

Security Implications and Mitigation Strategies for One-To-Many Order Preserving Encryption in Cloud Data Search

Sedhu Madhavan, Dr. Lipsa Nayak

Master of Computer Application, Vels University, Chennai

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.140400080>

Abstract: Cloud computing offers a flexible and efficient method for data sharing, benefiting both individuals and society. However, users may hesitate to store shared data on external servers due to concerns about the sensitive nature of the information. To address this, implementing cryptographic access control is essential. Identity-based encryption (IBE) serves as a valuable cryptographic approach to establishing secure data-sharing systems. Nonetheless, access control needs to be dynamic. When a user's authorization expires, there must be a mechanism to revoke their access, ensuring they cannot retrieve either previously or newly shared data. To achieve this, we introduce the concept of Revocable-Storage Identity-Based Encryption (RS-IBE), which ensures both forward and backward security by incorporating user revocation and cipher text updates.

We further present a concrete RS-IBE construction and validate its security within a defined model. Performance comparisons highlight the scheme's advantages in functionality and efficiency, making it a viable and cost-effective solution for secure data sharing. Additionally, implementation results showcase its practical applicability. The RS-IBE scheme is proven to be adaptively secure under the decisional ℓ -DBHE assumption in the standard model. Comparative analysis confirms that our approach is efficient and functional, making it suitable for real-world applications.

Keywords – Cloud computing, data security, Identity-Based Encryption (IBE), Revocable-Storage Identity-Based Encryption (RS-IBE), cryptographic access control, user revocation, forward security, backward security, cipher text update, secure data sharing, encryption mechanism, privacy protection, key management, access control policies, and cryptographic protocols.

I. Introduction

Cloud computing has transformed data storage and sharing by offering scalable, cost-effective, and flexible solutions. It enables seamless data access and collaboration, benefiting individuals and organizations alike. However, storing data on cloud servers raises security and privacy concerns, especially when handling sensitive information. Risks such as unauthorized access, data breaches, and loss of control over shared content make secure data management a critical challenge. To enhance security in cloud-based data sharing, cryptographic techniques are essential. Identity-Based Encryption (IBE) is an effective approach that enables encryption based on user identities, ensuring controlled access. However, traditional IBE lacks a mechanism to revoke access dynamically. In practical scenarios, users may lose authorization due to changes in roles or security threats. Without a proper revocation system, former users may still retrieve previously or newly shared data, compromising confidentiality. To address this issue, we introduce Revocable-Storage Identity-Based Encryption (RS-IBE), which incorporates user revocation and cipher text updates to provide forward and backward security. This ensures that revoked users are unable to access past or future encrypted data. Our proposed RS-IBE model is designed to enhance security in cloud-based data sharing, offering a practical, efficient, and scalable solution. Through security analysis and implementation, we demonstrate its effectiveness in real-world applications. With the rapid advancement of cloud computing, organizations and individuals increasingly rely on cloud-based solutions for efficient data storage and sharing. Cloud platforms offer scalability, cost-effectiveness, and accessibility, making them ideal for various applications, including healthcare, enterprise data management.

However, data security and privacy concerns remain significant challenges, as outsourcing sensitive information to cloud servers increases the risk of unauthorized access, data breaches, and cyber threats. To ensure secure data sharing in cloud environments, cryptographic techniques play a crucial role in protecting information from malicious entities. One such approach is Identity-Based Encryption (IBE), which allows encryption using unique user identities instead of traditional certificates. While IBE provides a structured access control mechanism, it lacks the flexibility required for dynamic environments where user privileges may change over time. A major limitation of traditional encryption schemes is the inability to revoke user access effectively. When a user's authorization expires or is revoked, they should no longer have access to previously or newly shared data. To address this challenge, we introduce Revocable-Storage Identity-Based Encryption (RS-IBE), a cryptographic framework that integrates user revocation and ciphertext updates to ensure forward and backward security. This means that revoked users cannot decrypt either past or future encrypted data, enhancing overall security. The proposed RS-IBE model is designed to meet the demands of modern cloud-based systems, providing efficient key management, adaptive security, and access control policies. Through theoretical analysis and practical implementation, we demonstrate that RS-IBE enhances data security, privacy protection, and secure data-sharing mechanisms, making it a viable solution for cloud computing environments.

Related Work

Several research studies have focused on enhancing data security and access control in cloud computing environments through cryptographic techniques. Traditional encryption schemes, such as Public Key Infrastructure (PKI), provide secure data sharing but often suffer from complex key management and scalability issues. To address these limitations, Identity-Based Encryption (IBE) was introduced by Shamir, allowing encryption based on user identities rather than requiring certificates. Although IBE simplifies key management, it lacks an efficient mechanism for user revocation, making it unsuitable for dynamic cloud environments. To overcome this challenge, researchers have proposed Revocable Identity-Based Encryption (RIBE) schemes, which integrate revocation mechanisms into IBE. Boneh and Franklin introduced IBE with key revocation, where a trusted authority updates user keys periodically. However, this approach increases the computational overhead, making it impractical for large-scale cloud systems. Later, fuzzy IBE and hierarchical IBE models were developed to improve flexibility, but they still required frequent key updates. In addition to encryption-based access control, various works have explored attribute-based encryption (ABE) for fine-grained data access in cloud storage. ABE enables data owners to define access policies based on attributes rather than user identities, allowing more flexible control. However, ABE schemes also face revocation challenges, requiring computationally expensive re-encryption processes. To address these issues, the concept of Revocable-Storage Identity-Based Encryption (RS-IBE) was introduced to provide both forward and backward security by revoking unauthorized users and updating cipher texts efficiently. Several studies have demonstrated the feasibility of RS-IBE in secure cloud storage, in data handling systems, and remote data-sharing applications. The proposed scheme builds on these existing approaches by integrating efficient key management, adaptive security models, and lightweight cipher text update mechanisms, ensuring practical implementation in real-world cloud environments.

RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period. Furthermore, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals:

Data confidentiality: Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the storage server. In addition, the storage server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.

Backward secrecy: Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

Forward secrecy: Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her. Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. To build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and ciphertext update. A revoked user is prevented from accessing previously shared data, as well as subsequently shared data. The proposed RS-IBE scheme is proved adaptive-secure. Our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

SYSTEM DESIGN AND IMPLEMENTATION

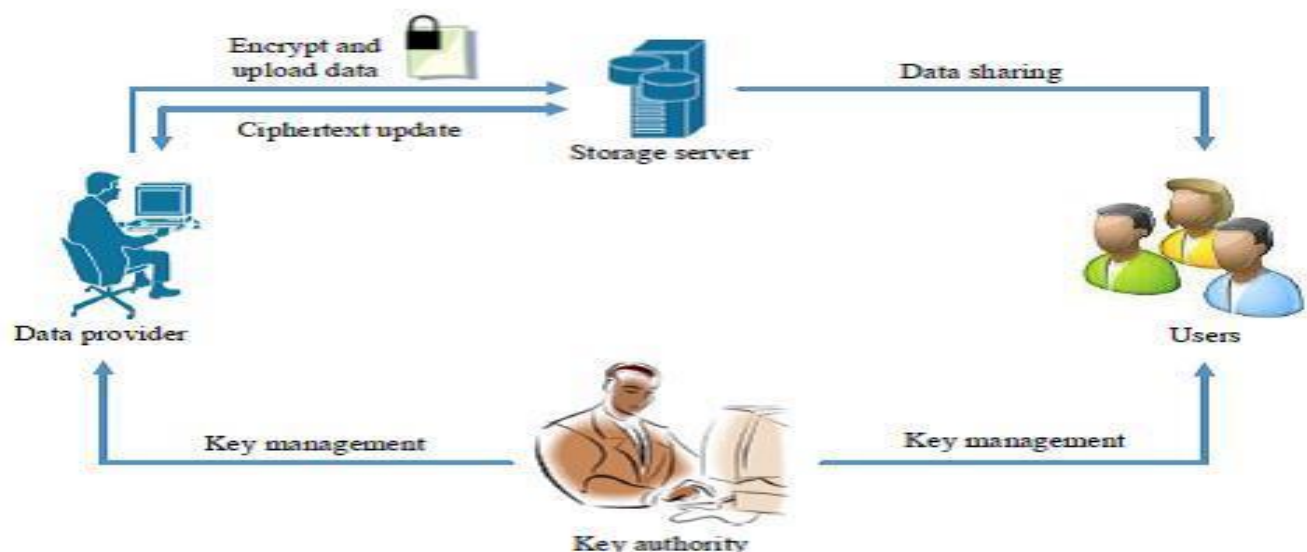


Fig 2.1 System Design

Data Owner: The data owner is responsible for managing files within the system. They must first register with a unique username and password. Upon successful registration, the data owner can log in and access the storage platform. From their dashboard, they can upload files to the cloud server, where the files are stored in an encrypted format for security. The data owner has the ability to view the list of uploaded files and modify them while ensuring encryption is maintained.

Storage Server: The storage server is managed by an administrator, who has authority over various operations within the system. The administrator can log in to the admin panel and access information about uploaded files, data owners, data users, and revoked users. If a user has been revoked due to security concerns, the admin has the ability to reinstate their access by un-revoking them, restoring their permissions.

Key Authority: The key authority is responsible for generating encryption keys for uploaded files. When a data user requests access to a file, the key authority verifies the request, checking details such as the data owner's name, file name, and requester's information. If the request is valid, the key authority generates a unique key and securely transmits it to the respective data user, enabling them to access the file.

Data User: A data user must register in the system before gaining access. Once registered, they can log in and request files uploaded by their respective data owners. To download a file, the user must know the file name and the corresponding data owner's name. Using these details, they submit a key request to the key authority. After verifying the request, the key authority generates and provides the encryption key. The user can then use this key to decrypt and download the file securely.

Revoked User: If a data user enters an incorrect key while attempting to access a file, the storage server may detect this as unauthorized access and classify them as a potential attacker. As a result, the system immediately blocks the user's access, preventing them from logging in, requesting keys, or downloading files. The administrator can review the details of the blocked user, including the file they attempted to access. After verifying that the user was not engaging in malicious activity, the admin can reinstate their access. Once unrevoked, the user regains full access to the system and its features.

System Implementation:

The implementation phase is where the theoretical design of a project is transformed into a fully functional system. This stage is crucial for ensuring the success of the new system and instilling confidence in users regarding its effectiveness and reliability. A well-structured implementation process requires careful planning, an assessment of the existing system, and an understanding of any constraints that might impact deployment. It also involves designing appropriate strategies for a smooth transition and evaluating different changeover approaches to minimize risks. During implementation, the focus is on deploying the system into actual operation, which includes user training, site preparation, and data migration. A key consideration is ensuring that the transition does not disrupt the organization's ongoing activities, allowing for seamless integration of the new system.

Literature Review:

HuaqunWang ;Yuqing Zhang , Provable information ownership (PDP) is a probabilistic verification procedure for cloud specialist co-ops (CSPs) to describe the customer data in right manner without downloading the entire information. Zhu et al. proposed the development of an effective PDP conspire for multi-cloud stockpiling. They considered the presence of various CSPs to agreeably store and keep up the customers' information. By then, in perspective on homomorphism obvious response and hash document pecking request, they presented an accommodating PDP (CPDP) plot from the bilinear pairings. They ensured that their arrangement satisfied the security property of data soundness. Tragically this comment shows that any noxious CSP or the poisonous facilitator (O) can deliver the significant response which can pass the check paying little heed to whether they have deleted all the secured data, i.e., Zhu et al's. CPDP plot can't fulfill the property of learning soundness. At that point, we talk about the cause and seriousness of the security defects. It suggests that the aggressor can get the compensation without putting away the customers' information. It is critical to clear up the logical reality to plan increasingly verify and reasonable CPDP conspire in Zhu et al's. framework design and security model

S. Vishnupriya ; P. Saranya ; A. Rajasri , Cloud stockpiling is another business answer for remote reinforcement redistributing, as it offers a deliberation of boundless extra room for customers to have information reinforcements in a compensation as you-go way. Anyway it is crucial for cloud specialist organizations (CSPs) to give security procedures to dealing with their capacity administrations. We handle this issue by actualizing the system for multi-cloud stockpiling in which the customer's information is controlled with fine grained strategy based access control. Furthermore an effective agreeable Provable information ownership (CPDP) plot is planned which offers a productive check on the honesty and accessibility of put away information. The proposed framework incorporates tending to two security issues. First give certifications of access control in which just approved gatherings can get to the re-appropriated information. Second gives agreeable PDP plan to help dynamic adaptability on numerous capacity servers. Broad security and execution examination demonstrate that the proposed plans are very effective and provably secure.

Lino Abraham Varghese ; S. Bose , A Text-manager application which consolidates the Co-usable provable information ownership conspire enables the client to transfer documents, demand for a test/confirmation check, see the substance of the record in a protected way and permits him/her to review the documents which he put away in the cloud. High security is ensured on the grounds that the information of the client goes through two dimensions of capacity. The calculation centers around expanding

security, without remunerating on execution. The assailant may see the substance of the document, which is twofold scrambled. On the off chance that the cloud specialist organization, changes the substance of the cloud, it will be recognized amid the confirmation checking stage, which is performed before the client endeavors to see the substance of the record. Further, client can alter powerfully with new substance, which likewise gets encoded and put away in the cloud. Client can download the substance and later transfer it with changes. The correspondence between outsider server and cloud server is trusted, as correspondence depends on trade of open - private RSA keys.

AnnamalaiRajendran ; V Balasubramanian ; T Mala , In the cloud computing environment multi storage cloud technique has been popularly used by many organizations to mitigate disaster recovery and to increase the flexibility for the user. The data being outsourced by the client in a storage server may get corrupted. This leads to a threat to the integrity of the client's confidential data. We utilize a procedure called Provable Data Possession (PDP) [1] utilizing which we check the honesty of the redistributed information in an untrusted server without recovering the whole document from the cloud server or having a duplicate of the information. Personality Based Encryption (IBE) and other PDP plans are utilized for its execution. To actualize PDP (provable Data Possession) in confirming the uprightness of the redistributed information we use HMAC (Hashed Message Authentication Code). A message digest is produced utilizing HMAC with the mix of a mystery key. A mystery key is produced for the client personality by running a setup calculation which performs Identity Based Encryption (IBE). One of the Cloud Service Provider (CSP) will go about as a combiner. The verification produced by the Cloud specialist organization is checked by the customer who will go about as a verifier. The Cloud Service Provider is accounted for if the confirmation created by the proved isn't right.

Jian Mao ; Yan Zhang ; Pei Li ; XiandongXu ; Teng Li ; Jianwei Liu Information proprietorship checking is an important method to manage ensure the reliability and availability of re-appropriated data in remote circulated stockpiling. In any case, most existing approaches simply considered the single cloud pro community (CSP) circumstance. Past game plans can't satisfy the essential that to check the decency of the whole record on spread CSPs through a lone test response joint effort organize.

Li Haoyu ; Li Qingpeng ; Zhang Longjun ; GaoZhiqiang, With the fast development of distributed storage, numerous clients store the information in cloud to decrease stockpiling costs. In any case, guaranteeing information respectability when utilizing questionable administration is an issue. By presenting the multi-expanding tree (MBT) and bilinear pairings innovation, we propose an information uprightness check conspire dependent on MBT. The plan can viably disentangle the procedure of the dynamic update and backing the multi-granular unique tasks by structuring a lightweight framework model and building a straightforward check tree. Security investigation and the test results demonstrate that the plan can oppose malignant assault from cloud server. Contrasted and the plan dependent on Merkel hash tree (MHT), our plan can successfully decrease the processing cost of substances and improve the check effectiveness significantly.

Boyang Wang ; Hui Li ; Xuefeng Liu ; Fenghua Li ; Xiaoqing Li , Cloud registering empowers clients to effectively store their information and essentially share information with others. Because of the security dangers in an untrusted cloud, clients are prescribed to process check metadata, for example, marks, on their information to ensure the respectability. Numerous instruments have been proposed to enable an open verifier to effectively review cloud information uprightness without getting the whole information from the cloud. In any case, apparently, none of them has considered about the productivity of open check on multi-proprietor information, where each square in information is marked by numerous proprietors. In this paper, we propose a novel open check system to review the uprightness of multi-proprietor information in an untrusted cloud by exploiting multisignatures. With our system, the check time and capacity overhead of marks on multi-proprietor information in the cloud are free with the quantity of proprietors. Also, we exhibit the security of our plan with thorough evidences. Contrasted with the clear augmentation of past instruments, our system demonstrates a superior execution in tests.

II. Methodology

The proposed system follows a structured approach to ensure secure file storage, controlled access, and efficient key management. Initially, Data Owners and Data Users must register with a unique username and password, ensuring secure authentication before accessing the system. Once authenticated, the Data Owner can upload files to the storage server, where all files are encrypted to maintain confidentiality. The Data Owner also has the ability to view and manage uploaded files in an encrypted format. The Storage Server administrator oversees the platform by managing uploaded files, monitoring registered users, and handling revoked users. If necessary, the administrator can revoke or restore access based on security protocols.

The Key Authority plays a crucial role in key management by generating and distributing decryption keys. When a Data User requests access to a file, the Key Authority verifies the file details, including the Data Owner's name and file name, before generating and securely sending the corresponding decryption key. The Data User, upon receiving the key, can decrypt and download the requested file. However, if a Data User enters an incorrect key, the system identifies a potential security threat and immediately revokes access, preventing further login attempts. The revoked user remains blocked until the Storage Server administrator verifies and reinstates them after reviewing attack logs.

By implementing this structured methodology, the system ensures a high level of security, preventing unauthorized access while allowing legitimate users to securely store and retrieve files. The encryption, authentication, and revocation mechanisms work together to protect data integrity and maintain a secure environment for all stakeholders.

Test Cases

TEST CASE ID	TEST CASE TITLE	TEST CASE DESCRIPTION	TEST CASE STEPS	EXPECTED RESULT	ACTUAL RESULT	STATUS
01	Testing the functionality of java development overview	Testing the functionality of net beans.	Run the java code.	The software starts to compile and execute the program.	The software starts to compile and execute the program.	Pass
02			The software takes the User login details	The java software takes the input of user login details and corresponding details	The java software does not take the input of user login details and shows error	Fail
03			The main program displays the restored.	The execution stops and displays the login pages and allows users to login.	The execution stops and displays the login pages and allows users to login.	Pass
04			Now run the form validation module code.	The software starts to compile and execute the process.	The software starts to compile and execute the process.	Pass
05			Now run key generation module code	The software starts to compile and execute the process.	The software starts to compile and execute the process.	Fail

III. Conclusion And Future Works

This system provides a secure and efficient framework for file storage and access control. By implementing user authentication, encryption mechanisms, and key-based access, the model ensures data confidentiality and prevents unauthorized access. The role-based structure—including Data Owners, Storage Servers, Key Authorities, and Data Users—enhances security and accountability within the system. Additionally, the revocation mechanism helps mitigate security risks by blocking potential attackers. Overall, this system enables a trustworthy data-sharing platform while maintaining integrity and confidentiality.

In the future, the system can be enhanced by implementing multi-factor authentication (MFA) for Data Owners and Data Users to strengthen security. Additionally, integrating AI-based anomaly detection can help identify and prevent malicious activities before revocation, reducing false-positive blocks. The adoption of decentralized storage solutions, such as block chain or distributed ledger technology, can further enhance data integrity and eliminate single points of failure. Expanding role-based access control (RBAC) mechanisms will allow more granular permissions based on user roles and file sensitivity, improving overall security. Performance optimization techniques, including efficient encryption and decryption processes, can help reduce latency and enhance system efficiency. Moreover, integrating mobile applications and cloud-based storage solutions will provide greater accessibility and scalability, making the system more adaptable to evolving user needs.

References

1. HuaqunWang; Yuqing Zhang , On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multi-cloud Storage. IEEE Transactions on Parallel and Distributed Systems Year: 2014 Volume: 25 , Issue: 1 ,Pages: 264 - 267
2. S. Vishnupriya ; P. Saranya ; A. Rajasri , Secure multi-cloud stockpiling with strategy based access control and helpful provable information ownership , Date of Conference: 27-28 Feb. 2014.
3. Lino Abraham Varghese ; S. Bose , Integrity check in multi distributed storage.
4. AnnamalaiRajendran ; V Balasubramanian ; T Mala , Integrity check utilizing Identity based Provable Data Possession in multi stockpiling cloud.
5. Jian Mao ; Yan Zhang ; Pei Li ; XiandongXu ; Teng Li ; Jianwei Liu2014 Communications Security Conference (CSC 2014), ETCIC: A mistake tolerant substance trustworthiness checking plan in multi-cloud putting away .
6. Li Haoyu ; Li Qingpeng ; Zhang Longjun ; GaoZhiqiang ,Integrity Verification Scheme for Dynamic Cloud Data Based on Multi-Branching Tree . Year: 2017 Pages: 365 - 368 IEEE Conferences

7. Boyang Wang ; Hui Li ; Xuefeng Liu ; Fenghua Li ; Xiaoqing Li , Efficient open check on the respectability of multi-propriator information in the cloud
8. Praveena.A ;Sasikala.C ,Multi expert quality based encryption against information trustworthiness and versatility issues in cloud information administrations.
9. Su Peng ; Fucai Zhou ; Qiang Wang ; ZifengXu ; JianXu , Identity-Based Public Multi-Replica Provable Data Possession. IEEE Access Year: 2017 Volume: 5 Pages: 34-45
10. S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in storages," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 384–394, 2014.
11. X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," *Computers, IEEE Transactions on*, 2014, doi:10.1109/TC.2014.2315619.
12. C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in storage storage," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 468–477, 2014.
13. Azure. (2014) Azure storage service. [Online]. Available: <http://www.windowsazure.com/>
14. Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: <http://aws.amazon.com/s3/>
15. K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563, 2012.
16. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure storage storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.
17. G. Anthes, "Security in the storage," *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.
18. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.
19. B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the storage," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2904–2912.