Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Application of CP-ABE Scheme in Data Sharing System for confidentiality

Akash Koli[1], Gajendrasingh Chandel[2]

[1]*Department of IT,SSSIST,sehore MP*
[2] *HOD Department of IT,SSSIST sehore MP*

Abstract—CP-ABE Scheme (Cipher text policy attribute-based encryption) can become the promising cryptographic solution in distributed systems such as social network s and cloud computing. The trending development of network and computing technology enables the user to share their data through the online social networks such as Facebook, or uploading the personal data on Google Vault. The people are using the advantages of new technologies but they are also concern about their personal data security. The current issue with data sharing systems is the enforcement of access policies. CP-ABE scheme enables the encryptor to define attribute set over a universe of attributes that a decryptor needs to decrypt the cipher text, thus each user with a different set of attributes is allowed to different pieces of data as per the security policy.

Keywords-component; Data sharing, attribute-based encryption, revocation, access control, removing escrow.

I. INTRODUCTION

The trending development of network and computing technology enables the user to share their data through the online social networks such as Facebook, or uploading the personal data on Google Vault. The people are using the advantages of new technologies but they are also concern about their personal data security. People would like to make their private or sensitive information accessible only to the authorized persons.

Attribute based encryption is a promising technique that achieves a fine grained data access control. It provides a way of defining access policies based on different attributes of the requester. Cipher text policy attribute based encryption enables an user to define the attribute over set over a universe of attributes that a decryptor user needs.

Applying the CP-ABE scheme in data sharing have some issues of one of them is escrow problem the key generation center can decrypt every cipher text addressed to specific users by generating their attribute keys. This would be a security threat to owner's data. Another issue is key revocation since some users may change their associate attribute at some time , key revocation or update for each attribute is necessary in order to make system secure.

II. LITERATURE SURVEY

ABE scheme have two types (KP-ABE) Key policy ABE and (CP-ABE) Cipher text policy. In CP-ABE the attributes are used to describe users credentials and an encyptor determines a policy on who can decrypt the data as it gives the access policy decisions on the hands of data owners so more appropriate for data sharing systems.

Removing Escrow : The Existing ABE scheme are constructed on the base architecture where a single trusted authority has power to generate the whole private keys of users with its master secret key. In this the issue arises that the KGC can decrypt every cipher text addressed to users in the

system by generating their secret keys.To resolve this distributed KP-ABE scheme used that solves the key escrow problem in multi authority systems. 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 user identities.

2.1 Key Revocation Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.

2.2 Removing Escrow

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information.Thus, the key escrow problem is inherent such that the KGC can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time.

Chase and Chow presented a distributed KP-ABE scheme that solves the key escrow problem in a multi-authority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this k ind of fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with the other authorities in the system to generate a user's secret key. This results in $O(N^2)$ communication overhead on the system setup phase and on any rekeying phase, and requires each user to store $O(N^2)$ additional auxiliary key components besides the attributes keys, where N is the number of authorities in the system. Recently, Chow 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. However, we found that this cannot be adapted to ABE systems due to mainly two reasons. First, in Chow's protocol, identities of users are not public anymore, at least to the KGC, because the KGC can generate users' secret keys otherwise. Since public keys (attributes in the ABE setting) are no longer "public," it needs additional secure protocols for users to obtain the attribute information from attribute authorities. Second, since the collusion attack between users is the main security threat in ABE, the KGC issues different personalized key components to users by blinding them with a random secret even if the y are associated with the same set of attributes. The random secret is unique and should be consistent with the same user for any possible attribute change (such as adding some attributes) of the user. However, it is impossible for the KGC to issue a personalized key component with the same random secret as that of attribute key components to a user, since the KGC can by no means know which random secrets (used to issue a set of attributes key components) are assigned to which users in the Chow's key issuing protocol.

III. PROPOSED SYSTEM

we propose a novel CP-ABE scheme for a secure data sharing system. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing center in the proposed scheme

IV. KEY MANAGEMENT ARCHITECTURE FOR DATA SHARING SYSTEM

In this the key generation center will generate the public and master code parameter for CP-**ABE scheme**. It will perform the key issuing, key revoking, and updating attribute key for users. It will permit differential access rights to individual users based on their attributes Key generation center. It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes

Data server will provide data sharing facilities and also prohibit unauthorized users to access, store data. Data-storing center. It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing c corresponding contents services. The data-storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control.

User as a Data Owner: A user who is sharing or uploading data to the server. Data owner defines the access policies for data distribution just like on social network that who can see the profiles or the posts.

User as Client Access only: A user is one who wants to access the data from server who having the permission possessing the set of attributes satisfying the user policies. After this he would be able to decrypt the cipher text and accessing the desired data.

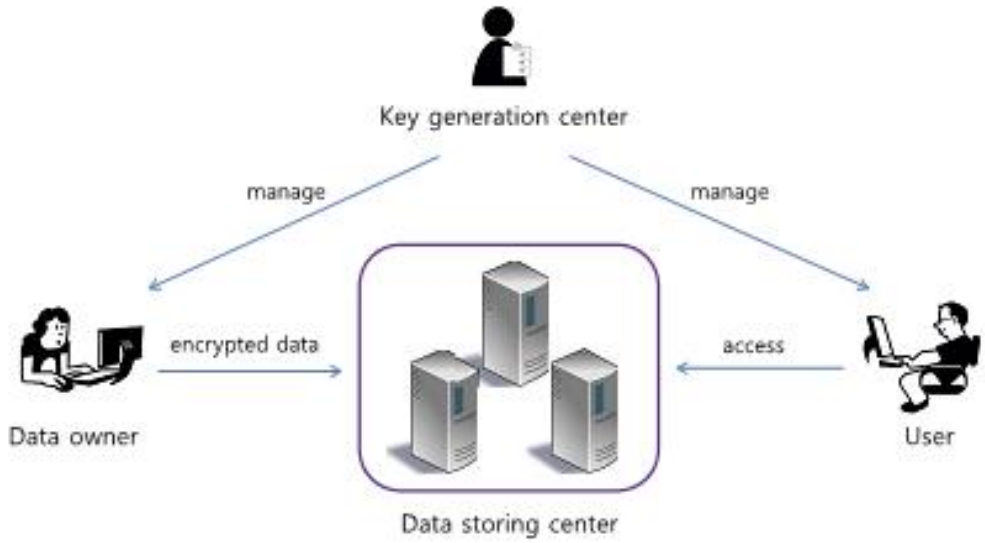

FIG4.1 DATA SHARING ARCHITECTURE

V. TECHNIQUE OR ALGORITHM

To applying CP-ABE in the data sharing system, In CP-ABE, the key generation center (KGC) generates private keys of users by applying the KGC's master secret keys to users' associated set of attributes. A cipher text policy attribute-based encryption (CP-ABE) system consists of four fundamental algorithms: Setup, Encrypt, KeyGen and Decrypt.

Setup: Setup takes as input a security parameter and returns a public key PK and a master key (Private Key) MK. The public key is used for encryption. The master key, held by the central authority

KeyGen: KeyGen takes as input the public key PK and a master key (Private Key) MK.

Encrypt. Encrypt takes as input the public key PK, a message M and an access structure W. It returns a cipher text CT such that a private key generated from attribute set S can be used
decrypt CT.

Decrypt: Decrypt takes as input a cipher text CT. It returns the message M if S satisfies W, where S is the attribute set used to get MK

Key Update: When a user comes to hold or drop an attribute, the corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively. The key update procedure is launched by the KGC when it receives a join or leave request for some attribute groups from a user.

VI. SNAPSHOT

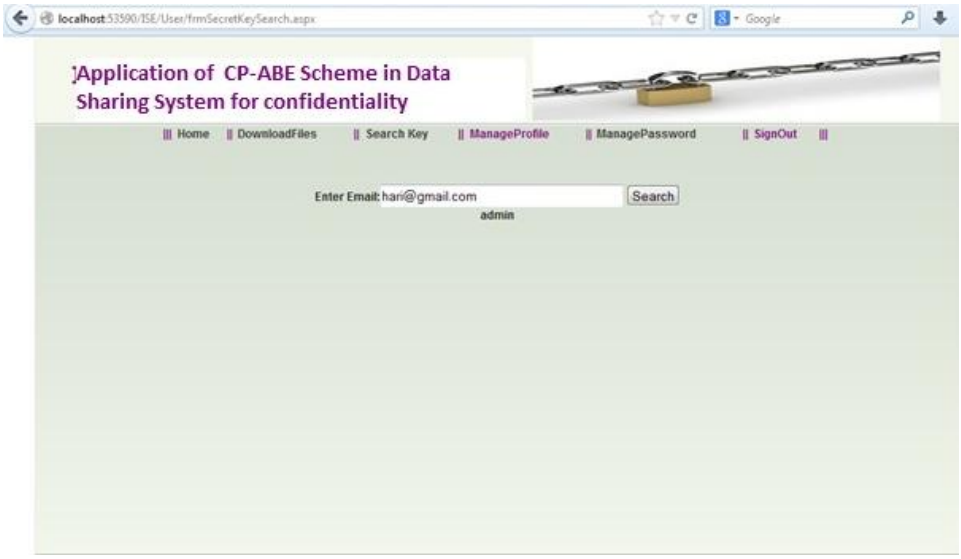

FIG 6.1 USER ADMIN

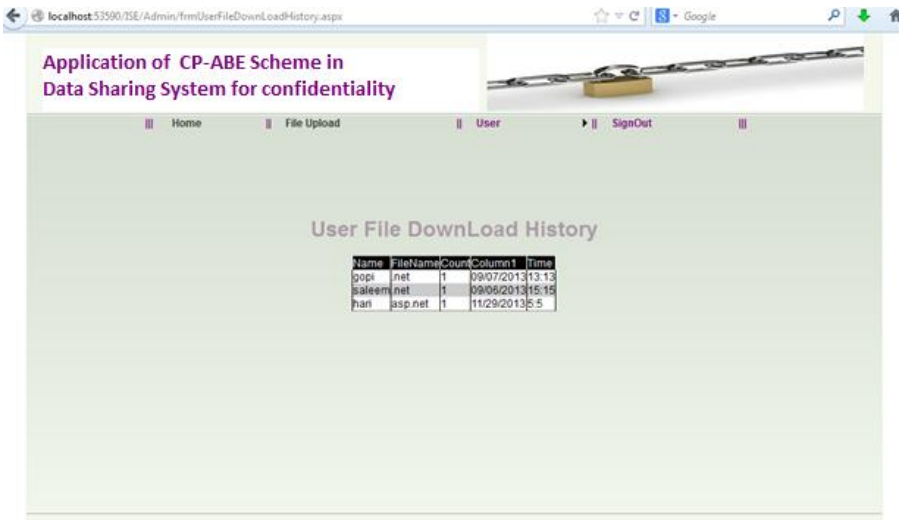

FIG 6.2 FILE DOWNLOAD HISTORY

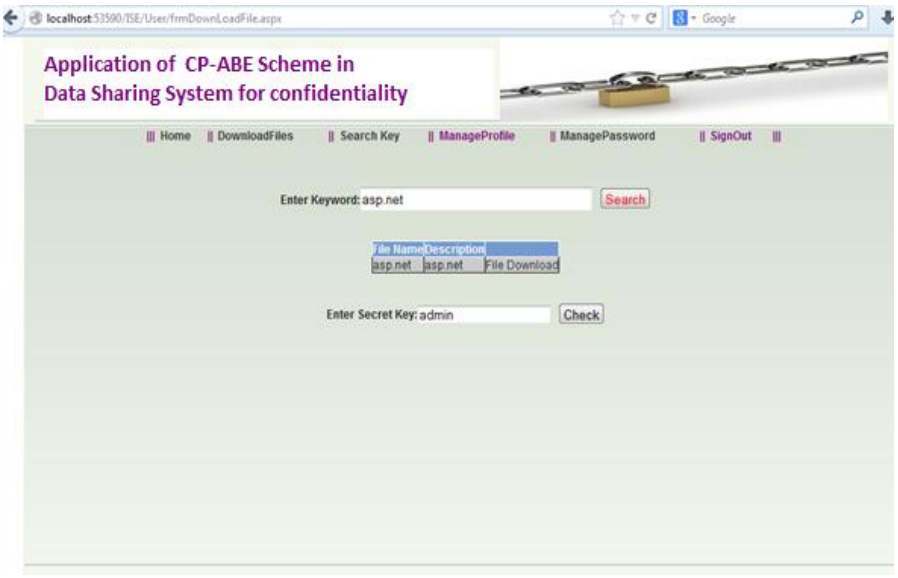

FIG 6.3 SECRET KEY BY KGC

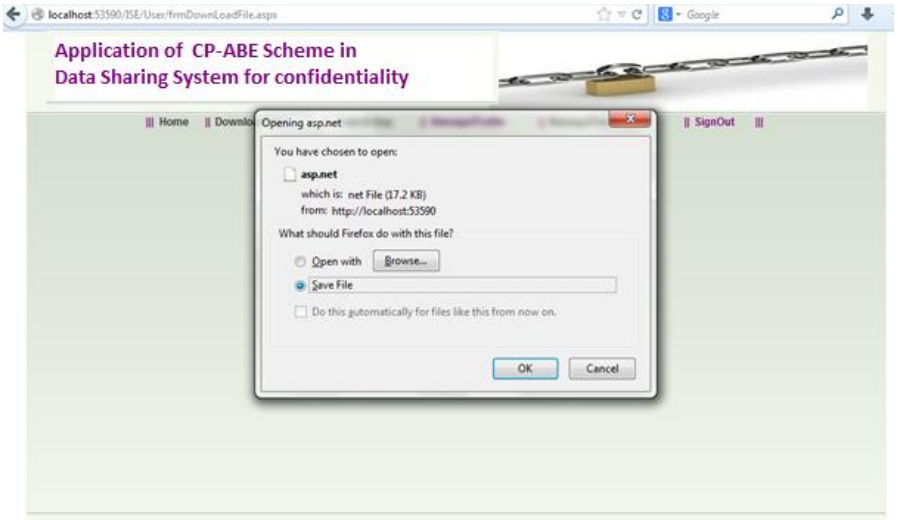

FIG 6.4 FILE DOWNLOAD DECRYPT

VII. CONCLUSION

The proposed scheme enhances confidentiality in the data sharing system against any adversarial outsiders without corresponding enough credentials. The proposed scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the cipher text policy attribute-based encryption. Therefore, the proposed scheme achieves more secure and fine-grained data access control i n the data sharing system.. It also provide Secure two-party communication between the key generation center and the data storing center for social networking area. Also in future enhancement can be used for multimedia files effectively.

REFERENCES

[1] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,"Mediated Ciphertext-Policy Attribute-Based Encryption and ItsApplication," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.

[2] 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

[3] J. Bethen cou rt , A.Sahai, and B. Water s, " Ciphertext- Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[4] S.S.M. Chow, "Removing Escrow from Identity-Based Encryp-tion," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography(PKC '09), pp. 256-276, 2009.

[5] 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.

[6] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryp-tion with Efficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

