervasive Systems," IEEE International Workshop on Policies for Distributed Systems (POLICY), 2003.
[7] E. Bertino et al., "Intrusion Detection in RBAC-Administered Databases," IEEE Computer Security Foundations Workshop, 2005.
[8] K. Ren et al., "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

