International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Secure Dynamic Groups Data Sharing with Modified Revocable Attribute-Based Encryption in Cloud

Dileep Kumar Murala, Sandeep Kumar Panda, Santosh Kumar Swain

Abstract*: Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Although it causes many security issues, cloud service providers are not at the same level of trust as users. To preserve the privacy of data against non-trusted Cloud Service Provider (CSP) files, current solutions implement Cryptographic methods (for example, encryption methods) and deliver decryption keys only to authorized users. However, data sharing in the cloud among authorized users remains a difficult problem, especially when it comes to dynamic user groups. Most of the research on dynamic group data exchange has been done in the cloud with many algorithms, such as Attribute-Based Encryption (ABE), Ciphertext Attribute-Based Encryption (CP-ABE) to provide better security in dynamic cloud users with multiple authorities, but they still face challenges, either lack of performance or rely on a trusted server, and are not suitable for distribution with the problem of eliminating attributes. Thus, the Revocation user cannot get shared data before and after. To solve this in particular, we first suggest an effective Modified Revocable Attribute-Based Encryption (MR-ABE) system with the quality of ciphertext allocation by applying and integrating both Identity-Based Encryption (IBE) and CP-ABE techniques. It can provide confidential forward / backward of encrypted data by delivering user revocation attributes and updating encrypted text simultaneously. Next, we perform Fine-grained access control and data exchange for on-demand services with dynamic user groups on the cloud. Experimental data show that our proposed system is more efficient and scalable than the latest generation solutions.

Keywords: Attribute-Based Encryption, Cloud Security, Dynamic Group Data Exchange, Fine-grained access, Identity Based Encryption, Privacy, Revocation.

Manuscript published on November 30, 2019.
* Correspondence Author
Dileep Kumar Murala*, School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha, India. Email: dileepkumarmrecw@gmail.com
Sandeep Kumar Panda, Computer Science and Engineering, Faculty of Science and Technology, ICFAI Foundation for Higher Education, Hyderabad, Telangana, India. Email: skpanda00007@gmail.com
Santosh Kumar Swain, School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha, India. Email:sswainfcs@kiit.ac.in

I. INTRODUCTION

Cloud computing is a model that offers large computing space and a huge memory space at low cost. It allows users to get the expected support regardless of time and position on different platforms (for example, mobile devices and personal computers), thus, provides an excellent convenience for cloud users . Among the many cloud computing help, cloud storage help, such as Apple iCloud, Microsoft Azure, and Amazon S3, can help provide an easy and easy way to share data over the Internet, which offers many benefits to our society . But also suffers from various security threats, which are the main concerns of cloud users. First, the outsourcing of data to the cloud server indicates that data is out of control of users. This can cause the user to delay because external data generally includes basic and sensitive data. Second, data is frequently shared in an open and obnoxious environment, and the cloud server will be the victim of attacks [1]. More, the cloud server itself can detect user data for illegal revenue. Third, data distribution is inactive. That is, when user support ends, he/she must no longer control the prerequisites for obtaining shared data before and after. Therefore, when outsourcing data to the server in the cloud, customers must also manage access to such data so that only currently authorized users can receive data outsourcing [8].

One of the medium offerings provided through the project providers is the data garage. Despite the advantages of the garage in the cloud, it faces many difficult situations that can prevent a rapid boom if not solved. Consider a reasonable utility that allows the organization to store data and percentages of its employees or departments across the cloud. With the cloud, the enterprise can free itself completely from the living burden of storing and keeping information. However, this also poses a security risk to the privacy of the statistics. Specifically, customers do not trust CSP at all. At the same time, the log files saved in the cloud can be encrypted and encrypted. To solve this problem, the simple solution is to encrypt the information and then load the encrypted records into the cloud [11]. However, traditional encryption techniques for sharing statistics within the cloud are neither effective nor flexible. An advanced, easy-to-use encryption method that allows you to share garage assets to the fullest and allows you to share data at a certain level. Using Attribute-Based Encryption is one of the most cunning tools for handling certain entries and sharing encrypted data. However, applying ABE without delay to real applications is not always clean due to many practical concerns [2].

On multi-authority cloud storage device, user functions can be dynamically modified. The consumer may be entitled to some new jobs or to cancel some existing jobs [8]. You must change your information to access permissions for this reason. However, modern methods of attribute cancellation rely primarily on a trusted server or total performance loss and now are not enough to solve the cancellation management issue to control access to the garage machine data in the cloud [3].

Dynamic user Groups are very popular in cloud storage, for example, because of a person's expiration or modifications to the People Club and the theft/obligation/ misuse of a person's credentials. In dynamic user groups, revoked customers are a major protection issue that you want to address effectively [11]. However, the problem of managing user deletions in the cloud storage is that a Revocable consumer can, however, decrypt the old encrypted text that was allowed before it was revoked. To resolve this issue, you may need to update the encrypted text saved in the cloud storage, which you include through the Allied (un-trusted) cloud server. In the literature, proxy encryption is recommended to replace the legal decryption of encrypted text content, and this approach is included in ABE for encrypted text encryption. It may be updated (for example, CSP for cancellation purposes). However, proxy encryption coverage requires initiating encryption/updates in the CSP to allow the encrypted text content to be updated. From a reasonable use point of view, it is incredibly recommended that CSP replaces cryptographic text frequently, without the need for any context directories [4].

II. REVIEW OF LITERATURE

Many encryption systems, including IBE, offer the most useful access control. It limits users' ability to choose encrypted data at a certain level. Encryption features based on CP-ABE features are a promising time designed to control the access of encrypted records. There are two types of CP-ABE structures: CP-ABE, in which all attributes are controlled by an identical authority. Some government characteristics CP-ABE come from unique areas and are controlled with the help of specific authorities. CP-ABE is a multi-authority machine accessible in the cloud system, where customers can implement multiple options and record owners use to access quality coverage in various government features and share statistics. However, due to the difficulty of cancellation, these multi-authority CP-ABE schemes cannot be implemented simultaneously from several agencies to address access to the facts to the cloud garage machine. It is suggested that you rely on some distinct cancellation schemes based entirely on a trusted server for attribution level cancellation. We understand that stats owners cannot rely entirely on servers in the cloud, so technologies to eliminate traditional features are not now suitable for cloud storage structures [5].

Li Lin. [6] describe, cloud computing is vital to protecting data privacy, because a privacy leak can save your customers from using cloud offerings. To ensure the confidentiality of records, we suggest Priguarder, a new way to overcome access and discover confidentiality. This procedure includes 3 steps for the cloud service provider: consumer registration, arrival logs, and access to information. In each grade, customers can choose two ways to interact with the cloud provider, directly and indirectly. Through indirect design, a resource deployment system was introduced to make the user identity specific and the distinctive functions confidential in the three domains. In addition, new protocols for direct access to controls have been proposed to improve the interaction between customers and cloud service providers, taking advantage of record encryption and time stamp technology. We described the use of our methodology in the Amazon S3 context. Complete theoretical analysis and simulation experiments were completed, which demonstrated the effectiveness of Priguarder.

XiaoyuLi [7] proposed ABE can fulfill the right of default entry for function control within the cloud garage, especially for encrypted text content coverage features. Because user privileges can be issued across multiple entities, pop-up encryption is essential to enforce access based on attributes to handle encryption of external information in encrypted text coverage for multiple entities. However, most current structures based on government agencies are not evidence of cost overruns and cancellation or exhaustion of costs in price accounting. In this report, we recommend an access controller based primarily on the functions of multi-power cloud garage chassis structures with complete security. In our proposed scheme, anyone can retrieve outsourcing data if that is useful if they have enough encrypted attribute keys with access coverage and permission key on the subject of outsourcing records. Also, the proposed chart provides fixed-length text content and a small calculation cost. In addition to accepting cancellation of the attribute level, our proposed plan allows the event owner to cancel at the consumer stage. Safety analysis, general performance comparisons, and experimental results show that our proposed scheme is not always the safest but also practical.

Sushmita Ruj [9] introduced Accurate access to processing is a request for information stored on cloud-like servers. Because of the large amount of data, decentralized master management plans are higher than important plans. Encryption and decryption usually have a very high and ineffective price, while users access records from a restricted resource. We recommend encoding based on the ABE attribute with fast encryption and external decryption. The basic idea is to divide the encryption into stages, and the initial processing step is offline when the tool is not in use and when the step is online while encrypting the records with the policy. This makes encryption faster and greener than current decentralized ABE schemes. To decrypt outsourcing, statistical clients must do so. It is necessary to create an encrypted decryption key model that allows an un-trusted proxy server to decrypt partially encrypted text in simple text statistics. Data users can decrypt partially encrypted text content without a high price match.

III. PROPOSED MR-ABE MECHANISM

In this approach, we propose a modern way to ABE access control for active user groups in the cloud server scenario. Especially, we offer a state-of-the-art Modifiable Attribute-Based Encryption with Revocable (MR-ABE) scheme that enables cloud storage to encrypt encrypted data to cope with cancellation without a delegate key. Get up to date and perform high-performance at the same time. Here, we first recommend an Attribute-Based Encryption (ABE) with a revocable scheme, where an active and protected revocation method is intended to determine the attribute revocation difficulty in the system. We have an effective attribute Revocable scheme in the sense that bear a lower connection cost and an account cost, it is safe in the sense that it can bring a lot of backward secrecy and forward secrecy [12]. Also, in this paper recommending an Identity Based Encryption scheme with integrating of Ciphertext policy attribute-based encryption to provide an identity for particular files and cloud users to uniquely identify. Using MR-ABE design, we offer a protected and detailed monitoring system for accessing data and sharing cloud-based service applications on demand. In particular, we use cloud-based broadcast movies as a typical example . We show that our method presents a viable solution for applications that require complete access control and ongoing user updates for large groups of users. This cancellation method is useful because it lowers the cost of communication and computer overhead. It is both safe to forwarding and backward. Our scheme does not require complete reliance on the server, as the master update is implemented by the server, and the certificate issuer. The following algorithm describes the key updates [8].

A. Algorithm1: $KU\ Nodes\ (BT, RL, t)$:

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

Our proposed MR-ABE uses Binary Tree Structure to get proficient Revocation. To explain the revocation procedure, we offer several signs first. Root Specify the root node $\varepsilon Binary\ tree\ BT$ and set of nodes on $Path(\eta)$.The path from ε to leaf node η(including ε and η) without leaf node θ, we'll let it stand on the left θ_l and right child θ_r sides, respectively.

Here given time period is t and the revocation list is RL.

η_t, t_i , indicates that the node η_t and revoked time period is t_i and the algorithm provides output is Subset Y [9].

The total number of time periods T is comprised of the following polynomial-time algorithms:

- $\mathbf{Setup}(1^\lambda, T, N)$: Setup algorithm takes as input. Security parameter λ, bound time T and the Number of maximum system users N are, and it returns the results public parameter PP and master secret key MSK , and it is connected with $Revocation\ list\ RL = \emptyset$ and $State\ st$.
- $\mathbf{PKGen}(PP, MSK, ID)$:$PP, MSK$ 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 an updated list st.
- $\mathbf{KeyUpdate}(PP, MSK, RL, t, st)$: 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.
- $\mathbf{Encrypt}(ID, t, PP, M)$: It takes input as a $identity\ ID, PP$, and time $period\ t \leq T\ and\ message\ M \in \mathcal{M}$ to be encrypted. The output is $CT_{ID,t}$.
- $\mathbf{DKGen}(SK_{ID}, PP, KU_t)$: Here, this algorithm takes input as a KU_t , SK_{ID} and PP Generates the Decryption is as a $DK_{ID,t} ID$ for with $time\ t$.
- $\mathbf{CTUpdate}(CT_{ID,t}, PP, t')$:$PP, CT_{ID,t}$ and time period is taken as input by Cipher text algorithms and time period $t' \geq t\ and\ its\ output\ updated\ ciphertext\ CT_{ID,t}$
- $\mathbf{Revoke}(ID, RL, PP, st, t)$: this algorithm takes an $identity\ ID \in I\ to\ be\ revoked, PP$ as an Input and $revocation\ list\ RL$ revocation $time\ t \leq T$, state st and it $update\ RL$ is to a new one

B. $Algorithm2: CTEncode$

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

Here,

Time t

bounded system life time T are input and,

bit string t of the size $log_2 T$

The above algorithm is used to reduce the complexity of the space. Processing the Ciphertext and the Cipher Text Delegation.

C. System Architecture

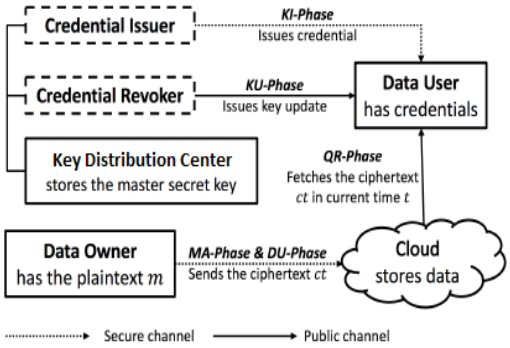

Fig.1. Proposed Model.

The data owner sends ciphertext ct to cloud storage in real-time, and the data user can then query the cloud storage to access the ciphertext. Assuming that the data user issues a query, the data owner sends the original ciphertext ct to cloud storage in a pledge, and the data user can then query the cloud storage to access the ciphertext. Assuming that the data using queries $t_1 \geq t$ then the cloud service provider transfers updated encrypted data ct_{t1} to the user. And this encrypted data decrypted by the user if he/ she satisfy access policy given by the data owner and it is not revoked t_1 [10].

IV. RESULTS AND DISCUSSIONS

Table-I: Execution time for Encryption in ABE, CP-ABE, MR-ABE.

File size (KB)	ABE (ms)	CP_ABE (ms)	MR-ABE (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

Table.1 shows Execution time for file Encryption in various algorithms like ABE, CP-ABE, and MR-ABE. The file size is taken in the KB and Execution time taken in milliseconds format.

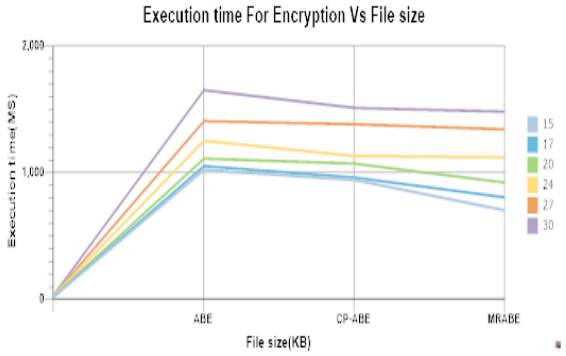

Fig.2. Execution time for Encryption Vs File size.

Fig.2 shows a comparison between various algorithms like ABE, CP-ABE, and MR-ABE. Here x-axis indicates about File size between various algorithms and Y-axis indicates Execution time for Encryption. As shown in the chart Proposed MR-ABE algorithm can take less execution time for File Encryption compares with previous algorithms.

Table-II: Execution time for Decryption in Various algorithms.

File size (KB)	ABE (ms)	CP_ABE (ms)	MR-ABE (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.II shows Execution time for Decryption between ABE, CP-ABE, and MR-ABE.

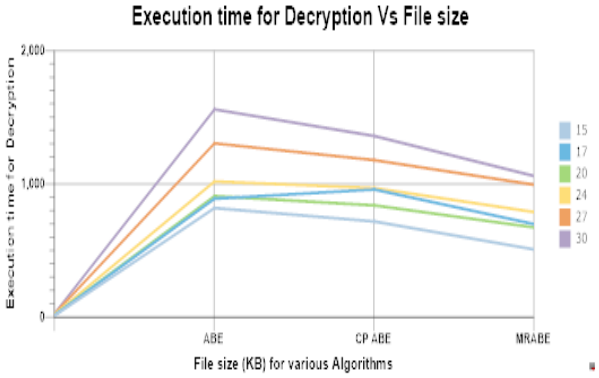

Fig. 3. Execution time for Decryption and File size.

The above figure 3 shows the comparison between different algorithms such as ABE, CP-ABE, and MR-ABE. The X-axis here indicates the file size between different algorithms, and the Y-axis indicates the execution time for encryption.

As suggested in the chart, the MR-ABE algorithm may take a shorter execution time compared to the earlier algorithm in file encryption.

V. CONCLUSION

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In cloud Environment, Data sharing between Dynamic Groups become a more challenging issue. Because there is a revocable chance users can also access Data after they are left from the group. To end this, The Revocable attribute-based encryption preserving ciphertext delegation is a valuable fundamental for allowing secure data sharing via a third-party storage assistance provider such as cloud storage. In this paper, we proposed effective Modified Revocable Attribute-Based Encryption (MR-ABE) Technique with the quality of ciphertext Allocation by performing and uniquely mixing both Algorithms of Identity-Based Encryption (IBE) and Ciphertext Attribute-Based Encryption (CP-ABE) to provide safety data sharing between Dynamic Groups and provide forward/backward secrecy.

Further, the fine-grained access control mechanism is implemented to Authenticated Data access. The Proposed MR-ABE scheme is proved adaptive-secure in the standard model, more effective and compared with the previous Methods. MR-ABE algorithms compared with earlier algorithms ABE, CP-ABE. The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

REFERENCES

1. H Kavitha, 2018, "*Access Control Over Secured Data in Public Cloud Server*", pp. 493-498.
2. KaipingXue, Peilin Hong, 2017, "*RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage*", pp. 953-967.
3. Qi Li, 2017, "*Multi-authority attribute-based access control scheme in M-Cloud, which features highly regarded universe and decryption outsourcing* ", pp. 1-7.
4. V. Goyal, A. Sahai, 2008, "*Bounded Ciphertext Policy Attribute-Based Encryption*'', pp. 579-591.
5. Jin Li, 2013, ''*Identity-Based Encryption with Outsourced Revocation in Cloud Computing*,'', pp. 1-12.
6. Li Lin, 2018, "*PriGuarder: A Privacy-Aware Access Control Approach Based on Attribute Fuzzy Grouping in Cloud Environments*", pp. 1882-1893, 2018.
7. XiaoyuLi, Jie Chen,2017, "*Two-Factor Data Access Control with Efficient Revocation for Multi-Authority Cloud Storage Systems*", pp. 393-405.
8. Dileep Kumar Murala, 2019,*" A Novel Hybrid Approach for Providing Data Security and Privacy from Malicious Attacks in the Cloud Environment",* Vol. 11, 06-SP, PP. 1291-1300.
9. Sushmita Ruj, 2015, "*Decentralized Access Control on Data in the Cloud with Fast Encryption and Outsourced Decryption*", pp. 1-6.
10. Yingjie Xue, Peilin Hong, 2016, "*A Location-Aware Attribute-Based Access Control Scheme for Cloud Storage*", pp. 1-6.
11. Dileep Kumar Murala, 2019,*" A Survey on Cloud Computing Security and Privacy Issues and Challenges",* Vol. 11, 06-SP, PP. 1291-1300.
12. A.B. Lewko, 2010, ''*Fully secure functional encryption: Attribution-based encryption and (classified) internal product encryption* ", pp. 62-91.

AUTHORS PROFILE

Dileep Kumar Murala, pursuing a Ph.D. in the School of Computer Engineering, KIIT deemed to be University since 2017. He received M. Tech degree from the Department of Computer Science Engineering, Andhra University Engineering College (A), Vishakhapatnam, in 2011 and he received the B. Tech degree from the Department Of Computer Science Engineering, Gudlavalleru Engineering College (GEC), JNT University, Kakinada in 2009. 2 patents in his credit. His academic interests lie in Cloud Computing, security and privacy, Blockchain technology, Wireless Sensor Network, Data Mining, and Information Security. He has published 19 international journals and 1 international conference.

Sandeep Kumar Panda , was completed a Ph.D. at the School of Computer Engineering at KIIT University, India. He is presently working as Associate professor in ICFAI Foundation for Higher Education, Hyderabad. 6 patents in his credit. His academic interests lie in Human Factors, especially, Usability Engineering and Human-Computer Interaction: constructing a conceptual framework for User preferences, developing a user, heuristic and tool based usability evaluation method, and analyzing human cognitive processes based on users judgments for interactive applications. His interested area also includes Blockchain technology, Machine learning, Neuroscience and cloud computing. He is the member of IEEE and ACM. He has published 20 international journals and 10 international conferences.

Santosh Kumar Swain , has received his Ph.D. at the School of Computer Engineering at KIIT University, India. He is presently working as professor in KIIT Deemed to be University, Bhubaneswar, Odisha. His academic interests lie in Software Engineering, Web Engineering, Human-Computer Interaction, Cloud Computing, and Wireless Sensor Network. 2 patents in his credit. He has published 50 international journals and 30 international conferences. He is a member of LMISTE and MCSI.