Efficient Security in Decentralized Cipher text-Policy Attribute-Based Encryption

Neethu. A. N[1], M. Prem Kumar[2]
[1, 2] Department of Computer Science
[1, 2] PPG Institute of Technology, Coimbatore, India

Abstract- *Cipher-policy attribute-based encryption (CP-ABE) is more efficient and flexible encryption method and provides solution to the problem of anonymous access control by the encryptor, the encryptor control the access structure when encrypting a message. In this paper, a privacy-preserving decentralized CP-ABE (PPDCP-ABE) and protect user's privacy. In our PPDCP-ABE scheme, each authority can work independently without any collaboration to initial the system and issue secret keys to users. Furthermore, a user can obtain secret keys from multiple authorities without them knowing anything about his global identifier and attributes. In the proposed system, when encrypting a message, the encryptor can select an access structure for each authority and encrypt the message under the selected access structures so that a user can decrypt the cipher-text if his attributes satisfy all the access structures. In addition to this key aggregation concept is used. One can decrypt more than one file using key aggregation concept.*

Keywords- Decentralization, privacy, Cipher text, Attribute based encryption.

I. INTRODUCTION

In network society, users can be authenticated and identified by their distinct attributes such as nationality, civil status, applicable minority status, etc., which are either binary or discrete numbers from pre-defined finite sets [1]. In central authority scheme, it monitors the universal attributes and distributes secrete keys to users accordingly. A user can decrypt a cipher text if and only if there is a match between the attributes which he holds and the attributes listed in the cipher text. Since it can protect the confidentiality of sensitive data and express flexible access control, So the ABE schemes have been focused extensively [2,5,6,7,8,9].

To reduce the trust on the central authority, a multi-authority ABE (MA-ABE) scheme is proposed [10]where multiple authorities must cooperate with the central authority to initialize the system.

Attribute-based encryption provides good solutions to the problem of anonymous access control by specifying access policies among private keys or cipher texts over encrypted data. In cipher text-policy attribute-based encryption (CP-ABE), each user in the system is associated with a set of attributes, and data is encrypted with access structures on attributes. A user is able to decrypt a cipher text only if his attributes satisfy the cipher text access structure. CP-ABE is very appealing since the cipher text and data access policies are integrated together in a natural and effective way. All the previous privacy-preserving MA-ABE (PPMA-ABE) schemes [2, 3, 4] only the privacy of the global identifier (GID) has been considered. Currently, no scheme addressing the privacy of the attributes has been proposed. And it is extremely important as a user can be identified only by some sensitive attributes.

In this paper, a privacy-preserving decentralized CP-ABE (PPDCP-ABE) is proposed to reduce the trust on the central authority and protect user's privacy. In our PPDCP-ABE scheme, each authority can work independently without any collaboration to initial the system and issue secret keys to users. In the proposed system, when encrypting a message, the encryptor can select an access structure for each authority and encrypt the message under the selected access structures so that a user can decrypt the ciphertext if his attributes satisfy all the access structures. In addition to this key aggregation concept is used. One can decrypt more than one file using key aggregation concept.

II. LITERATURE SURVEY

John Bethencourt [11] presented a system for realizing complex access control on encrypted data called cipher text-policy attribute-based encryption. This techniques encrypts the data and kept confidential even if the storage server is un-trusted; And the method secure against collusion attacks and works based on system attributes which describe a user's credentials. The method is closer to traditional access control methods such as role-based access control (RBAC) and the system provides performance measurements.

L. Cheung [12] studied about CP-ABE schemes and proposed a basic scheme that provide secure under the decisional bilinear Diffie-Hellman (DBDH) assumption and applied CCA secure extension using one-time signatures.

They also introduce hierarchical attributes to optimize the basic scheme - reducing both ciphertext size and encryption/decryption time while maintaining CPA security.

A. Lewko [13] presented two fully secure functional encryption schemes such as i) a fully secure attribute-based encryption (ABE) scheme. ii)a fully secure (attribute-hiding) predicate encryption (PE) scheme which was developed for inner-product predicates. He constructed ABE scheme that supports arbitrary monotone access formulas which was a new approach on bilinear pairings. A scheme was proposed in which any polynomial number of independent authorities monitor the attributes and distribute secret keys [14] and it can tolerate an arbitrary number of corrupt authorities.

Jinguang Han[15] proposed a privacy-preserving decentralized CP-ABE (PPDCP-ABE). In the system each authority can work independently without any collaboration to initial the system and issue secret keys to users.

III. PROBLEM DEFINITION

The user must convince each authority that the attributes for which he is obtaining secret keys are monitored by the authority as the authority cannot know his attributes. And the authority can interact with the user to generate correct secret keys for him even if he does not know the user's identifier and attributes. The secret keys derived from authorities can be used together to decrypt a cipher text. The encryptor can select an access structure for each authority and encrypt the message under the selected access structures so that a user can decrypt the cipher text if his attributes satisfy all the access structures.

IV. PROPOSED SYSTEM

We propose a privacy-preserving DCP-ABE (PPDCP-ABE) scheme where the central authority is not required and each authority can work independently without any cooperation. As a notable feature, each authority can dynamically join or leave the system, namely other authorities do not need to change their secret keys and reinitialize the system when an authority joins or leaves the system. Each authority monitors a set of attributes and issues secret keys to users accordingly. Especially, a user can obtain secret keys for his attributes from multiple authorities without them knowing any information about his attributes. Therefore, the proposed PPDCP-ABE scheme can provide stronger privacy protection compared to the previous PPMA-ABE schemes where only the GID is protected.

The encryptor can select an access structure for each authority and encrypt the message under the selected access structures so that a user can decrypt the ciphertext if his attributes satisfy all the access structures. In addition to the access structure, in the proposed system, Data owner can also be encrypting 2 or more similar files with the common key. So the user can decrypt more files by using that single key. By using Attribute Based Encryption we can achieve these goals. Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. It defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE).

In addition to this key aggregation concept is used. One can request more than 1 file. For the similar group of files, a folder key is set. Using that key, users can decrypt group of files.

V. MODULE DESCRIPTION

A. Provider Module

The provider access the system with the respective username and password. Providers are the data owners who wish to share the files among the users. Before this, providers need to register in the system with their personal details. These details include providers name, email id, mobile number, address etc.

B. User Registration

User registered with their personal details like user first name, last name, mobile, email id, address etc. Each authority can dynamically join the cloud or leave the system, and other authorities do not need to change their secret keys and reinitialize the system when an authority joins the system or leaves the system. User should also submit their Id proof in order to share the files from the cloud storage.

C. Data Encryption with Access Structure

In this process the provider can upload the file that he/she needs to share among the users. Before uploading, encryption should be done in order to protect the secret information of data. The data owner can also select an access structure for each authority and encrypt the message under the selected access structures so that a user can decrypt the cipher text if his attributes satisfy all the access structures.

D. Key Policy

Key aggregating policy is introduced with which even the Data owner can encrypt 2 or more similar files with the common key. So the user can decrypt more files by using that single key. By using Attribute Based Encryption we can achieve these goals.

E. Request Data

Users can login to the system and can view the files. If user needs to access the contents of the files, he/she need to send the request to the data owner to obtain the decryption key. The data are stored in the database. This data should be viewed by the appropriate data owner.

F. Valid User Authentication

All the user requests are stored in the database. The data owner can provide the secret keys to the requested users. The data owner can check the user are valid or not by viewing their ID. If the user is valid, data owner provide the keys to users. If not that case, the requested users cannot access the files till data owner process the request.

G. Decrypting Data

After authenticating the user, data owner provides the key to the requested users. Users can decrypt the files by using the key. Users can also request single file or group of files. In order to download more files from the storage, users need to request the aggregate key. The secret keys derived from authorities can be used together to decrypt a ciphertext. Only the granted users access the files from the cloud storage.

H. File Deleting

If the data owner is not willing to share the files in the storage after some time, the data owner have the option to delete the files from the storage. So the users are not allowed to view the files after deleting the file.

ARCHITECTURE DIAGRAM

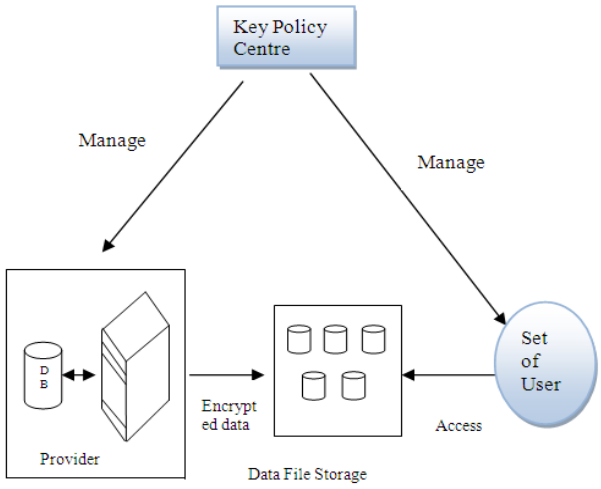

Fig: 1 Architecture diagram

VI. RESULT ANALYSIS

It provides the users' privacy and protection with decentralization and issue secret keys to users. A user can obtain secret keys from multiple authorities without knowing anything about the global identifier and attributes and during encrypting a message, the encryptor can select an access structure for each authority and encrypt the message under the selected access structures so that a user can decrypt the cipher text if his attributes satisfy all the access structures and an aggregation key concept is used with which One can decrypt more than one file using key aggregation.

Fig: 2 Registration process

Figure 2 shows the registration process for new user or owner in the cloud. The registration process is done with their unique ID card proof for identify his/her trust and

security. The user can login with the user name and password and type. The user can view the user profile.

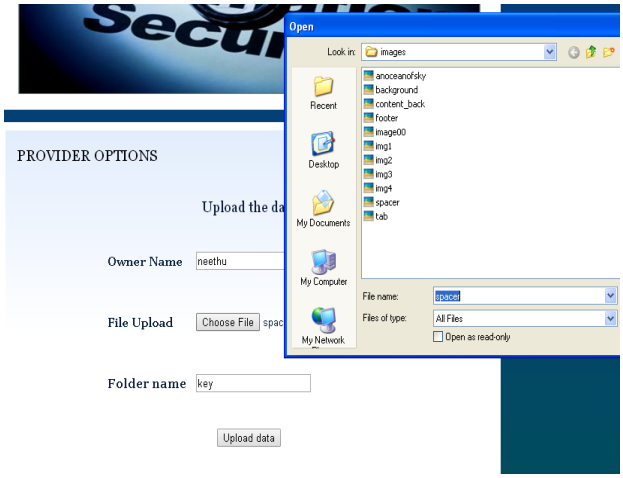

Fig 3: Upload file to the cloud with a key

The user can upload or download or share files in the cloud with their secret key. Figure 3 shows file upload by the user in the cloud with a key. To delete the file from the cloud that is uploaded by the data owner by providing the name which will be verified.

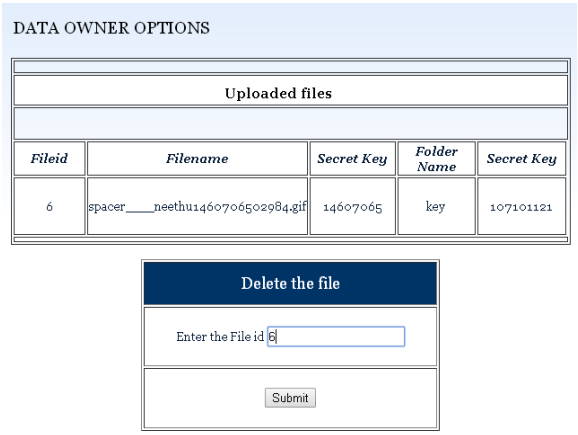

Fig 4: Provide the key for file deletion.

The data owner can delete the file from cloud with the file id of that particular file. Figure 4 shows the screen shot to delete a file from the cloud with its File Id.

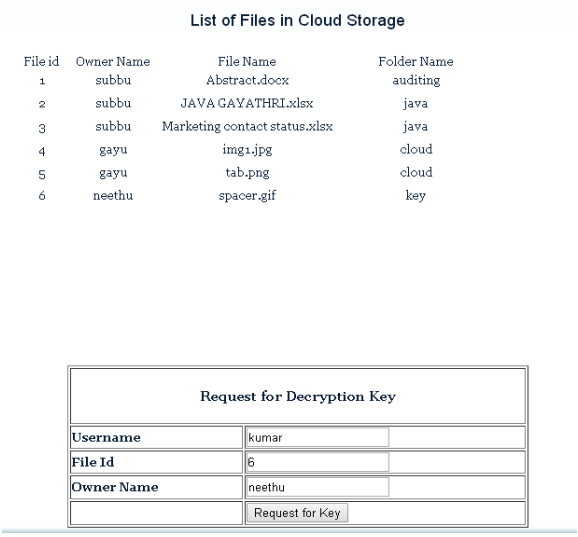

Fig 4: Requesting decryption key from the data owner.

To access a file from the cloud which is encrypted when uploaded the other user rather than data owner request for the key to data owner to decrypt and access the file in the cloud. Figure 4 show the user requesting for decryption key to access the file. The data owner provides secret key to the user with which the user can view the file from the list uploaded files in the cloud storage.

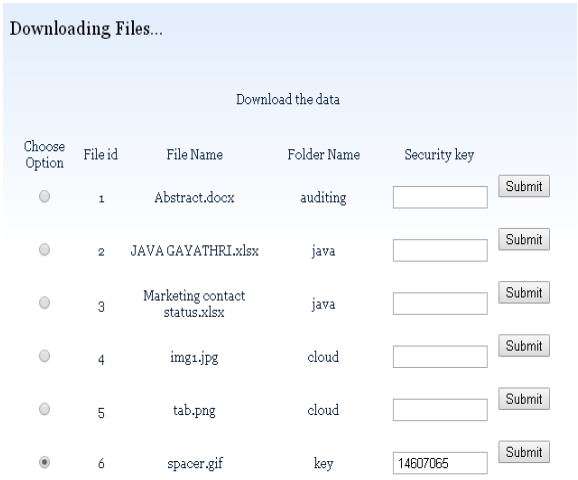

Fig 5: Downloading file

Figure 5 show downloading file by the user from the cloud storage with the key provided by the data owner.

Fig 6: Aggregate file download.

The system also provides aggregate file downloading or more files downloading from a folder of same type with a secret key is the added advantage for the proposed scheme.

VII. CONCLUSION

The system provides the users' privacy and protection with decentralization and issue secret keys to users. A user can obtain secret keys from multiple authorities without knowing anything about the global identifier and attributes and during encrypting a message, the encryptor can select an access structure for each authority and encrypt the message under the selected access structures so that a user can decrypt the cipher text if his attributes satisfy all the access structures. In addition to this key aggregation concept is also included. One can decrypt more than one file using key aggregation concept. The proposed scheme provides the perfect solution for privacy issues and is selectively secure when compare to the previous schemes.

REFERENCES

[1] P. Bichsel, J. Camenisch, T. Gro, and V. Shoup, " Anonymous credentials on a standard java card". InProc: CCS'09 , pages 600–610. ACM, 2009.

[2] M. Chase and S. S. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proc. 16th ACM Conf. CCS, 2009, pp. 121–130.

[3] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[4] H. Qian, J. Li, and Y. Zhang, "Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure," in Information and Communications Security (Lecture Notes in Computer Science), vol. 8233. Heidelberg, Germany: Springer-Verlag, 2013, pp. 363–372.

[5] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6632. Heidelberg, Germany: Springer-Verlag, 2011, pp. 568–588.

[6] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong,and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in Proc. 6th ASIACCS, 2011,pp. 386–390.

[7] A. Beime, "Secure schemes for secret sharing and key distribution,"Ph.D. dissertation, Dept. Comput. Sci., Technion—Israel Inst. Technol., Haifa, Israel, 1996

[8] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust threshold DSS signatures," in Advances in Cryptology (Lecture Notes in ComputerScience), vol. 1070. Heidelberg, Germany: Springer-Verlag, 1996, pp. 354–371

[9] M. Green and S. Hohenberger, "Blind identity-based encryption and simulatable oblivious transfer," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 4833. Heidelberg, Germany:Springer-Verlag, 2007, pp. 265–282.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571. Heidelberg, Germany:Springer-Verlag, 2011, pp. 53–70.

[11] John Bethencourt; Amit Sahai ; Brent Waters "Ciphertext-Policy Attribute-Based Encryption." 2007 IEEE Symposium on Security and Privacy (SP '07) , pp:321 - 334

[12] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. CCS, 2007, pp. 456–465.

[13] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6110. Heidelberg, Germany: Springer Verlag, 2010, pp. 62–91.

[14] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography (Lecture Notes in Computer Science), vol. 4392. Heidelberg, Germany: Springer-Verlag, 2007, pp. 515–534.

[15] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au, "Improving Privacy and Security in Decentralized Cipher text-Policy Attribute-Based Encryption" IEEE transactions on information forensics and security, vol. 10, no. 3, March 2015.