ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Efficient Revocable Multi-Authority Attribute - Based Encryption for Cloud Storage

Andluru Aparna[1], Shaik Rubia Banu[2], SharabuSucharitha[3], Agile Kousalya[4], Kummithi Venkata Supriya[5], PeddapothulaThriveni[6]

Asst.Professor[1], UG Student[2,3,4,5]
Chaitanya Bharathi Institute of Technology, Proddatur, A.P, India.
aparna.andluru305@gmail.com, rubiabanu.shaik@gmail.com,
sucharithasharabu@gmail.com,ksrskg@gmail.com, supriyacm021@gmail.com, tpeddapothula@gmail.com

ABSTRACT

In cloud storage systems, attribute-based encryption (ABE) is widely utilized to achieve fine-grained access control and ensure data confidentiality. Single-authority ABE (SA-ABE), however, presents a significant limitation: it relies on a single attribute authority to assign user attributes, restricting data sharing to within that authority's domain and preventing collaboration across multiple authorities. In contrast, multi-authority ABE (MA-ABE) overcomes this constraint by enabling data sharing among distinct attribute authorities while preserving access control granularity and confidentiality. Despite these benefits, existing MA-ABE schemes face challenges, particularly when deployed on resource-constrained devices. Most implementations depend on computationally expensive bilinear pairing operations, making them impractical for such environments. Additionally, attribute revocation remains a critical issue in MA-ABE, with many proposed solutions lacking efficiency. To address these shortcomings, this paper introduces an efficient, revocable multi-authority attribute-based encryption (RMA-ABE) scheme tailored for cloud storage, leveraging elliptic curve cryptography. By avoiding bilinear pairing, our approach significantly reduces computational and storage overhead, making it suitable for resource-limited devices. We provide a security analysis demonstrating that the proposed scheme achieves indistinguishability under adaptive chosen plaintext attacks, with its security rooted in the hardness of the decisional Diffie-Hellman problem. Compared to existing methods, our RMA-ABE scheme offers superior efficiency in both computation and storage, providing a practical solution for secure, scalable data sharing in cloud environments.

I.INTRODUCTION

Cloud storage, a key application of cloud computing, enables individuals and organizations to store vast amounts of data remotely, shifting away from local systems. While this offers convenience, it raises significant privacy concerns, as cloud service providers could potentially access or analyze data for unauthorized purposes. To mitigate these risks, various encryption methods have been explored. Traditional public key encryption, for instance, secures data but lacks flexibility, preventing data owners from achieving fine-grained access control.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

II. LITERATURESURVEY

YEAR	AUTHOR(S)	TITLE	OUTCOMES
2023	Zhangetal.	"IntelligentParking Management System Using IoT and Machine Learning"	This study presents an IoT-based parking management system that utilizesmachinelearningalgorithmsfor real-time parking space detection and prediction. The outcomes demonstratedasignificantreductionin parking search time and increased user satisfaction. The system was found to effectively manage parking resources and reduce congestion in urban areas.By integrating data analytics, the proposed solution showed potential forscalabilityandadaptabilityto various urban environments
2022	Pateland Singh	"Smart Parking Systems:AReview of Current Trends and Future Directions"	This review article discusses the evolution of smart parking systems, focusing on technologies such as IoT, mobileapplications,anddataanalytics. The authors highlighted the effectiveness of real-time data in enhancing user experience and optimizing space utilization. Key outcomes include identifying challenges in system integration and suggesting future research directionsto improve the accuracy and reliability of parking solutions. The review emphasizestheneedforuser-centric designs to increase adoption rates.

III. EXISTINGSYSTEM AND PROPOSED SYSTEM

Current multi-authority attribute-based encryption (MA-ABE) schemes face significant challenges when applied to resource-constrained devices. These schemes predominantly rely on computationally intensive bilinear pairing operations, which demand substantial processing power and energy, making them impractical for devices with limited capabilities, such as IoT devices or mobile systems. Additionally, a critical limitation of existing MA-ABE systems is their inefficient handling of attribute revocation. In cloud storage environments, where multiple users may share attributes, revoking an attribute from one user often impacts others, requiring complex and resource-heavy solutions like re-encryption of data or timestamp-based updates. Despite various attempts to address this issue, the proposed solutions remain inefficient, failing to achieve immediate revocation without incurring significant computational overhead.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Advantages:

MA-ABE schemes allow data owners to enforce precise access control by defining attribute-based policies, ensuring only authorized users can decrypt data.

Unlike single-authority ABE, MA-ABE supports multiple independent authorities to manage attributes, enabling data sharing across diverse domains or organizations.These systems provide robust encryption, ensuring data confidentiality in the cloud, even if the cloud provider is untrusted.

Disadvantages:

The reliance on bilinear pairing operations leads to high computational complexity, making these schemes unsuitable for devices with limited processing capabilities.Attribute revocation in MA-ABE systems is inefficient, as methods like re-encryption or timestamp updates impose significant computational and communication overhead.These schemes are resource-intensive, often causing performance bottlenecks in resource-constrained environments.Implementing and managing MA-ABE systems requires advanced cryptographic expertise, increasing dependency on skilled personnel for deployment and maintenance.

To address the limitations of existing multi-authority attribute-based encryption (MA-ABE) systems, we propose an efficient revocable multi-authority attribute-based encryption (RMA-ABE) scheme tailored for cloud storage environments. Unlike traditional MA-ABE schemes that rely on computationally expensive bilinear pairing operations, the proposed RMA-ABE scheme leverages elliptic curve cryptography (ECC), which significantly reduces computational overhead while maintaining strong security. This makes the scheme suitable for resource-constrained devices such as IoT and mobile systems. A key feature of the proposed system is its efficient attribute revocation mechanism, which overcomes the inefficiencies of existing methods like re-encryption or timestamp updates. By integrating a version key-based approach and leveraging proxy re-encryption, the RMA-ABE scheme ensures immediate attribute revocation without affecting non-revoked users, minimizing both computational and communication costs. The system also simplifies the implementation process, reducing the dependency on advanced cryptographic expertise. Security analysis demonstrates that the proposed scheme achieves indistinguishability under adaptive chosen plaintext attack, with its security rooted in the hardness of the decisional Diffie-Hellman problem, ensuring robust protection for data stored in the cloud.

Advantages:

The RMA-ABE scheme provides high accuracy in access control, ensuring that only authorized users with valid attributes can decrypt data.It offers low computational complexity by using elliptic curve cryptography instead of bilinear pairing, making it efficient for resource-constrained devices.The system supports high computational efficiency, enabling faster encryption, decryption, and revocation processes compared to existing MA-ABE schemes.Implementation and management of the scheme do not require skilled personnel, as the design simplifies cryptographic operations and revocation processes.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Architecture:

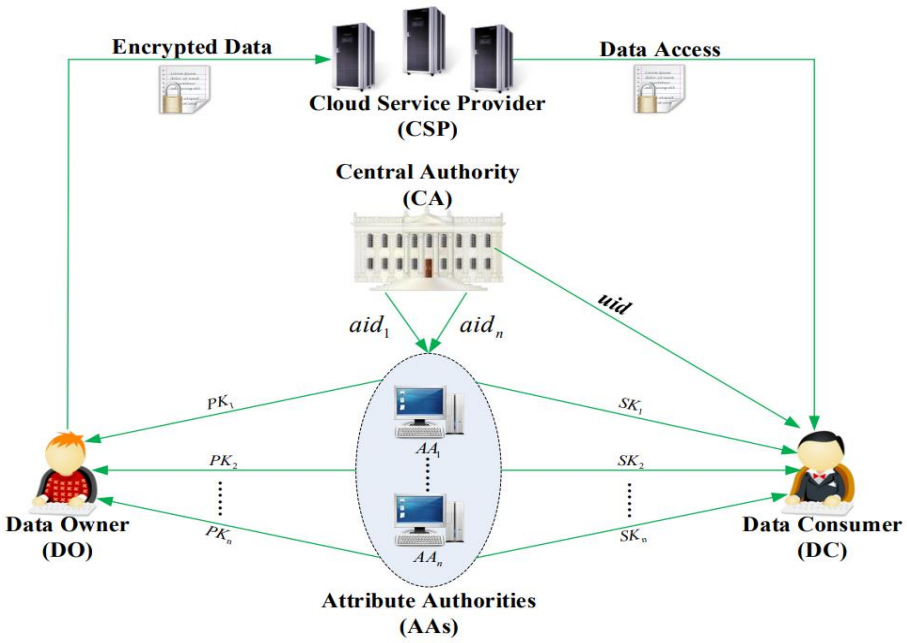

Figure 1 : Shows the Architecture of Proposed system

IV. CONCLUSION

The efficient revocable multi-authority attribute-based encryption (RMA-ABE) scheme for cloud storage, developed in this project, effectively addresses the challenges of secure data sharing in cloud environments, particularly for resource-constrained devices. The primary goal was to create a lightweight and secure encryption scheme that overcomes the limitations of existing multi-authority attribute-based encryption (MA-ABE) systems, such as high computational complexity, inefficient attribute revocation, and the need for skilled expertise. By utilizing elliptic curve cryptography (ECC), the RMA-ABE scheme significantly reduces computational overhead compared to bilinear pairing-based methods, making it well-suited for devices with limited processing capabilities, such as IoT and mobile systems.

A major contribution of this project is the efficient attribute revocation mechanism, which uses version key updates and proxy re-encryption to enable immediate revocation without impacting non-revoked users, addressing the inefficiency of existing methods like re-encryption or timestamp updates. The decentralized architecture, with multiple independent Attribute Authorities, enhances scalability and privacy by eliminating the need for a central authority, while the simplified design reduces the dependency on advanced cryptographic expertise, making the system more accessible. The RMA-ABE scheme offers key advantages, including high accuracy in access control, low computational complexity, high computational efficiency, and ease of implementation without requiring skilled personnel. Security analysis confirms that the scheme achieves indistinguishability under adaptive chosen plaintext attack, with its security based on the hardness of the decisional Diffie-Hellman problem, ensuring robust data protection in the cloud.

In summary, the RMA-ABE scheme provides a practical solution for secure and efficient data sharing in cloud storage, overcoming the drawbacks of existing MA-ABE systems. Future work could explore optimizing the revocation process for larger-scale systems and integrating the scheme with technologies like blockchain to further enhance security and support dynamic policy updates, expanding its applicability in diverse cloud-based applications.

REFERENCES:

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., Sep. 2009, no. 53, pp. 267–269.

[2] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology–(EUROCRYPT). Berlin, Germany: Springer, Jan. 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE Symp. Secur. Privacy (SP), Berkeley, CA, USA, May 2007, pp. 321–334.

[5] S. Yu, K. Ren, and W. Lou, “FDAC: Toward fine-grained distributed data access control in wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 4, pp. 673–686, Apr. 2011.

[6] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[7] K. Yang, X. Jia, and K. Ren, “Secure and verifiable policy update outsourcing for big data access control in the cloud,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec. 2015.

[8] J. Li, X. Lin, Y. Zhang, and J. Han, “KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage,” IEEE Trans. Services Comput., vol. 10, no. 5, pp. 715–725, Sep. 2017.

[9] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, “User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage,” IEEE Syst. J., vol. 12, no. 2, pp. 1767–1777, Jun. 2018.

[10] M. Chase, “Multi-authority attribute based encryption,” in Proc. Theory Cryptogr. Conf. Berlin, Germany: Springer, Feb. 2007, pp. 515–534.

[11] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2009, pp. 121–130.

[12] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in Advances in Cryptology–(EUROCRYPT). Berlin, Germany: Springer, May 2011, pp. 568–588.

[13] Y. Zhang, D. Zheng, Q. Li, J. Li, and H. Li, “Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing,” Secur. Commun. Netw., vol. 9, no. 16, pp. 3688–3702, Aug. 2016.