ATTRIBUTE BASED SECURE DATA SHARING SCHEME WITH EFFICIENT REVOCATION IN CLOUD COMPUTING

Elavarasan .G[1], Dr. S.Veni[2]

ABSTRACT

In recent days, the cloud computing is one of the emerging field. It is a platform to maintain the data and privacy of the users. To process and regulate the data with high security, the access control methods are used. The cloud environment always faces several challenges such as robustness, security issues and so on. Conventional methods likeCipher text-Policy Attribute-Based Encryption (CP-ABE) are considered for providing the data security, but still theproblem exists like thenon-existence of attribute revocation and minimum efficient. Hence, this research workparticularly discussesvarious features of attribute based access control mechanismto maximize the efficiency.Initially, an objective coined out in this work is to definethe attributes for aset of users. Secondly, the data is to be re-encrypted based on the access policies defined for the particular file. The re-encryption process renders information to the cloud server for verifying the authenticity of theuser even though theowner is in offline.The main advantage of this workevaluates multiple attributes and allows respective users who possess those attributes to access the data.The result proves that the proposed Attribute based Secure Data sharing scheme with Efficient Revocation (EABDS)is a fine grainedattribute structure.

Keywords : Cloud computing, Authorization, Efficient revocation, Data encryption key, Security analysis

I. INTRODUCTION

In technical advancement, each personal and sensitive data are stored under remote data storage server. Based on the user requirement the data may be accessed from any location. In such cases, the data transfer and processing may be effectively maintained. If there is anyinappropriate process then the respective user faces serious risk. Hence, it is important to secure the data and give access permission to the particular user. These processes may carefully follow with the mechanism termed as secure and efficient Access Control(AC). As shown in the figure 1, the high-level architecture of cloud computing is illustrated.

The cloud service is separated into three categories, namely cloud Service under consumer side, Cloud service creator and it is controlled by cloud service provider. The cloud provider invests and builds three different types of service architecture layers. The layers are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

[1]Ph.D (FT) Research Scholar, Department of Computer Science, Karpagam University, Karpagam Academy of Higher Education Coimbatore, Tamil Nadu, India
[2]Assistant Professor & Head, Department of Computer Science, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India

Apart from these layers, Business Process as a Service (BPaaS) layer enables these three layers by SaaS as top layer, IaaS on hardware and PaaS is coupled above IaaS. By considering all these layers, the cloud provider needs to integrate and enable all the layers to provide exact service to the user.

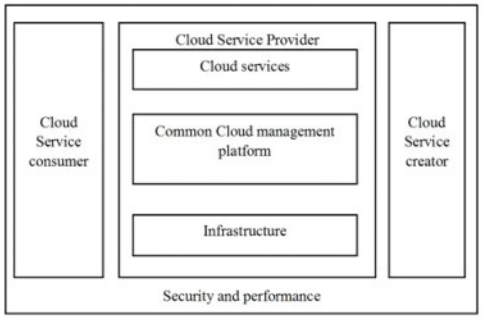

Figure 1. Cloud Computing Architecture

The user gets proper service through Application ProgrammingInterface (API), based on the requirement the user can pay the amount and utilize it. This process is provided by cloud storage services (e.g. Google Drive and Microsoft OneDrive). The cloud storage service has several challenges to maintain the privacy and security.While entering into sensitive data, the privacy is to be maintained at safe and secure. Some traditional methods store the data directly without any encryption. Hence, there is a need for encryption processto handlesensitive data. This encryption module kept before the user uploading unit.

In conventional methods, the user utilized the symmetric-key algorithm for encrypting the data. At some time the user need to retrieve the data there is a need for decryption using a symmetric key.However, it is not secure because the user shares data withthe other users. To overcome this problems the private key is considered for evaluating the data security. But in shared conditions the user can encrypt the data with the help of shared user'spublic key. Since, the problem occurs due to three critical tasks. Initially, the data owner needs to obtain the public key which is considered on encryption side. Next, the there is a need for storing the data repeatedly. Finally, it results in utilization of large resources leads re-encryption of data. In order to solve these problems, the proposed research methodology focused on attribute based controlling strategy. In 2005, the authors Sahai and Waters proposed an Attribute-Based Encryption (ABE)scheme for utilizing the user's identity as attributeto encrypt anddecrypt the data. The ABE concept utilizes the user's identity to verify the public key and reduce the repetition of data. The advantages of attribute based encryption is that the computation time is reduced for decryption, re-encryption and downloading the entire data.

In this research part, the construction of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is addressed and analyzed with the Hur's scheme. To address and find the problem, some techniques arereviewed based on encryption and decryption. In this system framework, a user key will be associated with an arbitrary number of attributes which is expressed as strings. The main objective of this

research is to focus on implementing the new concepts for certifying the security, integrity and authenticity for cloud data storage. These objectives are needed because the outsourced data requiresflexible accesscontrol for users. In existing methods, the access controlmodule requires to share the sensitive data. Therefore, in this work a desirablemethod that the access policy of the data will be controlled by the attribute authority and partial encryption and decryption data owner.

The main contributions are listed as follows.

1) This paper introduces a new opinion for Data Sharing Attribute with efficient Revocation.
2) Several encryption, decryption and key generation methodologies are reviewed.
3) A new scheme is proposed to adapt the encryption and decryption standards.
4) To verify the effectiveness, the proposed Enhanced Attribute based Secure Data sharing scheme with Efficient Revocation (EASDE) is compared with the existing two modules namely, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Hur's Scheme are considered for comparison.
5) Make scalable and fine-grained access control.

The remaining part of this paper is organized as follows: In section II, the detail survey is carried out with detail description of traditional methods used for encryption, decryption and secret key components. The functional evaluation and requirements based on the problem identification is given under the section III. The research methodology is carried out with detail block diagrammatic representation in section IV. Under section V, the performance evaluation is carried out to compare the existing two methods with the proposed method to find the optimal solution. Finally, the paper is summarized in the section V and suggested some future extension.

II. Literature Review

Some traditional methods are discussed under this section. The Identity-Based Encryption (IBE) is one of the alternative ways to public key encryption. It reduces the complexity in Public Key Infrastructure (PKI). While considering the Private Key Generator (PKG), the efficient revocation is not achieved because of overhead computation. Hence, Li et al., (2015) introduced an outsourcing computation into IBE. It supports key generation,key-issuing and key-update processes with several offloads. Apart from this model, the Refereed Delegation of Computation model is also constructed for providing secure transfer.

In public key cryptosystems, the revocation functionality is considered as an important task and many researchers concentrated on this topic. Revocation is forced because of secret key corruption or it expires. Another aspect is reducing the workload in delegation of key generation module. Hence, Seo et al., (2013) introduced the revocation process to efficiently reduce the workload. It also

considered the Decisional Bilinear Diffie-Hellman assumption to manage the open problem addressed by Libert and Vergnaud (2009). Similarly, Liang et al., (2013) carried out the research in Cipher text-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE). It coined out the Chosen-Cipher text Attacks (CCA) problem to manage the security. It is constructed under random oracle model. It also explained with the help of real time medical data sharing.

Liang et al., (2014) defined the notion for Proxy Re-Encryption (PRE). The methodology used here is to encrypt the ciphertext based on the arbitrary length index. It helps to improve the flexibility of users and provide proper decryption process.In vast internet services, the configurable computing resources are the main module in providing the efficient data sharing. Sur et al., (2013) introduced the certificate-based proxy re-encryption under different data outsourcing scheme. Qian et al.,

(2015) particularly concentrated on Personal health record (PHR) service. In medical field, the cloud storage plays a major role in providing the information exchange. For this purpose, the storage is managed by the third parties and may exposure to user data. They proposed a privacy-preserving PHR that supports fine-grained access control and efficient revocation.

The Naruse et al., (2015) identified the problem in CP-ABE and provide Linear Secret Sharing Schemes (LSSS) access structure without any key generation scheme. It is processed by allocating the encryption scheme and delegating the revocation process for providing the support and maintains the secure module by totally eliminating the attacks. In some cases, the security models are invented by hidden policies based on AND-gate access structure. But still the problem exists. Hence, Xu and Lang (2015)introduced a tree-based access structure CP-ABE scheme with hidden policy (CP-ABE-HP).

Han et al., (2014) proposed a privacy-preserving decentralized CP-ABE (PPDCP-ABE) scheme. Nowadays online social media plays a vital role among entertainment. Facebook, Twitter and Myspace are the best example. Based on the Online Social Networks (OSNs) several researchers were focused, likewise Jahid et al., (2011) introduced a method Encryption-based Access Control in SocialNetworks with Efficient Revocation (EASiER). It deals with the attribute-based encryption by dynamic group membership. It is applied as a prototype application in face book. Similarly, Sun et al., (2010) proposed a privacy preserving scheme.

The traditional methodnamed as threshold ABE system is carried out by Sahai and Waters (2005) results in limitations, (i.e.,) the threshold semantics are not very expressive and it limits the overall design. To overcome such effects the Goyal et al., (2006) introduced the key-policy attributebased encryption system. The overall design is carried out by constructing a user's key associated with tree access structure by accessing the ciphertext

associated with a set of attributes. It is the extended work of Sahai-Waters techniques.

Chase and Chow (2009) discussed some advanced access structures for providing the encryption scheme by constructing the attribute of a ciphertextpolicy. It's main motive is to improve the attribute revocation efficiency. Since, it has some limitation while utilizing the high-level system requirement. Similarly, the usability limitation is identified in Bethencourt et al., (2007). The Authors concentrated more on cipher text based policy attribute encryption. It focused on several distributed systems, in that if a user passes a certain set of attributes then a user should only be able to access data. Its objective is to improve the expressiveness of access control scheme by removing the limitation that in a cipher text at most once each attribute can only appear.

Goyal et al., (2008) presented a bounded ciphertext policy attribute based encryption. It support advanced access structures and several number of theoretic assumption to provide security proof. The advantage mentioned here is performance improvement by decreasing the network traffic and its limitation iscommunication capacity is very low.

Database system is the prerequisite for day-to-day business that holds a lot of sensitive Information. Hence, database management and its security become essential as the measure of database growth. Access control model outlines which who can perform which operations on which data. Discretionary and Role based access control model and the alternative way to maintain the database security that provides confidentiality, Integrity, availability.

In most existing cases, different domains attributes are managed by each authority. Likewise, the author Chase(2007) gave an implementation ofmulti-authority attribute-based encryption system. The only challenge faced by multi-authority ABE is collusion attacks between users. To design such systems there is a need for finding the expressive ABE systems. The encryption module is to be designed by following all these conditions and provide more advantageous. The Key Encryption Keys (KEKs) are used to construct the auxiliary keys for key management.

Hota et al., (2011) proposed a modified DiffieHellman key exchange protocol byaddressing a challenging problem in capability based access control technique. The problem identified is that the outsourced data can access only by the valid users and creates the problem of key distribution. Akinyele et al., (2011) carried some research with medical records. It is designed to store the data by generating the self-protecting Electronic Health Record (EHR). It results in advantage because the storage can be accessed even if the health provider is offline. Since, it the medical institutions are used here to encrypt the plaintext data and it is stored in a hospital SSL web server. Then the data is accessed by the user by decrypting the data using ABE private key. Finally, the process is completely stored in a Google health server. To realize exact and fine-grained access control, this section reviewed some recent topics. Further, the problem is identified and listed in upcoming section.

III. Problem Definition

According to the above studies and methods, some basic requirementsand functional evaluations are considered based on the performance. Initially, the data confidentiality is to be maintained while encryptingthe data.Next important task is maintaining the fine-grained access control. It states that each user has unique way to access the own data, even if the users exist in a group the access right may not be thesame.Next, backward secrecy is to be maintained to follow the access policy. Finally, the important need is user revocation. If the user leaves the cluster, the theme will revoke the user's access right from the cloud storage server. The revoked user cannot access any shared information within the cluster, as the result a user doesn't have access right. If all the above requirements are satisfied then the scalability is achieved properly. To verify all these requirements and evaluation, the Hur's scheme and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) are particularly analyzed to compare with proposed method.

IV. Research Methodology

In local data management, the data owner (DO) is used to store large amounts of data in cloud by reducing theoverall cost. In many existing systems, the security is one of the serious issue because, if the data protection mechanism is disabled then the cloud service provider (CSP) access all the data of the user. These issues may results in serious limitation and CSP may utilize the data for commercial benefits. Hence, it is one of the toughest challenge present in the cloud computing. It is rectified by issuing fully trusted Key Authority (KA). Then, the expressiveness of attribute set is another concern to solve this issue.

In many existing standards, CP-ABE has the access policy which is one of the binary state over attributes. It is represented as "1 - satisfying" and "0 - not-satisfying". The Key-Policy Attribute-Based Encryption (KP-ABE) is a set of attributes of the privacy key need to satisfying the access policy. It helps the user to decrypt the encrypted data. Apart from this the user can't obtain the encrypted data. Similarly, the CP-ABE scheme implies that the access policy is associated with the encrypted datawiththe user's set of attributes to describe the user's private key. In these cases, the encrypted data satisfies the access policy based on the defined attributes set. Hence, the user can decrypt the encrypted data.

The Cipher-text attribute based scheme manages the tree access policy which is selected by the encryption unit. Similarly, decryption follows the encryption standard. It helps to decrypt the data very easily and secure. Hence, CP-ABE is selected instead of KP_ABE. The pseudo code flow for CP-ABE is represented as follows:

i. Initializing the input security

ii. Take input message 'M',

iii. Start encryption with credentials and policy

iv. After completion perform decryption by considering the input 'M' and 'pk'

v. Compare if two input matches then perform decryption.

vi. Else exit.

The author Hur proposed several phases of access control schemes. In that an immediate attribute revocation technique is processed by combining the CP-ABEwith Naor (2001) algorithm named as minimum subset-cover. It utilizes the binary Key Encryption Key (KEK) tree to deliver the keys in group. However, it has some drawbacks with regard to security and scalability. To overcome this issue, an improved security scheme is proposed by same author by considering a key escrow problem and user revocation in attribute-based data sharing.

The new efficient revocation process is carried out by the following steps.Initially, the Key attributes authority assigns the control section. It provides the public key generation to maintain the encryption and decryption. Then the private key is generated for maintaining the client which is used for decrypting the file. These keys are maintained by the key server. The access key is built for encryption process with the user role. The algorithmic overall process is listed below.

i. Initialize and Setup the security parameter. It is processed by Trusted Authority (TA).

ii. Generate the key 'M','PK' and 'A'. Where, M is the master key, 'PK' is the set of public parameters and 'A' is the set of user attributes. The given secret key is transferred to the Data Users(DU).

iii. The algorithmic model enables the encryption to process the M as encrypted data and T as access structure. Throughout the process is controlled by Data Owners (DO).

iv. Re-Encrypt is a process run by Cloud Service provider (CSP). The access structure is controlled by the set of attributes. The unique identify is processed by the attributes keys to revoke the user list.

V. Finally, the decryption algorithm runs by Data Users by considering the input public key parameters with the output access structure.

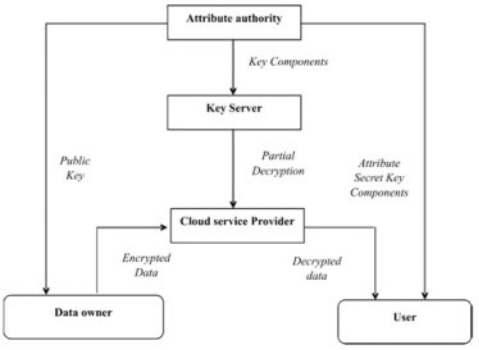

Figure 2. Proposed Efficient Revocation scheme

The system model is framed by initializing the generator as *gi* of a bilinear group $G_{n.}$ the bilinear mapping function is denoted as $e:G_{n0}*G_{n0} \rightarrow G_{n1}$. Here the security size of the group is denoted as 'k'.

by considering all these parameters, the setup phase initialize the public parameters

as $PK = G_{no}, g, h = g^{\beta}, e(g, g)^{\alpha}$

$MK = (\beta, g^{\alpha})$

Where, α and β are the two random variables.

After completion of master key, the secrete keys with some attributes are processed by DUs are listed.

$$D = \frac{g(\alpha + r)}{\square}\beta$$

The re-encryption is based on combining the initial key and the access policies defined for the particular file. It helps to maintain the renders information to cloud server for verifying the authenticity of user even though the owner is offline. The re-encryption process combines the outsourced data from Cipher Text to transfer it to data owners. The algorithmic role is to make the CSP active while the encryption and server is offline. It helps in updating the each attribute revocation event under revoked user list. This results in a exact expressiveness of the access policy and privacy is preserved. The dynamic revocation helps to modify the access policies or file attributes.

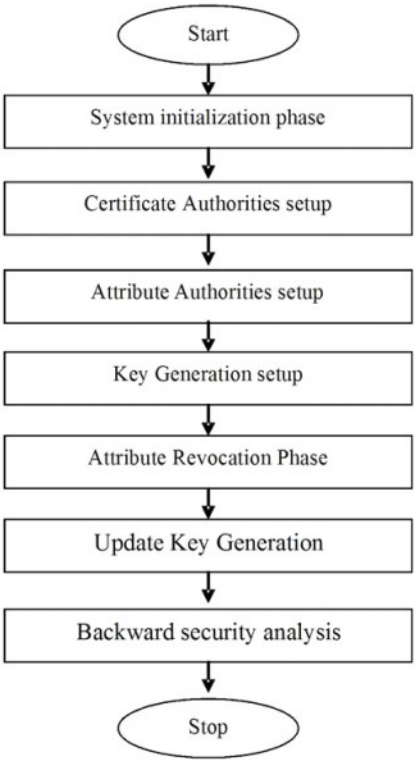

Figure 3. Flow Chart for proposed EABDS scheme.

The proposed access control scheme is controlled by several modules. The system initializes the values to generate the key with respect to the Certificate Authorities (CA). Then CAselects some random values as master key and performs the security access. The Attribute Revocation Phase will update the keys with respect to the key generation process. The revoked key is updated to provide the forward

security. Finally, the processes are tested by adding new users and provide sample attributes to satisfy the access policies.

V. Performance Evaluation

The performance analysis of proposed scheme is carried out by comparingwith traditional Hur's Scheme and CP-ABE in terms of key generation time, encryption time and decryption time. This investigation provides a revocable Fine-grained scheme that can support efficient attributerevocation. It is also an effective data access control scheme for multi-authority cloud storage systems. While considering the attributes the decryption overhead for users is reduced indirectly.

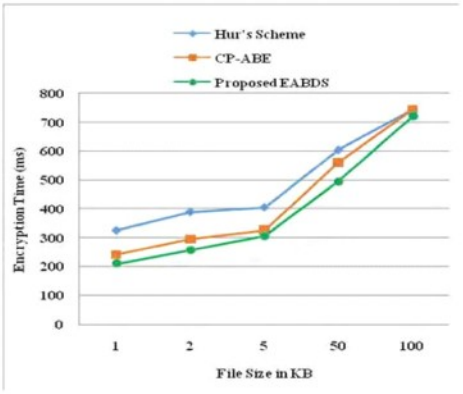

Figure 4. Encryption time comparison

As shown in the figure 4, the encryption time is compared to find the computation efficiency between our scheme and traditional methods. The time of encryption is more or less linear with respect to the file size. The proposed encryption unit is more efficient because the owner first encrypts the data by with the help of certificate authority and sends the ciphertext to the attribute authorities before sending it to server. The process is simplified by random value generation. The Least encryption time of a file size 1KB is 215ms and its maximum encryption time is 721ms at 100KB of attributes. This evaluation helps to improve the performance of EABDS scheme. Table I shows the comparison between proposed EABDS scheme and two traditional schemes. The proposed scheme spends less computation cost than Hur's Scheme while doing encryption and decryption.

Table I Comparison of computation cost

		Hur's Scheme	CP-ABE	Proposed EABDS Scheme
User (Decryption)		(k+log *l*) exp +(sk+1)	Exponent Calculation + paring	Exponent Calculation
Cloud (Decryption)		0	A finite field of the order that has the potentialto increase decryption time	0
Re-vocation	Re-vocation applicants	User	Attribute Authorities	User
	Key updating of other user's	Yes	Yes	No
	Re-Encryption	Yes	No	Yes

The key generation processes enables the Attribute Authorities outcome and provide secure

identification to the cloud server. During this process, the computation time is to be noticed for generating the effective key. The maximum key generation time is 122ms in proposed method. While increasing the number of attributes the time sequence is also increased. If it is maintained as low as possible, then the revocation process results in simple manner. Figure 5 proves that the proposed scheme has least key generation time when comparing it with other two conventional models namely Hur's scheme and CP-ABE.

Another important aspect is decryption time which is represented in figure 6. The user need to recover the data as it transmitted from the server. Hence, decryption module is also one of the key verification to provide secure process. Correspondingly, the user should first decrypt the model with its own key and decrypt the data along with the secret key. In this proposed scheme, the user utilized the secret key for performing the decryption, which is more efficient than the other concepts.

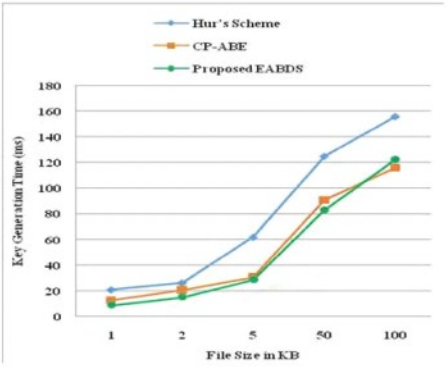

Figure 5. Key generation time with respect to user attributes

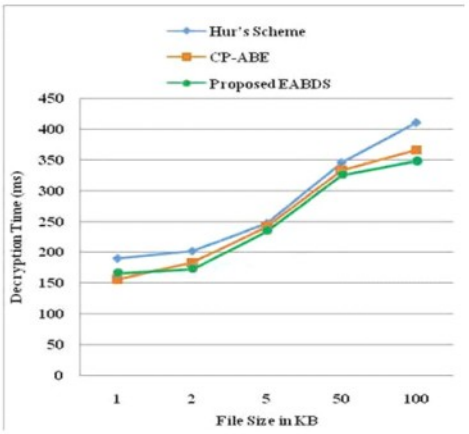

Figure 6. Decryption time representation

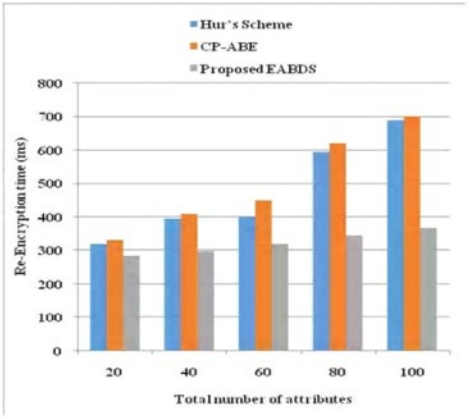

Figure 7. Re-encryption analysis

The re encryption process is shown in the figure 7. The Re-Encryption (RE) is a useful process that allows a data owner to delegate the access rights of the encrypted data which is stored in a cloud storage system. The Re-encryption process helps to maintain the attribute-based encryption setting to another encryption under a new access policy. For this process, the re-encryption time is analyzed here to maintain the effectiveness of the revocation scheme. It is summarized that the proposed EABDS scheme has the difference of 52% then the CP-ABE scheme.

VI. Conclusion

In this research, we have proposed new efficient attribute based data sharing scheme that overcome many of the cited difficulties. The presented access control models address some requirements for minimizing the encryption time, decryption time, re-encryption time and key generation time. It is reviewed and carried a flexible, trust-aware fine-grained access framework for attribute based access control mechanism. The implementation gives access to the models that suit the requirements of cloud computing security issues. The encryption unit has low computation time that proves it is efficient when the attributes varies. Similarly, the key updating process and revocation process utilized the whole module of access control. In future, extend this work by incorporate heterogeneity in the access control mechanism. Further, the model can be extended to performmore security of data with less computation complexity.

References

1. Akinyele, J. A., Pagano, M. W., Green, M. D., Lehmann, C. U., Peterson, Z. N., & Rubin, A. D. (2011, October). Securing electronic medical records using attribute-based encryption on mobile devices. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 75-86). ACM.

2. Chase, M. (2007, February). Multi-authority attribute based encryption. In Theory of Cryptography Conference (pp. 515-534). 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. Han, J., Susilo, W., Mu, Y., Zhou, J., & Au, M. H. (2014, September). PPDCP-ABE: privacy-preserving decentralized ciphertext-policy attribute-based encryption. In European Symposium on Research in Computer Security (pp. 73-90). Springer International Publishing.

5. Hota, C., Sanka, S., Rajarajan, M., & Nair, S. K. (2011). Capability-based cryptographic data access control in cloud computing. International Journal of Advanced Networking and Applications, 3(3), 1152.

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

7. Jahid, S., Mittal, P., & Borisov, N. (2011, March). EASiER: Encryption-based access control in social networks with efficient revocation. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 411-415). ACM.

8. Li, J., Li, J., Chen, X., Jia, C., & Lou, W. (2015). Identity-based encryption with outsourced revocation in cloud computing. Ieee Transactions on computers, 64(2), 425-437.

9. Liang, K., Au, M. H., Liu, J. K., Susilo, W., Wong, D. S., Yang, G., ... & Xie, Q. (2014). A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, 9(10), 1667-1680.

10. Liang, K., Fang, L., Susilo, W., & Wong, D. S. (2013, September). A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. In Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on (pp. 552-559). IEEE.

11. Libert, B., & Vergnaud, D. (2009). Adaptive-ID secure revocable identity-based encryption. Topics in Cryptology–CT-RSA 2009, 1-15.

12. Naruse, T., Mohri, M., & Shiraishi, Y. (2015). Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating. Human-centric Computing and Information Sciences, 5(1), 8.

13. Qian, H., Li, J., Zhang, Y., & Han, J. (2015). Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. International Journal of Information Security, 14(6), 487-497.

14. Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 457-473). Springer Berlin Heidelberg.

15. Seo, J. H., & Emura, K. (2013, February). Efficient delegation of key generation and revocation functionalities in identity-based encryption. In Cryptographers' Track at the RSA Conference (pp. 343-358). Springer Berlin Heidelberg.

16. Sun, J., Zhu, X., & Fang, Y. (2010, March). A privacy-preserving scheme for online social networks with efficient revocation. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). IEEE.

17. Sur, C., Park, Y., Shin, S. U., Rhee, K. H., & Seo, C. (2013, July). Certificate-based proxy re-encryption for public cloud storage. In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on (pp. 159-166). IEEE.

18. Xu, R., & Lang, B. (2015). A CP-ABE scheme with hidden policy and its application in cloud computing. International Journal of Cloud Computing, 4(4), 279-298.

19. Yang, K., & Jia, X. (2014). DAC-MACS: Effective data access control for multi-authority cloud storage systems. In Security for Cloud Storage Systems (pp. 59-83). Springer New York.

20. Chase, M., & Chow, S. S. (2009, November). Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 121-130). ACM.

21. 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

22. V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded Cipher text Policy Attribute Based Encryption," in Proc. 35th Int'l Colloquium on Automata, Languages, and Programming (ICALP'08), 2008, pp. 579-591.

23. Naor, D., Naor, M., & Lotspiech, J. (2001, August). Revocation and tracing schemes for stateless receivers. In Annual International Cryptology Conference (pp. 41-62). Springer Berlin Heidelberg.