International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Optimal integrity Policy for Secure Storage of Encrypted Data using Cloud Computing

T.N.Ranganadham, G.I.K.Durga Bhavani, M.Rudra Kumar

Abstract*: Cloud computing is very common at reduced price because of its computing and storage ability. To reduce storage costs, an ever increasing number of information are being moved to the cloud. Then again, since the cloud isn't completely dependable, they are usually encrypted before uploading to shield information protection from outsiders and even the cloud server. However, many activities on encrypted information, such as searching, are difficult to conduct. Searchable encryption has emerged to solve this issue. It is much less effective to search for encryption in multi-user environment than in single-user environment. As a foundation of attribute-based encryption to solve this issue a multi-user searchable system is suggested. Our system also keeps information safe in opposition to the cloud server in the cloud. It enables users with suitable permissions to conduct encrypted information search activities. Furthermore, customers generate search tokens instead of information holders. We demonstrate that in our system, token privacy and index privacy are all around ensured. No helpful data about search tokens and ciphertexts can be obtained from the cloud server and illegal users. Our scheme's ciphertexts are constant in size, reducing our scheme's time-complexity and bandwidth overhead.

Keywords*: Token privacy , Index privacy, Cloud Computing, Encryption and Decryption.

I. INTRODUCTION

Our today's society progressively relies on digital data collection, processing and sharing. Communication and networking are becoming more and more omnipresent and ad hoc thanks to the fast innovations in sensor, wireless and networking techniques. Driven by the explosive development of hardware and software capacities, computing energy becomes a government utility, and data is often stored on centralized servers to promote omnipresent access and sharing. The system's data is generally delicate and of elevated importance, while the system's confidentiality may be jeopardized by multiple safety breaches. Therefore, safety and privacy mechanisms need to be developed urgently in order to safeguard the authenticity, integrity and confidentiality of the data gathered and to regulate the disclosure of personal information. To accomplish this, there is a lack of centralized trusted parties in omnipresent networking; system users tend not to trust remote data servers when managing their data. They make it unsuitable for traditional networked information systems to create present security solutions. Users provide storage and company information to the cloud service provider. In addition, if their private information is revealed to their company rivals or public, the entrepreneurs will experience the critical implications. To mitigate safety problems in the cloud, many data security methods are created. Current approaches to data security concentrate only on data security in which random key generation procedures follow cryptographic solutions. But minimum data integrity is affected by the prevalent safety method. Key loss in standard cryptographic methods crashes the information owner's initial information. ABE is a public key encryption method that enables users to encrypt and decrypt emails based on user characteristics. For a specific user, the cipher texts are not encrypted in the ABE scheme. Rather, a set of characteristics or a policy over characteristics is connected with both the cipher texts and decryption keys. The user can only decrypt a cipher text when the decryption key matches correctly with the cipher text. ABE schemes are categorized as ABE (KP-ABE) based on key policy and ABE (CP-ABE) based on cipher text policy. The KP-ABE system is based on the user's attribute connection and decryption keys.

II. RELATED WORK

The Searchable Encryption technology tackles the search problem on the encoded files and enhances cloud storage and cloud computing practicability. It has greatly enhanced the usefulness as well as the accessible encryption adequacy. Multi-participant searchable encryption enabled the sharing of information among many individuals, where approved information users could search the files uploaded by information owners. Our work highlights multi-user model studies in searchable systems. The attribute-based encryption (ABE) systems attract the extensive focus of scientists in latest years with the growth of cryptography. It is an effective system for dealing with open access control situations issues. ABE was first launched by Sahai and Waters and allows access control over encrypted information using a number of generic characteristics linked to both the client secret key and the ciphertext [1]. ABE has two supplementary types: key-policy attribute-based encoding (KP-ABE) and attribute-based encoding (CP-ABE) ciphertext-policy. In CP-ABE, the ciphertext is associated with an access structure consisting of threshold gates between attributes; a user can decrypt a ciphertext if and only if the ciphertext access structure is satisfied by his / her attributes associated with his / her secret key, whereas the situation in KP-ABE is reversed.

Manuscript published on 30 September 2019.
***Correspondence Author(s)
T.N.Ranganadham, Assistant Professor, Department of CSE, Annamacharya Institute of Technology & Sciences, Rajampet, Andhrapradesh, India-516126.
G.I.K.Durga Bhavani*, PG Student, Department of CSE, Annamacharya Institute of Technology & Sciences, Rajampet, Andhrapradesh, India-516126. Email: bhavani.kurnool@gmail.com
M.Rudra Kumar, Professor & HOD, Department of CSE, Annamacharya Institute of Technology & Sciences, Rajampet, Andhrapradesh, India-516126.

CP-ABE is regarded to be more appropriate for outsourced data access control in the cloud data sharing scheme than KP-ABE because it provides DOs more immediate access policy command, and access policy implementation takes place within the cryptography. Under the descriptive cluster template, the first building of CP-ABE [2] is suggested.

One of the biggest hurdles for CP-ABE practical apps, however, is how consumers can revoke the characteristics. The reader should not be allowed to decrypt the ciphertext that needs the item to decrypt when a customer no longer has one of his / her characteristics. This is generally called revocation of the item, and forward privacy is the respective safety property. Since each variable can be exchanged by various customers and a customer can have more than one attribute, coping with property revocation in CP-ABE environments in a straightforward manner creates severe pressure on both main power and DOs owing to re-keeping the big amount of confidential codes of customers and updating the ciphertext. Therefore, in practical situations, the problem of asset revocation in CP-ABE is cumbersome.

This problem was first discussed by Pirretti et al.[3] in the ABE system by establishing an expiry date for user characteristics. In order to decrease the cost and difficulty of the past one, Touati et al.[4] suggested in CP-ABE an image revocation solution called the batch-based approach which refreshes the required hidden numbers components of the customers at each location. Therefore, in the CP-ABE system, these methods did not accomplish an instant revocation of the attribute.

Several CP-ABE schemes have recently been suggested with an instant revocation of the attribute. Ibraimi et al.[5] suggested a system called guided ciphertext-policy attribute-based encryption (mCP-ABE) to solve the disadvantage of scheduled object revocation by incorporating a techniqueof dividing the secret key of a user into two stocks with CP-ABE[2]. However, this scheme cannot guarantee privacy forward because the person who no longer has a ciphertext entry permit can still decrypt it using the decryption coin from the prior decryption. Yu et al.[6] suggested their system with attribute revocation in order to decrease the load imposed on the key authority as the primary responsibility of instant attribute revocation in CP-ABE. By contemplating the assistance of a semi-trusted proxy client and incorporating web re-encryption techniquewith CP-ABE[2], this system achieves an attribute revocation alternative. But this system, relative to other systems, entails heavy cost computing and space on each revocation attribute. By pairing a broadcast revocation scheme [7] with CP-ABE [2] and by contemplating a semi-trusted proxy participating in the decryption phase, Jahid et al. [18] suggested a system to obtain an attribute revocation alternative without re-encoding non-revoked clients and re-encoding current ciphertexts. This scheme cannot provide forward privacy because the method of identity revocation does not update the exact parameters in ciphertexts. In addition, for each variable, it can only revoke the predefined number of clients. Moreover, for each variable, it can only revoke the predefined number of customers. Additionally, introducing a fresh customer to the scheme can cause the rekeying of current customer buttons, which in a big or extremely dispersed setting poses a prospective scalability problem.

Using dual authentication system combining CP-ABE [2] with minimum subset-cover algorithm [7], Hur et al.[8] suggested a system with an instant feature revocation method. In this scheme, the semi-trusted enterprise information service manager performs the primary part in the image revocation process and uses a binary important encoding key (KEK) computer to provide non-revoked customers with collective account numbers, where a KEK tree is constructed for the universe of all machine customers. However, this system still has some disadvantages in terms of flexible, safety, and scalability, such as additional information customers (DUs) overhead processing, susceptible to collusion assault by colluding customers. The scheme was suggested to eliminate intensive computing at the utility provider by decreasing the volume of a ciphertext and a secret key. Cai et al. [9] managed to revoke the characteristic in CP-ABE by means of a slow re-encoding system to decrease the price of re-encoding in [8], where DOs should remain internet all the time to re-encode information. The revocation of the characteristic in the CP-ABE system therefore remains an open problem for further progress. By solving this problem, we suggest a revocable CP-ABE system element by having advantage of the over-encoding mechanism[10] and CP-ABE[2] system and evaluating the semi-trusted cloud service supplier (CSP) involved in decryption procedures to send decryption tokens to approved customers. Our primary points can be described as follows: First, under the comparable premise in prior work, we are giving the building of an attribute-revocable CP-ABE system where the CSP is supposed to be honest but curious. The suggested system allows for versatile, effective and safe attribute-based entry command with object revocation in the cloud data sharing system on outsourced information. Second, we provide our scheme's safety and efficiency assessment.Our scheme has the following advantages:

a. It is flexible. Our scheme does not require priori knowledge of the size of total users in the system and potentially revocable users per attribute.
b. It is secure. Our scheme guarantees forward secrecy and collusion attack from users that might be triggered by users that are affected by attribute revocation events.
c. It is reasonably efficient. Our scheme is reasonably efficient in terms of storage, communication, and computational overhead as it delegates most of the heavy tasks to the semi-trusted CSP and it achieves an attribute revocation mechanism with the history-independent technique.

III. PROPOSED SYSTEM

A. System Model

Data owner, data user and cloud server are the three primary entities. Following the figure1, data owners encrypt their files $F = \{f_1, f_2, \cdots, f_n\}$ into the ciphertexts $C = \{c_1, c_2, \cdots, c_n\}$ using some symmetric encryption. Because the encryption of the file is prevalent, in this document we do not address it in detail.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A predefined keyword dictionary W_D={ w_1,w_2,⋯, w_m} is required, of course. According to the keyword dictionary, each information proprietor constructs its encrypted inverted index. We can use the file identifier for comfort in the real implementation rather than the record itself put away in the file. Finally, the information proprietor transfers the majority of the above data to the cloud server. When a keyword is searched by the data user, he utilizes his features to create search token. After the token has been obtained, the cloud server conducts the index search and returns the result to the customer.

B. Algorithm

The Data upload, query, and data download are the three components of our scheme based on the model specified in figure 1 . Several algorithms are respectively implementing each portion.

Data Upload: The data owner and system perform this portion. Before uploading, the owner creates a safe inverted index and encrypts files.

(*msk*, *pk*) ← *Setup*(*U*, 1λ). This probabilistic algorithm outputs the master key msk and the public key pk when entering a safety parameter λ and the attribute set U (which contains all user attributes).

(*cphW*, *cphF*) ← *Enc*(*S*,*WD*, *F*, *pk*). The probabilistic encryption algorithm generates the encrypted index and the ciphertext of files after receiving the access policy S, keyword dictionary WD={ w1,w2,⋯,wm} and file set F={ f1,f2,⋯,fn}. Due to the effectiveness, the file encryption is performed using some easy symmetrical encryption.

Query**:** The cloud server along with the data user execute this portion. For the keyword he wishes to query, the user produces token. sk ← KeyGen (Attr, msk, pk). The probabilistic algorithm produces the secret important sk given the user's Attr characteristics, master key msk, and public key pk.

tok ← TokenGen(pk, sk,w). This algorithm is used with the secret important sk and the keyword w to be queried to produce token tok.

Data Download: The cloud server executes this portion. The cloud server operates on the information search algorithm in cloud storage after obtaining the search token. Then it downloads and returns the matched files ciphertexts to the user.

rslt ← *Search*(*tok*, *cphW*, *cphF*). This deterministic algorithm outputs theciphertext of the files *cphF* if *cphW* can matched with the *tok*, outputs otherwise.

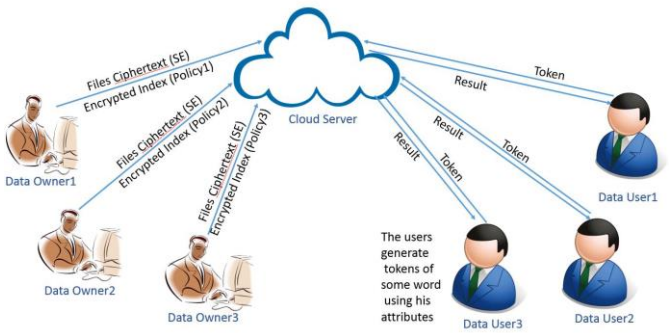

Fig1: System Model

IV. PERFORMANCE ANALYSIS

This analysis shows the experimental assessment of our effective encryption system based on the file hierarchical attribute.

Consider a files under authority F= (F_1,..... F_m) that perform Domain Granularity for each fresh user under distinct domain. Suppose the domain authority DA has a certain number of characteristics with a private key. If DA wants to delegate some of the attributes, the cost will generate linearly with the number of subsets to be assigned. The analyzed performance parameters are discussed as follows:

A. Setup Time

For its configuration activities, each specified number of attributes has linear cost-wise rises. Our suggested work is inferred better than prior CP-ABE from the specified Figure 2.

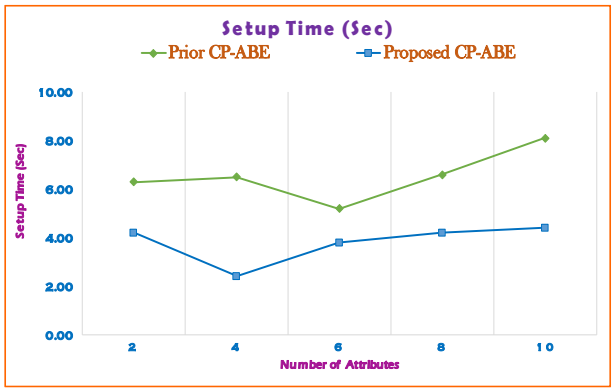

Fig 2: Setup Time

B. Key Generation Time

Generally, storage system costs are determined from the generation and choice of its characteristics. The cost and time to authorize the customers is determined according to the generation of characteristics. From Figure 3, it is inferred that with time-varied characteristics our suggested CP-ABE reduces linearly

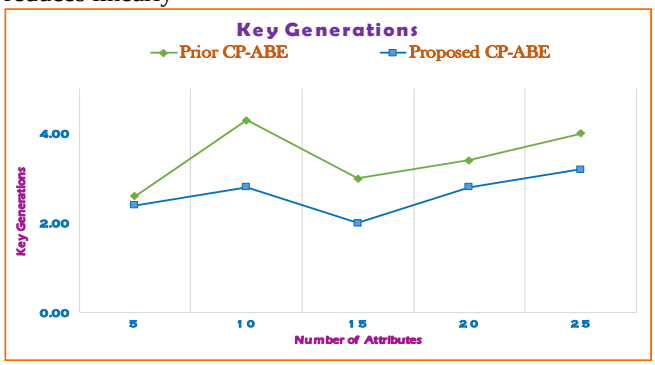

Fig 3: Key Generation Time

C. Encryption Time

To accomplish the success of our suggested system, the most important factor is encryption time. If the time taken to encrypt is greater, the size of the storage will also increase linearly and degrade the file storage process efficiency. Our suggested system now uses less time to encrypt the information shown in Figure 4.

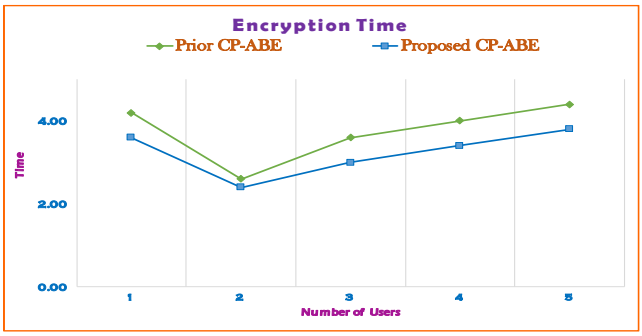

Fig 4: Encryption Time

D. Decryption Time

The time taken to decrypt was based on the structure of the access tree. Depending on the access tree and main structure, the decryption time is distinct. It assumes that in the main structure connected with the personal key there is only 1 subgroup with 40 characteristics. As shown in Figure 5, the decryption time is proportional to the number of leaf nodes required for decryption, and the access tree level does not affect the decryption time. Obviously, here too, the time taken to carry out the operation of the suggested scheme is less than in previous job.

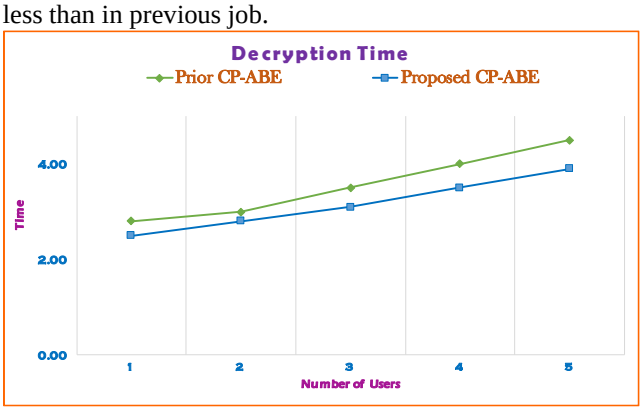

Fig 5: Decryption Time

V. CONCLUSION

Cloud Security is a significant component of cloud computing technology that shares most of the information. The users of the cloud are unaware of the information stored and its safety parameters. Previous works have been aided in the development of cloud storage systems ' encryption and decryption costs. In this document, we have suggested an enhanced and effective encryption method based on file hierarchical attributes that devises the standard of the method of encryption and decryption. The files are organized in hierarchical form in the first phase in order to facilitate the recovery process. For each uploaded file accessed in tree-based structure, the file index is retained. In the second phase, an Improved Ciphertext Policy-Based Encryption attribute designing the access control layer, where we have effectively organized encrypted documents in a hierarchical system with decreased storage and time-consuming encryption and decryption. Experimental assessment is assessed in terms of setup time, important generation, encryption and decryption.

REFERENCES

1. Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, Attribute-based encryption for fine-grained access control of encrypted data, Proceedings of the 13th ACM conference on Computer and communications security, October 30-November 03, 2006.
2. J.Bethencourt, A. Sahai, and B.Waters, “Ciphertext-policy attribute based encryption,” in Proc.IEEE Symp. Security and Privacy, Oakland, CA,2007
3. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, ‘‘Secure attributebased systems,’’ in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS). New York, NY, USA: ACM, 2006, pp. 99–112.
4. L. Touati and Y. Challal, “Efficient cp-abe attribute/key management for iotapplications,” in Computer and Information Technology (CIT), 2015 IEEE International Conference on. IEEE, 2015.
5. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, ‘‘Mediated ciphertext-policy attribute-based encryption and its application,’’ in Information Security Applications, H. Y. Youm and M. Yung, Eds. Berlin, Germany: Springer, 2009, pp. 309–323.
6. S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Achieving secure, scalable, and fine-grained data access control in cloud computing,’’ in Proc. 29th IEEE INFOCOM. Piscataway, NJ, USA: IEEE Press, Mar. 2010, pp. 534–542
7. D. Naor, M. Naor, and J. Lotspiech, “Revocation and tracing schemes for stateless receivers,” in *Proc. of Annual Intl. Cryptology Conf.*, 2001, pp. 41-62.
8. J. Hur and K.-N. Dong, “Attribute-based access control with efficient revocation in data outsourcing systems,”*IEEE Trans. on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, 2010.
9. B. Cai, L.-T. Xiong, J. Ye, and Z. Tang, “A scheme supporting efficient attribute revocation for cloud storage based on CP-ABE,” in *Proc. of the 3rd Intl. Conf. on Computer Science and Service System*, 2014, pp. 736-740.
10. H. Shimiz, Y. Kakimoto, and I. Sano, “Over-encryption: Management of access control evolution on outsourced data,” in *Proc. of the 33rd Intl. Conf. on Very Large Data Bases*, 2007, pp. 123-134.