IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Ciphertext-Policy Attribute based Data-Sharing with Enhanced Productivity and Security

Kavita Patil[1], Vidya Chitre[2]

M.E. Student, Information Technology, Vidyalankar Institute of Technology, Mumbai, India[1]

Assistant Professor, Information Technology, Vidyalankar Institute of Technology, Mumbai, India[2]

Abstract: Online data sharing systems and social networks provides security through the cryptographic solutions. For this, Cipher text Policy Attribute Based Encryption is mostly suitable for distributed data sharing systems since the data owner has full control to put in force access policies and updating the policies. Even if the CP-ABE has various advantages, it has a major drawback known as the Key Escrow problem. The Key Generation Center may perhaps decrypt any messages addressed to the specific users by generating their private keys. This is not appropriate for data sharing scenarios where the data owners would like to make their own private data only accessible to elected users key. So, this proposed System would help to fixed key escrow problem using a modified Escrow free Key generation Protocol. The improved Escrow free Key generation protocol ensures that neither the Key Generation Center nor the Data storing center can generate the secret keys individually. Instead the Key Generation Center and the Data storing center generate parts of secret key which are then integrated by the user. So as a result, the Escrow free Key issuing protocol will completely eliminates Key Escrow problem as well as the data owner would like to make their private data only accessible to designated users. Hence to overcome this problem fine-grained data access control provides a way of defining access policies based on different attributes of the users or the data object and the security is enhanced in order to send private keys by the data owner or the users .So the issue of key-escrow problem is resolved by issuing 2-pc protocols in system which will definitely protect the secure key escrow problem. As well as to improve the security Data integrity checking will be done. So as a result this Proposed System will help us to obtain more security and performance.

Keywords: Attribute Based Encryption (ABE), Cipher text Policy Attribute Based Encryption (CP-ABE), Data Integrity, Key Generation Center (KGC), Third Party Auditor (TPA).

I. INTRODUCTION

By generating users private keys the Key Generation Center (KGC) could decrypt any messages addressed to specific users. This is ill suited for data sharing scenarios where the data owner would like to make their private data accessible to only a designated users key. To prevail against this problem we propose one problem known as escrow problem which means that it's a written contract delivered to a third party and Attribute-Based Encryption (ABE).The ABE is a promising cryptographic approach and also it is a fine-grained data access control mechanism which provides a way to defining access policies based on various different attributes of the requester, environment and the data object. The KGC can decrypt each and every cipher text addressed to specific users by generating their attribute keys. So, in the data sharing systems, this could be a potential threat to the data confidentiality or privacy.

In ABE scheme, attributes plays very important role. To generate a public key Attributes are to be isolate so it is used for encrypting data and to control user's access it can be used as an access policy.

The access policy is flavoured in two-key policy & cipher text policy.

i) key-policy attribute: It is used for describing encrypted data as well as policy implemented on user's key
ii) cipher text policy: It is the access structure proceeding on the cipher text.

The access structure can be either in monotonic or it can be non-monotonic. ABE schemes have following benefits:

a. It reduces the communicational overhead of the Internet
b. It is a fine grained access control.

Now a day, putting data on untrusted storages like cloud space makes difficult challenges to the secure data and sharing of data. So, to resolve these challenging issues cryptographic methods are implied. Along with key management, the Cryptographic methods also have scalability in data access control. ABE is one of the techniques that are more suitable for storing data with encryption. By issuing 2-pc protocols the issue of key-escrow problem is resolved in system, which will protect the scene of key-escrow problem. The parameters [4] like performance and security are satisfied for handling the data in disturbed way in data sharing networks.

A cloud storage service permits data owner to put their data to the cloud. It provides access for data to the users. As the cloud server and the data owner are in the different trust domain, the semi-trusted cloud server cannot be relied to carry out the access policy. Both are not in same trust domain. To address this challenge, traditional methods generally requires data owner to encrypt the data and distribute the decryption keys to authorized users. Normally such methods involve high overhead and complicated key management on data owner.

In this paper, design contains an access control framework for cloud storage systems that achieves a fine-grained access control depends up on an adapted Ciphertext-Policy Attribute-based Encryption (CP-ABE) approach.

The proposed scheme achieves:

A. The key escrow problem could be resolved by escrow-free key issuing protocol, which is constructed by using the secure two-party computation between the data-storing center and key generation center

B. The security and performance analyses point towards that the proposed scheme is effectual towards securely manage the distributed data in the data sharing system.

II. RELATED WORK

As a use of internet increases day by day. The people puts their data online such as social data centers, websites like Facebook, Google, Twitter and cloud services also store and shared the data to enterprise. All the People can share their private data such as images, messages, photos on these web sites. This data is highly confidential for them but they are an aware of data security so that sometimes an unauthorized user can use their data in wrong intention for example they can use forged data for terrorist activity with the intention of attack. People communicate with each other via e-mail to share their data which is confidential so there is a need of data security. So for the security reason data needs to be in encrypted at the respective sites. So that authorized people will get data from authorized user only.

First cryptographic approach such as Attribute Based Encryption is proposed by VipulGoyal, PandeyAmit and Sahaiz Brent [1] Waters with fine grained data access. It provides way to define access policy based on different attribute. In ABE system user key's and cipher text associated with set of descriptive attributes and particular key can decrypt a particular cipher text if there is match between the attributes. This type of encrypting data have an drawback it can be selectively shared only coarse grained level that means private key shared with another party. The Sahai and Waters proposed the Threshold ABE system for error tolerant identity based encryption scheme in which ciphertext associated with set of attributes S and user private key associate with both threshold parameter and another set of attribute. In order to decrypt a ciphertext at least k attribute overlapped with cipher text and private keys. The drawback of Threshold ABE is threshold semantic are not expressive. Sahai and Waters proposed the new Attribute based encryption, in this scheme private keys can represent any access formula including non-monotone. It can handle any access structure that represent Boolean formula such as AND,OR, Not and so.

To resolve this issue Vipul Goyal proposed a new encryption technique is called as KP-ABE that means Key Policy Attribute Based Encryption in 2006. In this system, cipher text is associated with the set of attributes and private key is associated with specified access structure.

The KP-ABE allow users to decrypt the Ciphertext. To decrypt the Ciphertext, there should be at least k attributes overlapped between key structure and ciphertext. In the KP-ABE system, it define secret sharing scheme of data scheme where the access structure involved threshold. First time Shamir and Balkley proposed the secret sharing scheme in which to create a secret one condition get satisfied like two or more parties should come together then it will form a secret.

The secret sharing scheme specifies tree access structure. In this, interior node consist of AND & OR gate and leaves consist of different parties. Any set of parties which fulfill the tree come together and reconstruct the secret. In KP-ABE system, leaves are associated with attributes and user key is associated [3] with tree access Structure. The user is able to decrypt the Ciphertext if and only if attributes are associated with Ciphertext which satisfies key access structure. The main difference between KPABE and secret sharing scheme is, in KP-ABE parties have forbidden and in secret sharing scheme, it allows cooperation between different parties.

In the paper of Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems by Junbeom Hur et al., in data outsourcing scenario one of the most challenging issues is the enforcement of authorization policies and the support of policy updates. For these issues, CP-ABE is a promising [8] cryptographic solution for enforcing access control policies defined by a data owner on outsourced data. Still, the problem of applying ABE with an outsourced architecture leads to several challenges through the user revocation and attribute.

In this paper, an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with user revocation capability and an efficient attribute is proposed. The fine-grained access control can be achieved by dual encryption mechanism which is advantageous to the attribute-based encryption and selective group key distribution in each attribute group. This paper is concentrate on how to apply proposed mechanism to securely manage the outsourced data. The analysis result indicates that the proposed scheme is efficient and secure in the data outsourcing systems.

Mediated CP-ABE and Its Application In CP-ABE by Luan Ibraimi et al, in this user's secret key is associated with the a set of attributes, and ciphertext is associated with an access policy. The user can decrypt the ciphertext if and only if the attribute set of user's secret key satisfies with the access policy specified in ciphertext. There are Several CP-ABE schemes have been introduced,still problems like attribute revocation needs to be addressed. In this paper, mCP-ABE that is a mediated CP-ABE which is extended CP-ABE with instantaneous attribute revocation is proposed.

Lewko et al, in paper Revocation Systems with Very Small Private Keys‖, Security and Privacy (SP) .The Outcomes of this technique has a two key contributions like first is new scheme has ciphertext size above $O(r)$, where r is the number of revoked users, and the size [9] of public and private keys is merely a \emph{constant}

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

number of the group elements from an elliptic-curve for a group of prime order. In addition, the public key permits to encrypt an vast number of users. This system is the first to accomplish such parameters [9]. They have given two versions of their scheme: first is a simpler version which prove to be selectively secure in the standard model under a new, but non-interactive assumption, and another version is a new dual system's encryption technique was of Waters to attain adaptive security below the d-BDH and decisional Linear assumptions. Second, this techniques can be used to realize ABE systems with non-monotonic access formula so key storage become more efficient than prior solutions.

Now a days, Security is a most important thing in the data sharing. Most of the peoples are stored their data on external storage server. So that they can able to share their data among various users. Most of the time user data is very sensitive because this data contains personal information of users. So, there is a need to improve into security measures. Leakage of the data is the main problem in the data sharing System. The data can be protected by encrypting it with proper security key.In the cloud, the leading problem of storing the encrypted data lies in revoking the access rights from the user. A user whose authority is repeal will still preserve a copy of keys issued earlier, and thus can decrypt data in the cloud. The naïve classified solution is, the data owner must instantly re-encrypt the data, so that the receiver will make a request for the key, once the request was received by the data owner, either he can send the key or decline the request. This solution leads to a performance bottleneck, mainly when there is a frequent user revocation. Another alternative solution is to apply the proxy re-encryption technique which is also known as PRE technique. This approach is called as command–driven re-encryption scheme, while receiving the commands from data owner the cloud server executes the encryption.

The main drawbacks are:

1. with some decryption software, We can easily decrypt the data without the security key which is assigned by the data owner.
2. For the highly sensitive data, Only single key is used.
3. If suppose key is forgot we cannot able to send multiple key request to the data, and also we cannot decrypt the data without the key

III.PROPOSED SYSTEM

In proposed system to develop the data sharing using Attribute Based Encryption (ABE) Algorithm. With the help of this system data becomes more secure than the existing system. To applying CP-ABE in the data sharing system, for users KGC generates private keys by applying the KGC's master secret keys to users' corresponding set of attributes.

Benefits:

a. It's a very secured data transfer with advanced encryption technique so the other person cannot decrypt it easily.
b. Here we used ABE system which provides more security for our data.
c. The receiver can send multiple key requests to the data owner for the single data.

So to improve data security, proposed System would consist of TPA Module. In this module TPA has monitors the data owners by verifying the data owner's file and stored that file in the database. Also TPA checks the CSP that means cloud service provider, it finds out whether the CSP is a authorized or not. It helps to ensure the data owner's data being stored in the cloud is valid or not. Data integrity is achieved by using by HMAC algorithm and it generates the 16 bit hexadecimal code to inspect the integrity of the data file.

HMAC is a method that uses the same concept like MAC by means of a secret shared key, but it also uses other cryptographic hash functions like for example, HMAC-SHA1, HMAC-MD5, HMAC-RIPEMD, etc.

a. It is a Small block of data generated with a secret key and appended to a message
b. HMAC (RFC 2104)
   i. Uses hash instead of cipher for speed
   ii. Used in SSL/TLS and IPSec

So to improve data security, proposed System would consist of TPA Module.

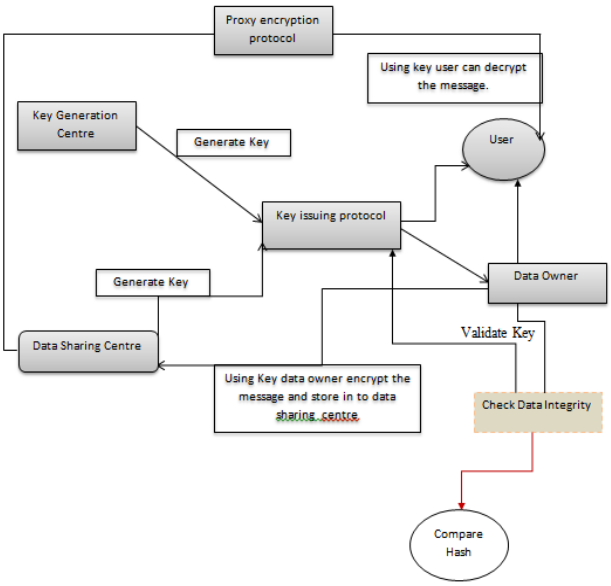


Fig.1 Proposed System

In this module, TPA has monitors the data owners by verifying the data owner's file and stored that file in the database. Also TPA checks the CSP that means cloud service provider, it finds out whether the CSP is a authorized or not. It helps to ensure the data owner's data being stored in the cloud is valid or not. Data integrity is achieved by using HMAC algorithm and it generates the 16 bit hexadecimal code to inspect the integrity of the data file.

Data Integrity Checking using HMAC-

a. While Data retrieved from the server, it needs to be checked whether the received data is Valid or not.

DOI 10.17148/IJARCCE.2015.41138

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

b. Data storage correctness is more significant besides secured outsourcing of data in cloud.
c. Data owner has to audit to verify data integrity of received data from the cloud server.
d. Data owner used HMAC algorithm which is hash-based Mac Algorithm for the verification of the data being received from the cloud.

IV. MODULES

Proposed System consists of following modules:

A. User Module:

1. Register with OTP
To upload or download a file the user must register to the cloud. While registration, user has to provide necessary details. Only the authenticated user is registered who can upload/download a file. To authenticate a user OTP is generated to check authentication. The OTP is sent on user's provided mobile no. After verification the user is registered successfully to the cloud.

2. Login:
User will login with the provided user name and password only when he is registered to the cloud with same user name and password.

3. File Upload:
User can save file on cloud. To preserve the privacy of the file, the file is encrypted using Attribute Based Encryption. Using ABE a key is generated for that particular file, so that the file cannot be downloaded by any other user without access permission. The key is mailed to owners provided email id.

4. File Download:
Any user can search a file on cloud. As the confidentiality of the file is maintained user has to request for download to the owner of the file. If the owner wants to permit the requested user to view or download the file he can provide the requested user with an access key which is generated in the application for each request. With this access key only the permitted user can view or download file as each time a new access key is generated to every request. The file is first decrypted with the provided access key form the owner and then it can be viewed or downloaded by the user. After a user downloads the file user can make changes in that downloaded file if required and will upload the tampered file.

5. Tampering:
Owner will be provided with the details of the tampered file if any. If the owner wants the tampered file to replace original file owner can make the replacement. Also if the owner finds a particular user tampering file or does not wishes to grant access to that user than owner can block that particular user from viewing or requesting owners file.

B. TPA Module:

TPA will view the downloaded files and will check the metadata of files to see if the files are tampered. All the details of auditing of downloaded files will be saved in a temporary database with metadata changes. These details are forwarded to the Admin for necessary actions. It should be noted that TPA cannot view any file only the metadata of the files are checked.

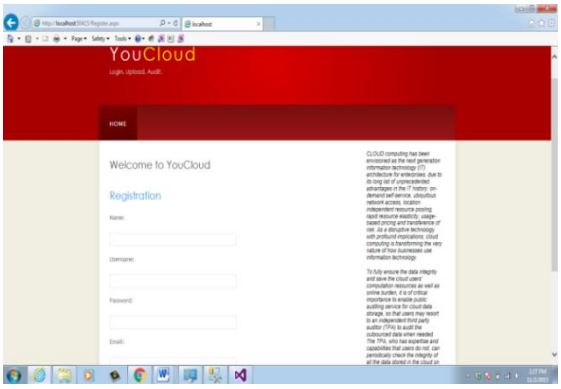
C. Admin Module:

1. View tampered details:
All the details of the downloaded files provided by Third Party Auditor (TPA) are checked by the admin. The details of the files which are not tampered and are only downloaded are deleted from that temporary database by the Admin. The remaining tampered files are reported to their respective owners.

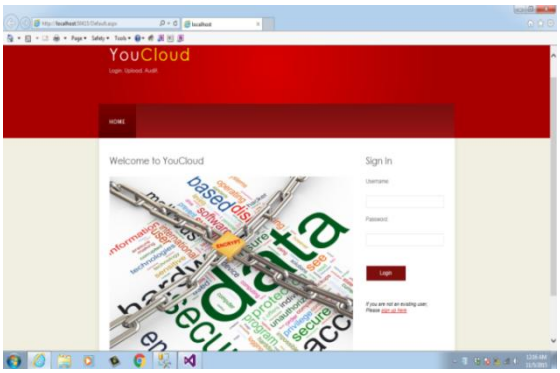
2. Report to owner
If the Admin finds a file tampered by any user, the details of the users and the tampered file are provided to their respective file owner. Owner will check if he wants to replace the file or keep it original.

V. SCREENSHOTS

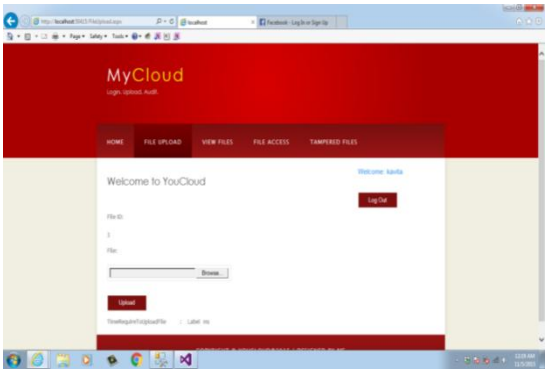
1. REGISTRATION:



2. LOGIN SCREEN



3. FILE UPLOAD



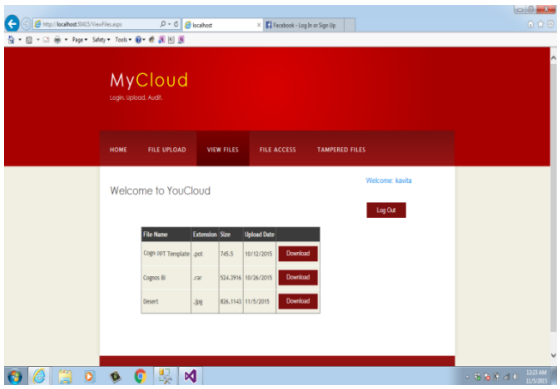
DOI 10.17148/IJARCCE.2015.41138

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

4. VIEW FILES



VI. CONCLUSION

To achieve more security in data access control, the proposed system demonstrated to gain more efficient and secure access. By providing the access policies to user, It becomes very easy to manage the data of data owner. This proposed system will achieved Data privacy and confidentiality in the data sharing system by adding data integrity checking against any outsiders and system managers without proper credentials. Hence this system is more secure and confidential.

REFERENCES

[1] John Bethencourt, amitsahai, brentwaters,"Ciphertext-Policy Attribute-Based Encryption", https://www.cs.utexas.edu/.

[2] [2] NuttapongAttrapadung, Beno,,Elie de Panafieu,"Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts" , D. Catalano et al. (Eds.): PKC 2011, LNCS 6571, pp. 90–108, 2011.

[3] VipulGoyal, OmkantPandey,AmitSahai,Brent Waters," Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", https://eprint.iacr.org/2006/.

[4] Ms.Snehlata V.Gadge,"Analysis and Security based on Attribute based Encryption for data Sharing", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-3)

[5] V.Abinaya, V.Ramesh,"Attribute Based Mechanism Using Cipher Policy Verification", IJARCST 2014 Vol. 2 Issue Special 1 Jan-March 2014

[6] M. Pratheepa1, R. Bharathi2," Improving Security and Efficiency in Attribute Based Data Sharing", Volume 3 Issue 1, January 2014

[7] Taeho Jung , Xiang-Yang Li ,Zhiguo Wan, Meng Wan, "Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption", Information Forensics and Security, IEEE Transactions on (Volume:10 , Issue: 1) Page(s):190 - 199

[8] JunbeomHur , Dong Kun Noh,"Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems",Issue No.07 - July (2011 vol.22)pp: 1214-1221

[9] AmitSahai,Brent Waters," Revocation Systems with Very Small Private Keys",pp:1-19 Luan Ibraimi, Milan Petkovic, SvetlaNikova, Pieter Hartel and Willem Jonker, "Mediated Cipher text-Policy Attribute-Based Encryption and Its Application", Information Security Applications, Lecture Notes in Computer Science, DOI:10.1007/978-3-642-10838-9_23, Pp309-323,2009.

[10] Lewko,Allison;Sahai,Amit;Waters,Brent"Revocation Systems with Very Small Private Keys, Security and Privacy", IEEE Symposium, May 2010, 978-1-4244-6895-9, pp 273 – 285, 2010.

[11] Alexandra Boldyreva, VipulGoyal, Virendra Kumar,"Identity-based encryption with efficient revocation", Proceedings of the 15th ACM conference on Computer and communications security, ISBN: 978-1-59593-810-7, pp417-426, 2008.

[12] Shucheng Yu, Cong Wang,KuiRen, Wenjing Lou, "Attribute based data sharing with attribute revocation", Proceedings of the 5th ACM Symposium on Information, ISBN:978-1-60558-936-7,pp261-270, 2010.

[13] Ling Cheung, Calvin Newport, Provably secure cipher text policy ABE, Proceedings of the 14th ACM conference on Computer and communications security, ISBN:978-1-59593-703-2,pp 456-465, 2007

BIOGRAPHIES

Kavita Patil received her B.E degree in Computer Engineering from Mumbai University in 2013 and currently pursuing M.E. degree from Mumbai University, Maharashtra, India. Her current research interests are Cloud Computing and Networks**.**

Vidya Chitre is working as Assistant Professor in Vidyalankar Institute of Technology. She has received the B.E degree in Computer Engineering from Mumbai University in 1998 , and M.E. in 2002 and currently pursuing her Ph.D. from Mumbai University. Her current research interests are Big data and Cloud Computing**.**