SECURE AND ENERGY EFFICIENT DATA SHARING IN PUBLIC CLOUD THROUGH MOBILE DEVICES

A. K. JAITHUNBI
Research Scholar, Anna University, Chennai, India
jaithunbi28@gmail.com

S. SABENA
Assistant Professor, Anna University – Regional Centre, Tirunelveli, India
sabenazulficker@gmail.com

L. SAIRAMESH
Visiting Faculty, Anna University, Chennai, India
sairamesh.ist@gmail.com

Abstract: *The people wants to reduce the search time and retrieve the relevant information by using the cloud database instead of search the data in all over the internet. In this most of the service providers make their database as public that will be used by any people who wants to store and share the data in closed group and they want to access in mobile environment. But, while sharing data among multiple users of multiple owners requires identity privacy to obtain the specific owner's data. In this paper, a secure data sharing scheme for individual users for specific data owner is proposed to retrieve the data in the public cloud through mobile devices. By creating individual signature for individual user with respect to each group and broadcasting encryption techniques dynamically. This proposed system uses Individual User attribute based encryption (IU-ABE) for encryption and decryption of storage information and access by any mobile devices in an energy efficient manner. Meanwhile, the storage overhead and encryption computation cost of proposed system are independent based on the number of users access the data.*

Keyword: *attribute based encryption, digital signature, data sharing, energy efficiency, mobile device, security*

1. Introduction

Cloud computing is defined as a model for providing a convenient on-demand network access. It mainly used for sharing resources as a platform, storage and application servers. Sharing and utilizing the data in the mobile environment is the primary issue in public cloud before handling the transactions of files among the servers in any locations. Service providers are the responsible for making the security of enhancing the data and availability of data only for the authorized users. The only solution is to provide the cryptographic techniques to the data sharing among the closed user group in public cloud through mobile devices. Many cryptographic techniques are offered for data security in this type of environment. Among them, digital signatures provide the authentication and authorization to the data owner for view and update the information in public cloud. Mainly, we need the secure for sharing the data securely among the group. For that, digital signature provides the better authentication for the users among the user where only the authorized users can view and update the information. Digital signatures enable the "authentication" and non-repudiation of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

One of the most fundamental services offered by cloud providers is data storage from the data owners can access the information through any mobile devices. However, it also poses a significant risk to the confidentiality of those stored files and access through any kind of devices. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans while sharing information among other user's. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to many challenging issues such as energy efficiency, computational cost and processing power for mobile devices.

2. Literature Survey

Cloud security is one of the major researches where the cloud service needs to increase their efficiency. Cloud security includes the access control, authentication through digital signature, algorithms for key generation and cipher text. Some of the related works for secure cloud environment using ABE are discussed in this section.

In [1], authors proposed a access control module in distributed manner. In their approach they did not provide client verification. Moreover their work only achieves multiple read and single write i.e, the different clients are allowed to read the data but only the owner of the data are allowed to edit the data that were stored in cloud. In [2], article discussed about access control which gaining more important in online social networking where users store their data and share among a selected group. In this case security and privacy are groups. In their work they encrypted the data under few strategy where an Attribute Based Encryption (ABE) is utilized. They were also proposed only the client with matching set of attributes are able to decrypt the saved data. Re-encryption technique proposed in [4] where the encrypted data is again re-encrypted. This methodology helps to avoid the problem that occurred once the user revocation occur. If any user exit from the group then the user can try to re-enter the group with their colleague id. This methodology helps to avoid re-entry of revocated user. The article [3] proposed an access control gives privacy preserving authentication in cloud. In this framework they proposed a centralized approach where single key distribution center contains secret key and attributes of all users. In this scheme they provide a symmetric key approach. The main disadvantage of this approach is single KDC which leads to single point failure.

Another work proposed in [5] shows enhanced security for cloud data with the combination of digital signature and encryption algorithm. In this paper, authors explain the performance of MD5 and SHA-512 digital signature algorithm with the combination of ECC, AES, RSA and other symmetric key algorithm. Finally, they conclude that the combination of ECC with SHA-512 will provide the better security than other techniques. But this combination needs more time for signature generation and verification when compared to other existing technique.

In [7], researchers proposed a Key-aggregate searchable encryption and instantiating the concept through a concrete KASE scheme, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. In [6], multi authority access control mechanism is described to provide a secure and trust for public cloud storage.

CLOAK is based on stream cipher and takes the help of an external server for the generation and distribution of cryptographically secure pseudo-random number (CSPRN) given [8]. In order to enhance the security of our protocol, they use the concept of symmetric key cryptography. In CLOAK, the core encryption or decryption operation is performed within the mobile devices to secure data at its origin. The security of CSPRN is ensured using deception method. In CLOAK, all messages are exchanged securely between mobile and the server with mutual identity verification.

SeDaSC method [9] provides Data confidentiality and integrity, Access control Data sharing (forwarding) without using compute-intensive re-encryption, Insider threat security and forward and backward access control. The comparison is based on the time consumption during key generation when the group is created and on the turnaround time for encryption methodology provides assured deletion by deleting the parameters required to decrypt a file.

Two specialized encryption mechanisms that support secure image reproduction from encrypted candidate selection is described in [10].Two vital observations: 1) The correlation between two images can be measured by the number of matched features, i.e., the more matches they share, the more similar they are. 2) The matched features can be detected by the concept of LSH, i.e., the more common LSH keys two features have, the more similar they are. Honest-but-curious is a Threat Assumption. Leveraging the correlated encrypted image datasets to enable a secure and efficient cloud-assisted data sharing service for mobile devices with privacy assurance where up to 90 percent of the bandwidth consumption and a considerable energy cost at the mobile client can be saved.

3. Proposed System

Secure data sharing in dynamic group environments needed the group signature and broadcasting techniques to share the information and keys among them. This may lead to the unwanted signature generation for all users who are all don’t require the data from the specific data owner. And also user revocation also lead to heavy overhead to provide the group signature for all the user’s when the individual single user required the data from the particular data owner.

The approach discussed in this proposed system is to provide decentralized access control approach that supports anonymous authentication without knowing the users identity before storing data. Only valid users who are matches with signature and keys are able to decrypt the stored data. It also supports creation, modification and reading data that stored in cloud. An Individual User Policy Attribute based encryption (IUP-ABE) technique is used where data are encrypted and decrypted based on user requested attributes.

To achieve secure trusted data sharing for dynamic groups in the cloud, we expect to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users. Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the cipher text increase with the number of revoked users.

Thus, the heavy overhead and large cipher text size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this challenge, the group manager computes the revocation parameters and makes the availability of data by migrating them into the cloud. Such a design can significantly reduce the computation over head of users to encrypt files and the cipher text size. Specially, the computation overhead for user's encryption operations and the cipher text size are constant and independent of the revocation users. We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. The untrusted environment represents not only the cloud database and also the access device which get information through the proper credentials. The data owner can access the data from any device such as laptop, mobiles, etc., by using their credentials. If this is the case, then there is a need for energy efficient mobile environment for do all computational perspectives. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

System initialization can be done by creating a cloud architecture in which data owner creates an account with cloud server. Further, more users can join with data owner to share files. This is possible through making a request to data owner. During registration process users need to fill their personal information which will be evaluated by data owner to provide an approval for data access in cloud. Once, user got registered with the cloud system, he is free to access any file until life time expiry or revocation on the basis of request. Initially, Data Owner collects attributes relevant to the data file units and are encrypted, then uploaded to cloud server. Policy engine used in the system automatically runs and generates access structure of the data file. Also, generates user's public key. Once the access structure satisfies the attributes given by the user the decrypted file can be downloaded by them.

User Registration is after successful creation of cloud setup, users need to get registered with the system through user registration process. While registering, users need to submit their personal details for completion of registration process. But, the system guarantees Identity privacy. During registration process, user got unique identity I and access structure T. This generates secret key S k for I. Data file F can be then encrypted by using I's Public Key P_k to generate Cipher text C. User revocation is the process of removal of user from system user list which is performed by Data Owner. The system keeps Revocation List (RL) for each attributes. For the user to be revoked, his access structure is removed from RL, so that they can't have more access to cloud.

File Upload is that, before uploading files, Data Owner assign File identity ID to selected data files and then encrypts file using his public key P_k. Along with encryption attributes for encryption is added. File Access is Users can access data files if they have valid secret key. While accessing files, user's secret key is validated against access structure of the user. If it satisfies user’s access structure, decrypted data file can be downloaded by Data Consumer.

File Deletion can be performed by Data Owners, if they no longer needed that files. For file deletion, Data Owner wants to provide File Identifier along with secret key. If owner’s signature is verified successfully then cloud server positively deletes the file with specified identity.

For implementation 3 algorithms are used, details given in below.

Algorithm 1: Key Generation

```
Step 1: Input Private key (A, x), and System parameter (P, U, V, H,W) And data M.
Step 2: Select random numbers
Step 3: Set and Computes the following values$T_1$,$T_2$ ,$T_3$ ,$R_1$,$R_2$,$R_3$,$R_4$,$R_5$
Step 4: Set c =f(M;$T_1$; $T_2$; $T_3$;$R_1$;$R_2$;$R_3$;$R_4$;$R_5$) Construct the following numbers
Step 5: Return = ($T_1$, $T_2$, $T_3$, c )
Step 6: Generate a valid group signature on M.
```

Algorithm 2: File encryption

```
Step 1: Set System parameter (P, U, V, H, W) and Signature = ($T_1$, $T_2$, $T_3$, c )
Step 2: Compute the Following value.
Step 3: if c = f (M, $T_1$, $T_2$, $T_3$ ) Return true
Step 4: else Return false
```

Algorithm 3: Key verification and File Decryption

```
Step 1: Set System parameter (P, U, V, H, W) and Signature = ($T_1$, $T_2$, $T_3$, c)
Step 2: Compute the Following value.
Step 3: if c = f (M, $T_1$, $T_2$, $T_3$) Return true
Step 4: else Return false
```

Algorithm 4: Revocation Verification

```
Step 1: Input System Parameter ($H_0$,$H_1$,$H_2$), Group signature and set of revocation Key $A_1,\ldots,A_r$
Step 2: Set temp = e ($T_1$,$H_1$)e($T_2$,$H_2$)
Step 3: for i=1 to n If e ($T_3 – A_i$,$H_0$) == temp Return valid End if End for Return invalid
```

3.1 System Initialization

Select a prime q, and groups G_1 and G_2, which are of order q. We define the mapping ˆe :$G_1 \times G_1 \rightarrow G_2$. Let g_1, g_2 be generators of G_1 and h_j be generators of G_2, for j ∈[tmax], for arbitrary tmax. Let H be a hash function. Let A0 = ha0 0 , where a0 ∈Z is chosen at random. (T_{Sig},T_{Ver}) mean T_{Sig} is the private key with which a message is signed and T_{Ver} is the public key used for verification. The secret key for the trustee is TSK = (a0, T_{Sig}) and public key is TPK = (G_1,G_2,H, g_1,A_0, h_0, h_1, . . . , ht_{max}, g_2, T_{Ver}).

3.2 User Registration

For a user with identity U_u the KDC draws at random K_{base}∈G. Let $K_0 = K_1/a0_{\ base}$. The following token γ is output γ = (u,K_{base},K_0, ρ), where ρ is signature on u‖ K_{base} using the signing key T_{Sig}.

3.3 KDC setup

We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. The architecture is decentralized, meaning that there can be several KDCs for key management.

3.4 Attribute Generation

The token verification algorithm verifies the signature contained in γ using the signature verification key T_{Ver} in TPK. This algorithm extracts K_{base} from γ using (a, b) from ASK[i] and computes $K_x= K1/(a+bx)$ base , $x \in J[i, u]$. The key K_x can be checked for consistency using algorithm ABS.KeyCheck(TPK,APK[i], γ,K_x), which checks $\hat{}e(K_x,A_{ij}B_{xij}) = \hat{}e(K_{base}, h_j)$, for all $x \in J[i, u]$ and $j \in [tmax]$.

We first show that no unauthorized user can access data from the cloud. We will first prove the validity of our scheme. A user can decrypt data if and only if it has a matching set of attributes.

4. Energy Efficient Data Access through Mobile Devices

During communication through mobile devices, handover the data between the devices consumes more energy than actual data transmission happened in non-mobility device. This proposed system considers an intelligent log system which maintains the credentials information of the user’s and data owner’s in the edge cloudlet. This helps the cloud servers to identify the user’s by their identity which is available in the log file maintains in the cloudlet. This kind of profiling technique consumes more energy in mobile devices while creates the communication. That energy consumption becomes reduced in the proposed system using intelligent approach with this IUP-ABE.

The proposed intelligent log file system helps to identify the availability of information requested by the user and from where they have to access. If the requested service or information is available in the cloudlet then mobile device can access from the cloudlet which is an edge computing. Sometimes, the requested service may not be available in the cloudlet and the client has to access the information only through credentials from data owner then the user directed to access the cloud server in public cloud. By this approach, the unwanted communication between the devices in far distance may be avoided.

5. Experimental Set up and Result Analysis

The experiments are carried out to show the performance of proposed system based on parameters such as time taken for encryption and decryption, time for signature generation and verification and energy efficient of devices with different user attributes. The results compared some of the CP-ABE techniques to show the unique nature of KP-ABE and its importance in secure data sharing.

Experiments are carried out in Intel i7 processor computer where five Virtual machines (VM) are created and each VM acted as a data owner who shares the cloud database in host machine and cloudlets. The host machine act as a cloud server where the key generation and verification takes place for individual users takes place.

The log system is maintained at cloudlet to analyze the kind of request given by user and directed the user to cloudlet or cloud database in cloud server. There will be 100 users are created to access the data form same database but from different data owners whereas the 40 users are accessing through mobile devices. Each data owner have own the different key policy for accessing their data. Since, if the user wants to get the information from the different data owners they have to get specific key form the individual data owners and they have to locate the requested service through log system.

In this proposed system, we are not concentrating on different encryption algorithms for different data owner. All data owners using the same public key encryption algorithm but key distribution are different for each and everyone.

The signature generation and verification is directed by the cloud server which is in host machine. It's the individual user entry to access the cloud server and viewing the services available or viewing the service provider's with their data information.

Table 1 Time for encryption with key in data owner

Number of attributes	Time taken for encryption (s)			
	[11] EABDS		IUP- ABE	
	Non-mobile	Mobile	Non-mobile	Mobile
20	0.50	0.85	0.6	0.90
40	0.90	1.05	0.85	0.95
60	1.30	1.70	1.05	1.15
80	1.70	1.90	1.3	1.40
100	2.25	2.45	1.75	1.90
120	2.50	2.75	1.90	2.15
140	2.90	3.25	2.10	2.30
160	3.30	3.60	2.45	2.70
180	3.70	4.10	2.7	3.10

Table 1 shows the time taken for encrypting the given data for the user based on different attribute that the user need from the data owner. Our proposed approach is compared with [11], to show that IU ABE is more efficient in respect to the time taken for encryption in non-mobile and mobile devices. The same thing is shown in pictorial representation in figure 1.

Fig. 1. Time for encryption with key in data owner

Table 2. Time taken for decryption in user side

Number of attributes	Time taken for decryption (s)			
	[11] EABDS		IUP- ABE	
	Non-mobile	Mobile	Non-mobile	Mobile
20	0.10	0.15	0.10	0.15
40	0.15	0.25	0.15	0.25
60	0.27	0.40	0.25	0.35
80	0.40	0.65	0.35	0.50
100	0.65	0.95	0.55	0.75
120	0.85	1.10	0.70	0.95
140	1.15	1.45	0.90	1.10
160	1.45	1.85	1.10	1.35
180	1.70	2.10	1.25	1.55

Table 2 shows the time taken for decryption for both systems. In that, our proposed system is given the variable times for different attributes where as the [11] requires the same time for all number of attributes. And our proposed system requires different time period based on the attributes in non-mobile and mobile devices. Figure 2 is the diagrammatic representation of table 2.

Fig. 2. Time taken for decryption in user side

Energy efficiency is another parameter which is important in mobile devices. So, the experiments carried out only for the mobile devices requests. The overall energy consumption of the device based on the attributes and applications will be differ and it represented in percentage that how much energy consumed by battery of mobile device. Table 3 shows the energy consumption of the mobile devices for accessing the services from the cloudlet and cloud server database. The proposed approach IUP_ABE with intelligent log system consumes less energy in both cloudlet and cloud server database. Figure 3 represents the pictorial representation of the average energy consumption percentage of the mobile devices.

Table 3. Average Energy Consumption of Mobile Devices during Service Access

Number of attributes	Average Energy Consumption of Mobile Device Battery (%)		
	[11] EABDS	IUP-ABE	IUP- ABE with log system
20	20.0	19.0	19.0
40	28.8	26.5	25.0
60	35.0	32.4	29.8
80	41.0	38.2	34.5
100	49.5	42.0	39.0
120	59.0	48.8	43.5
140	65.0	53.5	48.0
160	73.0	58.3	53.8
180	80.5	65.7	57.5

Fig. 3. Average Energy Consumption of Mobile Devices during service access

6. Conclusion And Future Work

The secure data sharing scheme in public data storage accessed through mobile device using IUP-ABE technique is proposed in this paper. The proposed IUP-ABE provides privacy for individual user security while they access the data from the public cloud. The data privacy is maintained in public cloud by providing individual key for each user belonging to the specific data owner. Moreover, user revocation is also in trusted way by authenticating the user with their individual secure key for participating in the specific group of user's data. Experimental analysis shows that the time consumption and energy consumption for key generation, encryption and decryption in both non-mobile and mobile devices are less when compared to the previous existing systems. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

References

1. Ruj, S., Stojmenovic, M., Nayak, A.: *Decentralized access control with anonymous authentication of data stored in clouds*. *IEEE transactions on parallel and distributed systems*, *25*(2), 2014, pp.384-394..

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

3. Ruj, S., Stojmenovic, M., Nayak, A. : *Privacy preserving access control with authentication for securing data in clouds*. 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), May 2012, pp. 556-563). IEEE.

4. Wan, Z., Liu, J.E., Deng, R.H.: *HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing.* IEEE transactions on information forensics and security, 7(2), 2012, pp.743-754.

5. Tysowski, P.K., Hasan, M.A.: *Hybrid attribute-and re-encryption-based key management for secure and scalable mobile applications in clouds.* IEEE Transactions on Cloud Computing, 1(2), 2013, pp.172-186.

6. Selvakumar, K., SaiRamesh, L., Sabena, S., Kannayaram, G.: *CLOUD COMPUTING-TMACS: A Robust and Verifiable Threshold Multi-authority Access Control System in Public Cloud Storage.*

In Smart Intelligent Computing and Applications, 2019, pp. 365-373, Springer, Singapore.

7. Cui, B., Liu, Z., Wang, L.: *Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage*. IEEE Transactions on Computers, 65(8), 2016, pp.2374-2385.

8. Banerjee, A., Hasan, M., Rahman, M.A., Chapagain, R.: *CLOAK: A stream cipher based encryption protocol for mobile cloud computing*. IEEE Access, 5, 2017, pp.17678-17691.

9. Ali, M., Dhamotharan, R., Khan, E., Khan, S.U., Vasilakos, A.V., Li, K., Zomaya, A.Y.: *SeDaSC: secure data sharing in clouds*. IEEE Systems Journal, 11(2), 2017, pp.395-404.

10. Cui, H., Yuan, X., Wang, C.: *Harnessing encrypted data in cloud for secure and efficient mobile image sharing*. IEEE Transactions on Mobile Computing, 16(5), 2017, pp.1315-1329.