International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 4, Issue 1 (July 2014) PP: 06-10

CP-ABE Scheme with extended reliability factor and load balancing in distributed n/w

Miss. Snehlata V. Gadge[1], Dr. S. T. Singh[2]
[1]*Research Scholar, Department of Computer Science, Pune, India*
[2] *Professors, Department of Computer Science, Pune, India*

Abstract: *Several Data Security Methodology has been noticed, with recent adoption and spreading of data sharing. One of the most interesting and definitive approach is Cipher text-Policy Attribute-Based Encryption (CP-ABE).CP-ABE provides us with the indulgement of the access policies and its updates. It is used to set or control outsourcing of data sharing; it deals with the issues in CP-ABE. This solution allows encryptor to deals with the access control with respect to the access formula. The lacking of reliability factor lead to weaken the system, therefore we will amplify CB-ABE by introducing some factor. Key Generation center (KGC) and data storing center are the highlighted factors. KGC deals with the drawback of Key escrow problem. As KGC can decrypt the users data as per KGC`s concerns, causing threat to the data sharing Systems. This is not favorable for the distributed scheme where KGC is not trustworthy. Along with the key escrow problem, we will be concerning with the problem of key-revocation that is degradation because of windows of vulnerability. These issues are solved by exploiting the features characteristics of Architecture. The problem of key-escrow is resolved using 2-pc protocol. And Key-revocation is proceeding by using proxy encryption.*

Keyword: *Distributed System, fair scheduling, Attribute, 2 pc, Access structure*

I. Introduction

In the recent days the networking and computing environments need safe and flexible pace to cope with the data sharing services in order to utilize time along the resources. Concerning to the matter of technology .People now days can smoothly share their data, exchange their talks online. People can easily contribute their happiness and express feelings towards each other by uploading their personal belonging like private data, chats or snaps by uploading onto the social networking site such as face book or LinkedIn. Apart from that they can upload their sensitive health records into data servers like Google Health or other private servers for cost saving. Along with the bashing effects of the internet, the need of high security also arises with proper setup and access controlling functionality. Incorrect use of the personal data by any storage server or unauthorized access by outsider can be threat to security model making misuse of data in a wrong way.

Attribute based encryption technique determines decryption`s capability on bases of uses attributes. This introduce us with the new public key primitive knows as Attribute based Encryption.ABE gives authority to user in such a way that encryptor to define set of attribute over a whole place of attribute that a decryptor should possess in order to decrypt the cipher text. User`s secret key is based on a set user`s credentials, and cipher is generated based on the policy generated. Forward approach in which data sharing should be stored, encrypted data before uploading to protect privacy were introduced in traditional public key infrastructure, data encryption process can be adopted, and the owner of data prior to uploading the data to encrypt data uses the public key users; If a user sends through the access request to the sharing, the sharing will return to the same cipher text data user a user to decrypt the data using private key. But this matter would lead to some problems: (1) to be able to encrypt data, the data owner needs to obtain the data user's public key to complete this; (2) a lot of storage overhead would spend because of the same plaintext with different public keys.

In order to overcome these limitations Attribute based encryption came into existence.ABE first identify user`s properties. ABE has advantage over traditional PKC ,as it favors' with one too many encryption instead of one to one.ABE as a set of attribute, is used to encryption and decryption of data.ABE comes in two flavors, 1) Cipher text-policy ABE 2) Key-policy ABE. In cipher text, attribute are mentioned to describe user`s credentials, encryptor determines policy whether who can decrypt data.CPABE is more promising concept for data sharing System as it allows to set access policy decisions in the data owner`s hand means secret key is associated with a set of attributes, while in key-policy, reverse is the process, attributes are used to notify encrypted data, and policy are built in user`s key. Sometimes it is not suitable in certain applications, as the owner of data has to trust the key issue; apart access structure is KP-ABE is a monotonic access structure. Negative attribute can`t be expressed, for excluding the entity with whom owner don`t want to share data. CP-ABE plans to address problem of KP-ABE that trust only key-issuer data.

Recently with new, safe, and effective methods that features-based method of data sharing System by exploiting a fine-grained data access control to implement sharing or distribution of data. Practically the better efficiency ,scalability and security ,overcoming the limitations of exiting methods shows the methods of its

credibility as it handles many requests to single user key generator system. Thus to achieve reliability, aiming to improve security, load balancing with increasing efficiency. In the further section II, we will be connecting with literature survey over various methods in data distributed system. In section III the proposed approach with its block diagram is depicted. In IV we will be dealing with the current state along with experimental setup and results. Finally conclusion and future work is predicted in section V.

II. Literature Survey

This section will be detailed with the different methods those are presented to solve the trust security issue and access policy controls in data sharing environment along reliability services.

- Sahai and B. Waters [5] introduced the concept of Fuzzy Identity Based Encryption, which allows for error tolerance between the identity of a private key and the public key used to encrypt a cipher text. They described two practical applications of Fuzzy IBE of encryption using biometrics and attribute-based encryption. They presented our construction of a Fuzzy IBE scheme that uses set overlap as the distance metric between identities. Finally, they proved our scheme under the Selective ID model by reducing it to an assumption that can be viewed as a modified version of the Bilinear Decisional Diffie Hellman assumption. As more sensitive data is shared and stored by third-party sites on the Internet, There is on these sites will need to encrypt data stored. Encrypt data to a drawback is that it selectively only a coarse-grained level can be shared (i.e., give your private key to another party). Features of working in our cryptosystem texts are labeled with sets and private keys which are able to decrypt cipher strength texts users are associated with access control structures.
- L. Ebrahimi, S. Nikova, M. Petkovic, P. Hartel, and W. Jonker [4] presented a mediated Cipher text-Policy Attribute-Based Encryption (CP-ABE) which is the extension of CPABE with attribute revocation. And demonstrate how to apply the mCP-ABE scheme to securely manage Personal Health Records.
- Chow [20] proposed an anonymous private key generation protocol in identity-based literature such that the KGC can issue a private key to an authenticated user without knowing the list of users' identities. It seems that this anonymous private key generation protocol works properly in ABE systems when we treat an attribute as an identity in this construction.
- Junbeom Hur [1] specified the cause cases of corruption of KGC and corrupted data storing center, He has provided with a proof of 2pc protocol. And presented new efficient and secured method for data sharing systems. But the limitation of this system was reliability and load balancing under real time environment.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

4.1 Problem Definition

The literature review presenting many methods for secure data sharing. In [1] we studied the approach which is presented for improving the security and efficiency in attribute-based data sharing. This method significantly overcomes the drawbacks of previous methods such as key escrow problem and scalability, processing speed. Following figure 1 shows the architecture of this method. However we have identified some problems in this system such as load balancing, reliability of system. In the existing system, the major role is played by key generation system. If the number of requests or communication is more, then load on key generation system becomes more and hence this resulted into slow response and cryptographic operations, therefore loads needs to be balanced. Another problem is, if the key generation system fails, or downs temporarily then whole security system downs. Hence needs to improve the reliability to this system.

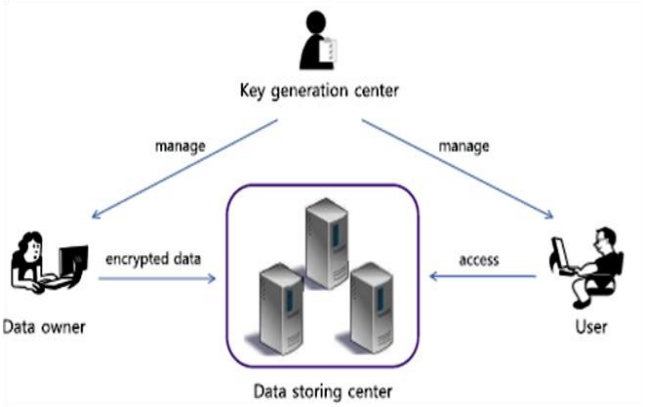

Figure 1: Architecture of Security Method presented in [1].

4.2 Access Structure

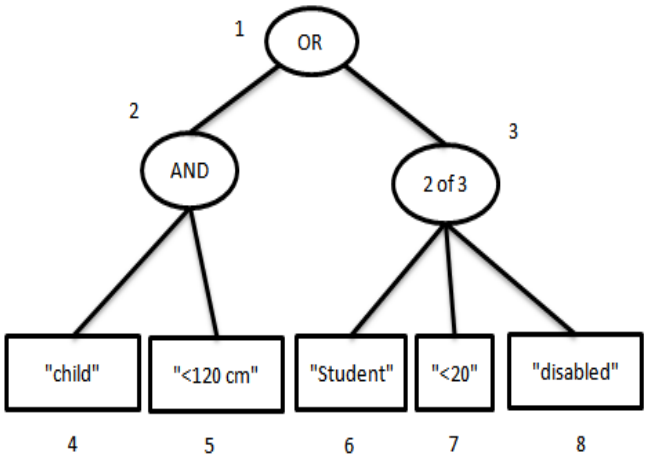

Figure 2: Example of Access Structure (Access policy)

Let T be a tree representing an access structure. Each non-leaf node of the tree represents a threshold gate, described by its children and a threshold value. . To facilitate working with the access trees, we define a few functions. We denote the parent of the node x in the tree by parent(x). The function att(x) is defined only if x is a leaf node and denotes the attribute associated with the leaf node x in the tree. The access tree T also defines an ordering between the children of every node, that is, the children of a node are numbered from 1 to num. The function index(x) returns such a number associated with the node x. Where the index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner.

4.3 Scope and Objectives

Main aim is to improve security with respect to distributed System, using third party protocol. By using load balancing technique we are providing reliability to system

- To maintain data integrity, confidentiality as well consistency etc.
- Third party will work like as web service so it's an assurance for security to client data which will store on server.
- The factor of reliability is improved by using load balancing technique
- To present the analysis of existing and proposed algorithms in order to claim the efficiency.

4.4 Proposed System Architecture

In this paper we are extending the method presented in [1] with aim of achieving the reliability, scalability, load balancing etc. The solution to overcome the limitations of existing method is to add the new backup key generation system which is having the same functionality which is presented in [1]. This increases the system extra resource as well as cost, but it's always better to have reliable, efficient and load balanced security system in place. Following figure 2 is showing the proposed system architecture. As showing in figure 2, there are two key generation center [1 and 2]. Rest all security algorithms and processes are same as given in [1]. Here we added following two functionalities for key generation for load balancing and reliability.

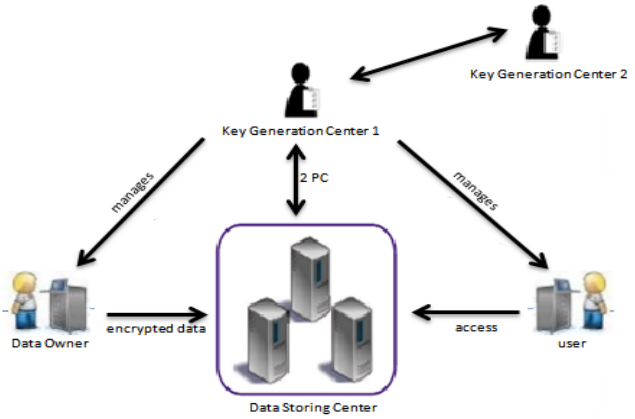

Figure 3: Proposed Architecture

4.5 Algorithms

4.4.1 Two PC Protocol

KGC with Data storing centre are involved in 2-PC protocol. The user needs to get connected with both the parties before getting the set of keys. The work of KGC is to authenticate users, along with the distribution of the set of attribute keys. The generation of secure 2-pc protocol takes places via. KGC and Data Storing Centre. It does the work of issuing the key components to user. So that user is able to generate secret key by combining the key components received from the both authorities. Thus in order to overcome the problem of key-escrow, 2-pc is introduced.

1. Init←setup ($1^{\square}$), works as trusted initialize and gives public key as output.
2. KGC generates public key and private key (PK_k,MK_k) ←KKGC()
3. Same as KGC generates the keys,Data Storing Center also generates the key,publiv and private key(PK_k,MK_k) ←KDSC()
4. KeycommD (MK_D,ID_t)↔ $Keycomm_k$(MK_k,ID_t,aux)
5. $SK_{K,ut}$←$IssueKey_K$(aux,s)
6. $SK_{u,ut}$←$IssueKey_D$()

4.4.2Dynamic Load Balancing using fair scheduling algorithm

1. Create set of Queues.
   {Queues statues is to be checked}
2. For each queue q1 in Q
3. While there are tasks in the queue do,
4. Assign demand rate of task,Xi
5. K=C/N
6. Xi<k
7. Assign Xi to ith task as fair rate (threshold)
   Else
8. Assign to ith task as fair rate.
9. Calculate fair completion time ti(x) that is time slice
   End while
   End loop
10. While (Load of any processor is greater than average load processor) do
    Selected for migration to other division
    End While
11. Calculation of turnaround time, initial time, time taken .etc

VI. Results of Practical Work

Following figure shows the practical work done. Figure 3 shows expected Performance graph. As shown in figure Number of user increases and this causing transferring of request to KGC2, improves the response time and efficient results as directed in the graph.

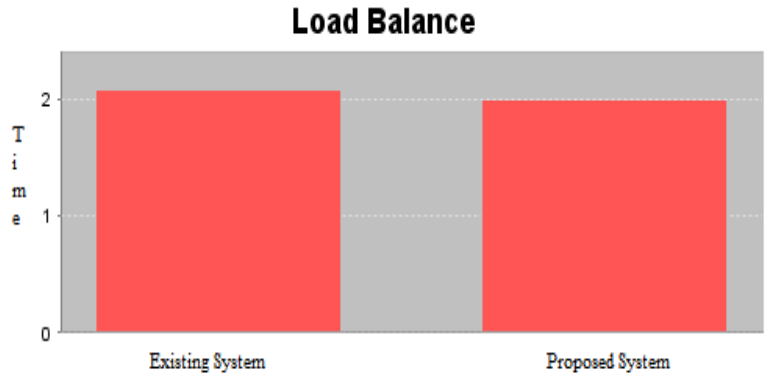

Figure 4 Performance graph

VI. Conclusion and Future Work

We have presented the system which is based on efficient security method. The existing scheme was based on attribute based data sharing security. New technique has been introduced by using the security approach along with that we are merging the load balancing technique, which cause faster response in case

primary source gets down or get overloaded. This results in decreasing the response time from 3rd party. The results presented are showing our current state of work over proposed approach. For future work we will first complete the practical analysis of proposed work and next will be try to enforce these policies on the multimedia files. As well improve the proposed results and security.

Acknowledgements

I am highly grateful to Prof. S. T. Singh, for his sincere advice and guidance in my work. I warmly express and acknowledge my special thanks.

REFERENCES

[1] Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 10, OCTOBER 2013.
[2] D.Khader," Attribute Based Authentication Schemes," PhD Dissertation University of Bath, 2009.
[3] M. S. Hwang and I. C Lin, Introduction to Information and Network Security (4ed, in Chinese)," in Mc Grew Hill. In Taiwan, 2011.
[4] L. Ebrahimi, Q. Tang, P. Hartel, and W. Jonker, Efficient and provable secure cipher text-policy attribute-based encryption Schemes, "In Proceedings of the In-formation Security Practice and Experience", pp. 1-12, 2009.
[5] A. Sahai and B. Waters, \Fuzzy identity based encryption," Advances in Cryptology", V EUROCRYPT, vol. 3494 of LNCS, pp. 457-473, 2005.
[6] D. Nali, C. Adams, and A. Miri, Using threshold attribute-based encryption for practical biometric- based access control," International Journal of Net-work Security, vol. 1, no. 3, pp. 173-182, 2005.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89-98, 2006.
[8] R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM conference on Computer and communications security, pp. 195- 203, 2007.
[9] J. Anderson, "Computer Security Planning Study," Technical Report 73-51, Air Force Electronic System Division, 1972.
[10] L. Ebrahimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Cipher text-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.
[11] Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Euro crypt '05), pp. 457-473, 2005.
[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
[13] J. Bettencourt, A. Sahai, and B. Waters, "Cipher text Policy. Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007.
[14] John Bettencourt, Amit Sahai, Brent Waters-'Cipher text-Policy Attribute-Based Encryption.
[15] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.
[16] S.S.M. Chow, "Removing Escrow from Identity-Based Encryption," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography (PKC '09), pp. 256-276, 2009.