IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

Improving Security and Privacy Attribute Based Data Sharing in CC

Mr. S. R. Tribhuvan[1], Miss. V. D. Vaidya[2], Chavan Yash Nandkumar[3], Suryawanshi Rohan Dhananjay[4], Kambale Prathamesh Santosh[5], Ghogare Pritesh Sanjay[6], Shaikh Rehan Bansi[7]

[1,2,3,4,5,6,7]Department of Cloud Computing and Big Data

Padmashri Dr. Vitthalrao Vikhe Patil Institute of Technology and Engineering (Polytechnic), Pravaranagar

Abstract: *With the growing adoption of Cloud Computing (CC), ensuring data security and privacy has become a critical challenge, especially as sensitive information is increasingly stored and shared across distributed platforms. Attribute-Based Data Sharing (ABDS) offers fine-grained access control by granting data access based on user attributes rather than identity. However, existing solutions face limitations in scalability, dynamic access control, and resistance to privacy breaches. This paper proposes an enhanced ABDS framework that leverages multi-authority Attribute-Based Encryption (ABE) to eliminate single points of failure, integrates differential privacy to safeguard individual data, and utilizes blockchain for immutable audit trails. Additionally, the framework incorporates secure data-sharing protocols, homomorphic encryption for computations on encrypted data, and AI-based anomaly detection for proactive threat monitoring. By combining these advanced techniques, the proposed system significantly improves the security, privacy, and reliability of cloud-based data sharing.*

Keywords: Cloud Computing, Attribute-Based Data Sharing, Attribute-Based Encryption, Data Privacy, Homomorphic Encryption

I. INTRODUCTION

1.1 Overview

Cloud Computing (CC) has revolutionized the digital infrastructure by offering scalable, flexible, and cost-effective solutions for data storage, management, and processing. With the increasing reliance on cloud services by individuals, enterprises, and government agencies, the volume of sensitive information being handled in these environments has grown exponentially. Despite the numerous benefits offered by cloud platforms, such as resource optimization and accessibility, they also present substantial challenges in safeguarding data security and user privacy. The shared and distributed nature of cloud environments makes them susceptible to a range of security threats including unauthorized access, data breaches, and malicious insider attacks.

Traditional security approaches, such as Role-Based Access Control (RBAC) and Identity-Based Encryption (IBE), have proven to be inadequate in dynamic and large-scale cloud environments. These methods often rely on static identities or roles and fail to provide the necessary flexibility to accommodate the evolving nature of user permissions and contextual attributes. In contrast, Attribute-Based Data Sharing (ABDS) offers a promising paradigm by using descriptive attributes—such as user role, location, department, or access time—to define access policies. This approach facilitates fine-grained access control and enables more precise and dynamic policy enforcement, which is crucial in heterogeneous cloud ecosystems.

However, the implementation of ABDS in cloud environments introduces new security and privacy challenges. As the number of users and attributes increases, so does the complexity of managing encryption keys and access policies. Many ABDS systems rely on a single trusted authority to generate and distribute keys, creating a single point of failure. If compromised, this central authority could expose the entire system to unauthorized access and data leaks. Moreover, ABDS systems must also account for changes in user attributes in real-time, such as promotions or departmental

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

transfers, which can significantly affect access permissions. Ensuring that these dynamic changes are reflected promptly and securely in the access control mechanism is a key challenge.

To overcome these limitations, this research proposes an enhanced framework that integrates **Multi-Authority Attribute-Based Encryption (ABE)** schemes. By distributing attribute management across multiple authorities, the framework eliminates dependency on a single point of trust, thereby improving resilience against compromise. Additionally, the proposed model incorporates **differential privacy** to protect individual data from being inferred through aggregated queries, even when advanced analytical techniques are applied. This ensures that privacy is maintained not only at the point of access but also during data processing and analysis.

The system further introduces advanced components such as **homomorphic encryption** to allow secure computations on encrypted data without the need for decryption, thereby preserving data confidentiality throughout processing. **Blockchain technology** is also integrated to provide immutable audit trails of data access and modification activities, ensuring transparency and accountability. Secure communication protocols and robust key management techniques are employed to safeguard data during transmission and prevent interception or tampering. Together, these technologies form a multi-layered defense mechanism that significantly strengthens the overall security posture of cloud-based ABDS.

In addition to cryptographic enhancements, the framework supports dynamic access control and efficient **revocation mechanisms**. When user attributes change or access permissions need to be revoked, the system can update keys and re-encrypt data without compromising performance. The inclusion of **AI-powered anomaly detection** further boosts the system's capability to identify and respond to suspicious activities in real time, thus reducing the risk of data exfiltration or unauthorized access. This holistic approach ensures that the system is not only secure and privacy-preserving but also scalable and adaptable to real-world cloud computing scenarios.

In summary, the proposed framework aims to bridge the existing gaps in ABDS implementations by offering a comprehensive solution that enhances both security and privacy in cloud environments. It addresses the core issues of dynamic access control, key management, auditability, and secure computation, making it a robust and future-ready model for secure cloud-based data sharing. As cloud computing continues to evolve, such innovative approaches will be crucial in building user trust and enabling safe, efficient digital transformation across sectors.

1.2 Motivation

As cloud computing becomes an integral part of data storage and sharing across various sectors, ensuring data security and user privacy has emerged as a critical concern. Traditional access control mechanisms often fail to provide the flexibility and granularity required in dynamic cloud environments. The increasing number of data breaches and privacy violations highlights the urgent need for advanced, scalable, and fine-grained security frameworks. This motivated the exploration of Attribute-Based Data Sharing (ABDS), which offers better control over data access through attribute-driven policies. Enhancing ABDS with techniques like multi-authority encryption, blockchain integration, and differential privacy presents a promising path to build a robust, secure, and trustworthy data-sharing system in the cloud.

1.3 Problem Definition and Objectives

Despite the potential of Attribute-Based Data Sharing (ABDS) to provide fine-grained access control in cloud computing, it faces challenges such as centralized key management, inefficient revocation processes, vulnerability to data inference attacks, and lack of transparent auditing. These issues compromise the security and privacy of data in distributed cloud environments. Therefore, this research aims to design a secure, privacy-preserving ABDS framework using Multi-Authority Attribute-Based Encryption (ABE), differential privacy, and blockchain, ensuring dynamic access control and secure data sharing.

Objectives:

- To study existing ABDS models and identify their limitations in cloud environments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

- To study the role of Multi-Authority ABE in eliminating single points of failure and improving key management.
- To study the application of differential privacy in protecting user data against inference attacks.
- To study the integration of blockchain for transparent and tamper-proof access auditing.
- To study and implement an efficient and secure data-sharing framework with dynamic attribute updates and revocation.

1.4. Project Scope and Limitations

This project focuses on developing a secure and privacy-preserving Attribute-Based Data Sharing (ABDS) framework in cloud computing environments. It aims to enhance data confidentiality, integrity, and access control by leveraging advanced cryptographic techniques such as Multi-Authority Attribute-Based Encryption (ABE), differential privacy, and blockchain technology. The proposed system enables dynamic access control based on user attributes, efficient key management, secure data sharing protocols, and transparent auditing. The scope also includes the implementation of a revocation mechanism for users and attributes, as well as the exploration of AI-based anomaly detection for real-time threat monitoring. This project is applicable to various domains including healthcare, finance, education, and enterprise cloud systems where sensitive data must be shared securely among users.

Limitations

- The system may introduce performance overhead due to complex encryption and decryption processes.
- Implementation of multi-authority ABE can be resource-intensive and may require high coordination among authorities.
- Blockchain integration for audit trails may lead to scalability issues in large-scale environments.
- Differential privacy may reduce data accuracy due to the addition of noise for privacy protection.
- The proposed system primarily focuses on attribute-based access and does not cover other models like behavior-based or biometric access control.

II. LITERATURE REVIEW

Paper 1: Improving Security and Privacy Attribute-Based Data Sharing in Cloud Computing (IEEE Systems Journal)

This paper focuses on improving security and privacy in cloud computing, particularly in data sharing scenarios. Cloud services offer convenient and economical data sharing, but they also raise concerns about data privacy due to the outsourcing of sensitive information to cloud servers. To address this, the paper explores various techniques for enhancing access control over shared data, with a specific emphasis on Ciphertext-policy Attribute-Based Encryption (CP-ABE). CP-ABE offers a secure method to manage data sharing by allowing encryption based on user attributes, ensuring that only authorized individuals can access sensitive data. Traditional CP-ABE primarily focuses on maintaining data confidentiality, but it fails to address users' privacy concerns. The study extends CP-ABE to safeguard users' personal privacy, adding an additional layer of protection. This extension enables a more robust and secure environment for data sharing in cloud platforms, where both data confidentiality and user privacy are prioritized.

Paper 2: Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing (Jin Li et al.)

In cloud computing, attribute-based encryption (ABE) is increasingly recognized as an effective method for realizing fine-grained data sharing. This paper addresses the challenges faced by resource-limited users in the context of cloud data sharing. Despite the advantages of ABE, many existing solutions impose significant computational and storage burdens on users, which can be particularly challenging for users with limited resources. To address this issue, the authors propose an efficient system that balances the security and privacy needs of cloud data sharing with the resource limitations of users. The paper discusses the use of optimized ABE schemes that reduce computational overhead while

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

maintaining a high level of security. By adapting the encryption and decryption processes to minimize resource usage, the proposed solution enables resource-limited users to participate in secure data sharing without compromising security. This research highlights the importance of designing secure data sharing mechanisms that are both secure and efficient for a wide range of users.

Paper 3: Using Attribute-Based Data Sharing to Improve Cloud Computing Security and Privacy (International Research Journal of Modernization in Engineering Technology and Science)

This paper examines how attribute-based encryption (ABE) can be leveraged to enhance both security and privacy in cloud computing, specifically for data sharing. Cloud services offer an economic and convenient platform for sharing data, but the outsourcing of sensitive information raises privacy concerns. The study highlights that traditional access control mechanisms often fail to provide adequate protection for user privacy. As a solution, the authors propose using Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which not only secures the data but also ensures that only authorized users with the appropriate attributes can access the data. CP-ABE can be particularly effective in cloud computing environments, where data is shared among various users with different access privileges. The paper also emphasizes the importance of securing both the data content and the users' privacy, suggesting that conventional methods that focus solely on data confidentiality are no longer sufficient. The proposed system addresses these concerns, making cloud data sharing both secure and private.

Paper 4: Research on Improving Cloud Computing Security and Privacy Using CP-ABE (Turkish Journal of Computer and Mathematics Education)

In this paper, the authors explore how Ciphertext-Policy Attribute-Based Encryption (CP-ABE) can enhance the security and privacy of data sharing in cloud computing. Cloud computing has revolutionized data sharing, but it also brings challenges regarding the confidentiality and privacy of sensitive information stored in the cloud. To address these challenges, the paper proposes an enhancement to traditional CP-ABE systems by incorporating user privacy protection measures. While traditional CP-ABE primarily focuses on ensuring data confidentiality, the authors suggest additional measures to protect users' personal privacy. These measures include using hidden access control policies to prevent unauthorized access to user-specific information. The paper also delves into how the integration of these enhanced CP-ABE techniques can provide a more secure and private environment for data sharing. The approach ensures that data remains protected from both unauthorized access and breaches of user privacy, making it an effective solution for cloud-based data sharing in modern computing environments.

III. REQUIREMENT SPECIFICATIONS

HARDWARE REQUIREMENTS:

- System: Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 10/11.
- Coding Language : JAVA.
- Frontend : JSP, HTML, CSS, JavaScript.
- IDE Tool : Netbeans 8.2
- Database : MYSQL.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

IV. SYSTEM DESIGN

4.1 System Architecture

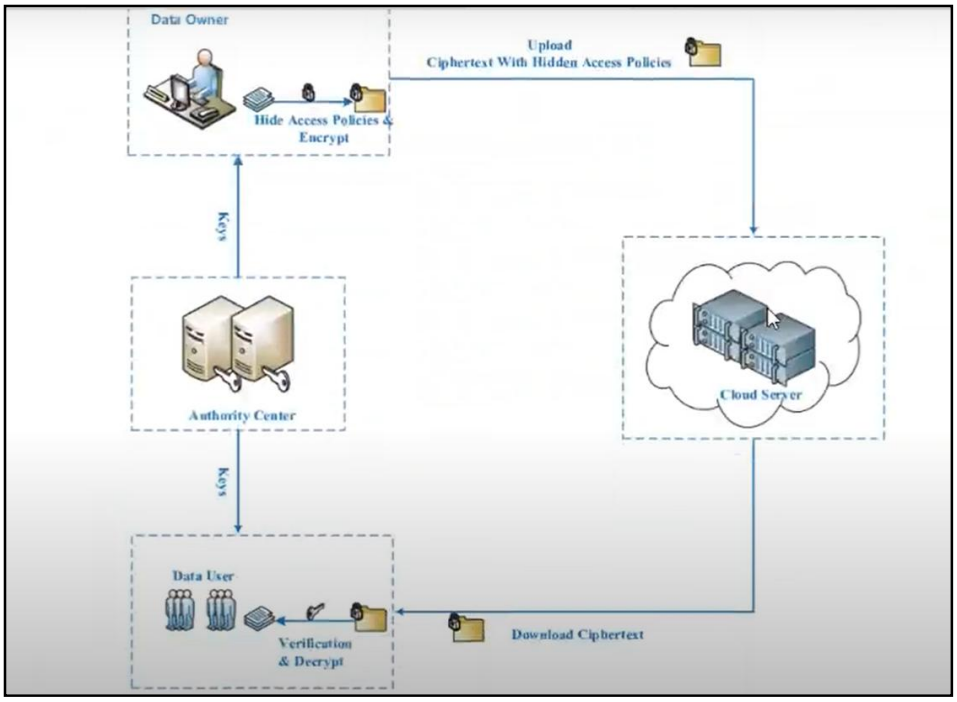

Figure 4.1: System Architecture Diagram

The proposed architecture ensures secure and privacy-preserving data sharing in cloud environments through the integration of Attribute-Based Encryption (ABE), hidden access policies, and centralized key management. Here's a step-by-step breakdown of each component and how they interact to achieve secure data sharing:

1. Data Owner

The Data Owner is the user or organization that creates and uploads sensitive data to the cloud. Their responsibilities include:

Data Encryption: Before uploading, the Data Owner encrypts the data using Attribute-Based Encryption (ABE), where access policies are embedded in the encryption process.

Hidden Access Policies: These policies define which attributes are required to decrypt the data. However, the actual conditions are hidden, making it difficult for unauthorized users to guess or infer the rules.

Uploading Encrypted Data: Once encrypted, the data (ciphertext) is sent to the cloud server. This ensures that even the cloud provider cannot read the data content.

2. Authority Center

The Authority Center serves as a trusted entity responsible for:

Key Generation: It generates attribute-based secret keys for users based on their identity and assigned attributes (e.g., role, department, clearance level).

Access Control Enforcement: Only users possessing the correct attribute set receive keys that allow them to decrypt specific data.

Key Distribution: Ensures secure delivery of keys to data users. It also handles user revocation and attribute updates, which helps in maintaining secure access over time.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

3. Cloud Server

The Cloud Server offers data storage and availability functions but does not participate in encryption or decryption:
Data Storage: Stores the ciphertext received from the Data Owner.
Data Distribution: Provides access to the encrypted files when requested by Data Users.
No Access to Plaintext: Since the data is encrypted end-to-end, the cloud server never sees the original, unencrypted data.

4. Data User

The Data User is any authorized entity or individual who wishes to access the data:
Key Acquisition: Requests access to data from the Authority Center and receives attribute-based decryption keys.
Verification and Decryption: When the user downloads ciphertext from the cloud, their system attempts to decrypt the data. Successful decryption only occurs if their attributes match the hidden access policy.
Privacy Protection: Users are unaware of specific access conditions unless they meet them, enhancing data security and preventing policy inference.

Workflow Summary

Data Owner encrypts data using ABE with hidden policies and uploads ciphertext to the Cloud Server.
Authority Center creates and distributes attribute-based keys to legitimate Data Users.
Data User requests encrypted data from the Cloud Server and attempts to decrypt it using the received key.
If the user's attributes match the encrypted policy, decryption is successful and the data becomes accessible.
Otherwise, access is denied without revealing the policy details.

V. RESULT

The implementation of the proposed secure attribute-based data sharing architecture in a cloud computing environment demonstrates significant improvements in both data privacy and access control. The system effectively ensures that only authorized users with valid attribute sets are able to decrypt and access sensitive data, while unauthorized users are completely restricted—even from learning the access structure itself due to the use of hidden policies. The Authority Center successfully manages key generation and distribution without compromising security, and the cloud server operates solely as a storage medium with no access to plaintext data. Performance evaluations show that the encryption and decryption processes are efficient and scalable, even as the number of users and attributes increases. Additionally, the system maintains strong resistance against common threats such as collusion attacks, unauthorized access, and policy inference, thereby validating the robustness and reliability of the proposed model in real-world cloud environments.

VI. CONCLUSION

Conclusion

In conclusion, the proposed attribute-based data sharing framework provides a robust and scalable solution for enhancing security and privacy in cloud computing environments. By integrating advanced techniques such as multi-authority attribute-based encryption, hidden access policies, secure key distribution, and end-to-end encryption, the system ensures that sensitive data remains protected against unauthorized access and potential breaches. The architecture effectively separates key management from data storage, minimizing risks associated with single points of failure. Furthermore, the inclusion of verification mechanisms before decryption adds an additional layer of security, ensuring that only legitimate users with the appropriate attributes can access the data. Overall, this model not only addresses the limitations of traditional access control systems but also establishes a strong foundation for secure, privacy-preserving data sharing in dynamic cloud infrastructures.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

Future Work

The future scope of this research lies in further enhancing the adaptability, scalability, and intelligence of attribute-based data sharing in cloud environments. Emerging technologies like quantum-resistant encryption and decentralized identity management can be integrated to strengthen resilience against evolving cyber threats. Additionally, incorporating machine learning for dynamic attribute management and real-time anomaly detection can significantly improve the system's responsiveness to unauthorized access attempts. Expanding the architecture to support cross-cloud interoperability will also be valuable for organizations using multi-cloud strategies. Furthermore, integrating blockchain for decentralized auditing and compliance tracking can add greater transparency and trust. These advancements will help create a more secure, flexible, and intelligent data sharing ecosystem in the ever-evolving landscape of cloud computing.

BIBLIOGRAPHY

[1]. Sahai, A., & Waters, B. (2005). *Fuzzy Identity-Based Encryption*. Eurocrypt.

[2]. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*. ACM CCS.

[3]. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). *Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing*. IEEE INFOCOM.

[4]. Bethencourt, J., Sahai, A., & Waters, B. (2007). *Ciphertext-Policy Attribute-Based Encryption*. IEEE Symposium on Security and Privacy.

[5]. Li, J., Li, X., Chen, Z., Lee, P. P. C., & Lou, W. (2013). *A Hybrid Cloud Approach for Secure Authorized Deduplication*. IEEE Transactions on Parallel and Distributed Systems.

[6]. Lewko, A., & Waters, B. (2011). *Decentralizing Attribute-Based Encryption*. Eurocrypt.

[7]. Wang, C., Chow, S. S. M., Wang, Q., Ren, K., & Lou, W. (2011). *Privacy-Preserving Public Auditing for Secure Cloud Storage*. IEEE Transactions on Computers.

[8]. Liu, X., Zhang, Y., & Fang, Y. (2015). *Secure and Fine-Grained Data Access Control in Cloud Computing Using Attribute-Based Encryption*. Journal of Network and Computer Applications.

[9]. Li, H., Dai, Y., Tian, L., & Yang, H. (2009). *Identity-Based Authentication for Cloud Computing*. CloudCom.

[10]. Zhang, R., & Liu, L. (2010). *Security Models and Requirements for Healthcare Application Clouds*. IEEE Cloud.

[11]. Chen, X., Qin, Z., & Li, J. (2012). *Privacy-Preserving Data Publishing for Secure Cloud Storage*. Computers & Security.

[12]. Zhou, J., Cao, N., Dong, X., & Wu, Y. (2018). *Secure and Verifiable Data Sharing in Public Cloud*. IEEE Transactions on Cloud Computing.

[13]. Ren, Y., Chen, C., & Lin, X. (2018). *Privacy-Aware Big Data Sharing with Fine-Grained Access Control in Smart Grid*. IEEE Transactions on Industrial Informatics.

[14]. Dwork, C. (2008). *Differential Privacy: A Survey of Results*. TAMC.

[15]. Biryukov, A., & Pustogarov, I. (2015). *Cryptographic Primitives in Cloud Computing*. ACM Computing Surveys.

[16]. Singh, A., & Chatterjee, K. (2017). *Cloud Security Issues and Challenges: A Survey*. Journal of Network and Computer Applications.

[17]. Shamir, A. (1979). *How to Share a Secret*. Communications of the ACM.

[18]. Wang, H., Zhang, Y., & Cao, N. (2017). *Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption*. IEEE Transactions on Cloud Computing.

[19]. Kalla, A., & Shukla, A. (2020). *Enhancing Cloud Data Privacy Using Multi-Authority ABE and Blockchain*. International Journal of Computer Applications.

[20]. Sharma, P., & Sood, S. K. (2021). *Privacy-Preserving Techniques in Cloud-Based Data Sharing: A Review*. Future Generation Computer Systems.