AN EFFECTIVE SECURITY MECHANISM FOR DOCUMENT ENCRYPTION IN CLOUD USING CP-ABHE

[1]Syeda Afia Hussaini, [2]Dr. K. Saravanan
[1]PG Scholar, M.Tech, Dept of CSE, Shadan Women's College of Engineering and Technology Hyd, T.S, INDIA
[2]Professor, Dept of CSE, Shadan Women's College of Engineering and Technology Hyd, T.S, INDIA

Abstract: The existing technique CP-ABE can provide safe access control and information sharing policy in cloud. However, while encoding enormous number of documents/reports/archives, the cryptographic process of traditional schemes can be further improved. This should be possible through a reasonable methodology utilizing cipher text-policy attribute-based hierarchical encryption conspire named CP-ABHE. By practical, it means that both the computational power and storage size is more structured in CP-ABHE even without risking the data security. In CP-ABHE, the primary thought is to initially plan a lot of incorporated admittance trees based on the reports' attribute sets. At that point, the covetous methodology is utilized to assemble the trees bit by bit and develop the trees progressively by joining the small ones. Finally, all the reports on an incorporated admittance tree are encoded together. In correlation with the current plans, the leaves in such trees with a similar attribute share a secret number, which is utilized to encode the archives. Besides, the encryption technique can be made exceptionally secure by expanding security boundaries. This significantly improves the performance of CP-ABHE. The results demonstrate that the above proposed technique works very well in terms of protecting data, efficiency and the capacity size of the encoded text.

Index Terms: Cloud computing, attribute-based document collection encryption, encryption/decryption efficiency, information security.

1. INTRODUCTION

Cloud computing gathers and composes a lot of data technique assets to give secure, effective, adaptable and on demand administrations. Pulled in by these focal points, increasingly more undertaking and individual clients pattern to re-appropriate the neighborhood documents to the cloud. When all is done, the documents should be encoded prior to being moved operations to ensure them against spilling. On the off chance that the information proprietor needs to impart these documents to an authorized information client, they can utilize any accessible encryption techniques [9], [6], [2] or security protecting multi-keyword document search schemes [3],[8], [5] to accomplish this objective. Be that as it may, every one of these schemes can't give fine-grained admittance control instruments to the encoded documents.

The cipher text-policy attribute-based encryption (CP-ABE) technique can give secure access control and information sharing policy to the information clients in distributed computing. Nonetheless, while encoding an enormous archive set, the encryption/unscrambling effectiveness of existing plans can be additionally improved. This should be possible through a reasonable methodology utilizing cipher text-policy attribute-based progressive record assortment encryption conspires named CP-ABHE.

Existing ABE schemes can be separated into Key –Policy ABE (KP-ABE) schemes [11],[12] and Cipher Text-Policy ABE (CP-ABE) schemes [1], [10], [7]. Contrasted and KP-ABE schemes, CP-ABE schemes are more adaptable and appropriate for general applications. In the accompanying, we initially dissect the current ABE schemes in detail and further present the curiosity and advancement of the CP-ABHE scheme proposed in this paper. For comfort, we pick the schemes in [11] and [1] as instances of KP-ABE scheme and CP-ABE scheme, individually.

Both the KP-ABE and CP-ABE schemes are unreasonable to encode an enormous document collection on account of the accompanying reasons. To start with, the encryption cycle in both the two schemes is executed N times, prompting high calculation unpredictability. Second, there is a tradeoff between the size of the substance keys' cipher text and information clients' mystery keys. In KP-ABE, the quantity of mystery esteems in an information client's mystery key is amazingly huge for a document collection, forcing a weighty weight on the information client. In CP-ABE, the size of the cipher text is incredibly huge. Thus, CP-ABE scheme builds the information transmission sum between the cloud worker and information clients, which is an enormous test for the organization. This is sensible thinking about that the entrance structure of each document must be inserted into the cipher text or the mystery keys. Third, decoding the cipher text is additionally tedious thinking about that each document is scrambled separately. As of late, Wang et.al endeavored to improve the encryption efficiency and propose a record pecking order attribute-based encryption scheme named FH-CP-ABE. Nonetheless, this scheme zeroed in just on the most proficient method to encode a bunch of documents that share an incorporated admittance tree and subsequently it likewise can't be straightforwardly utilized to scramble a document collection.

In this paper, we plan an attribute-based document hierarchical encryption scheme named CP-ABHE which

performs well as far as calculation and storage space efficiency. The scheme comprises of two modules including coordinated admittance tree development and tree encryption. We initially propose a calculation to create the incorporated admittance trees for a document collection. The main plan objective of the calculation is diminishing the quantity of coordinated admittance trees which can significantly improve the encryption/ unscrambling efficiency. The summary of the paper is as follows:

- An algorithm to build the incorporated admittance trees gradually for the report collection is proposed and it can significantly diminish the quantity of the access trees.
- A record collection hierarchical encryption scheme is proposed. All the records that share an incorporated admittance tree are encoded together which can significantly improve the encryption/decryption efficiency. Also, the secret key extending issue is understood appropriately.
- The security of CP-ABHE is theoretically demonstrated and the adequacy of the incorporated admittance tree development algorithm is breaking down in detail. Likewise, an intensive correlation between CP-ABHE, KP-ABE and CP-ABE as far as encryption/decryption efficiency and storage capacity is given.
- Data proprietor is answerable for gathering records and doling out a legitimate attribute set to each report. The records are encoded in two stages. Each report is first encoded by a symmetric encryption algorithm with a unique key. At that point, the keys are encoded by ABE-schemes. Finally, both the encoded records and keys are moved operations to the cloud worker.
- To search the intrigued archives with regards to the cloud worker, an information client first needs to enroll herself to the CA center. At that point, the CA center allocates an attribute set to the information client and sends an attribute-related secret key to the information client.
- The authorized information client can send question solicitations to the cloud worker.
- Once an inquiry demand is gotten, the cloud worker initially communicates with the CA center to check the personality of the information client and an ID certification message is gotten when the information client is authorized. For an authorized query, the cloud server employs a search engine to search the encrypted document collection and get the related cipher texts to the query. Note that only the documents whose attributes match the data user are returned.
- Having received the encrypted documents and content keys, the data user first decrypts the content keys by her attribute-related secret key and then decrypts the documents based on the content keys. At last, the document retrieval process is completed.

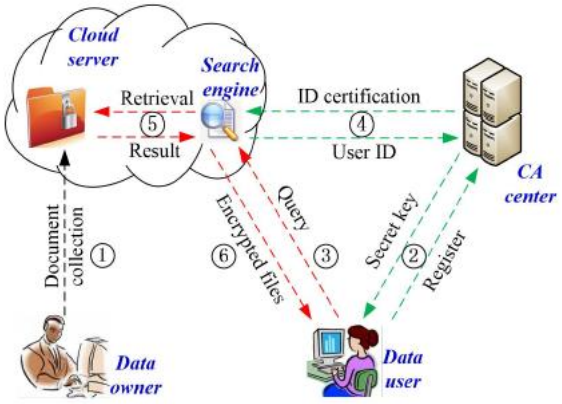

Fig 1: Workflow of the process

II RELATED WORK

ABE schemes have been broadly investigated in the writings. The fuzzy identity-based encryption (Fuzzy IBE) scheme proposed by Sahai and Waters is generally treated as the ABE origin. Sahai and Waters first utilize the term ABE in the field of data security. Motivated by Fuzzy IBE, numerous ABE schemes are planned including KP-ABE schemes and CP-ABE schemes. Goyal et al. has proposed the KP-ABE. Despite the fact that KP-ABE can give fine-grained admittance control, it confines its thoughtfulness regarding the droning access structure as it were. Further, they demonstrate the scheme's security based on decisional bilinear Diffie-Hellman supposition. Yang et al. propose a scheme which performs well as far as both access structure expressivity and security. CP-ABE schemes are more adaptable and appropriate for general applications and numerous assortments of CP-ABE schemes have been proposed in the writings. In CP-ABE schemes, the entrance structures are installed in the CT and every information client is doled out with a lot of attributes. An information client can decode a CT if and just if their attribute matches with the entrance structure.

CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

The commitment of this work center around the difficulty that emerge when the sensitive data is to be seen by the various clients of specific attributes like police records of the offender is to be seen by the FBI specialist. He sets the attribute that public official in San Francisco of the board chain can just view the document. In such cases, the issue emerges when the information is dispersed across various workers. This causes trouble in such expressive access control.

To address this issue, CP-ABHE is planned. In this the individual encoding their archive needs to indicate number of attributes and related structure and the client's private key will be related with these numbers. In this framework, the encoder should wisely conclude who should get to the encoded information. The principle highlight of this is to keep from agreement opposition for example two clients getting to a similar record simultaneously ought not have the option to share their attribute sets.

To finish up, this framework performs with the end goal that the client's private keys are indicated by attributes and the individual encoding the report needs to determine a policy identified with those attributes so as to get to information. The framework is poor regarding scalability and spotlights on arrangement obstruction. The computational overhead has proven to be normal.

FUZZY IDENTITY-BASED ENCRYPTION

The primary thought of this work is that the email address or other identity go about as a public key which diminishes the capacity of performing public key certification. Along these lines, this causes an issue that such identity doesn't exist for every individual.

The Fuzzy-IBE gives blunder resistance property so as to determine the above issue. In this framework the biometrics can be utilized as a security boundary alongside attributes to encode the report. A client with a secret key can unscramble the code text scrambled with the public key just inside a specific separation.

To close, this gives similar execution when contrasted with CP-ABE scheme and has high computational power. Moreover, this scheme ends up being effective and solid.

ATTRIBUTE-BASED ENCRYPTION FOR FINE-GRAINED ACCESS CONTROL OF ENCRYPTED DATA

The commitment of this work is to zero in on settling the difficult that emerge when the client stores his own subtleties like email address over the internet. The measure of data put away on such locales is defenseless against assaults and there is a cause for worry that the information can be undermined.

The key component of this framework is the KP-ABE scheme utilizes set of engaging attributes while scrambling the code text. The private key indicates an entrance structure that shows which sort of encoded information this key can decipher.

The efficiency of the scheme is considered regarding figure text size, private key size and time for calculation. The quantity of gathering components will be equivalent to the quantity of attributes in the code text. The encryption technique acts in the exponential structure.

PRIVACY-PRESERVING MULTI-KEYWORD RANKED SEARCH OVER ENCRYPTED CLOUD DATA

The commitment of this work to determine the problem that emerges when the client store the information in the cloud. The cloud has huge number of on-request information clients and colossal information is redistributed in the cloud. Subsequently, the trouble emerges so as to meet the necessities of execution and scalability while the reason for looking through information ought to stay simple.

The goals are:
To investigate the problem of multi-keyword positioned search over encoded information in cloud and keep up exacting protection necessities for security reason.
Two MRSE models are proposed based on likeness record.
Multi – keyword positioned search plans a looking through technique which permit multi-keyword inquiry and gives closeness positioning outcomes for information recovery Meets the protection necessities and forestall spilling of data the objective is to accomplish usefulness and protection with low computational overhead

To close, multi-keyword problem is settled. Two MRSE schemes are given to accomplish protection. After exhaustive examination and examinations, results exhibit that protection and efficiency is ensured and genuine informational indexes shows low calculation and communication overhead.

III PROPOSED WORK

A practical CP-ABHE archive collection Encryption scheme named CP-ABHE is proposed which performs well as far as computation and storage space efficiency. The scheme comprises of two modules including incorporated admittance tree development and tree encryption. Right off the bat, an algorithm to create the coordinated admittance trees for a report collection is proposed. At that point, the reports that share an access tree are encoded together. By practical, it implies that CP-ABHE is more effective in both computation and storage space without giving up information security.

Fig.1 describes the workflow of the process which mainly comprises four entities: the data owner, data user, certificate authority (CA) center and cloud server. The entire process of querying a set of interested documents for a data user includes 6 phases:

Data owner is responsible for collecting documents and assigning a proper attribute set to each document. The documents are encrypted in two phases. Each document is first encrypted by a symmetric encryption algorithm with a unique content key. Then, the content keys are encrypted by ABE-schemes. At last, both the encrypted documents and content keys are outsourced to the cloud server.

To search the interested documents in the cloud server, a data user first needs to register herself to the CA center.
Then, the CA center assigns an attribute set to the data user and sends an attribute-related secret key to the data user.
The authorized data user can send query requests to the cloud server. In this paper, we assume that the cloud server is trustable. Otherwise, we may need to further integrate the secure kNN algorithm into our scheme to encrypt the document vectors and query vectors [3], [8], [5].
Once a query request is received, the cloud server first communicates with the CA center to check the identity of the data user and an ID certification message is received if the data user is authorized.
For an authorized query, the cloud server employs a search engine to search the encrypted document collection and get the related ciphertexts to the query. Note that only the documents whose attributes match the data user are returned.
Having received the encrypted documents and content keys, the data user first decrypts the content keys by her attribute-related secret key and then decrypt the documents based on the content keys. At last, the document retrieval process is completed.

A. SYSTEM ARCHITECTURE

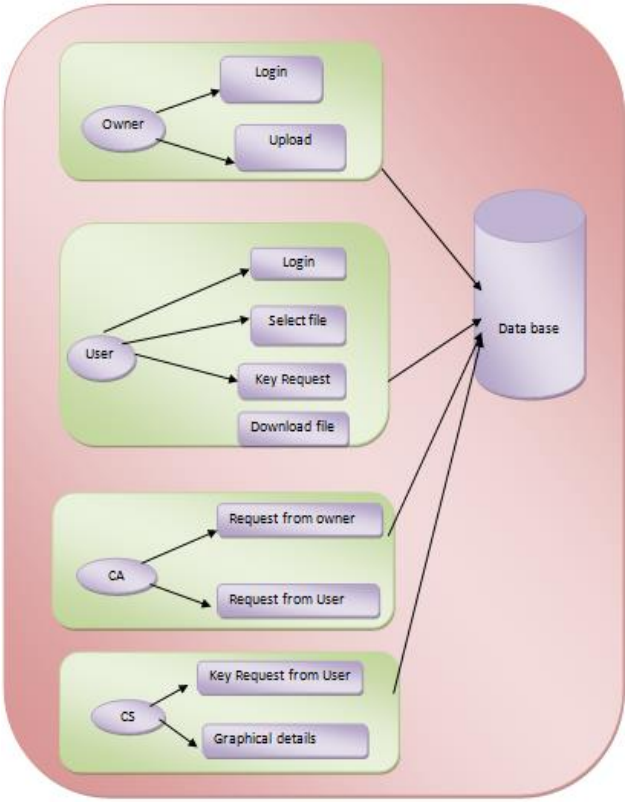

Fig 2: System Architecture

B. METHODOLOGY

A useful CP-ABHE archive assortment Encryption scheme named CP-ABHE is proposed.
The commitments of this paper are principally summarized as follows:

- A calculation to develop the coordinated admittance trees gradually for the record assortment is proposed & it can fundamentally diminish the quantity of the entrance trees.
- A record assortment hierarchical encryption scheme is proposed. All the archives that share a coordinated admittance tree are encoded together which can fundamentally improve the encryption/decoding productivity. Also, the mystery key growing issue is illuminated appropriately.
- The security of CP-ABHE is hypothetically demonstrated & the adequacy of the coordinated admittance tree development calculation is analyzed in detail. Also, an exhaustive correlation between CP-ABHE, KP-ABE & CP-ABE as far as encryption/unscrambling effectiveness & extra room is given. The modules are as follows:

1. Data Owner

This is the first module of this project. Data owner is responsible for collecting documents & assigning a proper attribute set to each document. The documents are encrypted in two phases. Each document is first encrypted by a symmetric encryption algorithm with a unique content key. Then, the content keys are encrypted by ABE-schemes. At last, both the encrypted documents & content keys are outsourced to the cloud server.

2. Data user

This is the second module of this project. In this module, when data user wants to search require data in cloud first user need to register. After login user put request to owner & CA for authentication. The authorized data user can send query requests to the cloud server. For authorized user will get secret key for decrypt the data.

3. Cloud server

This is the third module & has main responsibility. Cloud can login & able to get information about user & owner. The authorized data user can send query requests to the cloud server. For an authorized query, the cloud server employs a search engine to search the encrypted document collection & get the related cipher texts to the query.

4. Cloud Authenticator

To search the interested documents in the cloud server, a data user first needs to register to the CA center. Then, the CA center assigns an attribute set to the data user & sends an attribute-related secret key to the data user. Once

a query request is received, the cloud server first communicates with the CA center to check the identity of the data user & an ID certification message is received if the data user is authorized.

IV. RESULT

The aftereffects of the proposed framework show that the client can get to the encrypted reports if and just in the event that he can pass all the security components through the ace keys produced in his email address. Subsequently, this makes the proposed framework more made sure about when contrasted with the current schemes without influencing the storage space efficiency. The proposed framework is upgraded further regarding noteworthy component like hunt key symbolic which is created at the hour of client search menu where the client needs to enter the symbolic number so as to enter the ace key. Another upgraded highlight of this framework would be the chart yield which shows the tally of the record being gotten. To finish up, the outcomes portray that the encryption/decryption efficiency of the framework is expanded and the storage limit is diminished keeping the framework exceptionally made sure about.

Fig 3. user enters master key

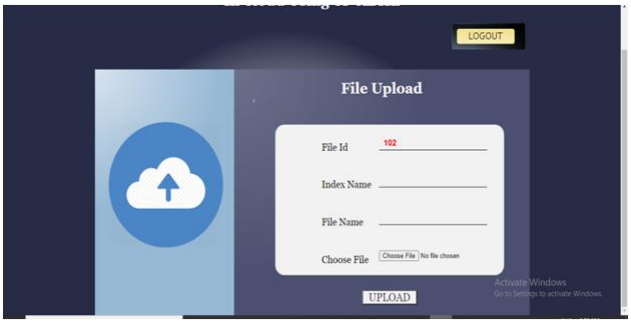

Fig 4. Data owner uploads file

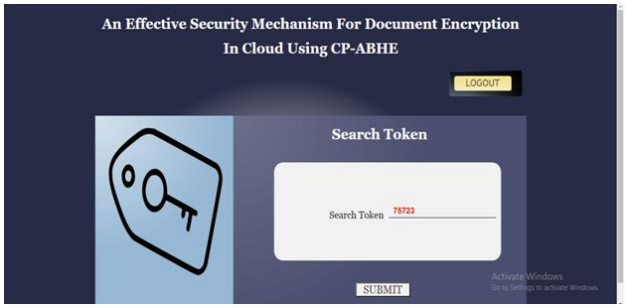

Fig 5. key request details at cloud authorization side

Fig 6. Search token is generated

Fig 7. Encrypted file format

Fig 8. downloaded file

V. CONCLUSION AND FUTURE SCOPE

A hierarchical document collection encryption scheme is designed. First an incremental algorithm to construct the integrated access trees of the documents and decrease the number of trees is designed. Then, each integrated access tree is encrypted together and the documents in a tree can be decrypted at a time. Different to existing schemes, the secret numbers for the nodes of the trees is

constructed in a bottom-up manner. In this way, the sizes of CT and secret keys significantly decrease. The proposed system is enhanced further in terms of significant feature like search key token which is produced at the time of user search menu where the user has to enter the token number in order to enter the master key. Another enhanced feature of this system would be the graph output which shows the count of the file being accessed At last, a thorough performance evaluation is provided including security analysis, efficiency analysis and simulation. Results show that the proposed scheme outperforms KP-ABE and CP-ABE schemes in terms of encryption/decryption efficiency and storage space.

This scheme can be additionally improved in a few angles: First, the entrance strategy expects that the access trees are made out of just "AND" gates. Broadening the flexibility and adaptability of the entrance strategy is one of the most significant examination headings. Second, the archives are scrambled before re-appropriating and a promising assignment is the manner by which to effectively look through the intrigued reports over the code messages. Finally, the attention is on the static record assortment and how to proficiently encode/unscramble a powerful archive assortment will be likewise explored later on.

REFERENCES

[1] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption, Security and Privacy," IEEE Symposium on. IEEE, 2007: 321-334.

[2] D. Boneh, B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. of TCC, 2007, pp. 535-554.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222-233, Jan. 2014.

[4] A. D. Caro, V. Iovino, "jPBC: Java pairing based cryptography," IEEE Symposium on Computers and Communications. IEEE Computer Society, 2011:850-855.

[5] C. Chen et al., "An efficient privacy-preserving ranked key-word search method," IEEE Trans. Parallel Distrib. Syst., vol. 27, no, 4, pp. 951-963, Apr. 2016.

[6] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS, 2006, pp. 79-88.

[7] H. Deng, Q. Wu, B. Qin, et al., "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," Information Sciences, 2014, 275(11):370-384.

[8] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546-2559, Sep. 2016.

[9] P. Golle, J. Staddon, B. Waters, "Secure conjunctive key-word search over encrypted data," in Proc. of ACNS, 2004, pp. 31-45.

[10] V. Goyal, A. Jain, O. Pandey, et al., "Bounded ciphertext policy attribute-based encryption," Automata, languages and programming, 2008: 579-591.

[11] V. Goyal, O. Pandey, A. Sahai, et al., "Attribute-based encryption for fine-grained access control of encrypted data," Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006: 89-98.

[12] J. Han, W. Susilo, Y. Mu, et al., "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," IEEE Transactions on Parallel & Distributed Systems, 2012, 23(11):2150-2162.

AUTHOR'S PROFILE

Ms. SYEDA AFIA HUSSAINI has completed her B.E (CSE) from Deccan College of Engineering and Technology, Osmania University Hyderabad. Presently, she is pursuing her Masters in Computer Science and Engineering from Shadan Women's College of Engineering and Technology, Hyderabad, TS, India.

Dr. K. SARAVANAN received the Ph.D. degree in Information and Communication Engineering from Anna University, Chennai. He has 13 years of teaching experience. His areas of interest include information security, wireless sensor networks, Data mining and Network security. At present he is working as a professor in Department of computer science and Engineering at Shadan Women's college of Engineering and Technology, Hyderabad. He has published 39 papers in International Journal, 30 papers in National and International Conferences. He is an active reviewer in Elsevier, Springer, Inderscience and many other journals.