A COLLABORATIVE KEY MANAGEMENT IN CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION FOR CLOUD

[1]Mayur N. Ghuge, [2]Dr. Prashant N. Chatur,
[1]M. Tech., [2]Head of Department,
[1,2]Computer Science and Engineering,
[1,2]Government College of Engineering, Amravati

Abstract : ***With improvement in technology, sharing data with other is convenient. Sharing of cloud based outsource data on mobile devices require some promising in-fracture to secure data over cloud. Cipher-text policy attribute-based encryption (CP-ABE) is a technique, which provides fine-grained access to outsourced data over cloud. However, this technique has some drawback with key management. Front-end device like mobile, tab etc. of client side has limited privacy protection, so if keys are held by them client risk key exposure that is hardly noticed. To overcome these issues collaborative key management protocol in CP-ABE (CKM-CP-ABE) is proposed, In this protocol private are generated issued and stored in distributed manner fine grained immediate attribute revocation mechanism is provided for key update. In this protocol, multiple key authorities manage their attributes independently. Different attribute set are used which allows user to define their own access policy, so at time of decryption client need to match the access policy attribute first many users can be allowed to encrypt/decrypt different part of data. This protocol not only solve problem of key exposure but also help to reduce client decryption overhead.***

IndexTerms - Access Control, Attribute set, Attribute based encryption, Cipher text, key escrow, key exposure, Collaborative Key Management.

I.INTRODUCTION

Cloud computing is a technology that allows software and hardware for computation and storage to be shared on the internet. In recent years, there has been an increase in the usage of cloud computing by governments and companies. This increase in the use of cloud services can be explained by several benefits it provides, namely high mobility and flexible scalability, which can lead to better cost control. However, the increasing shift to cloud-based solutions also raises concerns over the deliberate or accidental disclosure of private data by cloud service provider. Although cloud computing is much more powerful than personal computing, it brings new privacy and security challenges, as users relinquish control by outsourcing their data they no longer having physical possession of it. Consequently, The data owners demand high levels of security when they outsource their data to a cloud; although they usually encrypt their data when storing it in a cloud server, they still want control over it.

In recent years, new methods have developed to complement trust in contractual agreements by encryption models enforcing data confidentially. Direct employment of traditional cryptographic primitives cannot achieve the data security required. Thus, a considerable amount of work has directed towards ensuring the privacy and security of remotely stored shared data using a variety of systems and security models. These have mainly focused on preserving users' privacy while realizing desired security goals, without introducing excessively high levels of complexity to the users at the decryption stage. To solve these issues, Cipher-text policy attribute-based encryption (CP-ABE) has employed to preserve privacy and guarantee data confidentiality against the cloud. In CP-ABE, each user is associated with a set of attributes and the data has encrypted with access structures based on attributes. A user is able to decrypt a cipher text if and only if his/her attributes satisfy the cipher text access structure. However, there are two issues still exist when applying CP-ABE to Cloud data sharing applications directly:

- The outsourced owners lack some effective methods to handle key escrow problem where the so called honest but curious cloud servers attempt to access the outsourced data and may cause privacy leakage.
- The user revocation is extremely hard to implement efficiently.

The existing cryptographic schemes either have privacy flaws or provide security at the expense of performance; therefore, the challenge of achieving the dual goals of privacy preserving with effective cloud data sharing remains unresolved. This lead to the necessity to find a scheme that will ensure data owners privacy and confidentiality over the outsourced data. An enhanced CP-ABE scheme is proposed for outsourcing data securely over cloud by removing the key escrow as well by enforcing fine grained data access control. It explores how user secret keys are generated using secure Two-phase commit protocol (2PC) to overcome key escrow problem and prevent the curious KA or DS from deriving the private keys individually. Proposed scheme achieves immediate user revocation on each attribute set.

II.RELATED WORK

Numerous solutions may be envisaged to exchange encrypted data with a cloud provider in a secure manner, such that the cloud provider is not directly entrusted with key material, but naive schemes often prove difficult to scale.

Sahai and Waters [1] introduced the concept of attribute based encryption (ABE). Instead of encrypting to individual users, in ABE system, one can embed an access policy into the cipher text or decryption key. Besides, ABE also has collusion resistance property, Thus, data access is self-enforcing from the cryptography, requiring no trusted mediator. ABE can be viewed as an extension of the notion of identity-based encryption (IBE) in which user identity is generalized to a set of descriptive attributes instead of a single string specifying the user identity. Compared with IBE [1], ABE has significant advantage as it achieves flexible one-to-many encryption instead of one-to-one, it is envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control.

Goyal, Pandey, Sahai, & Waters [3] were the first team to achieve secure data access control with provable security in cloud computing using KP-ABE. However, by revealing some of the users attributes to cloud, these systems were unable to fully preserve users privacy. Conversely, the HIBE-based scheme [4] utilizes hierarchical encryption to ensure data security in a cloud, but this introduces too many private keys for each user to be managed efficiently. These schemes either have privacy flaws or provide security at the expense of performance; therefore, the challenge of achieving the dual goals of privacy-preserving with effective cloud data sharing remains unresolved.

A Secure Outsourced ABE system has been proposed, which supports both secure outsourced key-issuing and decryption, also rids all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider and a Decryption Service Provide. Leaving only a constant number of simple operations for the attribute authority, eligible users to perform locally and an outsourced ABE construction is proposed which provides checkability of the outsourced computation results in an efficient way [5].

In [6] Liu, Huang, & Liu proposed a new approach for fine-grained access control and secure sharing of signcrypted (sign-then-encrypt) data for personal health recoreds. They call it Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) which satisfies the requirements of cloud computing scenarios for PHR. CP-ABSC combines the merits of digital signature and encryption to provide confidentiality, authenticity, unforgeability, anonymity and collusion resistance

In [7] Cheng, Wang, Ma, Wu, Mei, & Ren present a new efficient revocation scheme where original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. They applied the efficient revocation scheme to the ciphertext-policy attribute-based encryption (CP-ABE) based cryptographic cloud storage. This show that the efficient revocation scheme can reduce the data owner's workload if the revocation occurs frequently.

III. PROPOSED WORK

This propose a collaborative key management protocol in cipher text policy attribute-based Encryption (CKM-CP-ABE) aiming to enhance security and efficiency of key management in cloud data sharing. This proposes scheme for outsourcing data securely over cloud by removing the key escrow during key generation as well by enforcing fine-grained data access control. It explores how user secret keys are generated using secure Two-phase commit protocol (2PC) to overcome key escrow problem and prevent the curious KA or DS from deriving the private keys individually. It also highlights how the proposed scheme does achieves immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the CP-ABE. Figure 1, Shows the model of system, this system is composed of the following parties:

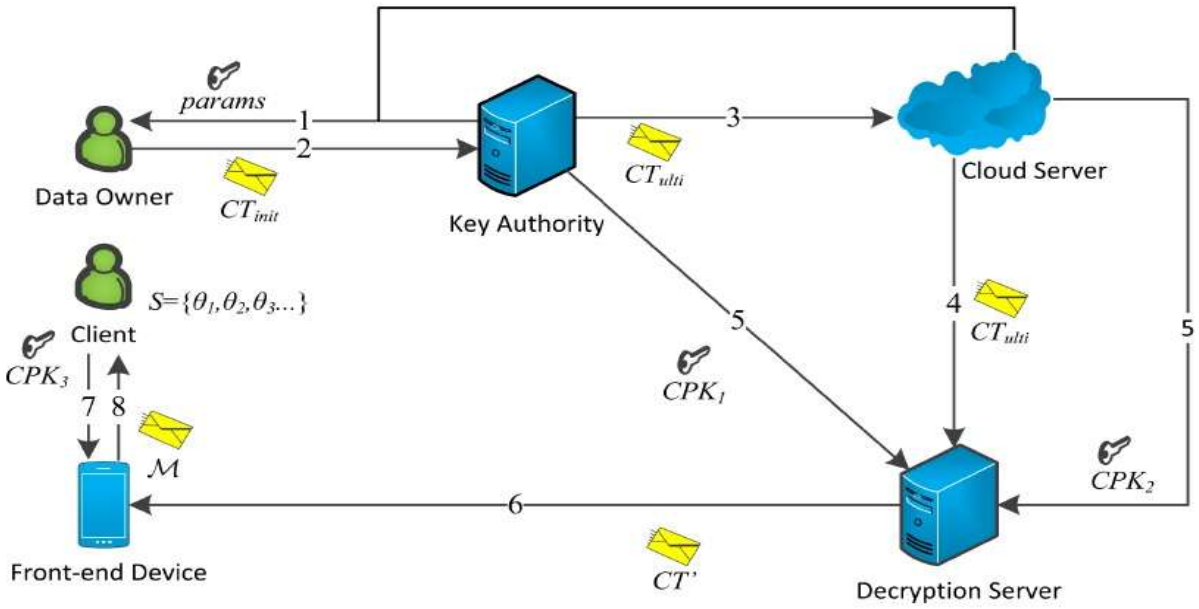

Fig. 1: CKM-CP-ABE System model

1. **Client :** Is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the cipher text and obtain the data.
2. **Key Authority :** 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.
3. **Cloud Server :** 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 corresponding contents services. The data-storing center is another key authority that generates personalized user key with the KA, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control.
4. **Decryption Server :** It is an entity within the organization that authenticates the data owners and users. The DS is involved in generating user key with KA and CS to prevent these two parties to collude and guess the user secret keys.
5. **Data Owner :** It is a client who owns data, and wishes to upload it into the external data storing center for ease of sharing. A data owner is responsible for defining access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it.

Proposed system is based on some assumptions such as:

- Both KA and the DS, are assumed to be semi-trusted. Therefore they and should be deterred from accessing plaintext of the data to be shared; meanwhile, they should be still able to issue secret keys to users. In order to realize this somewhat contradictory requirement,

the two parties engage in the arithmetic 2PC protocol with master secret keys of their own, and issue independent key components to users during the key issuing phase. The 2PC protocol deters them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the KA does not collude with the CS since they are honest. Otherwise, they can guess the secret keys of every user by sharing their master secrets.

- Data owner can not only store data files but also constitute the access policy to his data files.
- The Cloud servers are always online and they are assumed to have abundant storage capacity and computation power. At the same time, a cloud administrator may read the contents of user data stored in the cloud for nefarious reasons or simply out of curiosity. Thus, data stored in the cloud should remain encrypted at all times, and any required transformation of it should not reveal the plaintext in the process.
- All communications between data owners/users and cloud servers are assumed to be secure.

IV. ALGORITHMS

Two-Party Computation:

Flow of this protocol is presented in fig.3 this protocol involve KA & CS in arithmetic computation

- CS and KA engage in secure 2PC, in which it takes input from CS and KA and return private output.
- CS and KA choose random exponent and return to each other.
- KA computes the output that is received from CS and return result to CS.
- CS compute the data received from KA and obtain initial key components.

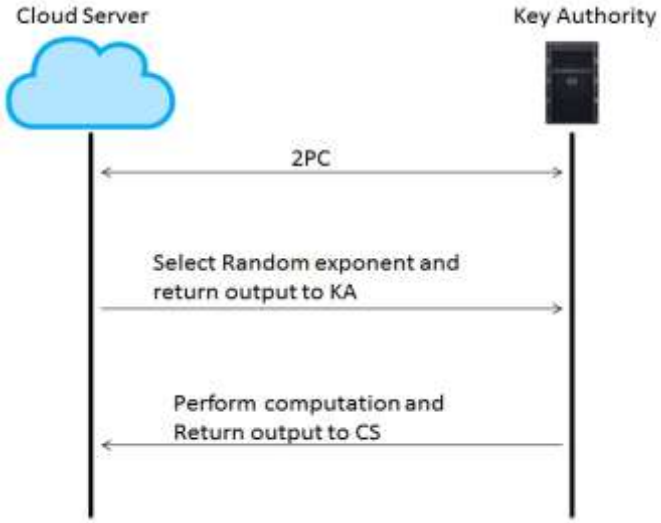

Fig. 2: Two Party Computation

AES Algorithm :

The encryption process uses a set of specially derived keys called round keys. These keys are applied along with other operations, on an array of data that holds exactly one block of data the data to be encrypted. This array we call the state array. The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others. These algorithm are used to file content are convert plaint text to cipher text.

Following are the AES steps of encryption for a 128-bit block:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data.

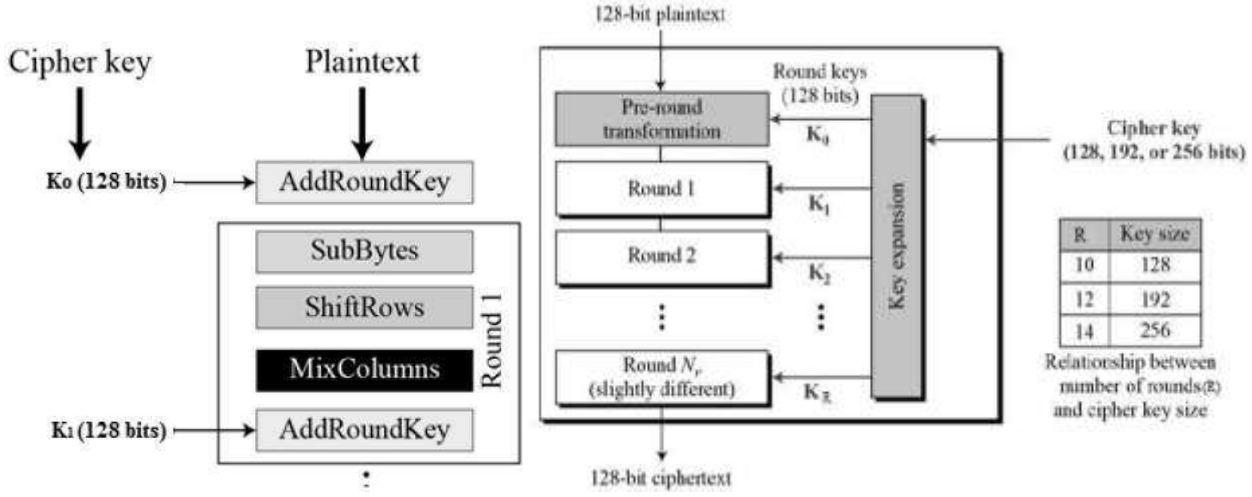

Fig. 3: AES Encryption Process

V. SYSTEM ANALYSIS

5.1 Performance Analysis

Performance evaluation is presented to show the benefit of the proposed scheme compared to previous one. We considered several random access structures and attribute sets that we can meet in a real system. The encryption time of CPA-ABE is linear with the number of leaf nodes of the used access structure. So it's enables fine grained access control to data but induces important processing overhead with complex access policies like the ones used in academic systems. However, measuring the decryption time is more difficult since it significantly depends on the used access tree and the set of involved attributes[11]. To show this, time overhead of encryption and decryption is compute while varying the number of leaf nodes of access structure. Fig. 4 and Fig. 5 present performance evaluation of encryption and decryption operations.

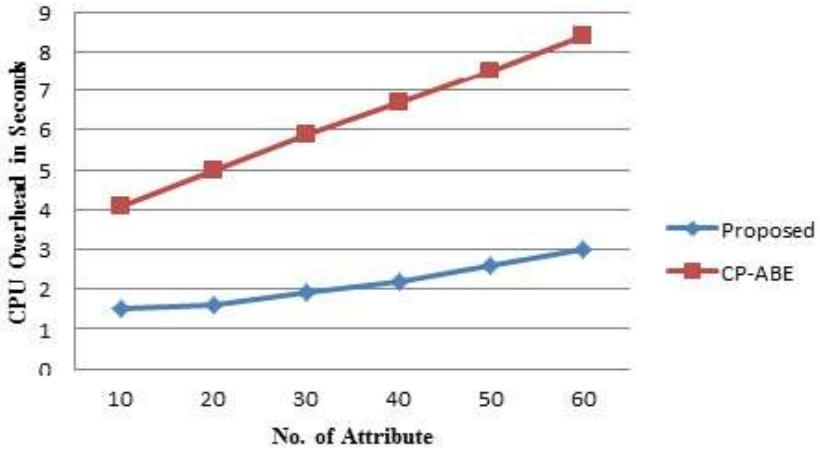

Fig. 4: Encryption Evaluation

CP-ABE consumes more time than our solution in both encryption and decryption[12]. These results match our expectations and show that our control access scheme is more efficient in terms of cryptographic operations. The proposed scheme uses AES to encrypt the data file. Since AES is faster than, the whole encryption and decryption time is reduced. This reduction varies between 5% and 15% for encryption, and between 15% and 20% for decryption in the studied samples. Notice that these performance evaluations consider as the significant gain over previous systems.

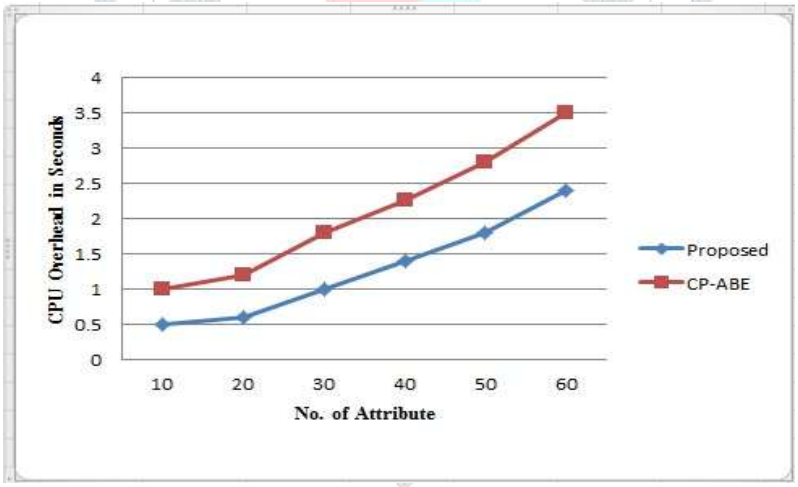

Fig. 5: Decryption Evaluation

5.2 Comparative Analysis

A table summarizing the proposed scheme against previous scheme appears in Table 2. As is evident the proposed scheme offloads more activities from data owner to data storing centre e.g. cloud and minimizes the workload required for key generation and revocation. In comparison to the scheme recently proposed in Hur et al[8], this work involves local authority to address key escrow problem and prevent the assumption that KA and CS will not collude with each other to guess the secret key of every users by sharing their master secrets. User revocation is realized at attribute level in both Hur et al [8], creates a binary key encryption key tree for the universe attribute of users and utilizes to distribute the updated attribute group keys to the users. However, in this work the user revocation is realized by encrypting the updated attribute key under new access structure that prevents the revoked users to decrypt and receive the valid attribute key for data access.

Table 1: Comparison of current protocol with previous protocol

Characteristic	[8]	[9]	[10]	Current Protocol
System Model	Owner, Authority, CSP	Owner, CSP	Owner, CSP, Authority	Owner, CSP, Trusted authority and local authority
Cryptographic technique	CP-ABE	KP-ABE	CP-ABE	CP-ABE
Participating actor in user data encryption task	Data owner	Data Owner	Data Owner, attribute authority	Data Owner

Re-encryption and key generation task	CSP	Data Authority	Attribute Authority	CSP
Mechanism for user revocation	Multiple attribute key generation	Multiple attribute key generation	Multiple attribute key generation	Multiple attribute key generation
Participating actor in cloud data re-encryption task	CSP in lazy fashion	CSP in lazy fashion	Attribute Authority	CSP in lazy fashion
Mechanism for key update	Binary key encryption tree	Process access subtree	Process dual access subtree	Process access subtree

VI. CONCLUSION

The privacy of the data in the cloud-computing environment is a serious issue that requires special considerations. Proposing and implementing an improved CP-ABE scheme to outsource data securely over cloud enforcing a fine-grained data access control and exploiting the characteristic of the data sharing system. The proposed scheme features a key issuing mechanism that removes key escrow during the key generation. The user secret keys are generated through a secure two-party computation such that any curious KA or CS cannot derive the private keys individually. Thus, the proposed scheme enhances data privacy and confidentiality in the cloud against any system managers as well as adversarial outsiders without corresponding 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 CP-ABE. Therefore, the proposed scheme achieves more secure and fine-grained data access control over the data outsourced on cloud.

REFERENCES

[1] Guofeng Lin, Hanshu Hong, And Zhixin Sun, "A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing", IEEE Access on Wireless Communication and Sensor Network Technology, 2017.

[2] Sahai, A., & Waters, B. (2005). 'Fuzzy identity-based encryption'. In Advances in Cryptology EUROCRYPT 2005 (pp. 457-473). Springer Berlin Heidelberg.

[3] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). '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).Acm.

[4] Wang, G., Liu, Q., & Wu, J. (2010, October). 'Hierarchical attribute-based encryption for fine-grained access control in cloud storage services'. InProceedings of the 17th ACM conference on Computer and communications security(pp. 735-737). ACM.

[5] Rafath, N., Ghouri, W., & Raziuddin, S. (2015). 'Security in Cloud using Ciphertext Policy Attribute-Based Encryption with Checkability'. International Journal of Innovative Research in Computer and Communication Engineering.

[6] Liu, J., Huang, X., & Liu, J. K. (2015). 'Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption'. Future Generation Computer Systems, 52, 67-76.

[7] Cheng, Y., Wang, Z. Y., Ma, J., Wu, J. J., Mei, S. Z., & Ren, J. C. (2013). 'Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage'. Journal of Zhejiang University SCIENCE C, 14(2), 85-97.

[8] Hur, J. (2013). 'Improving security and efficiency in attribute-based data sharing. Knowledge and Data Engineering', IEEE Transactions on, 25(10), 2271-2282.

[9] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). 'Achieving secure, scalable, and fine grained data access control in cloud computing'. InINFOCOM 2010, Proceedings (pp.1-9) IEEE.

[10] Ming, Yang, et al. 'An efficient attribute based encryption scheme with revocation for outsourced data sharing control'. Instrumentation, Measurement, Computer, Communication and Control, 1st International Conference on. IEEE, 2011.

[11] Bethencourt, J., Sahai, A., & Waters, B. (2007, May). 'Ciphertext-policy attribute-based encryption'. In Security and Privacy, 2007. SP'07. IEEE Symposium on (pp. 321-334). IEEE.

[12] B.Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptogr., 2011, pp. 53-70.

[13] M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Secur. Symp., 2011, pp. 34.

[14] J. Lai, R. H. Deng, C. Guan, and J.Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354, Aug. 2013.

[15] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 10, no. 10, pp. 2119-2130, Oct. 2015.

[16] M. Chase and S. S. M. Chow, "Improving privacy and security in Multi authority attribute-based encryption," in Proc. ACM CCS, 2009, pp. 121-130.

[17] S. Easwarmoorthy, S. F, and A. Karrothu, "An efficient key management Infrastructure for personal health records in cloud," in Proc. WiSPNET, Mar. 2016, pp. 1651-1657.

[18] D. Pletea, S. Sedghi, M. Veeningen, and M. Petkovic, "Secure distributed key generation in attribute based encryption systems," in Proc. ICITST, Dec. 2015, pp. 103-107.

[19] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). IEEE

[20] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," Proc. ACM Conf. Computer and Comm. Security, 2006.