

CR-IBE based data sharing and revocation in the cloud

P. Raja Sekhar Reddy *

K. Ravindranath [†]

Department of Computer Science and Engineering

Koneru Lakshmaiah Education Foundation

Greenfields

Vaddeswaram

Andhra Pradesh

India

Abstract

Storing information on the cloud lets users access data quickly. Owners send their files to cloud servers to save money and use helpful tools. Keeping shared data online beyond direct control worries more people about privacy and security. Issues with sharing data in the cloud are a major concern. Several methods can protect user privacy and securely share group information. This paper introduces a secure dynamic way for groups to share and take away access to data using identity-based encryption that can change (R-IBE). A new cloud-based method for sharing data with revocable identity-based encryption (CR-IBE) is suggested. It allows stopping user access. The proposed method is compared to existing attribute-based encryption schemes for how long they take to run and decode. Tests show the proposed method provides better protection and privacy.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Cloud computing, Group data sharing, Cloud service provider, Dynamic groups, Revocation.

1. Introduction

It Cloud computing is the latest generation that allows users to access data through a web connection. Records can be easily and quickly shared over the Internet using a paid service with on-demand access. Cloud computing, mainly used by groups and companies, provides ample

* E-mail: prreddy.cvsr@gmail.com (Corresponding Author)

[†] E-mail: ravindra_ist@kluniversity.in

parking space at a reasonable price. Cloud providers have met the primary [1] demand for high-performance processing and log storage. Many cloud computing providers offer cloud computing, including Amazon, Dropbox, Google App Engine, and others.

Today, cloud computing is a generation that allows a person to access data stored on a remote server [2]. This can be done easily and quickly manually via the Internet, with the operator being paid according to the usage of the guard. Cloud computing, in particular, is used for businesses and businesses and provides a large amount of data sharing at a low cost. One of the most essential services is information storage, which a cloud sender provides. Information leakage and data privacy are security concerns from data storage and sharing. Confidential or susceptible data is stored in the cloud.

The data exchange between individuals or member organizations raises several issues. They are efficiency, information integrity, and information owner privacy. Providing privacy and integrity are the most challenging tasks for mobile companies. The current machine offers a convenient information-sharing scheme for dynamic people [3]. Without secure communication channels, this approach uses simple key distribution so that the organization administrator presents non-public keys to users. The scheme can achieve standard granular access manipulation. It protects against collusion attacks through organization signatures that provide revocation to the casualty. User Cancellation Safe Mode: Canceled clients cannot receive authentic information reports even though they interact with the untrusted cloud.

2. Review of Literature

In recent years, researchers have focused on improving the security of storage machines. CFS and NASD are examples of real-world systems. CFS is designed for single-person workstations and relies on passwords entered by that person to encrypt logins [4]. User-supplied keys, including intelligent and innovative drives, are used as proof of authentication on NASD-distributed devices. Securing community visitors and protecting them from external attacks is the primary goal of NASD and SNAD. Access to confidential data may be restricted to unauthorized users. For personal records in cloud computing,

It allows contracting encryption on another device equipped with its unique encryption mechanism [14]. This research considers the transition between traditional full identity-based and attribute-based encryption

and provides concrete productivity insights into using proxy re-encryption mechanisms. This paper proposes a simplified identity-based dynamic entity statistics exchange scheme for cloud computing, mainly based on a set of transplanted entity signature rules to authorize and authenticate identity. For group members to share data correctly, we use a multi-owner lookup encryption mechanism to understand the organization's data sharing.

They generalized [5] the features required for ciphertext delegation using an encoding syntax for modularity and created a hosting-based generalized delegation algorithm. In their new form, they dictate the access rights form, which usually specifies the dimensions of the ciphertext in a defined manner. The entry period assigned to the systems is best aligned with the validation and revocation of access systems. Through transmission examples, we show that our approach applies without difficulty to existing CP-ABE schemes, which consist of non-uniformly shaped people with admittance.

In this article [6], we introduce IBE outsourcing computing to solve the essential problem of identity revocation and support a revocable based IBE mechanism in server-assisted deployments. Their mechanism divests most of the operations connected to crucial generation during key issuance and key replacement strategies to the critical update cloud operator issuer, ideally for PKG and nationwide customers. Leave a constant series of simple operations using a unique technique to avoid collisions: we use a hybrid private key for every user, with an identifier problem and a time problem. Occurs, and to determine, another gate is given. In addition, we suggest a few different productions that feel safe under the recently revised computer referee delegation model.

In this article [7], they verified a unique and fast scheme entirely based on the CP-ABE principle to make it faster concerning user attribute reduction. In this scheme, they created a special tree, T_2 , with the original input shape to organize the tree, T_1 when a user requests encrypted text within the CSP, the CSP first attempts to decrypt the CT_2 , which is encrypted by accessing the same T_2 tree securely with the same subset of secret keys. For attribute indexes provided by individual usage. If the CSP can effectively crack it, it proves that it can access the CT_1 crypto text content, and the CSP will send CT_1 to the user.

Introducing [8] feature institutional keys has provided a feature revocation scheme based entirely on encryption based on ciphertext features. In this way, secret keys are changed dynamically, and the need to revoke functions on the spot is met. Authentic equivalence guarantees

over all its ciphertexts, or a different ciphertext, was provided [13]. A proof-of-equity cloud computing identity-based encryption technique was proposed [9] developed CP-ABE and uses two linear pairs to provide users with fine-granularity access to ciphertext search and manipulation capabilities. They provided a safe, green, first-class information delivery method called ACPC. Access control directly in P2P Garage Cloud.

Although these [10] methods adopt a feature-based approach to protecting user privacy, they no longer satisfy individual feature privacy [11]. They have suggested a privacy-related information-sharing technique called SAPDS. In [12] SAPDS, the attribute encryption scheme determines how garage overhead and a large amount of verbal exchange are generated. The structures above allow user organizations and anyone accessing shared documents to access the same information. Typically, these group permissions are used to protect encryption keys. Sharing multi-tenant data for enterprises while maintaining privacy across an untrusted cloud remains a mission.

3. Proposed System

In this suggested plan, a strong and protected group data-sharing method is presented, using cloud-based identity-based encryption (CR-IBE) that can be taken back. This novel way allows any person in a group to share data safely through a cloud setting that cannot be trusted. The main benefit is how well it can quickly help changing groups. New users given entrance can right away decode data documents uploaded before they became involved without needing get in touch with the first people who owned the data. Our proposed system allows users to easily remove themselves through a new encrypting method, removing the need to change others' secret codes. Importantly, the amount of encrypting and processing work stay the same no matter how many users leave. This keeps it fast and limits how much leaving users slow it down. Our proposed solution includes ways to keep personal information private while allowing group members to use cloud resources together. Any member can stay anonymous when using shared things online. This gives extra protection by hiding who people are while sharing. Also, the manager of the group can show real names if there are problems. They make sure the group stays honest and responsible.

3.1 Our contributions are:

1. For databases of ciphertext content, we found shared records to be comfortable and efficient shared auditing for multi-user operation.
2. We suggest an efficient data auditing scheme with new features, including vector commits primitives with traceability and accounting, mismatched organization key settlement, and organization signing.
3. The evaluation results show that our system is comfortable and efficient, as we offer security and performance analysis that allows you to get data storage and return to the cloud.
4. Authorized duplicate verifying within the hybrid cloud architecture supports multiple duplication structures, and this authorized de-duplication scheme has a relatively low overhead compared to regular operation.

3.2 System Architecture

As shown in the Figure 1, the proposed architecture divided into various modules as described below,

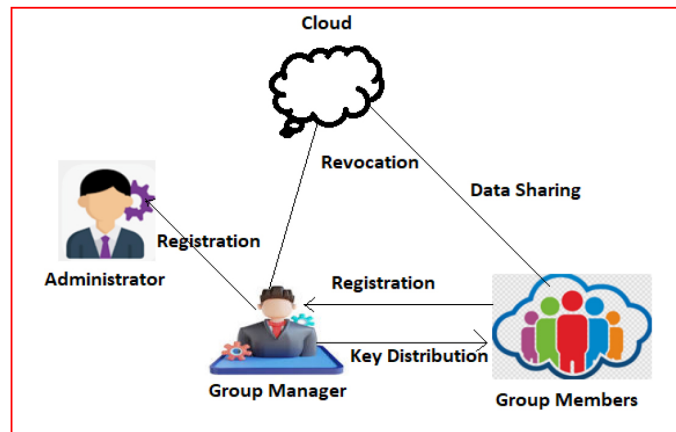


Figure 1

Proposed System architecture

- **Cloud Server:** Cloud, a top resource storage, offers reliable data storage. Group access managed by a revocation list. Cloud server is honest but curious, ensuring data integrity.

- Group Manager/Admin: The group administrator works through the corporation administrator. We consider group admin to be fully trusted by other events.
- Group Members: Group members are registered users, so anyone can store their private data on a cloud server and share it with others within the group. Both group administrators and group members can log in with their login information. After a successful login, the group admin assigns each member's newly delivered cloud user keys, using bilinear mapping, and sends them to the corresponding group peers. An ID-based ring signature scheme consists of the following algorithms:

Setup, PKGen, KeyUpdate, Encrypt, DkGen, CTupdate, and Revoke.

Setup($1^\lambda, T, N$): The setup rules take as input. Security parameter λ , time constrained time T and the number of most device clients is N , the effects return the general parameter and the PP secret key MSK , and it is connected with *Revocation list* $RL = \emptyset$ and *State* st .

PKGen(PP, MSK, ID): PP, MSK takes as an input by a private key Generator Algorithm and Identity $ID \in I$ and it produced a private key SK_{ID} for ID and updated list st .

KeyUpdate(PP, MSK, RL, t, st): this algorithm takes input as a MSK, PP and Key update time $t \leq T$, *Revocation List* RL , state st and the output is KU_t .

Encrypt(ID, t, PP, M): it takes input as a identity ID, PP , and time period $t \leq T$ and message $M \in M$ to be encrypted. The output is $CT_{ID,t}$.

DKGen(SK_{ID}, PP, KU_t): Here, this algorithm takes input as a KU_t, SK_{ID} and PP and Generates the Decryption is as a $DK_{ID,t}$ for ID with time t .

CTUpdate($CT_{ID,t}, PP, t'$): $PP, CT_{ID,t}$ and time period are taken as an input by Cipher text algorithms and time period $t' \geq t$ and its output updated ciphertext $CT_{ID,t'}$

Revoke(ID, RL, PP, st, t): this algorithm takes an identity $ID \in I$ to be revoked, PP as a Input and revocation list RL and revocation time $t \leq T$, state st and its update RL to a new one.

Algorithm1: KU Nodes (BT, RL, t):

```

1.  $X, Y \leftarrow \emptyset$ 
2. for all  $(\eta_i, t_i) \in RL$  do
3.   if  $t_i \leq t$  then
4.     Add Path( $\eta_i$ ) to  $X$ 
5.   end if
6. end for
7. for all  $\theta \in X$  do
8.   if  $\theta_i \notin X$  then
9.     Add  $\theta_i$  to  $Y$ 
10.  end if
11. if  $\theta_r \notin X$  then
12.   Add  $\theta_r$  to  $Y$ 
13. end if
14. end for
15. if  $Y = \emptyset$  then
16.   Add the root node  $\varepsilon$  to  $Y$ 
17. end if
    return  $Y$ 

```

Algorithm 2: CTEncode

```

1. function CTEncode( $t, T$ )
2.    $t \leftarrow TEncode(t, T)$ 
3.    $chk \leftarrow false$ 
4.   for  $i \in [\log_2 T]$  do
5.     if  $t[i] = 1$  and  $chk = false$  then  $t[i] = 1$ 
6.   else
7.      $chk \leftarrow true$ 
8.      $t[i] = 0$ 
9.   end if
10.  end for
11.  return  $t$ 
12. end function

```

Algorithm:3 Decrypt

```

1. Decrypt_file (F') {
2. /* algorithm to decrypt file downloaded from cloud
   storage */
3. /* to transform Cipher text in file F' into Clair
   text in file F */
4.
5. /* Phase 1: Decrypt AES Key with RSA Algorithm */
6.
7. for  $k' \leftarrow 1$  to SizeOf( $K'$ ) do
8. {

```

```

9. k=DEC_RSA(k')
10. }
11. return(K)
12.
13. /* Phase 2: Decrypt Cipher text with AES Algorithm
*/
14. for B'←1 to number Of Block(F') do
15. {
16. B=DEC_AES(B',K)
17. }.
18. return(F)
19
1.  Decrypt_file(F){
2.  to decrypt file downloaded from cloud storage * /
3.  transform Cipher text in file F
    into Clair text in file F * /
4.  Phase 1 : Decrypt AES key with RSA
    algorithm * /
5.  for k' ← 1 to Size of (K') do
6.  {
7.  k = DEC_RSA(K')
8.  }
9.  return(K)
10. 2/*Phase : Decrypt Cipher text with AES
    algorithm
11. for B' ← 1 to number of Block(F') do
12. {
13. B = DEC_AES(B',K)
14. }
15. return(F)

```

4. Results and Discussions

This let us see how well our chosen identity-based encryption method, called CR-IBE, could perform. Other existing techniques work well for sharing data within groups when you can revoke access later.

Table 1
Summary of ABE, CP-ABE, CR-IBE Encryption time

File size (KB)	ABE (ms)	CP_ABE (ms)	CR-IBE (ms)
15	1020	940	700
17	1050	960	803
20	1110	1070	920
24	1250	1130	1120
27	1405	1380	1340
30	1650	1510	1480

This Table 1 compares several approaches such as ABE, CP – ABE, and CR – IBE. The file size for different methods is shown on the x-axis, while the y-axis shows how long it takes to encrypt files. The graph shows that the suggested CR-IBE method requires less time to encrypt files than earlier techniques.

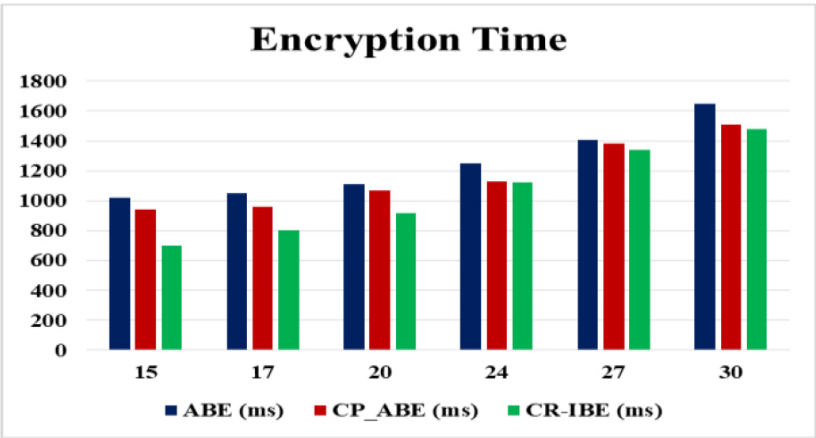


Figure 2
Representation of Different file size Vs Time taken for Encryption

This Figure 2 looks at how well different methods handle file decryption. Methods shown include ABE, CP – ABE, and CR – IBE. The horizontal line shows file sizes for each approach. The vertical line shows how long it takes to decrypt files. C R – I B E seems to decrypt files faster than older decryption techniques based on these results.

Table 2
Summary of decryption execution time for different Algorithms

File size (KB)	ABE (ms)	CP_ABE (ms)	CR-IBE (ms)
15	820	720	510
17	890	960	700
20	910	840	675
24	1020	970	790
27	1305	1180	995
30	1560	1360	1060

The above Table 2 shows Execution time for Decryption between ABE,CP-ABE, and CR-IBE. Figure 3 shows the comparison decryption time.

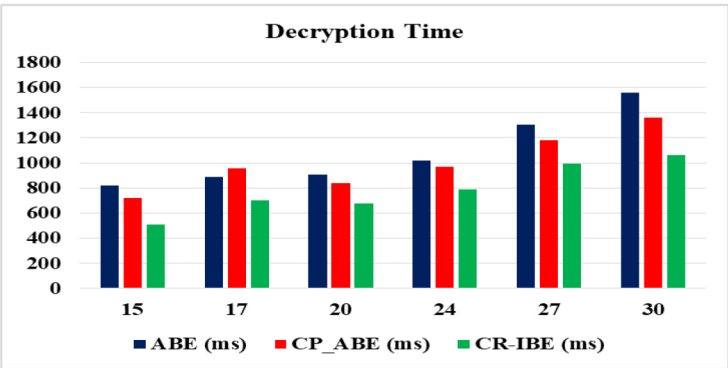


Figure 3
Representation of Different file size Vs Time taken for Decryption

5. Conclusion

Cloud computing provides a convenient way to group data sharing with users in the cloud environment. It protects the data kept in the cloud by using some encryption techniques. One of the primary benefits the cloud service requests is group data sharing in a dynamic environment. This paper describes a novel method for sharing cloud storage data using a cloud-based revocable identity-based encryption method. The proposed novel method supports efficient user revocation and allows new users to access the cloud server. A public revocation list can perform effective user

revocation without changing the secret keys of the remaining users in the group. The newly added users can decrypt files inside the cloud before sharing them. The experiments were conducted on the various schemes of ABE, CP-ABE, and CR-IBE in the scenario of execution time for file encryption and decryption. The experimental results show that the proposed system provides better results than the previous methods regarding encryption and decryption time.

References

- [1] G Ravindra Reddy, and A V Vamshi Krishna, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", pp.111-118 (2017).
- [2] Tran Viet Xuan Phuong and Willy Susilo, "Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions", pp.35-45 (2016).
- [3] Surya Nepal & Dongxi Liu, "Ciphertext-Delegatable CP-ABE for a Dynamic Credential: A Modular Approach", pp.3-20 (2019).
- [4] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for Resource Allocation of Grid Computing," in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.
- [5] Muhammad Waqas and ShanshanTu, "A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing" (2021).
- [6] J.Wu and T.Wang, "CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing , pp.160482-160497 (2019).
- [7] Jianfei.S and Hu.X, "Comments on Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing", pp. 461-462 (2017).
- [8] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.
- [9] K. Mohanty and K. Sakurai, "A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing", pp. 241-256 (2017).

- [10] Sharma, S.K., Kumar, A., Digital Image Transformation Using Outer Totality Cellular Automata. Machine Intelligence Techniques for Data Analysis and Signal Processing. Lecture Notes in Electrical Engineering, vol 997. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-0085-5_69.
- [11] S. Xu and Y. Mu, "A new revocable and re-delegable proxy signature and its application", pp.380–399 (2018).
- [12] Ajani, S. N., Khobragade, P., Dhone, M., Ganguly, B., Shelke, N., & Parati, N., Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. *International Journal of Intelligent Systems and Applications in Engineering*, 12(7s), 546–559 (2023).
- [13] L. Jiang, Guo D, 2 "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage", pp. 13336–13345.
- [14] X. Huang, and Lou W., "New publicly verifiable databases with efficient updates", pp. 546–556 (2015).