International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 613 – 618

Proof Verification and Attribute Based Re-Encryption of Shared Data over Public Cloud

Mr. Swapnil R. Patil
Department of Computer Engineering
PVPIT PUNE
swapnil5400@gmail.com

Prof. N. D. Kale
Department of Computer Engineering
PVPIT PUNE
navnath1577@yahoo.co.in

Abstract— Cloud storage is the best and proficient approach to handle our information remotely. In any case, since information proprietors and clients are more often than not outside the trusted area of cloud specialist co-ops the information security and get to control is the critical component at the season of delicate information put away in the cloud. Additionally, now days there are distinctive systems are accessible for information sharing and saving security of information proprietor and client. Key Escrow is the one of the significant issue now a day. We can't keep full trust over the key power focus since they might be abuse their benefits. This is unsatisfactory for data sharing circumstances. In this paper we concentrated the current procedure for sharing the information from information proprietor to information client. The methodology propose an enhanced two-party key issuing convention that can ensure that neither key power nor cloud specialist co-op can bargain the entire mystery key of a client exclusively. The method also present the idea of quality with weight, being given to upgrade the statement of characteristic, which cannot just extend the expression from paired to discretionary state, additionally help the intricacy of get to approach. In this manner, both capacity cost and encryption many-sided quality for a cipher text are eased. Attribute based encryption is an open key based encryption that empowers get to control over encoded information utilizing access strategies and credited qualities. In this paper we propose proof verification module which verify proof of shared file and is received by data consumer when file shared by data owner and also a method which applies re-encryption (ABE) of a shared file here the attributes of data consumers are used to generate key.

Keywords-*Data Confidentiality, Key Authority, Access Control policy, Data Sharing, Attribute-based encryption, Removing escrow, weighted attribute, Cloud computing.*

*****

I. INTRODUCTION

In current era there are bunches of quickly developing patterns and cloud registering is one of them. Cloud gives simple, proficient stage to store information, secure information, and get to information at any area with the assistance of web. Additionally it gives client adaptable foundations, storage room and execution. Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the scenario of cloud computing [1], [10]. In a CP-ABE, client's mystery key is portrayed by a trait set, and ciphertext is connected with a get to structure. DO is permitted to characterize get to structure over the universe of traits. A client can unscramble a given ciphertext just if his/her trait set matches the get to structure over the ciphertext. In a CP-ABE, users secret key is described by an attribute set, and ciphertext is associated with an access structure[1]. DO is allowed to define access structure over the universe of attributes[1]. A user can decrypt a given ciphertext only if his/her attribute set matches the access structure over the ciphertext. Utilizing a CP-ABE framework specifically into a cloud application that may yield some open issues Firstly, all clients' mystery keys should be issued by a completely trusted key power (KA). This brings a security hazard that is known as key escrow issue. By knowing the mystery key of a framework client, the KA can unscramble the entire client's ciphertext, which remains altogether against to the will of the client. The weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but also to simplify access policy. Thus, the storage cost and encryption cost for a ciphertext can be relieved. Assume there is a formal structure in college, in which instructors are characterized into showing partner, speaker, related teacher and full educator [1]. We circulate the heaviness of the characteristic for every kind of the instructors as 1, 2, 3, and 4. In this way, these qualities can be indicated as "Educator: 1", "Educator: 2", "Instructor: 3" and "Instructor: 4", individually. For this situation, they can be signified by one trait which has quite recently extraordinary weights. Specifically, it can be arbitrary state properties, for example, "Instructor: showing associate, teacher, relate educator, full teacher". We here accept that an get to arrangement is spoken to as: T ("Lecturer" OR "Partner Teacher" OR "Full Professor") AND "Male", and the current CP-ABE plans are executed on the type of get to strategy T. On the off chance that our proposed plan is sent, the T can be rearranged as T' "Teacher: 2" AND "Male", since the characteristic "Instructor: 2" indicates the base level in the get to approach and incorporates "Teacher: 2", "Instructor: 3" "Instructor: 4" as a matter of course. In this manner, the capacity overhead of the comparing ciphertext and the

computational cost utilized as a part of encryption can be lessened.

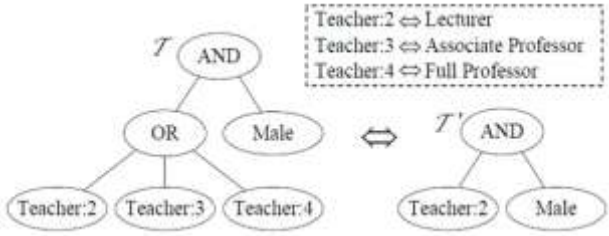

Fig. 1. Two equivalent access structures of a ciphertext. T represents a general access policy in the existing CP-ABE schemes. T' denotes an improved access policy in the proposed scheme [1]

These two structures are appeared in Fig.1. Likewise, our technique can be utilized to express bigger quality space than any time in recent memory under a similar number of qualities. For instance, if both the property space and weighted set incorporate n components, the proposed plan can portray n2 distinctive potential outcomes. Interestingly, the current CPABE plots just show 2n conceivable outcomes.

II. REVIEW OF LITERATURE

The literature survey that containing study of different schemes available in Attribute Based encryption(ABE).That are KP-ABE,CP-ABE, Attribute-based Encryption Scheme with Non-Monotonic Access Structures, ABE and MABE. Also include advantage, disadvantage and a comparison table of each scheme based on fine grained access control, efficiency, and computational overhead and collusion resistant. Shulan Wang, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, WeixinXie [1] revisit attribute-based data sharing scheme in order to solve the key escrow issue but also improve the expressiveness of attribute, so that the resulting scheme is friendlier to cloud computing applications. They proposed an improved two-party key issuing protocol that can guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. Moreover, they introduce the concept of attribute with weight, being provided to enhance the expression of attribute, which can not only extend the expression from binary to arbitrary state, but also lighten the complexity of access policy. Therefore, both storage cost and encryption complexity for a cipher text are relieved. An efficient file hierarchy attribute-based encryption scheme (FH-CP-ABE) is proposed by Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen and WeixinXie [2]. The layered access structures are integrated into a single access structure, and then the hierarchical files are encrypted with the integrated access structure. The cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time costs of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CPABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control. Kaitai Liang and Willy Susilo proposed [3] a searchable attribute-based proxy re-encryption system. When compared to existing systems only supporting either searchable attribute based functionality or attributebased proxy re-encryption, this new primitive supports both abilities and provides flexible keyword update service. Specifically, the system enables a data owner to efficiently share his data to a specified group of users matching a sharing policy and meanwhile, the data will maintain its searchable property but also the corresponding search keyword(s) can be updated after the data sharing. The server however knows nothing about the keyword(s) and the data. The new mechanism is applicable to many real-world applications, such as electronic health record systems. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in this work [4]. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the same time. Besides, this scheme achieves security against chosen plaintext attacks under the k-multi linear Decisional Diffie-Hellman assumption. The extended CP-ABE mechanism with multi-authorities (MA-ABE) is designed [5] for the practical application. In this paper, authors proposed an efficient and secure multi authority access control scheme transfer the computing to the cloud server. This scheme implements partial decryption operation in cloud server and improves the user's decryption efficiency, which can be applied to the scenario of access to the Internet using mobile devices. An attribute based encryption scheme introduced by Sahai and Waters in [6] and the goal is to provide security and access control shows that how to reduce a communication overhead between cloud server and data owner using public key compression technique for fully homomorphic encryption scheme over the integers. Whenever we use the cloud, user expects Data privacy, search accuracy and less communication overhead from the cloud service providers. In order tackle this TRSE (Two Round Searchable Encryption) scheme has been proposed which achieved high data privacy through homomorphic encryption and search accuracy through vector space model. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it use the access of monotonic attributes to control user's access in the system.

 ISSN: 2321-8169
613 – 618

III. EXISTING SYSTEM

A data owner (DO) is usually willing to store large amounts of data in cloud for saving the cost on local data management. Without any data protection mechanism, cloud service provider (CSP), however, can fully gain access to all data of the user. This brings a potential security risk to the user, since CSP may compromise the data for commercial benefits. Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the scenario of cloud computing. Firstly, all users secret keys need to be issued by a fully trusted key authority (KA). This brings a security risk that is known as key escrow problem. By knowing the secret key of a system user, the KA can decrypt all the users cipher texts, which stands in total against to the will of the user. Secondly, the expressiveness of attribute set is another concern. As far as we know, most of the existing CP-ABE schemes can only describe binary state over attributes, for example, 1 - satisfying and 0 - not-satisfying, but not dealing with arbitrary-state attribute.

Disadvantages:

1. User's secret keys need to be issued by a fully trusted key authority (KA). This brings a security risk that is known as key escrow problem.
2. The secret key of a system user, the KA can decrypt all the users cipher texts, which stands in total against to the will of the user.

.

IV. PROBLEM STATEMENT

Employing an ABE system directly into a cloud application that may produce some open problems; firstly, all users secret keys require to be issued by a fully trusted key authority (KA). This brings a security risk that is known as key escrow problem. By knowing the secret key of a system user, the KA can decrypt the entire usersciphertext, which stands in total against to the will of the user. Secondly, the expressiveness of attribute set is another concern. As far as we know, most of the existing an ABE schemes can only describe binary state over attribute, for example, 1 - satisfying and 0 - not-satisfying, but not dealing with arbitrary-state attribute.

V. PROPOSED SYSTEM

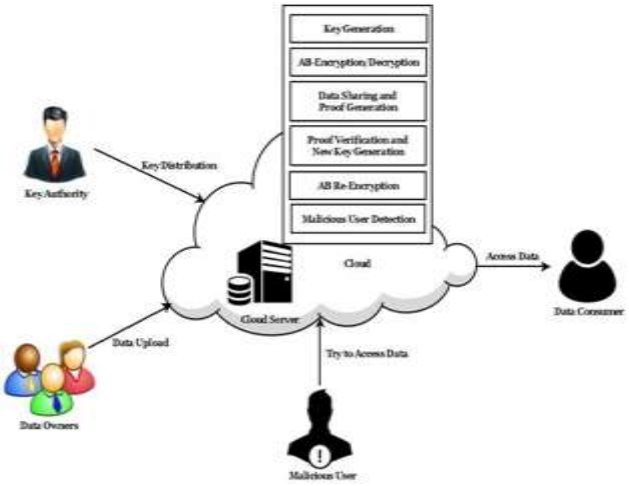

Fig. 2. Proposed System Architecture

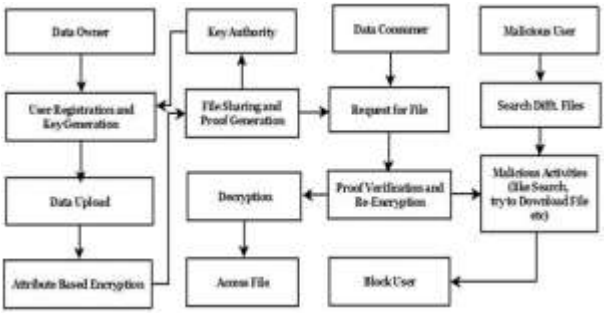

Fig. 3. Block Diagram

Above Fig. 2 shows architecture of proposed system and Fig. 3 shows block diagram of proposed system. It include following models:

- Key generation
- AB encryption
- Data sharing and proof generation
- AB-Re-encryption
- Proof verification and decryption
- Malicious user detection

The key generation module create unique key for each user based on different attribute of user which are received during registration phase. This key is used in encryption methodology which is AES (128-bit) so it called as attribute based (AB) advanced encryption standard i.e. AB-AES.

Cloud user knows as data owner upload data (file) over cloud and share it access other but with security as it only allow to access higher data to a particular user ; when user(data owner) share file over cloud then proof of shared file is generated and send it to the shared user which known as data consumer via mail. After sharing a particular file; this file reencryption using the new key based on shared user attribute and which is used only to access such shared file.

The proof verification and decryption module allows to access shared file before file is downloaded the shared proof is verified by system and then it decrypted by using new key which is generated at time of proof generation.

Module malicious user detection finds out or catch the userid which behavior abnormally or does malicious activities like search non-accessible file by to download or access file which does not have right. Then it blocked by system and listed under malicious user list.

VI. ALGORITHMS

A. Key generation:

1) Set of attribute UAtt(a1, a2,….an};
2) Get random number rn = random[26];
3) for(inti = 0; i<UAtt.length; i + +)
4) {
5) if (rn == (int)utt[i])
6) {
7) Key = utt[i];
8) }
9) }
10) ConvertToBaseString(key)

B. Proof generation:

1) Select shared user Sur;
2) Find attribute of Sur as UAtt[a1, a2,…….an];
3) Rn = random[26];
4) for(inti = 0; i<UAtt.length; i + +)
5) {
6) if (rn == (int)UAtt[i])
7) {
8) String ts[ ];
9) String bi = Random(9999).T oString();
10) for(int j = 0; j <bi.length; j + +)
11) {
12) ts[j] = UAtt[i] + bi.charAtt(j);
13) }
14) Key = key + ts;
15) }
16) }
17) Find proof = key.ConvertToBaseString();

C. Proof verification:

1) Take user input as proof or token Utoken.
2) R = Utoken = proof[algorithmB];
3) if (R == 0)
4) {
5) Access granted(sh_file);
6) }
7) Keygen(sh_user);
8) Encrpt(nkey, sh_file);

D. Malicious User Detection:

1) Record log for every activity Rlog[ ].
2) User search unshared or file which do not have right toaccess as Mlog[ ].
3) If Rlog[ ] <= Mlog[ ].
4) Add user in to Blku[ ] (Block user list).
5) Display block user list.

VII. MATHEMATICAL MODEL

Mathematical Model using Set Theory

1) Set Sfg as a proposed system.
2) Ukey is a key generated by key authority at a time ofuser registration:Ukey =∑Rnd(26) + UAtt
Where UAtt set of user Attribute,
S = {Ukey}
3) UF{f1, f2,……..f3} set of files uploaded by user:
S = {Ukey, UF}
4) Shpf{Shpf1, Shpf2,…..Shpfn} file shared proof generatedwhen data owner share file:
S = {Ukey.UF,Shpf}
5) Set of cipher file:
CphF{CphF1,CphF2,……CphFn}
CphF = AB-AES(Ukey.UF);
S = {Ukey,UF, Shpf,CphF}
6) Mur is a set of malicious users or blocked users:
if (Rlog[i] = MAct[i])
Mur[i] = Active user;
S = {Ukey,UF, Shpf,CphF,Mur}
7) MAct is a set of malicious activity:
S = {Ukey,UF, Shpf, SphF,Mur,MAct}
8) Find Set:
S = {Ukey,UF, Shpf,CphF,Mur,MAct}

VIII. DATASET USED

- Proposed system is used to share user data securely over public cloud, so the set of user files having different format like .doc, .pdf, .jpg, etc are considered as data set used in proposed system. They input file converted into the byte array and loaded (stored) in data base as binary data (sql database data type).
- A set of user with the attribute which are used in key generation and proof generation i.e key generation and proof generation algorithms (methods) are take i/p as users attribute of a Dataset to generate key proof respectively.

 ISSN: 2321-8169
613 – 618

- Set of encryption file and proof respectively generated by AB-AES encryption method which is sorted in the form of binary data.
- Every activity of each user is recorded by log and which is verified by malicious user detection module, so the log is a data set used to block user which behavior abnormally.

IX. RESULT ANALYSIS

A. *Data Transaction and Malicious User Detection:*

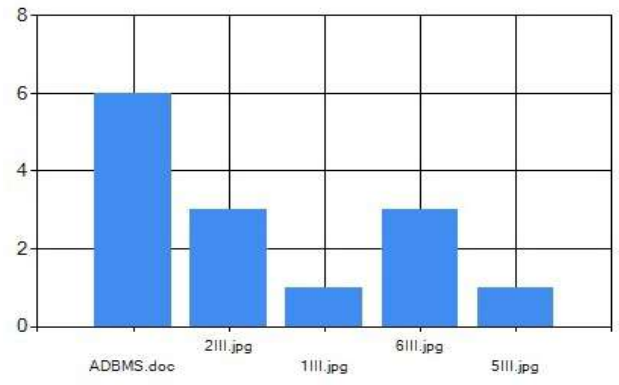

Fig. 4. Data transaction graph

Fig. 5. User Activities recorded by Malicious User Detection Module (Malicious User = Mlog<Nlog)

Fig. 6. User Activities recorded by Malicious User Detection Module (Malicious User = Mlog>Nlog)

Proposed System provide security for shared data over public cloud; Fig. 4 shows the data transaction graph for the files shared by a data owner and it accessed by different data consumer; Fig. 5 and Fig. 6 shows the activities of user to define where it is a malicious user or not.

B.Proof Verification and User Blocking:

Table 1 shows activities recorded when user requested for specific resource with proof which is must validate by system to grant access to requested user.

User ID	Valid Proof	Invalid Proof	Total Data Transaction	% Invalid Transaction	% Valid Transaction
1	17	25	42	59.52	40.48
2	31	75	106	70.75	29.25
3	84	22	106	20.75	79.25
4	74	12	86	13.95	86.05
5	29	49	78	62.82	37.18

Table 1: Proof Verification and User Blocking.

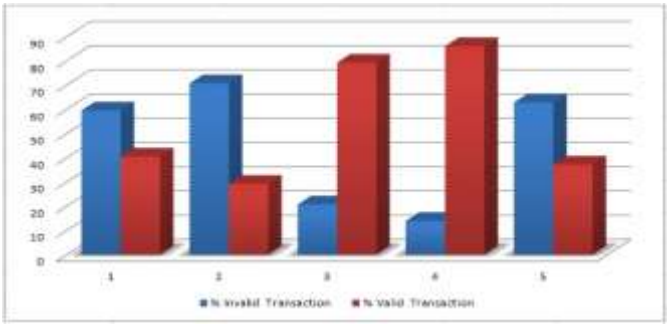

Fig. 7. Graph representation of Proof Verification and User Blocking.

C. *Comparison of ElGamalHomomorphic Cryptosystem and ABE Scheme:*

Tables 2 and Table 3 shows the comparison between two cryptographic methods from which Attributed based encryption method used for proposed system the attribute selection method based on random number selection with attribute number of resisted user.

Key Size	File Size	Key Generation Time (ms)	Encryption Time (ms)	Decryption Time (ms)
128	12K	0.2509	3.8202	2.3178
256		0.2537	3.9071	2.6024
512		0.2666	3.9914	2.9541
1024		0.2851	4.2651	3.1183
128	80k	0.2509	4.9425	3.2747
256		0.2537	5.0145	3.9902
512		0.2666	5.6291	4.1580
1024		0.2851	5.8947	4.4457

Table 2: Attributed based Encryption Scheme.

Key Size	File Size	Key Generation Time (ms)	Encryption Time (ms)	Decryption Time (ms)
128	12K	313	672	469
256		750	1479	875
512		1250	3328	1953
1024		40656	8754	5604
128	80k	234	3500	2437
256		297	7907	4203
512		1031	22616	11323
1024		15828	72041	36933

Table 3: ElGamalHomomorphic Cryptosystem.

X. CONCLUSION

In this paper, we designed an attribute based data sharing scheme in cloud computing. The improved key issuing protocol was presented to resolve the key escrow problem. It enhances data privacy and confidentiality in cloud system against the managers of KA and CSP as well as malicious system outsiders we created new key for shered file and reencrypt it, where KA and CSP are semi trusted. In addition, the weighted attribute was proposed to improve the appearance of attribute, which cant only describe arbitrary state attributes, but also reduce the complexity of access policy, so that the storage cost of ciphertext and time cost in encryption can be saved. Finally, we are presented the security analyses and performance for the proposed scheme, in which the results display high security and efficiency of our system. In this system, We record log and an analyzed it to determine user is malicious or not. If user behave abnormally like search non granted file or tried to download it.

ACKNOWLEDGMENT

It gives me pleasure and immense satisfaction to present this paper of topic Proof Verification and Attribute Based Re-Encryption of Shared Data over Public Cloud which is the result of solid support, expert direction and absorbed direction of my guide Prof. N. D. Kale to whom I direct my deep sense of gratefulness and humble thanks, for his treasured guidance.

REFERENCES

[1] Shulan Wang, Kaitai Liang, Joseph K. Liu, JianyongChen, Jianping Yu, WeixinXie ,"Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEETransactions on Information Forensics and Security, 2016.

[2] Shulan Wang, Junwei Zhou, Joseph K. Liu, JianpingYu,Jianyong Chen, WeixinXie ,"An Efficient File HierarchyAttribute-Based Encryption Scheme in CloudComputing", IEEE Transactions on Information Forensicsand Security, 2016.

[3] Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage", IEEE Transactions on InformationForensics and Security, 2015.

[4] JieXu, Qiaoyan Wen, Wenmin Li and ZhengpingJin,"Circuit Ciphertextpolicy Attribute-based HybridEncryption with Verifiable Delegation in CloudComputing", IEEE TRANSACTIONS ON PARALLELAND DISTRIBUTED SYSTEMS ,2015.

[5] Danwei Chen, Liangqing Wan, Chen Wang, Su Pan,YutingJi, "A Multi-authority Attribute-based EncryptionScheme with Pre-decryption", 2015 IEEE SeventhInternational Symposium on Parallel Architectures, Algorithms and Programming.

[6] J. Bettencourt, A. Sahai, and B.WatersCiphertext-policy attributebased encryption in Proceedings of IEEE Symposium on Security andPrivacy, pp. 321V334, 2007.

[7] V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, Multiauthorityattribute-based encryption with honest-but-curious centralauthority" International Journal of Computer Mathematics, vol. 89,pp. 3,2012.

[8] V. Goyal, O. Pandey, A. Sahai, and B.WatersAttribute-basedencryption for fine-grained access control of encrypted data," inProceedings of the 13th ACM conference on Computer andcommunications security, pp. 8998, 2006.

[9] Q. Liu, G. Wang, and J. Wu, Time based proxy re-encryptionscheme for secure data sharing in a cloud environment," InformationSciences .In Press, 2012.

[10] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secureattributebased systems. In Proceedings of the 13th ACM conference onComputer and communications security, pages 99 112. ACM Press NewYork, NY, USA, 2006.