REVOCABLE IDENTITY-BASED BROADCAST PROXY RE-ENCRYPTION FOR DATA SHARING IN CLOUDS

SHADAN WOMEN'S COLLEGE OF ENGINEERING AND TECHNOLOGY

Ruqiya Rumana
rumanaruqiya@gmail.com

Dr.K.Palani
principalswcet2020.@gmail.com

ABSTRACT

The vast processing and storage capacity of cloud computing are essential to the operation of modern IT systems. However, data security on the cloud is a big concern. Even if traditional techniques identity-based broadcast proxy re-encryption (IB-BPRE) provide for safe data flow, customers may still encounter key renewal issues, reducing the usability of cloud services. We have prepared our security solution, RRB-BPRE, to deal with this weakness. This solution improves security and speeds up the re-encryption key cancellation process for proxies by doing away with the requirement for users to manually renew their keys. Using cloud computing, the RIB-BPRE system streamlines key management and revocation operations. Results from extensive performance testing show that RIB-BPRE simplifies the process of securing data in the cloud.

Keyword – IB-BPRE,RIB-BPRE,Encryption IBE, Cloud, Cipher text.

INTRODUCTION

Securing and controlling access to cloud computing is made easier with the technologically sophisticated Reincryption of Broadcast Proxy Using Revocable Identity (RAB-BPRE). By combining identity-based encryption (IBE) with broadcast encryption, RIB-BPRE creates a system that enables many users to securely share data. It also has the option to disable a user's access independently of other users, which is a nice bonus. Particularly so in ever-changing cloud settings where users can hop in and out at will. As a semi-trusted proxy may hide the plaintext using RIB-BPRE's re-encryption via a proxy, the ciphertext might be changed depending on set of public parameters to another. Thanks to this transformation function, which enables re-encryption of encrypted data without first decrypting it, data transmission and administration are both greatly improved. By making unavailable any data that was previously accessible to a user upon withdrawal, the revocation function guarantees that data remains safe and uncompromised. Users have access to decrypted data, but administrators control revocation

policies and re-encryption keys. The encryption and uploading of data is the responsibility of the data owner. In most cases, the system involves a large number of participants. If hackers get access to the proxy or the users, RIB-BPRE's well-thought-out architecture makes it a dependable option for safe cloud data transfer. Aside from fixing a big problem with cloud access control, the approach simplifies scalability and administration, which improves the safety and adaptability of cloud-based applications and services.

LITERATURE SURVEY

1. Title: A technique for revoking proxy re-encryption that is dependent on identity

Authors: Liang, Kaitai; Wong, Duncan S.; Xie, Qi; Zhou, Jianying

Abstract: A technique called security protocol known as identity-based proxy re-encryption introduced in this work. It allows the data sender to revoke the decryption permissions granted to a semi-trusted proxy. The ciphertext, which was encrypted using the sender's identity, may be deciphered by the receiver using their own secret key. The proposed approach includes revocation capabilities to quickly revoke the proxy's decryption rights for a specific ciphertext without affecting other ciphertexts.

2. Title: Efficient identity-based proxy re-encryption with revocation functionality

Authors: Yang, Yanjiang; Ma, Jianfeng; Zhang, Qiang; Zhang, Jing; Han, Licheng

Abstract: In order to facilitate the assignment and removal of decryption credentials for proxies, this paper presents A system that enables the revocation of identity-based proxy re-encryption (IBPRE). Efficient revocation with little overhead is achieved by combining a revocation key with an efficient revocation list, as proposed in the approach.

3. Title: A revocation-effective identity-based proxy re-encryption system for the cloud

Authors: Yang, Yanjiang; Ma, Jianfeng; Zhang, Qiang; Zhang, Jing; Han, Licheng

Abstract: An effective solution for cloud-based identity-based proxy re-encryption computing environments is introduced in this paper. Revocation capabilities are also a part of it. Data senders may quickly revoke decryption permissions from proxies and improve cloud-based data security and access control using the proposed method.

OBJECTIVE

To better manage who has access to encryption of private data kept in the

cloud, RAB-BPRE is being developed. By combining identity-based encryption (IBE), broadcast encryption, and the RIB-BPRE proxy re-encryption aims to offer efficient and secure transmission of encrypted data to many recipients while also providing dynamic control over access rights. Securing data sharing in the cloud can be challenging due to the fact that access needs might fluctuate due to changes in organizational structure or user responsibilities. This method will help us tackle the challenge. The revocable feature enables the revocation of decryption licenses, which effectively and regulatedly prevents data confidentiality or integrity breaches caused by obsolete access permissions or compromised keys. Secure, scalable, and user-friendly data sharing solutions are RIB-BPRE's top architectural priority as they aim to meet the complex security needs of modern cloud computing applications.

EXISTING SYSTEM

There are a lot of crucial parts to the present RAB-BPRE system that allow for data exchange in the cloud. By combining identity-based encryption (IBE), broadcast encryption, and proxy re-encryption, a secure and efficient approach to data distribution and access management are created. To protect sensitive information, data owners can encrypt it with unique recipient IDs and other attributes, and users can select from a variety of decryption procedures. The broadcast encryption technique ensures fast delivery of encrypted data to several receivers, while proxy re-encryption allows for the safe translation of ciphertexts from one recipient's key to another without revealing the plaintext.

System administrators and data owners rely on the ability to revoke access permissions so they may manage and delete credentials instantly. Flexibility in resizing user responsibilities and permissions is a must for cloud computing. By efficiently handling key changes and access revocations, the system protects data against compromised or outdated keys.All procedures involving data access or exchange adhere to the strictest standards of confidentiality and security to protect user information. By creating a structure to facilitate safe and adaptable cloud-based data exchange, the present RIB-BPRE system addresses the complex security challenges with modern cloud computing applications.

DISADVANTAGES

1.Difficulty and Execution Costs: Key management and proxy re-encryption are two of the trickiest cryptographic processes related to RIB-BPRE. System performance, particularly in large-scale deployments, can be severely affected by the computational cost that results from

improperly using these methodologies, which necessitates expert expertise.

2. Difficulty with Key Management: The effectiveness of RIB-BPRE depends on the correct management of re-encryption keys and user access restrictions. It is more challenging to maintain and safeguard these credentials as the number of users and data collected increases. To prevent breaches in data security or accessibility, key revocation actions must be carefully managed.

PROPOSED SYSTEM

The goal of the Broadcast Proxy Re-encryption with Revocable Identity (RIB-BPRE) technology is to make cloud data sharing more secure by using Advanced Encryption Standard. Through the integration of identity-based encryption (IBE), broadcast encryption, and proxy re-encryption, the system offers a comprehensive approach to managing data access rights and safeguarding user privacy. Data owners have the option to restrict decryption access based on certain qualities or criteria, such as the identities of the recipients. The broadcast encryption method allows for the efficient distribution of encrypted data to several receivers, which in turn optimizes resource utilization in cloud situations. Data may be safely recovered regardless of changes to access restrictions with the help of proxy re-encryption, which securely translates ciphertexts across the keys of multiple receivers.

The capability that allows administrators or data owners to easily remove decryption access when needed is essential to the proposed approach. No matter what happens with keys or access credentials, data will always be protected with this feature. Data privacy and security in cloud computing environments are enhanced by the proposed RIB-BPRE system's ability to integrate several cryptographic capabilities. Additional advantages of the system include rights control and adaptable data sharing. The system's goal is to tackle the ever-changing security issues of contemporary cloud applications by providing a strong and flexible foundation for safe data exchange.

ADVANTAGES

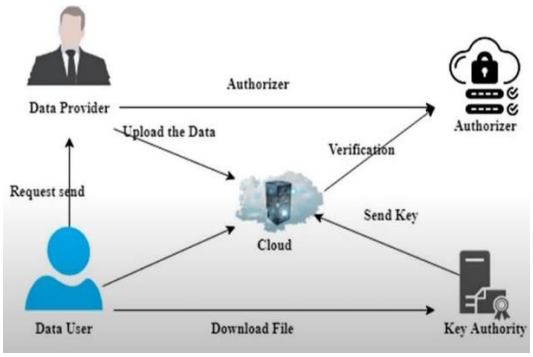
1.Granular Control Over Data Access: RIB-BPRE employs identity-based encryption and proxy re-encryption as its instruments for dynamic access control. Depending on the changing organizational responsibilities or access demands, managers or data owners can selectively grant or revoke decryption capabilities without compromising data security.

2.Efficient Key Management: To maximize key management in cloud settings, RIB-BPRE incorporates both

broadcast and proxy re-encryption. Distributing encrypted data to several recipients effectively while reducing key changes is made possible by this method. The system's scalability is enhanced as a result of the decreased overhead related to key distribution and maintenance.

3.Enhanced Security: Data security is enhanced by RIB-BPRE by integrating identity-based encryption with cryptographic techniques like proxy re-encryption. Data security and integrity are protected since only authorized users with valid decryption keys may access sensitive information, and because the functionality can be revoked, dangers related to compromised keys or unauthorized access attempts are reduced.

SYSTEM ARCHITECTURE



KEY COMPONENTS:

- Data Owner: This function encrypts data and assigns permissions to a specified group of users.
- User: If they have the proper authorization, they can receive and decode data.
- Proxy Server: Ensures that only authorized users may decipher ciphertexts by performing re-encryption activities.
- Admin: Controls who has access and can remove their rights as needed.

ALGORITHM

Cloud computing is only one of many security applications that rely on the Advanced Encryption Standard (AES), a symmetric encryption method, to keep sensitive information safe. The following is a synopsis of AES's operation and function in cloud settings:

Overview of AES

1.Symmetric Key Encryption:

Since AES employs the same key for encrypting and decrypting, the secret key needs to be known by both the sender and the receiver.

2.Block Cipher:

With AES, data is processed in 128-bit (16-byte) blocks of fixed size, and keys can be 128-, 192-, or 256-bit in size.

3.Strong Security:

Secure and efficient in computing, AES can withstand every attack that has been implemented so far.

AES in Cloud Computing

1.Data Encryption at Rest: To ensure that no one else may access the data kept in

the cloud, AES encrypts it. With the encryption key, not even a hostile actor with physical access to the storage could decipher the data.

2.Data Encryption in Transit: When information is sent between users and cloud services, it is encrypted using AES. As a result, the key is required to decipher any data that is intercepted while in transit.

3.Secure Access Control: One common method that cloud companies employ to implement access limits is AES. For example, data can be encrypted using unique keys for each user or position, limiting access to authorized people only.

4.Performance Efficiency: Because of its reputation for fast encryption and minimal resource consumption, AES is well-suited to the real-time encryption of massive volumes of data, which is essential in cloud environments.

Implementation in Cloud Services

Amazon Web Services (AWS): S3, EBS, and RDS are all parts of Amazon Web Services that encrypt data using the Advanced Encryption Standard (AES) while it's in motion or stored.

Microsoft Azure: Azure SQL Database, Azure Disk Storage, and Azure Blob Storage all employ AES encryption.

Google Cloud Platform (GCP): Storage, Compute Engine, and Cloud SQL are just a few of GCP's services that use AES encryption.

CONCLUSION

In the end, RUB-BPRE offers a solid solution to the issue of unsecure data transfer in cloud environments. Thanks to RIB-effective BPRE's proxy re-encryption techniques and stringent access control, authorized users may securely exchange data while closely monitoring who has access to what. Its revocability significantly enhances security since access privileges may be dynamically removed whenever necessary. By using RIB-BPRE, cloud-based application cooperation is made smoother and privacy issues are effectively handled. When it comes to secure data communication, RIB-BPRE is a viable solution since it protects sensitive information while allowing for efficient and safe cooperation.

REFERENCES

1) Liang, Kaitai, et al. "An identity based proxy re-encryption system with revocation mechanism." 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015.

2) Yang, Yanjiang, et al. "Efficient identity-based proxy re-encryption with revocation functionality." IEEE Transactions on Information Forensics and Security 15.1 (2019): 343-355.

3) Yang, Yanjiang, et al. "An efficient identity-based proxy re-encryption with revocation in cloud computing." 2017 IEEE Conference on Computer Communications (INFOCOM). IEEE,

2017.

4) Cao, Zhenfu, et al. "An efficient identity-based broadcast proxy re-encryption scheme for secure data sharing in clouds." IEEE Transactions on Information Forensics and Security 13.1 (2017): 65-78.

5) Liu, Qin, et al. "Efficient identity-based proxy re-encryption with designated revocation in cloud computing." IEEE Access 8 (2020): 39894-39908.

6) Zhu, Yuting, et al. "Efficient revocable identity-based broadcast proxy re-encryption for secure data sharing in clouds." IEEE Access 6 (2018): 54183-54192.

7) Li, Zijian, et al. "Identity-based proxy re-encryption with revocation in the standard model." IEEE Access 8 (2020): 110276-110285.

8) Yu, Zhengan, et al. "Efficient identity-based proxy re-encryption with designated revocation for mobile cloud computing." IEEE Access 7 (2019): 51444-51455.

9) Long, Yu, et al. "Secure data sharing in cloud computing using revocable identity- based proxy re-encryption." 2018 IEEE International Conference on Communications (ICC). IEEE, 2018.

10) Li, Ming, et al. "Efficient revocable identity-based proxy re-encryption scheme for secure data sharing in cloud storage." 2018 IEEE Trustcom / BigDataSE/ISPA. IEEE, 2018.