ADVANCEMENTS IN CLOUD SECURITY: A STUDY ON POLICY-BASED ACCESS CONTROL AND DATA ENCRYPTION MECHANISMS

Vibharani Prasad
Research Scholar Computer Science And Application
P.K. University, Shivpuri (MP),
Rathvibh56@Gmail.Com
Dr. Rohita Yamaganti
Assoc. Professor,
Sreenidhi Institute of Science & Technology, Hyderabad (Ts)
Rohita.Yamaganti@Gmail.Com

ABSTRACT

As organizations increasingly adopt cloud computing, ensuring robust security measures has become paramount. This research presents a comprehensive case study on the implementation of Policy-Based Access Control (PBAC) and data encryption mechanisms to enhance cloud security. The study investigates the effectiveness of PBAC in restricting access to sensitive data based on user roles, demonstrating a significant reduction in unauthorized access attempts. Additionally, the research evaluates the use of Advanced Encryption Standard (AES256) for data at rest and Transport Layer Security (TLS) for data in transit, confirming the absence of data breaches during the evaluation period.Performance assessments indicate that while the integration of PBAC and encryption mechanisms introduces a minimal overhead—approximately a 7% increase in average response times—the system remains well within acceptable performance thresholds. Furthermore, the implementation of Azure Key Vault for encryption key management has proven effective, providing automated key rotation and stringent access control, ensuring that only authorized personnel have access to sensitive encryption keys.This study highlights the dual advantages of enhanced security and efficiency, underscoring the significance of continuous monitoring and auditing processes to ensure compliance and identify potential vulnerabilities. The findings reinforce the feasibility of utilizing PBAC and data encryption as integral components of a secure cloud infrastructure, advocating for a well-defined security framework in cloud environments. Through this case study, the research contributes to the growing body of knowledge on cloud security practices, offering insights into scalable and flexible implementations that align with organizational security objectives..

Keywords: ***Cloud Security, Policy-Based Access Control (PBAC), Data Encryption, AES256, TLS, Azure Key Vault***

INTRODUCTION

A. Background and Motivation

In the era of digital transformation, cloud computing has emerged as a foundational technology, enabling organizations to leverage scalable computing resources, enhance operational efficiency, and drive innovation. Cloud computing offers on-demand access to a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services, which can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011). This paradigm shift has been instrumental in accelerating business processes, reducing costs, and fostering collaboration across different geographical locations.

Despite its numerous benefits, the widespread adoption of cloud computing has also introduced significant security challenges. As sensitive data and critical applications are migrated to cloud environments, ensuring their protection against unauthorized access, data breaches, and cyber-attacks becomes paramount. The dynamic and multi-tenant nature of cloud computing environments complicates the implementation of traditional security measures, necessitating the development of more sophisticated and adaptive security frameworks (Hashizume et al., 2013).

This research is motivated by the pressing need to enhance cloud security through innovative mechanisms that can effectively safeguard sensitive data and resources. The focus is on the implementation of policy-based access control (PBAC) and advanced data encryption mechanisms. PBAC allows organizations to define and enforce granular access policies, thereby restricting unauthorized access and mitigating potential security breaches (Hu et al., 2014). Meanwhile, data encryption mechanisms ensure the confidentiality, integrity, and availability of data, both at rest and in transit, by protecting it from unauthorized access and tampering (Goyal & Goyal, 2016).

B. Importance of Cloud Security

The importance of cloud security cannot be overstated in today's digital landscape, where data is considered one of the most valuable assets. Organizations across various sectors, including healthcare, finance, education, and government, rely heavily on cloud computing to store and process sensitive information. Consequently, any compromise in cloud security can lead to severe repercussions, such as financial losses, reputational damage, regulatory penalties, and loss of customer trust (Subashini & Kavitha, 2011).

One of the critical aspects of cloud security is ensuring that data remains confidential, meaning that it is accessible only to authorized users. Data breaches, where unauthorized entities gain access to sensitive information, pose a significant threat to this principle. For instance, high-profile data breaches involving cloud services have highlighted vulnerabilities that can be exploited by malicious actors (Chhabra & Dixit, 2013). These incidents underscore the need for robust access control mechanisms and encryption techniques to protect data from unauthorized access.

Additionally, data integrity is crucial in cloud environments. It ensures that data is accurate, consistent, and has not been altered in an unauthorized manner. Ensuring data integrity is essential for maintaining trust in cloud services and for the proper functioning of applications that rely on this data (Chen & Zhao, 2012). Encryption plays a vital role in maintaining data integrity by making it extremely difficult for unauthorized users to alter data without detection.

Furthermore, data availability, the assurance that data is accessible when needed, is another fundamental aspect of cloud security. Disruptions to data availability, whether due to cyber-attacks or service outages, can have severe operational impacts (Ardagna et al., 2015). By implementing policy-based access controls and robust encryption mechanisms, organizations can enhance the resilience of their cloud infrastructures, ensuring that data and applications remain available even in the face of security threats.

In summary, cloud security is a critical concern that requires comprehensive strategies to protect sensitive data and resources. The implementation of policy-based access control and data encryption mechanisms addresses key security challenges, enhancing the overall security posture of cloud environments. This research aims to provide valuable insights into these mechanisms, contributing to the development of more secure cloud computing infrastructures.

REFERENCES:

1. Goyal, S., & Goyal, P. (2016). Comparative study of symmetric and asymmetric cryptography techniques. International Journal of Advance Research in Computer Science and Management Studies, 4(3), 232238.
2. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
3. Chhabra, S., & Dixit, C. (2013). Security issues in cloud computing. In 2013 International Conference on Computing Sciences (pp. 213217). IEEE.
4. Ardagna, C. A., Asal, R., Damiani, E., & Vu, Q. H. (2015). From security to assurance in the cloud: A survey. ACM Computing Surveys (CSUR), 48(1), 2.

5. Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 1, pp. 647651). IEEE.
6. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 111.
7. Hashizume, K., Rosado, D. G., FernándezMedina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5.
8. Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., & Schnitzer, A. (2014). Policybased access control. In Encyclopedia of Cryptography and Security (pp. 911917). Springer.