EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.35-40
SANA ACADEMIC PRESS

Secure Scheme for Shared Data with Key Pair model over Encrypted Cloud Data

R. Thangapushpam[1], Jisha Liju Daniel[2] , N.Venkatesan[3]
[1]M.Phil Research Scholar, St. Peter's University, Chennai - 54.
pushpam_t@yahoo.com
[2]Assistant Professor, St. Peter's University, Chennai - 54.
[3]Assistant Professor, St. Peter's University, Chennai - 54.

Abstract *- Now a day cloud storage and shared service are becoming very famous. Current general auditing and user revocation mechanism for the integrity of shared data with efficient user revocation process in mind. But the security and performance of those process not effective. So By utilizing the idea of proxy re-signatures, the cloud is allowed to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. However, this new methodology is able to help batch auditing by verifying multiple auditing tasks simultaneously because of proxy mechanism. This new mechanism can significantly improve the efficiency of user revocation. Shared data will be handled with security manner with help of RSA algorithm. In addition, user can feel the performance of handling the shared data in the cloud since proxy handling the data in small pieces of files for download and upload operation.*

Keywords- *Proxy, Partitioning, user revocation, SMTP.*

I. INTRODUCTION

Cloud computing is mainly used for resource sharing and with very low-maintenance. The cloud service providers (CSPs), such as Amazon, are able to provide a various services to cloud users with the help of powerful various datacenters. Cloud Providers provides a fundamental service is data storage (Storage as-a service). An organisation allows its group members in the same group or department to store and share files in the cloud. By utilizing the cloud, the group members can be completely released from its local data storage and maintenance. A significant risk arises in confidentiality of those stored files. So, the users are not fully trusted the cloud servers operated by cloud provider while sensitive data stored in the cloud. With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a proxy re-signature, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

To increase the adoption of cloud storage, designed a virtual private storage services are based on cryptographic techniques. Service should provide confidentiality and integrity. The main benefits of a public storage services are availability, reliability, efficient retrieval, and data sharing. When preparing data to store in the cloud, the data processor begins by indexing it and encrypting it with a a*symmetric encryption* scheme (e.g., RSA), uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. Our contributions are summarized as follows:

- Cloud-offers data storage and sharing services to the group
- Public Verifier- TPA (Third Party Auditor) - Aim to check the integrity of shared data (via) Challenge- Response protocol with the cloud.
- Users(Who Share data as a group)- One original user + no of group users.

II. LITERATURE SURVEY

In public clouds, PPDP(proxy provable data possession) is a matter of crucial importance when the client cannot perform the remote data possession checking. We study the PPDP system model, the security model, and the design method. Based on the bilinear pairing technique, we design an efficient PPDP protocol. Through security analysis and performance analysis, our protocol is provable secure and efficient. PPDP protocol was not providing the efficient operation like search operation (Wang.H,2013).

Proofs of Ownership and Retrievability considering, the requirement of mutual validation.. In our PoOR scheme, clients can prove to the server their ownership of files and verify the retrievability of the files without uploading or downloading them.The result shows that the Poor scheme is efficient in computation performance, especially when the size of the file is large (Du.Ret al, 2014).

OPoR, a new cloud storage scheme involving a cloud storage server and loud audit server, where the latter is assumed to be semi-honest as well as ensure security against reset attacks launched by the cloud storage server in the upload phase.Security is an important problem in public cloud storage and those files are stored as flat file without any encryption logic. So this is kind of un-trusted model by data owner (Li.Jet al, 2015). Novel public auditing scheme with public verifiability and constant communication cost based on self-certified signature scheme in this paper. Thorough analysis shows that our proposed scheme is secure and efficient. The security of our scheme is based on the fixed inversion problem (FI) of the bilinear map and the inversion of hash function. Inversion problem (FI) of the bilinear map and the inversion of hash function was not a efficient model during search the keyword on the cloud (Zhang.J et al ,2014).New cloud storage architecture with two independent cloud servers, that is, the cloud storage server and the cloud audits erver, where the latter is assumed to be semi-honest. In particular, we consider the task of allowing the cloud audit server, on behalf of the cloud users, to pre-process the data before uploading to the cloud storage server and later verifying the data integrity. The introduction of cloud audit server eliminates the involvement of user in the auditing and in the pre-processing phases. Auditing server was not support the verification scheme during file size is large (Li.Jet al, 2013).

We revisited the two private PDP schemes. We show that the property of correctness cannot be achieved when active adversaries are involved in these auditing systems. More specifically, an active adversary can arbitrarily tamper the cloud data and produce a valid auditing. If we use the 100GB of file on cloud, then these auditing validation getting slow since it was used any indexing logic to validate the keyword(Ren.Y et al, 2014).

Attribute based provable data possessionscheme, which utilizes attribute based signature to construct the homomorphic authenticator. In the scheme, the homomorphic authenticator contains an attribute strategy. Only the verifier, who satisfied the strategy, can check the data integrity. In particular, the cloud storage service (CSS) in our scheme is stateless and independent of verifier. Moreover the scheme has more security features, including strong anonymity, unlink ability and conspiring to resistance. Security issue has arrived since homomorphic authenticator based mechanism is not giving more security (Yongjun Ren et al, 2014).

Third party verifier (TPV), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. In particular, to achieve efficient data dynamics, we improve the Proofof Retrievability model by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. Extensive performance analysis show that the proposed scheme is highly efficient. Cost expenses for Third party verifier (TPV) is high(Ni-Na.S et al,2011).Secure Scheme for Shared data is not effective on user revocation among the user group and there is no effective auditing mechanism to manage the data sharing from source to destination. Proposed system of this project is to improve the user security and manage the user revocation during the data transmission (source to destination). To achieve this, the proxy mechanism will be used to re-generate the secret code automatically. Also when group user add/remove, proxy automatically generate the key and share it to group except removed user from the group(Zhihua Xia et al, 2015).

III. SYSTEM MODELS AND ITS DESIGN GOALS

System Model

We consider a cloud computing architecture by combining with an example that an organisation uses a cloud to enable its employees in the same group or department to share files. The system model consists of three different entities: the cloud server, a group manager, and a large number of group members (i.e., the employees) as illustrated in Fig. 1

Cloud server is operated by cloud service providers and the fundamental service provides by them as storage as a service (SaaS). However, the cloud is not fully trusted by the group members. We assume that the cloud server is honest and trust them. So that cloud server will not maliciously delete or modify user data, by achieving data auditing schemes.

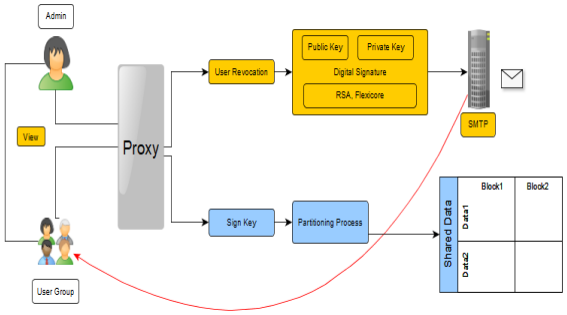

Fig. 1 System Model

Admin is responsible for system parameters generation, registering the user, revocating the group member and revealing the real identity in case of any dispute occur.

Group members are the registered users they will stockpile their private data into the cloud server and share the data among the group members. In our example, the employee plays the role of group members. It allows the group members to be dynamically changed, due to the staff resignation and the participation of new employee in the organisation.

Design Goals

Access control: Cloud Server allows only the authorized group member to store their private data in the cloud offered by cloud service providers as SaaS and it won't allow unauthorized group member to store their data in the cloud.

Data confidentiality: Data owner will store their data in the cloud and share the data among the group members. Who upload the data have rights to modify and delete their data in the cloud.

Traceability: In case of any dispute occurs it can easily traceable. If other group member delete the other group members data can be easily noticeable.

IV. THE PROPOSED SCHEME

The admin is responsible for user revocation with public and private Key, Proxy Automation on cloud, Data Sharing and Partitioning.

1. User Revocation with Public and Private Key

The group of user is going to download and upload the data or secret document in cloud. If anyone from the group is added/removed (called user revocation), the proxy will generate the new secret key for the operation. User can feel the operational speed during download and upload the document. Whenever create the user group, our system will create the private and public key (key pair) based on the security provider FlexiCoreProvider (RSA, FlexiCore) and these will be converted as a encrypt mode and stored in proxy system. Then user perform the download and upload operation, our system will ensure that encrypted key and user entered key should be equal.

2. Proxy Automation on cloud

Cloud will receive the document from client and do the partition of data (each 5MB) which was shared by user. Also cloud will manage the digital signature (private and public key) with help of proxy system as illustrated in Fig. 2.

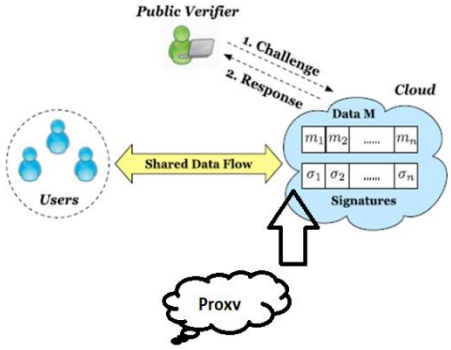

Fig. 2 Proxy Automation on cloud

Client and cloud will communicate via Java Web service API (Application Programming Interface).

Proxy is set of our coding and which will generate the secret key automatically based on the user revocation from the existing group. Also proxy will perform the partitioning of data based on the 5MB size data. So this will improve the user operation very fast since if user wants to edit the document, the user can download the particular patch alone.

Whenever user do revocation operation, our system will trigger the mail with Re-Gen key to the entire user within the group.

3. Data Sharing

Our core objective of this project is to share/hold the user data in the cloud with security manner. Whenever upload the data into cloud, system will verify the security model RSA, FlexiCore by making encryption and decryption (Cipher algorithm).

4. Partitioning

When we share the data, our system will perform the partitioning process and it will store into cloud.

V. ALGORITHM DETAIL

RSA Algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an symmetric cryptographic algorithm.

Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private.

Detail Logic

The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key.

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.

Key Generation Algorithm

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.

2. Compute n = pq and (phi) $\varphi = (p-1)(q-1)$.

3. Choose an integer e, $1 < e < \text{phi}$, such that $\gcd(e, \text{phi}) = 1$

4. Compute the secret exponent d, $1 < d < \text{phi}$, such that $ed \equiv 1 \pmod{\text{phi}}$.

5. The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q and phi secret. [We prefer sometimes to write the private key as (n, d) because you need the value of n when using d. Other times we might write the key pair as ((N, e), d).]

6. n is known as the modulus.

7. e is known as the public exponent or encryption exponent or just the exponent.

8. d is known as the secret exponent or decryption exponent.

RSA key pair

1. INPUT :Required modulus bit length, k.
2. OUTPUT: An RSA key pair ((N,e), d) where N is the modulus, the product of two primes (N=pq) not exceeding k bits in length; e is the public exponent, a number less than and coprime to (p-1)(q-1); and d is the private exponent such that $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Select a value of e from {3, 5, 17, 257, 65537}

3. repeat

4. p ← genprime(k/2)

5. until (p mod e) ≠ 1

6.repeat

7. q ← genprime(k - k/2)

8.until (q mod e) ≠ 1

9. N ← pq

10. L ← (p-1)(q-1)

11. d ← modinv(e, L)

12. return (N, e, d)

Encryption

- Obtains the recipient B's public key (n, e).
- Represents the plaintext message as a positive integer m, 1 < m < n.
- Computes the ciphertext c = me mod n.
- Sends the ciphertext c to B.

Decryption:

- Uses his private key (n, d) to compute m = cd mod n.
- Extracts the plaintext from the message representative m.

Digital signing

- Creates a message digest of the information to be sent.
- Represents this digest as an integer m between 1 and n-1.
- Uses her private key (n, d) to compute the signature s = md mod n.
- Sends this signature s to the recipient, B.

VI. RESULT ANALYSIS

The main purpose of this paper is to improve the efficiency of user revocation and to provide the more performance with security. But the existing model does not have efficient user revocation and security. We assume the cloud and an existing user have the same computation ability (Intel Core i5 2.5 GHz duel core Processor and 3 GB Memory) to perform user revocation and document download/upload process. We also assume the download speed and upload speed for the data storage and sharing services is 2 Mbps and 700 Kbps, respectively. But previously it happened 1 Mbps and 500 Kbps respectively, as illustrate as Fig. 3

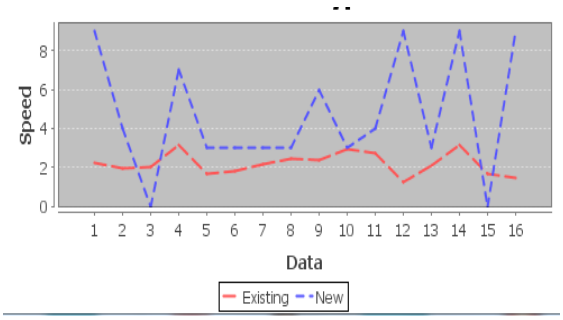

Fig. 3 Result Analysis between speed and data

The performance comparison between this project and the straightforward method during user revocation is presented below image. With our mechanism, the cloud is able to not only efficiently re-sign blocks but also save existing users' computation and communication resources. When the number of re-signed blocks is 500, which is only 0:05 percent of the total number of blocks, the cloud in Panda can re-sign these blocks within 11 seconds. In contrast, without our mechanism, an existing user needs about 22 seconds to re-sign the same number of blocks by itself. Both of the two revocation time are linearly increasing with an increase of k—the number of re-signed blocks, as illustrate as Fig. 4

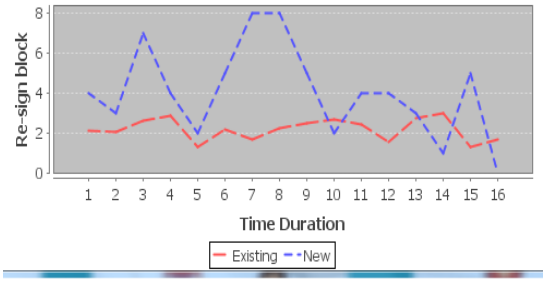

Fig. 4 Result Analysis between Re-sign block and Time duration

The Fig.4will illustrate as performance since we are using the partitioning process during upload.

VII. CONCLUSION

This paper has improved the user security and manages the user revocation during the data transmission. Proxy mechanism was used to re-generate the secret code automatically along with user revocation process. In addition proxy was performed the partitioning of large data into small pieces of files to improve the speed of download and upload the document on cloud.

REFERENCES

[1] Du. R; Deng. L; Chen. J; He. K; Zheng. M"Proofs of Ownership and Retrievability in Cloud Storage , Pages: 328 – 335,2014".

[2] Kuzu. M, Islam. M. S, and Kantarcioglu. M, "Efficient similarity search over encrypted data," in Data Engineering (ICDE), 2012 IEEE 28th,pp.1156-1167.

[3] Li. J; Tan. X; Chen. X; Wong.D.S; Xhafa. F" OPoR: Enabling Proof of Retrievability in Cloud Computing with Resource-Constrained Devices, Volume: 3,Pages: 195 ,2015".

[4] Li. J, Wang. Q, Wang. C, Cao. N, Ren. K, and Lou. W, "Fuzzy keyword search over encrypted data in cloud computing," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–5.

[5] Li. J; Tan.X; Chen.X; Wong. D.S "An Efficient Proof of Retrievability with Public Auditing in Cloud Computing , Pages: 93 – 98,2013".

[6] Ni-Na.S; Hai-Yan. Z " On Providing Integrity for Dynamic Data Based on the Third-party Verifier in Cloud Computing , Pages: 521 - 524, 2011".

[7] Ren. Y; Shen. J; Wang. J; Fang. L "Security Analysis of Delegable and Proxy Provable Data Possession in Public Cloud Storage, Pages: 795 – 798,2014".

[8] Wang. H "Proxy Provable Data Possession in Public Clouds, Volume: 6,Pages: 551 - 559,2013".

[9] Yongjun Ren; Zhenqi Yang; Jin Wang; Liming Fang " Attributed Based Provable Data Possession in Public Cloud Storage, Pages: 710 – 713,2014".

[10] ZhihuaXia,Xinhui Wang, Xingming Sun, and Qian Wang "Secure Scheme for Shared Data with Key Pair model over Encrypted Cloud Data ,vol.,no.,2015".

[11] Zhang. J; Zeng. W" Self-Certified Public Auditing for Data Integrity in Cloud Storage, Pages: 267 – 273,2014".