Attribute Based and Hierarchical Encryption Scheme for Documents in Cloud

Mr. Bukkacharla Kishore Kumar [1], Ms. Shaik Sheema [2]
[1] Assistant Professor, [2] M.Tech Scholor
Department of Computer Science and Engineering,
QIS College of Engineering & Technology, Ongole, Andhra Pradesh

Abstract

Ciphertext-policy attribute-based encryption can give fine-grained access control and secure information sharing to the information clients in distributed computing. Nonetheless, the encryption/decoding proficiency of existing plans can be additionally improved while encoding an enormous report assortment. Right now, propose a down to earth Ciphertext-Policy Attribute-Based Hierarchical record assortment Encryption conspire named CP-ABHE. By reasonable, we imply that CP-ABHE is increasingly effective in both calculation and extra room without giving up information security. In CP-ABHE, we first build a lot of integrated access trees based on the reports' attribute sets. We utilize the ravenous system to fabricate the trees steadily and develop the trees by progressively joining the little ones. At that point all the archives on an integrated access tree are encoded together. Distinctive to existing plans, the leaves in various access trees with a similar attribute share an equivalent mystery number which is utilized to scramble the archives. This enormously improves the exhibition of CP-ABHE. The security of our plan is hypothetically demonstrated based on the Decisional Bilinear Diffie-Hellman supposition. Reenactment results show that CP-ABHE performs very well as far as security, effectiveness and the capacity size of the ciphertext.

Keywords: Cloud computing, attribute-based document collection encryption, encryption/decryption efficiency, data security.

Introduction

Distributed computing gathers and arranges a lot of data procedure assets to give secure, proficient, adaptable and on request benefits. Pulled in by these points of interest, increasingly more endeavor and individual client's pattern to outsource the neighborhood archives to the cloud. By and large, the records should be encoded before being outsourced to ensure them against spilling. On the off chance that the information proprietor needs to impart these archives to an approved information client, they can utilize any accessible encryption systems [2], [6], [9] or protection

saving multi-keyword record search plans [3], [8], [5] to accomplish this objective. Be that as it may, every one of these plans can't give fine-grained access control systems to the scrambled records.

ABE plans can give entangled frameworks to expand the information clients' access ways. In ABE plans, each report is encoded independently and an information client can decode a record if her attribute set matches the access structure of the archive. Existing ABE plans can be separated into Key-Policy ABE (KP-ABE) plans [11], [15], [12] and Ciphertext-Policy ABE (CP-ABE) plans [1], [10], [7]. Contrasted and KP-ABE plans, CP-ABE plans are progressively adaptable and reasonable for general applications. In the accompanying, we initially dissect the current ABE conspires in detail and further present the curiosity and advancement of the CP-ABHE plot proposed right now. For comfort, we pick the plans in [11] and [1] as average instances of KP-ABE plan and CP-ABE conspire, individually.

Both the KP-ABE and CP-ABE plans are unreasonable to encode a huge archive assortment as a result of the accompanying reasons. In the first place, the encryption procedure in both the two plans is executed N times, prompting high calculation multifaceted nature. Second, there is a tradeoff between the size of the substance keys' ciphertext and information clients' mystery keys. In KP-ABE, the quantity of mystery esteems in an information client's mystery key is very huge for a record assortment, forcing a substantial weight on the information client. In CP-ABE, the size of the ciphertext is very huge. Thus, CP-ABE conspire builds the information transmission sum between the cloud server and information clients, which is an immense test for the system. This is sensible thinking about that the access structure of each archive must be implanted into the ciphertext or the mystery keys. Third, decoding the ciphertext is likewise tedious thinking about that each record is scrambled exclusively.

As of late, Wang et.al endeavored to improve the encryption effectiveness and propose a record hierarchy attribute-based encryption conspire named FH-CP-ABE [33]. In any case, this plan concentrated distinctly on the best way to scramble a lot of reports that share an integrated access tree and henceforth it likewise can't be straightforwardly utilized to encode an archive assortment.

Related Work

Attribute-based encryption plans have been generally explored in the literatures. The fuzzy personality based encryption (Fuzzy IBE) plot proposed by Sahai and Waters is generally treated as the root of ABE. Sahai and Waters first utilize the term "ABE" in the field of data security. Propelled by Fuzzy IBE, numerous ABE plans are planned including KP-ABE plans and CP-ABE plans. Goyal et al. broaden the Fuzzy IBE plot and propose the KP-ABE in [11]. In spite of the fact that KP-ABE can give fine-grained access control, it confines its thoughtfulness regarding the monotone access structure as it were.

Ostrovsky et al. build a KP-ABE plot which permits a client's private key can be communicated as far as any access equation over attributes. Further, they demonstrate the plan's security based on decisional bilinear Diffie-Hellman assumption.

Yang et al. propose a plan which performs well as far as both access structure expressivity and security. CP-ABE plans are increasingly adaptable and reasonable for general applications and numerous assortments of CP-ABE plans have been proposed in the literatures [1], [10]. In CP-ABE plans, the access structures are inserted in the ciphertext and every datum client is doled out with a lot of attributes. An information client can decode a ciphertext if and just if their be coordinated with one another.

Pirretti et al. present a novel secure data the executives engineering based on ABE natives. A policy framework which addresses the issues of various information clients is planned and used to scramble dispersed record frameworks. The hierarchical ABE (HABE) conspire [32] is proposed by joining a hierarchical IBE plot and a CP-ABE conspire. HABE plan can help the venture clients to effectively share classified information in distributed computing by all the while accomplishing fine-grained access control, superior, practicability, and versatility. Zhu et al. [39] likewise propose a document sharing plan in distributed computing based on ABE and the security and productivity of the plan are assessed.

Li et al. furnish a CP-ABE plot with effective information client denial for distributed storage. KSF-OABE conspire incorporates the keyword search work into the ABE plot which can improve the pursuit proficiency of ciphertexts. Despite the fact that all the above proposed plans can be utilized in distributed computing, they are intended for encoding a solitary record. They can't be straightforwardly utilized to scramble an enormous report assortment, in light of the fact that the encryption/decoding productivity is low on the off chance that we encode each document separately.

Implementation Methodology

Right now, design an attribute-based archive hierarchical encryption plot named CP-ABHE which performs well regarding calculation and extra room productivity. The plan comprises of two modules including integrated access tree development and tree encryption. We initially propose a calculation to produce the integrated access trees for an archive assortment. The most significant design objective of the calculation is diminishing the quantity of integrated access trees which can extraordinarily improve the encryption/decoding productivity.

The commitments of this paper are basically condensed as follows:

A calculation to develop the integrated access trees steadily for the report assortment is proposed and it can fundamentally diminish the quantity of the access trees.

A record assortment hierarchical encryption plot is proposed. All the records that share an integrated access tree are encoded together which can fundamentally improve the encryption/decoding proficiency. In addition, the mystery key extending issue is illuminated appropriately.

The security of CP-ABHE is hypothetically demonstrated and the adequacy of the integrated access tree development calculation is broke down in detail. Also, an exhaustive examination between CP-ABHE, KP-ABE, and CP-ABE as far as encyption/decoding productivity and extra room is given.

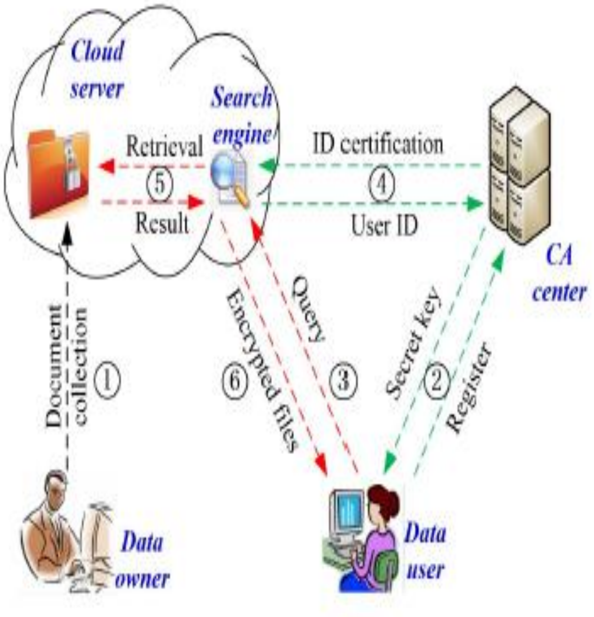

Fig1: The architecture of document outsourcing and sharing

System Design

Data Owner:

Right now, the information proprietor needs to enlist to the cloud server and get approved. After the approval from cloud information proprietor will scramble and add document to the cloud server where in after the option of record information proprietor View All Uploaded Files, View All Transactions.

Cloud Server

The cloud server deals with a cloud to give information stockpiling administration. Information proprietors scramble their information documents and store them in the cloud for offering to cloud End users and play out the accompanying activities, for example, View All Owners and Authorize ,View All Users and Authorize ,View All Cloud Files ,View All Transactions, View All Attackers ,View File Score Results ,View Time Delay Results ,View Throughput Results

CA

CA produces the substance key and the mystery key mentioned by the end user and furthermore View All Attackers.

End User

User needs to enroll and login for accessing the records in the cloud. User is approved by the cloud to check the enrollment. User needs to View All Files, Download.

Implementation Procedure

Here portrays the archive re-appropriating and sharing framework which predominantly contains four elements: the data owner, data user, certificate authority (CA) center and cloud server. The whole procedure of questioning a lot of intrigued archives for a data user incorporates 6 stages:

Data owner is answerable for gathering reports and doling out an appropriate attribute set to each archive. The archives are scrambled in two stages. Each record is first encoded by a symmetric encryption algorithm with a remarkable content key. At that point, the content keys are scrambled by ABE-plans. Finally, both the scrambled reports and content keys are outsourced to the cloud server.

To look through the intrigued records with regards to the cloud server, a data user first needs to enroll herself to the CA center Then, the CA center allocates an attribute set to the data user and sends an attribute-related secret key to the data user.

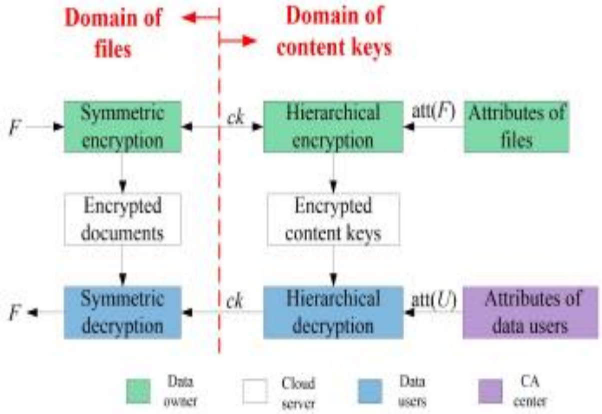

Fig2: The flow chart of document encryption and decryption

The approved data user can send question solicitations to the cloud server. Right now, accept that the cloud server is trustable. Else, we may need to additionally incorporate the secure kNN algorithm [35] into our plan to encode the record vectors and question vectors [3], [8], [5].

When an inquiry demand is gotten, the cloud server initially communicates with the CA center to check the character of the data user and an ID certification message is gotten if the data user is approved.

For an approved inquiry, the cloud server utilizes a web index to look through the scrambled report assortment and get the related ciphertexts to the question. Note that solitary the archives whose attributes coordinate the data user are returned.

Having gotten the encoded records and content keys, the data user initially decodes the content keys by her attribute-related secret key and then unscrambles the reports based on the content keys. Finally, the archive recovery process is finished.

Access Policy of Documents and Access Trees

Right now, expect that each record Fi is of a few attributes in att(Fi) and Fi can be accessed uniquely by the data users who have all the attributes in att(Fi). As appeared in howl figure 2 (a), we accept that the attribute word reference of a report assortment incorporates three fundamental attributes including "communication", "PC" and "system". Each report has at any rate one attribute and a few archives may have a few attributes, for example, the records in locale A, B, C and D. Right now, records in locale A can be accessed by the data users who possess all the three jobs of communication analyst, PC specialist, and system scientist. Obviously, the access structure of a report is monotone.

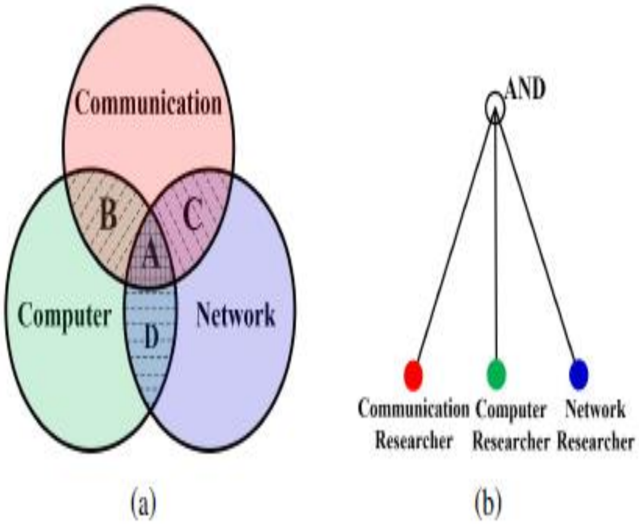

Fig3: (a) Assumption of access control strategy
(b) The access tree of the documents in region A

For instance, a data user who possesses the attributes of communication and PC specialist can access the reports in area B. Then, some other data users who have in any event these two attributes can likewise access the archives in district B. Contrasted and the limit based access policy proposed in [11], [1], [33], our access policy is stricter and increasingly reasonable for the archives with high security prerequisites, for example, individual wellbeing records.

We can speak to the access structure of a record by an access tree T. Under our access policy, the leaf hubs in the tree speak to the attributes identified with the archive and the root hub speaks to an "AND" entryway. The access tree of an archive in district An is appeared in Figure 2 (b) and the tree contains three leaf hubs speaking to three attributes. The root hub speaks to an "AND" door. Right now, the leaf hub set of an access tree is a subset of another access tree's leaf hub set, we can consolidate these two trees to another tree which is called an integrated access tree. Obviously, each non-leaf hub in the integrated access tree likewise speaks to an "AND" entryway.

Algorithm: Building Access Structure

Input: Document collection F = F1, F2, …. FN with attribute sets fatt(F1), att(F2), _ _ _ , att(FN)g
Output: A set of integrated access trees ST

```
Sort the files in F in ascending order based on the number of their attributes and obtain $F0 = \{F1, F2, \_\ \_\ \_ ; FN\}$ with identifiers $\{f1, f2, \_\ \_\ \_\ fN\}$
$ST = fg$, $C = fg$;
for $i = 1 : N$ do
    $S = att(Fi)$;
    Scan the access trees in ST in order;
    if S matches an scanned access tree X, i.e., $S(X) = 0$ then
        Insert the identifier of Fi into the root node of X;
        break;
    end if
    Rescan the access trees in ST in order;
    for a scanned access tree Y in ST do
        if S covers Y , i.e., $S(Y) = 1$ then
            $C = C \cup Y$, $S = S\ n\ att(Y)$;
        end if
    end for
    if S is empty then
        Build a larger access tree LT with root node r and all the access trees in C are the child nodes of r;
        Insert fi to r;
        Insert LT to ST and delete all the trees in C from ST ;
    else
        Build a larger access tree LT with root node r and all the access trees in C are the child nodes of r; In addition, all the left attributes in S are also inserted to the root node r as leaves;
        Insert fi to r;
        Insert LT to ST and delete all the trees in C from ST ;
    end if
end for
```

Execution Analysis

We theoretically contrast the proposed plan and KP-ABE and CP-ABE plots regarding encryption/unscrambling efficiency and extra room. For accommodation, some essential definitions are introduced first. We expect that $Gi(i = 0; 1)$ is a gathering or the time cost of a fundamental procedure on the gathering, for example, exponentiation or multiplication. Let Zp be the gathering f{0, 1, … p-1} and Ce be the time cost of a bilinear guide activity e. What's more, we define | * | as the quantity of components in *, L* as the length of a component in *.

It very well may be seen that the CP-ABHE plays out the best as far as all the estimations. The KP-ABE plot performs better than CP-ABE as far as encryption/unscrambling efficiency and the size of CT. Be that as it may, a colossal drawback of the KPABE plot is the secret key expanding problem. The CP-ABE plot performs better than KP-ABE as far as the size of PK, MSK, and SK. In any case, the size of the ciphertext is a lot bigger than that of KP-ABE conspire. When sending the ciphertext to the data users, the data transmission sum in CP-ABE is a lot bigger and it is a test for the systems. Furthermore, CP-ABE plan and CP-ABHE conspire are more adaptable than the KP-ABE plot, all things considered. All in all, theoretical examination shows that both KPABE and CP-ABE have their impediments and CP-ABHE consistently plays out the best.

Conclusion

Right now, design a hierarchical record assortment encryption plot. We first design a steady algorithm to develop the integrated access trees of the records and abatement the quantity of trees. At that point, each integrated access tree is encoded together and the archives in a tree can be decoded at once. Diverse to existing plans, we build the secret numbers for the hubs of the trees in a base up way. Right now, sizes of ciphertext and secret keys significantly decline. Finally, an exhaustive exhibition assessment is given including security examination, efficiency investigation, and recreation. Results show that the proposed conspire beats KP-ABE and CP-ABE plots as far as encryption/unscrambling efficiency and storage space.

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 multikeyword 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 attributebased 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 finegrained 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.

[13] J. Lai, R. H. Deng, C. Guan, et al., “Attribute-Based Encryption With Verifiable Outsourced Decryption,” IEEE Transactions on Information Forensics & Security, 2013, 8(8):1343-1354.

[14] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, “Fully secure functional encryption: Attribute-based encryp-tion and (hierarchical) inner product encryption,” in Proc. EUROCRYPT, 2010, pp. 62-91.

[15] A. Lewko, T. Okamoto, A. Sahai, et al., “Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,” International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2010:62-91.

Authors Profile

Mr. BUKKACHARLA KISHORE KUMAR has Received B.Tech from Jawaharlal Nehru Technological University (JNTU Anantapur) and M.Tech from JNTU(Anantapur). He is working as an Assistant Professor in the department of Computer Science and Engineering in QIS college of Engineering and Technology (Autonomous), Ongole.

Ms. SHAIK SHEEMA, M.tech scholar in Computer science and Engineering, QIS college of Engineering and Technology (Autonomous), Ongole. She has completed B.tech in Computer science and Engineering from RISE Gandhi Group of Institutions, Ongole.

.