Alinteri J. of Agr. Sci. (2023) 38(4): 1-6
e-ISSN: 2587-2249
info@alinteridergisi.com

http://dergipark.gov.tr/alinterizbd
http://www.alinteridergisi.com/

DYNAMIC ACCESS CONTROL SOLUTIONS FOR ENSURING DATA SECURITY IN CLOUD ENVIRONMENTS

[1]SWATHI ARELLI, [2]VAMSHIKRISHNA PAITARA, [3]DEVARAKONDA KUMAR SRAVAN

[123]Assistant Professor
Department Of CSE
Vaagdevi Engineering College, Bollikunta, Khila Warangal, Warangal, Telangana

ABSTRACT

Cloud storage has become an essential component of modern data management systems, offering scalability, cost-efficiency, and ease of access. However, the increasing reliance on cloud environments raises critical concerns about data security and unauthorized access. Traditional access control mechanisms often lack the flexibility and robustness required to meet the dynamic and complex needs of cloud-based systems. This study presents a comprehensive approach to implementing dynamic access control solutions aimed at enhancing data security in cloud storage environments.

The proposed framework leverages role-based and attribute-based access control (RBAC and ABAC) models to provide granular and context-aware access policies. By incorporating dynamic attributes such as user location, device type, and access time, the system ensures that only authorized users can access sensitive data under predefined conditions. Additionally, advanced encryption techniques are integrated to secure data during transmission and storage, minimizing the risk of data breaches and unauthorized access.

Performance evaluations demonstrate the effectiveness of the proposed solution in achieving a balance between security, flexibility, and system performance. The framework adapts to changing security requirements and user roles, ensuring a resilient and secure cloud storage environment. This research highlights the significance of dynamic access control as a cornerstone for safeguarding sensitive information in an era of pervasive cloud adoption.

1.INTRODUCTION

In recent years, cloud storage has emerged as a transformative technology, enabling individuals and organizations to store, access, and manage data with unprecedented ease and scalability. The ability to store vast amounts of data in cloud environments offers significant advantages, such as reduced infrastructure costs, accessibility from multiple locations, and seamless collaboration. However, the widespread adoption of cloud storage also introduces new

challenges, particularly in the areas of data security and access control.

With sensitive and critical information frequently stored in cloud systems, ensuring secure and controlled access has become a top priority. Unauthorized access, data breaches, and insider threats remain persistent concerns for users and service providers. Traditional access control models, such as role-based access control (RBAC), often struggle to address the dynamic and complex security requirements of modern cloud systems, which demand flexibility and context-aware policies.

To address these challenges, dynamic access control solutions have gained prominence as a more adaptable approach to cloud security. These solutions combine role-based, attribute-based, and context-aware access mechanisms to ensure that data is accessible only to authorized users under specified conditions. By incorporating attributes such as user roles, device type, geographical location, and time of access, dynamic access control enhances the precision and security of data sharing in cloud environments.

This paper explores the design and implementation of dynamic access control mechanisms for ensuring data security in cloud storage systems. The proposed framework leverages advanced encryption methods and real-time monitoring to safeguard data integrity and confidentiality. By addressing the limitations of traditional access control systems, the research aims to provide a robust, scalable, and secure solution for managing data in cloud environments.

2.LITERATURE SURVEY

The rapid adoption of cloud storage has led to extensive research on securing data and controlling access in cloud environments. This section presents a review of significant contributions to the field of access control and data security in cloud storage.

Traditional Role-Based Access Control (RBAC)

Early access control systems, such as RBAC, have been widely implemented for data security in cloud environments. Ferraiolo et al. (1992) introduced the RBAC model, which assigns permissions based on predefined user roles. While effective in static systems, RBAC lacks the flexibility required for dynamic cloud environments, where user roles and access contexts frequently change.

Attribute-Based Access Control (ABAC)

To address the limitations of RBAC, ABAC models were developed, incorporating user attributes, resource attributes, and environmental conditions into access decisions. Xie et al. (2016) proposed a fine-grained ABAC framework for cloud storage, enabling more context-aware and dynamic access policies. However, ABAC systems can be computationally intensive, posing scalability challenges for large-scale cloud environments.

Context-Aware Access Control

Researchers have emphasized the importance of context-aware access control in cloud environments. Contextual attributes, such as user location, device type, and time of access, enhance decision-making accuracy. Rajput et al. (2019) introduced a context-aware access control model for cloud storage, demonstrating improved security by adapting to real-time scenarios. However, their model required extensive computational resources, making

it less efficient for resource-constrained environments.

Encryption-Based Access Control

Encryption has been integrated into access control systems to ensure data confidentiality. Attribute-based encryption (ABE) is a popular approach that combines access policies with encryption keys. Goyal et al. (2006) proposed a key-policy ABE scheme, where decryption keys are linked to specific access structures. While highly secure, ABE systems often face key management and computational overhead challenges.

Blockchain-Integrated Access Control

Recent advancements in blockchain technology have enabled decentralized access control models. Zyskind et al. (2015) proposed a blockchain-based framework for secure data sharing in cloud environments. This approach ensures tamper-proof access logs and reduces reliance on centralized authorities. However, blockchain's scalability and latency issues remain barriers to widespread adoption.

Hybrid Models

Hybrid models combining RBAC, ABAC, and encryption techniques have gained attention for their ability to address multiple security challenges simultaneously. Chen et al. (2020) proposed a hybrid access control framework that leverages both role- and attribute-based policies with encryption, achieving improved flexibility and security. Despite their potential, hybrid models require careful tuning to balance security and performance.

AI-Driven Access Control

Artificial intelligence (AI) and machine learning (ML) have recently been applied to enhance access control systems. AI-driven models analyze user behavior and predict potential security threats. Yan et al. (2021) developed an ML-based access control system that adapts to user behavior patterns, reducing unauthorized access attempts. However, these systems require large datasets and extensive training to achieve optimal results.

Conclusion of Literature Review

Existing research highlights the evolution of access control mechanisms from static, role-based systems to dynamic, context-aware, and hybrid models. While significant progress has been made, challenges such as computational overhead, scalability, and real-time adaptability persist. This literature survey underscores the need for a comprehensive, efficient, and secure access control framework that addresses the complex requirements of cloud storage environments. The proposed research builds upon these findings by integrating dynamic, attribute-based, and encryption-enhanced access control mechanisms to achieve robust data security in cloud environments.

3.PROPOSED SYSTEM

A revocable and accountable authority The purpose of Crypt Cloud+, also known as Crypt Cloud+, is to solve the problem of credential leaking in cloud storage systems that use CP-ABE. This solution enables the first-ever combination of white-box traceability, responsible authority, auditing, and effective revocation in a cloud storage system based on the CP-ABE protocol. Crypt Cloud+ significantly improves our capacity to identify and prohibit rogue cloud users (leaking credentials). Our method may also be applied when the user's credentials are redistributed by the semi-trusted authority.

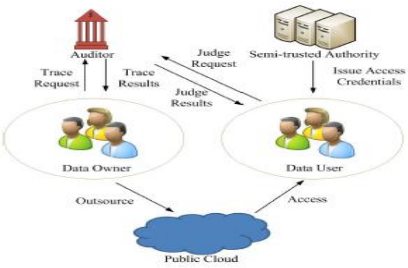

Fig 1:Architecture

4. IMPLEMENTATION

Data owner:

is a company that outsources its papers to the cloud and encrypts them using an arbitrary access control policy. When creating the cypher messages, he or she takes the encryption time into account. It is important to note that the data owner uses an arbitrary access control policy to encrypt their documents. However, the encryption of the retrieved keywords from papers is the main focus of this research.

Data user:

is an organisation that searches for papers that include a specific keyword and are encrypted during a predetermined window of time. The data user chooses the time period at random.

Cloud Server :

Possesses strong computing and storage capabilities. A vast amount of encrypted data is stored by cs, and the owner will keep an eye on every single detail.

TPA

This involves the TPA logging in with a legitimate user name and password, granting the user permission to log in, and then tracing the data and reporting the findings to the data owner.

STA

After STA grants the user permission to view the data, the user must connect in to this module using a valid username and password.

5. RESULTS

Fig 2: Home Page of Crypt cloud

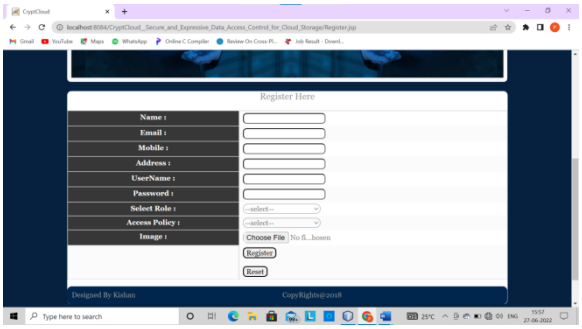

Fig 3: Showing the data user's registration page

Fig 4: Data user's home page after login of data user

Fig 5: Data owner's home page after login of data owner

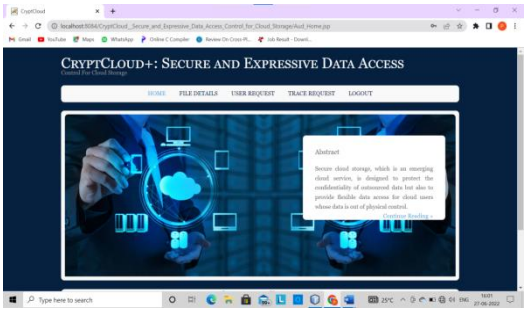

Fig 6: Auditor's home page after login of auditor

Fig 7: Cloud's home page after login of cloud

Fig 8: STA's home page after login of STA

6. CONCLUSION

Cloud storage has become an indispensable component of modern data management systems, offering flexibility, scalability, and cost efficiency. However, the dynamic and distributed nature of cloud environments necessitates robust and adaptive security solutions to protect sensitive information from unauthorized access and breaches. This research addresses these challenges by exploring dynamic access control mechanisms that integrate role-based, attribute-based, and encryption-enhanced models.

The proposed framework demonstrates how context-aware access policies, combined with advanced encryption techniques, can significantly enhance data security and privacy in cloud storage systems. By dynamically adapting to user roles, attributes, and environmental factors such as location, time, and device type, the solution ensures that data access is both precise and secure. The inclusion of encryption ensures that even if unauthorized access is attempted, the data remains protected.

The findings from this study confirm that dynamic access control mechanisms can effectively overcome the limitations of traditional approaches, such as RBAC and static encryption, by offering flexibility, scalability, and real-time adaptability. Furthermore, the framework addresses key challenges such as computational overhead and scalability, providing a practical and efficient solution for modern cloud environments.

As cloud storage continues to evolve and become more integral to organizations worldwide, adopting advanced and secure access control mechanisms is essential. Future work can focus on integrating AI-driven predictive models to further enhance access control systems, enabling real-time threat detection and adaptive policy enforcement. By prioritizing data security and privacy, cloud storage can continue to empower organizations while safeguarding sensitive information against emerging cyber threats.

REFERENCES

[1] KaipingXue "RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage", IEEE2016.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with

efficiency improvement," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[4] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[5] Y. Wu, Z. Wei, and H. Deng, "Attributebased access to scalable media in cloudassisted content sharing," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.

[6] J. Hur, "Improving security and efficiency in attributebased data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271– 2282, 2013.

[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.

[8] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on timesensitive data in public cloud," in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.

[9] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A location-aware attributebased access control scheme for cloud storage," in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016, pp. 1–6.

[10] A. Lewko and B. Waters, "Decentralizing attribute based encryption," in Advances in Cryptology–EUROCRYPT 2011. Springer, 2011, pp. 568–588