IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Data Sharing In Cloud Environments Using Attribute Based Proxy Re-Encryption With Integrated Revocation Mechanism

P. Kavipriya, Post Graduate
Department of Computer Science and Applications, Auxilium College(Autonomous),Gandhi Nagar-632006, Vellore District,TamilNadu,India.

Mrs.S.Shanthi
Assistant Professor,
Department of Computer Science and Applications, Auxilium College(Autonomous),Gandhi Nagar-632006, Vellore District,TamilNadu,India.

ABSTRACT- Cloud computing, which provides adequate storage and computation capability, has been a prevalent information infrastructure. Secure data sharing is a basic demand when data was outsourced to a cloud server. Attribute-based proxy re-encryption has been a promising approach that allows secure encrypted data sharing on clouds. With attribute-based proxy re-encryption, a delegator can designate a set of shared users through issuing a re-encryption key which will be used by the cloud server to transform the delegator's encrypted data to the shared users. However, the existing attribute-based proxy re-encryption schemes lack a mechanism of revoking users from the sharing set which is critical for data sharing systems. Therefore, in this article, we propose a concrete attribute-based proxy re-encryption with direct revocation mechanism (ABPRE-DR) for encrypted data sharing that enables the cloud server to directly revoke users from the original sharing set involved in the re-encryption key. We implemented the new schemes and evaluated its performance. The experimental results show that the proposed ABPRE-DR scheme is efficient and practical.

I. INTRODUCTION

Cloud computing has emerged as a pivotal information infrastructure due to its capacity for substantial storage and computational power. Utilizing cloud services allows users to alleviate the challenges associated with setting up local servers and managing data. Nevertheless, concerns regarding data security and privacy frequently arise, particularly because these services are typically managed by third-party providers. A notable example of this vulnerability occurred when private photographs of several female celebrities were leaked from Apple's cloud storage. To safeguard sensitive information, users are encouraged to encrypt their data prior to uploading it to the cloud, ensuring that only encrypted data is stored on the server. Encryption serves as a crucial method for maintaining data confidentiality, and attribute-based encryption (ABE) is a specific technique that facilitates fine-grained access control over outsourced data. In a standard ABE framework, the data owner is assigned a set of attributes that are utilized to encrypt the data intended for cloud storage. The ABE process must guarantee the confidentiality of the data, allowing only authorized users with the appropriate access rights to retrieve the encrypted information. While ABE offers detailed access control, it falls short in supporting data sharing in its encrypted form, which is essential for collaborative efforts. Additionally, an effective revocation mechanism is necessary for data sharing within collaborative systems, as users may exit the collaboration at any time.

An elementary solution to this dilemma is for Alice to apply her private key to decrypt the data sourced from the cloud server. After successfully recovering the original health data through decryption, she encrypts it according to the sharing policy P2 and uploads the ciphertext back to the cloud. This enables any party that complies with the sharing policy P2 to download and decrypt the ciphertext. Should a revocation take place, Alice simply needs to encrypt the health record using the revoked policy (such as P3). Nonetheless, this strategy is fraught with limitations. Firstly, it is not scalable; Alice must undergo the download-decrypt-encrypt routine each time there is a change in the sharing policy. This repetitive cycle fails to leverage the full capabilities of cloud services, which are intended to perform substantial computations for users. Furthermore, during each sharing transaction, Alice must be online, as her private key is required for every decryption step.

The process of maintaining local data can prove to be quite challenging for Alice, particularly when she seeks to share thousands of encrypted health records. An alternative approach involves the application of the attribute-based proxy re-encryption (ABPRE) technique to resolve these issues. In an ABPRE system, it is possible to produce a re-encryption key that allows for the transformation of ciphertext associated with access policy P1 into a different ciphertext associated with access policy P2. This re-encryption key is then sent to the cloud, where the cloud server can convert Alice’s ciphertext into a new ciphertext that adheres to the sharing policy. Should a revocation take place, Alice is required to generate a new re-encryption key for the remote cloud server to execute the precise transformation. Unfortunately, the generation of a new re-encryption key is also resource-intensive, as will be elaborated in Section IV-B. Furthermore, Alice must be online, akin to the first method, since her private key is essential for the re-encryption key generation process. This approach also fails to provide a direct means of revoking users from the original sharing policy.

II. LITERATURE SURVEY

TITLE: RS-HABE: Revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud

YEAR:2021

AUTHOR: J. Wei, X. Chen, X. Huang, X. Hu, and W. Susilo

DESCRIPTION:

This scholarly work unveils RS-HABE, a distinguished revocable-storage and hierarchical attribute-based access control scheme, meticulously designed for the secure sharing of e-health records in public cloud settings. The proposed architecture harmoniously combines revocable storage with hierarchical access policies, delivering an unparalleled level of fine-grained access control over sensitive healthcare data. By harnessing a hierarchical attribute structure, it grants secure access to e-health records for authorized users, contingent upon their specific roles or attributes. The revocable storage feature allows data owners to withdraw access to their information without the need for complete re-encryption, thus enhancing efficiency in dynamic healthcare environments.

TITLE: Key-policy attribute-based encryption with keyword search in virtualized environments

YEAR: 2020

AUTHOR: Y. Yu, J. Shi, H. Li, Y. Li, X. Du, and M. Guizani

DESCRIPTION:

This manuscript introduces an innovative key-policy attribute-based encryption (KP-ABE) framework, specifically designed to incorporate keyword search functionalities within virtualized settings. The architecture aims to tackle the complexities associated with secure data sharing in cloud computing, particularly in environments characterized by dynamic resources and user access. By integrating keyword search capabilities, this scheme empowers users to swiftly navigate through encrypted information while upholding stringent access control dictated by user attributes. The KP-ABE mechanism facilitates meticulous access management, ensuring that only individuals possessing the requisite attributes can decrypt and query the encrypted data. This sophisticated approach harmonizes encryption with keyword search, allowing users to retrieve pertinent information without jeopardizing security. It is adept at supporting virtualized environments, where data may be dispersed across multiple virtual machines or servers. The manuscript further emphasizes the scalability of the framework, rendering it ideal for extensive systems with a multitude of users and fluctuating workloads. Additionally, the scheme promotes secure and efficient access to encrypted data, enhancing data management and collaboration within cloud computing landscapes. This research significantly contributes to the ongoing advancements in securing virtualized cloud environments by presenting a formidable solution for secure data sharing, complete with keyword search capabilities.

TITLE: Ciphertext-Policy Attribute-Based Encryption: An Expressive Efficient and Provably Secure Realization

YEAR: 2011

AUTHOR: B. Waters

DESCRIPTION:

In this scholarly work, B. Waters unveils an innovative model for ciphertext-policy attribute-based encryption (CP-ABE), presenting a sophisticated, efficient, and demonstrably secure framework for managing access control within encrypted data. This advanced CP-ABE scheme facilitates adaptable and scalable access control policies linked to encrypted information, thereby enabling a nuanced approach to security. By empowering users to define access control policies grounded in their attributes, the model establishes a formidable mechanism for enforcing security while preserving data confidentiality. The emphasis of this research is on optimizing the scheme's efficiency, rendering it particularly well-suited for expansive applications such as cloud computing, where vast quantities of encrypted data must be securely shared and managed among diverse users. Furthermore, the paper substantiates the provable security of the proposed CP-ABE scheme based on established cryptographic principles. Waters' methodology is crafted to be both computationally efficient and richly expressive, allowing for the seamless implementation of intricate access policies while upholding robust security assurances. This work makes a substantial contribution to the domain of secure data sharing, tackling the pressing challenges of scalability and security inherent in attribute-based encryption systems. Ultimately, this paper sets a pivotal precedent for future advancements in data encryption and access control within distributed systems, particularly those necessitating flexible user access in response to dynamically evolving attributes.

TITLE: Ciphertext-delegatable CP-ABE for a dynamic credential: A modular approach

YEAR: 2019

AUTHOR: J. Kim, W. Susilo, J. Baek, S. Nepal, and D. Liu

DESCRIPTION:

This document presents an innovative modular framework for Ciphertext-Policy Attribute-Based Encryption (CP-ABE), facilitating ciphertext delegation to adapt to evolving credentials. This approach empowers data owners to grant access to encrypted information to various users based on credentials that may change dynamically, all without necessitating modifications to the foundational encryption architecture. The system is meticulously crafted to address scenarios where user credentials undergo frequent updates, making it exceptionally suited for environments characterized by swiftly shifting access control policies. Enhancing traditional CP-ABE, this scheme offers remarkable flexibility and superior support for dynamic access control in practical applications. Furthermore, it enables the delegation of access rights to additional users, rendering it particularly advantageous in collaborative settings where multiple stakeholders require shared access to sensitive information. The document underscores the advantages of this modular design, including its scalability and adaptability to a wide array of access control situations.

This system emerges as a more pragmatic solution to the challenges of attribute-based encryption, especially in contexts where access rights are subject to continual modification. The proposed framework enriches CP-ABE schemes, effectively overcoming the constraints of static access control systems.

TITLE: Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes

YEAR: 2018

AUTHOR: Y. Jiang, W. Susilo, Y. Mu, and F. Guo

DESCRIPTION:

This manuscript introduces a sophisticated enhancement to the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) framework, enabling the modification of access policies while safeguarding user attributes. This innovative extension is particularly advantageous in dynamic environments where access control policies must be frequently adjusted in response to shifting user roles or requirements. The proposed framework guarantees that user attributes remain unaltered, even as access policies evolve, thereby facilitating efficient and seamless updates. The capability to revise access policies without jeopardizing existing user attributes is a crucial feature for cloud systems, where data access demands are inherently fluid. Moreover, the paper elaborates on how this system elevates the flexibility and security of CP-ABE by empowering data owners to amend access policies as necessary, without the need for data re-encryption or the loss of user attributes. This significant advancement enhances the system's adaptability to real-world scenarios, where regular updates are essential to accommodate changing user roles, access levels, or other access requirements. The study underscores the critical importance of maintaining attributes during policy updates to ensure that access control remains both effective and efficient, thereby promoting secure and scalable data sharing

III. CONCLUSION

This project presents a robust solution for secure data sharing within cloud environments through the implementation of an Attribute-Based Proxy Re-Encryption (ABPRE) scheme, complemented by a direct revocation mechanism. It empowers Data Owners to maintain complete control over their sensitive information by facilitating secure data encryption, user-specific access permissions, and the capability to revoke access whenever necessary. This strategy not only protects the confidentiality and integrity of the data but also enhances resource management and optimizes cloud storage. By utilizing established encryption algorithms like AES and DES, the system ensures reliable protection of data both at rest and in transit. Additionally, the integration of re-encryption and access control mechanisms guarantees that only authorized users can access the data, thereby significantly mitigating the risk of unauthorized breaches. The system's flexibility allows Data Owners to dynamically manage access to their files, while the Admin plays a crucial role in overseeing and regulating user activities, adding an extra layer of security. The real-time revocation capability is a vital feature that addresses security concerns, ensuring that any changes in access privileges are promptly enforced, preventing unauthorized users from accessing sensitive information. Furthermore, this project lays the groundwork for future advancements, including the integration of more sophisticated encryption methods, machine learning for enhanced access control, and blockchain technology for improved data transparency and tracking. As cloud computing continues to advance, this system stands as a strong model for secure and efficient data management, with significant potential for wider application across industries that demand high levels of data protection.

IV. REFERENCES

1. J. Wei, X. Chen, X. Huang, X. Hu, and W. Susilo, "RS-HABE: Revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud," IEEE Trans. Dependable Secure Comput., vol. 18, no. 5, pp. 2301-2315, Sep./Oct. 2021.
2. Y. Yu, J. Shi, H. Li, Y. Li, X. Du, and M. Guizani, "Key-policy attribute-based encryption with keyword search in virtualized environments," IEEE J. Sel. Areas Commun., vol. 38, no. 6, pp. 1242-1251, Jun. 2020.
3. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive efficient and provably secure realization", Lecture Notes Comput. Sci., vol. 2008, pp. 321-334, 2011.
4. J. Kim, W. Susilo, J. Baek, S. Nepal, and D. Liu, "Ciphertext-delegatable CP-ABE for a dynamic credential: A modular approach," Proc. Australas. Conf. Inf. Secur. Privacy, pp. 3-20, 2019.
5. Y. Jiang, W. Susilo, Y. Mu, and F. Guo, "Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes," Int. J. Inf. Secur., vol. 17, no. 5, pp. 533-548, 2018.
6. X. Xie, H. Ma, J. Li and X. Chen, "New ciphertext-policy attribute-based access control with efficient revocation", Proc. Inf. Commun. Technol.-EurAsia Conf., pp. 373-382, 2013.
7. H. Cui, R. H. Deng, G. Wu, and J. Lai, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures," Proc. Int. Conf. Provable Secur., pp. 19-38, 2016.
8. X. Chen, J. Li, X. Huang, J. Li, Y. Xiang, and D. S. Wong, "Secure outsourced attribute-based signatures," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 12, pp. 3285-3294, Dec. 2014.
9. J. Chen and H. Wee, "Semi-adaptive attribute-based encryption and improved delegation for boolean formula," Proc. Int. Conf. Secur. Cryptogr. Netw., pp. 277-297, 2014.
10. J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2201-2210, Aug. 2014.