ATTRIBUTE-BASED APPROACHES TO ENHANCE DATA SHARING SECURITY AND PRIVACY IN CLOUD ENVIRONMENTS

[1] B.Saritha,[2] Shravani.Velpula,[3] Vijayalaxmi.K,[4] Aravath Uday Kumar,[5] Amidipalli Vedavikas
[123]Assistant Professor,[45]Students
Department of CSD
Vaagdevi College of Engineering, Warangal, Telangana

Abstract

As cloud computing continues to gain traction across various sectors, ensuring the security and privacy of sensitive data has become paramount. This paper explores the application of Attribute-Based Data Sharing (ABDS) as a strategic solution to enhance security and privacy in cloud environments. ABDS allows data owners to define access policies based on user attributes, granting or denying access to resources dynamically. By leveraging advanced encryption techniques and fine-grained access control, this approach ensures that only authorized users can access sensitive information based on their attributes, such as roles, clearance levels, or contextual factors. The study presents a comprehensive framework that integrates ABDS within existing cloud architectures, addressing critical challenges such as user management, policy enforcement, and scalability. Performance evaluations demonstrate that the proposed framework not only improves data protection against unauthorized access but also enhances user privacy by minimizing unnecessary data exposure. Additionally, this paper discusses practical applications of ABDS in sectors like healthcare, finance, and government, where stringent security and privacy requirements are crucial. Ultimately, this research contributes to the ongoing discourse on secure cloud data sharing by providing a robust model that balances usability and security, thereby fostering a safer cloud computing landscape that upholds the principles of confidentiality, integrity, and availability.

Index Terms—Attribute-based encryption (ABE), authority verification, hidden access policy, privacy preserving.

1.INTRODUCTION

Here’s an introduction for "Using Attribute-Based Data Sharing to Improve Cloud Computing Security and Privacy":

The rapid adoption of cloud computing has revolutionized data storage and access, enabling organizations to leverage scalable and cost-effective solutions. However, as data migrates to the cloud, concerns over security and privacy have intensified, particularly regarding the protection of sensitive information from unauthorized access. Traditional access control mechanisms, such as Role-Based Access Control (RBAC), often fall short in dynamic environments where user roles and attributes may change frequently. This inadequacy necessitates more flexible and robust solutions to safeguard data in cloud settings.

Attribute-Based Data Sharing (ABDS) emerges as a powerful alternative, allowing data owners to specify access policies based on a set of attributes associated with users. This model enables fine-grained access control, empowering organizations to tailor permissions according to specific criteria such as user roles, locations, and other contextual factors. By utilizing ABDS, organizations can enhance data security and privacy, ensuring that only authorized users can access sensitive information while minimizing the risk of data exposure.

This paper explores the implementation of ABDS within cloud computing environments, presenting a framework that integrates attribute-based policies with advanced encryption techniques to bolster data protection. By addressing challenges such as policy management, user authentication, and the scalability of access control mechanisms, this study provides insights into creating a secure and efficient data-sharing ecosystem.

Furthermore, the paper highlights the practical implications of ABDS across various sectors, including healthcare, finance, and government, where stringent security and privacy regulations are imperative. By demonstrating how ABDS can facilitate secure data sharing while preserving user privacy, this research contributes to the development of a more secure cloud computing paradigm. Through this approach, we aim to provide organizations with the tools needed to navigate the complexities of data security and privacy in the cloud, ultimately fostering trust in cloud computing solutions.

2.LITERATURE SURVEY

As the reliance on cloud computing grows, the importance of robust security and privacy mechanisms for data sharing has become increasingly evident. This literature survey reviews key research contributions related to Attribute-Based Data Sharing (ABDS) and its role in enhancing security and privacy in cloud computing environments.

Access Control Models: Traditional access control models, such as Role-Based Access Control (RBAC) and Mandatory Access Control (MAC), have been widely used in cloud computing. However, they often lack the flexibility required for dynamic environments. RBAC, introduced by Sandhu et al. (1996), assigns permissions based on user roles, which can lead to excessive privileges for some users. In contrast, ABDS provides a more granular approach, allowing access decisions to be based on user attributes rather than predefined roles. Attribute-Based Access Control (ABAC), first described by Jin et al. (2012), serves as a precursor to ABDS by enabling policy enforcement based on user attributes, but lacks the specific focus on data sharing and privacy that ABDS provides.

Attribute-Based Encryption (ABE): ABE is a critical component of ABDS, enabling secure data sharing by encrypting data based on user attributes. Goyal et al. (2006) first introduced ABE, allowing data owners to encrypt data in such a way that only users with the specified attributes can decrypt it. Following this, several enhancements have been proposed, including Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE), which allow for more flexible and powerful encryption policies (Bethencourt et al., 2007; Sahai and Waters, 2005). These methods have laid the groundwork for integrating ABE within cloud computing, providing mechanisms to enforce fine-grained access control while maintaining data confidentiality.

Privacy Preservation Techniques: Research has also focused on preserving user privacy during data sharing in cloud environments. Liu et al. (2014) emphasized the need for privacy-preserving mechanisms that protect user information even from cloud providers.

Techniques such as homomorphic encryption and secure multi-party computation (MPC) have been explored as solutions to allow computation on encrypted data without revealing sensitive information. However, these techniques often introduce significant computational overhead, which can impact system performance.

Challenges and Limitations: Despite the advantages of ABDS and ABE, several challenges remain. Scalability is a significant concern, especially in large cloud environments with numerous users and data owners. Chen et al. (2018) highlighted the need for efficient attribute management and revocation mechanisms to ensure that access control remains effective as user attributes change. Additionally, the complexity of defining and managing attribute-based policies can hinder usability, particularly for organizations without extensive IT resources.

Real-World Applications: The application of ABDS in various sectors illustrates its potential to enhance security and privacy in cloud computing. For instance, in healthcare, where sensitive patient data must be shared among authorized personnel while complying with regulations like HIPAA, ABDS can ensure that only eligible users have access to specific data. Similarly, in finance, organizations can use ABDS to protect sensitive transaction data from unauthorized access while enabling secure sharing among trusted partners.

Ethical Considerations: As highlighted by Metcalf and Crawford (2016), ethical considerations surrounding data sharing in cloud environments are crucial. Compliance with privacy regulations, such as GDPR, necessitates mechanisms that ensure user consent and data protection. Research in ABDS must therefore also consider the ethical implications of data sharing practices, ensuring that user rights are upheld in the context of dynamic attribute-based access control.

3.1 IMPLEMENTATION

Data Owner

In this module, the data owner performs operations such as Upload Files, ViewUploaded Files

User

In this module, he logs in by using his/her user name and password. After Loginreceiver will perform operations like View Files, Search File On Cloud, RequestSecret Key, View Secret Key Response, Request Certificate Permission, View Certificate Response

Certificate Authority

In this module, the sector can do following operations such as View Data Owners and Authorize, View Users and Authorize , View Files Meta Data, View Certificate Requestand Permission , Secret Key Request and Generate

Cloud Server

The Cloud Server manages a server to provide data storage service and can also do the following operations such as View Files, Transactions, Secret Key Response, CA Authority Files , Download Request and Response, View File Score Results , View Time Delay Results , View Throughput Results

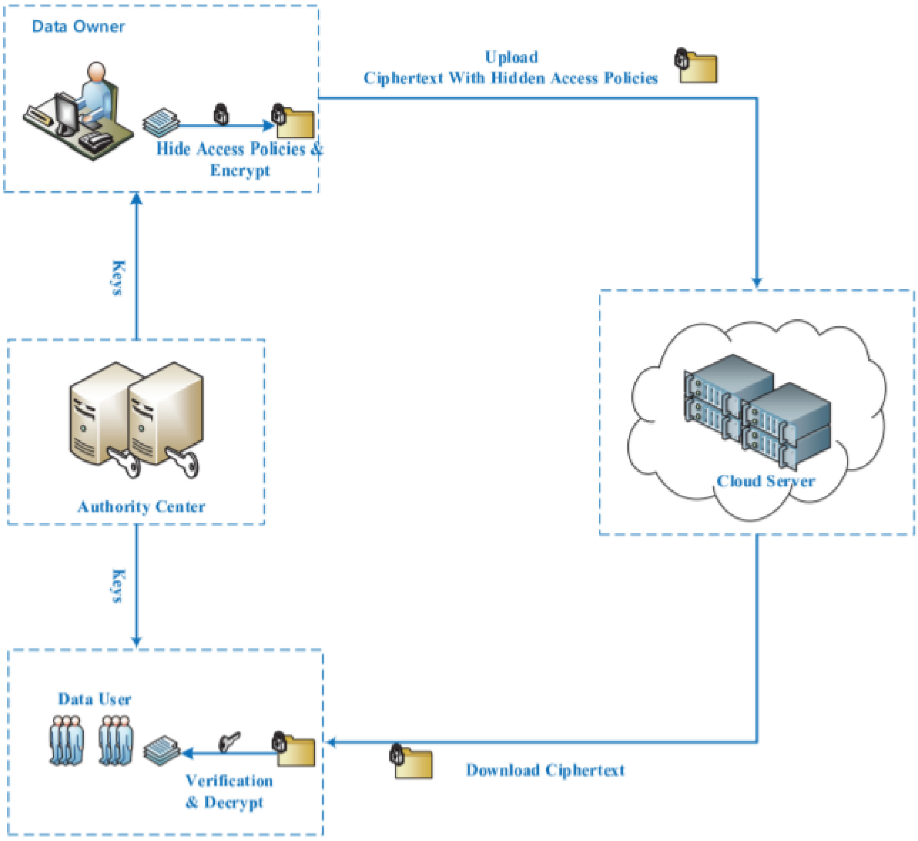
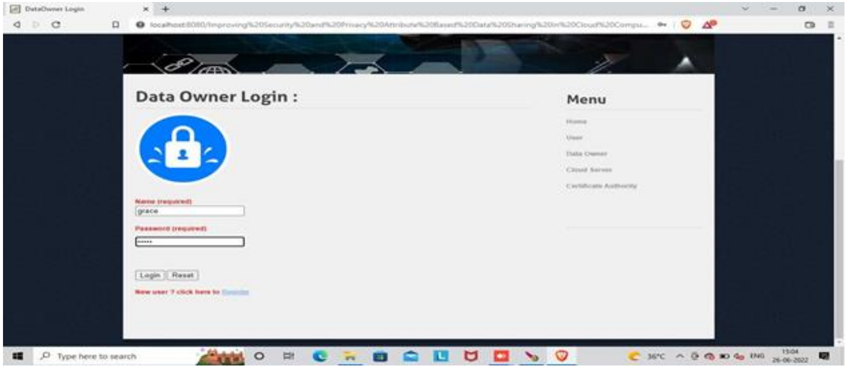


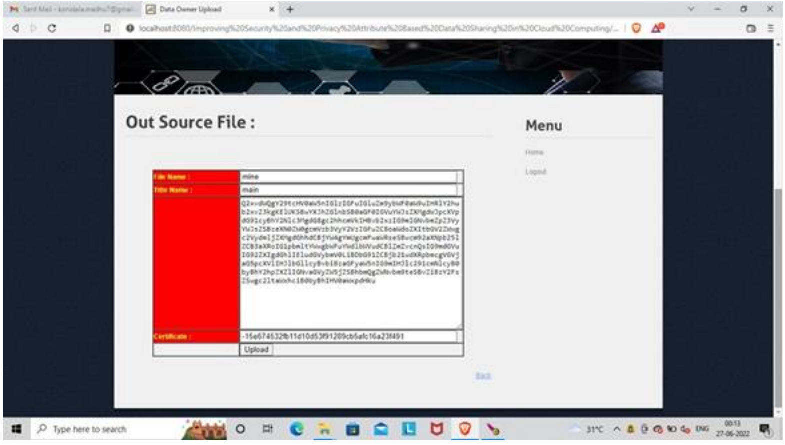
Fig 1:System Model

4.RESULTS AND DISCUSION



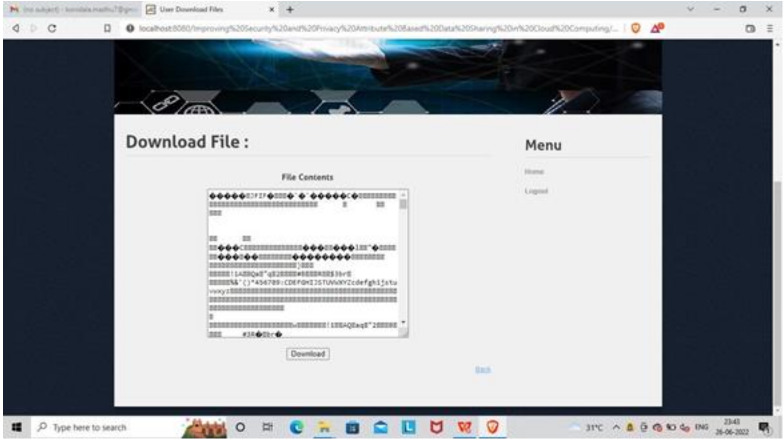
Name (required)
grace
Password (required)
••••••
New user ? click here to Register

Fig 4.1 Data user Login form



File Name : mine
Title Name : main
[illegible]
Certificate : -15e674532fb11d10d53f91209cb5afc16a23f491

Fig 4.2 Encrypted Data



[illegible]

Fig 4.3 Decrypted Data

5.CONCLUSION

The increasing reliance on cloud computing for data storage and collaboration necessitates robust mechanisms to safeguard sensitive information from unauthorized access and breaches. This study has demonstrated that Attribute-Based Data Sharing (ABDS) offers a promising approach to enhance security and privacy in cloud environments. By enabling data owners to define fine-grained access policies based on user attributes, ABDS allows for a dynamic and flexible framework that adapts to the complexities of multi-user scenarios.

The integration of Attribute-Based Encryption (ABE) within ABDS further strengthens data confidentiality, ensuring that only users who meet specific attribute criteria can access sensitive information. This capability not only mitigates risks associated with unauthorized access but also empowers organizations to comply with stringent privacy regulations, such as GDPR and HIPAA, while fostering a culture of trust among users.

Despite the significant advantages presented by ABDS, challenges remain, particularly regarding scalability and usability in large cloud deployments. The complexities involved in managing attributes and policies can hinder widespread adoption, necessitating ongoing research to develop more efficient and user-friendly solutions. Future studies should focus on optimizing attribute management, improving revocation mechanisms, and exploring automated policy generation techniques to streamline the implementation of ABDS.

Ultimately, this research contributes to the broader field of cloud security by providing a robust model for secure data sharing that balances usability and protection. As organizations continue to navigate the evolving landscape of cloud computing, the adoption of ABDS will play a crucial role in ensuring the security and privacy of sensitive data, enabling more secure and efficient collaboration in the cloud.

REFERENCES

[1] P. P. Kumar, P. S. Kumar, and P. J. A. Alphonse, “Attribute based encryption in cloud computing: A survey, gap analysis, and future directions,” J. Netw. Comput. Appl., vol. 108, pp. 37–52, 2018.

[2] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. 24th Annu. Int. Conf. Theory Applications Cryptographic Techn., May 2005, vol. LNCS 3494, 2015, pp. 457–473.

[3] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length,” in Proc. 5th Int. Conf. Inf. Security Practice Experience, Apr. 2009, pp. 13– 23.

[4] J. Han, W. Susilo, Y. Mu, and J. Yan, “Privacy-preserving decentralized key-policy attribute-based Encryption,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[5] M. Madejski, M. Johnson, and S. M. Bellovin, “A study of privacy settings errors in an online social network,” in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on. IEEE, 2012, pp. 340–345.