A Secure Authentic Anti Collusion Mechanism in Dynamic Groups in Clouds by Using 3 Pake and Chaotic Maps

M.S.Bennet Praba [1], Chamarthi Manoj Kumar [2], Konda Manikanta.Hari Nikhil [3], G.Dharani Krishna [4]
[1] Assistant Professor, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
[2, 3, 4] Student, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

Abstract – Cloud computing is the long term dream of data science and it has potential to transform a major part of IT industry .Cloud computing deals with both hardware for storage and applications over software as a service. In a present world with massive advancements in internet, cloud provides the assets over the internet. Few users sharing common resources can be formed into cloud groups .These groups can be either static or dynamic .In dynamic groups users can be either added or revoked, as the membership changes frequently maintaining privacy becomes a major concern .So, security must be provided to users in dynamic groups against collusion attacks .First, key exchange using 3PAKE algorithm is proposed.Second,Fine grained access can be achieved by our scheme, any active user can access the data but revoked users cannot access the data.Third,protection against collusion attacks such as revoked users cannot get files from untrusted clouds .Fourth, file encryption is done .Images and text documents are encrypted separately by using chaotic maps and AES respectively. Finally our system, can achieve fine adaptability, which means old users will not update their keys when someone new joins in the group and data remains secure during breach situation.

1. INTRODUCTION

Cloud computing is a shared multi-tenant. Cloud computing is used for storing infinite amount of data over remote locations [1]. In this resource are evenly distributed platform over various users, here internet serves as the medium for resource allocation. It can help clients or users to reduce their burden by transferring the local management systems into main servers.

However, security aspects become more challenging as we redistribute the data storage. In order to control security issues, files must be encrypted before uploading them into cloud server [2]. Lamentably, it is hard to design secure data sharing scheme, specifically for dynamic groups in cloud [3].

Dan Boneh et al [4], presented a encrypted storage system that provides secure data sharing on untrusted servers (protocols used are NFS,CIFS) .It must store all accessed information together with the file data. File data refers to both encrypted and signed data. It also allows file sharing with minimum bandwidth communication between other users. The main use of this scheme is although users have no control over the file server even then it is said to be secure. However, there are more advanced techniques.

Shucheng et al [5] says that sensitive user data confidential against untrusted servers, existing solutions usually applycryptographic methods by disclosing data decryption keys only to authorized users. Key policy attribute-based encryption is followed. Proxy re encryption, Lazy re encryption are used to secure the data sharing.

Liang X et al [6] says that two keys are given to a user after registration, one key is used for encryption and another key is used for decryption. The main drawback of this scheme is revocation of user is not supported.

Boyang Wang et al [7] proposed a scheme that achieves fine grained access and also avoids revoked users from getting passwords and access to the data. This overcomes the drawback of previous existing system. In this scheme existing users get private key to decrypt the file whereas user encrypts by using a public key. Sometimes revoked users get to know the private key by using decrypting algorithm. So, this scheme has certain defects in key exchange mechanism.

Rahul et al [8] proposed a decent approach for key exchange between users and server. This mainly helps in reducing the time taken for key distribution between individual users by allowing key reusability. Key is shared between three components mutually. Password authentication is explained in this process. Keys are reused in SSL/TLS communication channels. This is the process used for key exchange in our scheme.

S Kiran [9] explores and uses entrenched cipher, which is essentially the combination of AES and MD5 algorithms in combination to achieve more security. So, for decrypting the data, both algorithms must be decrypted in the respective manner.

Chaotic maps are used for image encryption [10]. So, finally ,we can assure users about file security , key exchange inside the cloud architecture.

2. RELATED WORK

A. A view of cloud computing

The data center containing hardware and software is called a cloud. Cloud storage services are a popular means for storing data and performing a collaborative work. New cloud providers have to compete against established ones such as Google, Microsoft drop box which offers a large amount of data. Anyone can use the clouds and upload the files in the cloud. When a cloud is made available to all users, it is called as public cloud whereas private cloud used by organizations for their own purpose.

B. Cryptographic cloud storage

building a Advances in networking technology and increase in need for computing resources have prompted secure cloud storage service on top of a public cloud architecture, where server is not completely many organizations to outsource their storage and computing needs. We consider the problem of trusted by client or user. So, server uses some advanced cryptographic measurements to encrypt the data, while data sharing. As cloud system becomes completely cryptographic, server can be trusted by client

C. Sirius: Securing remote untrusted storage

Sirius is a secure file system designed over insecure network p2p file systems such as NFS, CIFS, Oceanstore. Above all systems have no control over the remote system. Sirius uses a hash tree construction for file freshness. It also performs random access in some cryptographic file systems without the use of block server.

D. Achieving secure, scalable and fine-grained access

To keep sensitive data confidential against untrusted servers, existing system solutions apply only to authorized users. To overcome the issue regarding, we introduced combine techniques called attribute-based encryption, proxy re encryption, lazy re encryption. Data confidentiality of user access privilege and user secret key can be achieved. Formal security proofs show that our proposed scheme is secured under cryptographic model.

E.The data forensics in cloud computing

To implement undetermined area in cloud computing, we proposed a new secure origin scheme based on the bilinear pairing methods. As the data forensics and later survey in cloud computing, the proposed scheme is characterized by providing the data confidentiality on sensitive files stored in cloud, incognito authentication on user access, and origin tracking on disputed files.

F. Mona: Secure multi-owner data sharing for dynamic groups in the cloud

Mona, a data sharing scheme in the cloud proposed by Liu et al and point out some security attacks on it. There exists collusion attack on Liu et al's protocols. With the help of the collusion attack, the secure data access control has not been succeeded and the sharing data has not been well secured. Besides, there is one more security shortage in the user registration phase, which is how to protect the private key when sharing it in the unsecure communication channel

G .Session key reusability using 3 PAKE

Two parties can encrypt and authenticate their messages in order to protect the messages. Public key encryption schemes and signatures can be used but these schemes might lead to higher cost for certain applications. Another way of communicating securely is to first establish a common secret key via a key exchange protocol and then use this key to derive keys for symmetric encryption and message authentication schemes. The main aim of this scheme was to reduce the time required to establish a session by reusing the key value for consecutive sessions between the same pair of users. The users should be able to reuse their secret key value saving on time and costly computations needed for key generation.

H .Use key entrenched cipher

Algorithm used for computation of key should be difficult for hackers to reveal the key. In the proposed algorithm middle bit of the original data is taken as key. These bits are not transformed to any other form during the encryption. To enhance the security logical operations and Rail fence algorithm is applied. Entrenched cipher generally is a cipher which is formed by combination of rail and fence technique's and MD5 are used in our project.

I .chaotic-maps-based image encryption

A new parallel implementation for a Chaotic-based image Encryption method is proposed. The proposed method Performs the capabilities of the parallel computation environments in developing the performance of Chaotic-based encryption algorithms. The proposed parallel implementations are computed using different images of different sizes to check its validity.

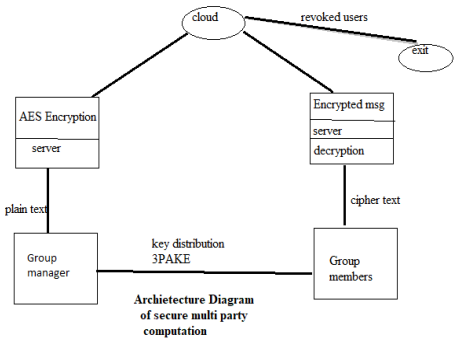
3. THREAT MODELLING

As the threat model, we propose our scheme based on Zhongma Zhu model [3], in which main focus is on design mechanism which mainly focuses on file sharing, fine grained access, data confidentiality. This existing system has some security issues regarding data encryption, key exchange, User authentication. So. In order to protect the information from eavesdroppers and attackers, some specific set of protocols are to be designed.

This is the required and desirable environment to describe the complete effects of our technique.

4. SYSTEM MODELS

The architecture of this scheme consists of three main units. Clients present in the dynamic group, group manager or server [7]. As we are explaining about key exchange between multiple parties, multiple clients are arranged in above shown manner. Server programs must be running on all client systems, so that data confidentiality can be achieved. Key exchange essentially follows key reusability technique [8], which means key will be generated only once and it is reused several times as shown.



Archietecture Diagram of secure multi party computation

5. DESSIGN GOALS

A. Key Distribution

Session key reusability mechanism [8] is used in this scheme. Password based authenticated key exchange helps in protecting keys from attackers. Mathematical functions aregiven to check the existence of this protocol. Theorems serve as the proof for key security.

B. Data Encryption

Data encryption is the most important part of cloud security maintenances. Data encryption is done by combining two algorithms AES and MD5 [9]. Cipher text is obtained by encrypting data twice and two keys are used for this.

C.Image Encryption

Image encryption is most important thing at present day. Chaotic maps are used for this particular task. Chaotic maps [10] encrypt images in a very less amount of time compared to other encryption techniques.

6. THE PROPOSED SCHEME

A. Bilinear Maps

Let G1 and G2 be additive cyclic groups of the same prime order q . Let e: G1×G1→G2denote a bilinear map constructed with the following properties: [3]

1. Bilinear: For all a, b∈Z∗q and P, Q∈G1, e (aP, bQ) =e(P, Q)ab.

2. Nondegenerate: There exists a point Q such that e (Q, Q) ≠1.

3. Computable: There is an efficient algorithm to compute e(P, Q) for any P,Q∈G.

B. Notations

Each user has a pair of keys (pk, sk), which is used in the asymmetric encryption algorithm, needs to be negotiated with the group manager on the condition that no Certificate Authorities and security channels are involved in. KEY is the private key of the user and is used for data sharing in the scheme. UL is the group user list which records part of the private keys of the legal group users. DL is the data list which records the identity of the sharing data and the time that they are updated.

C. Scheme

The scheme of our scheme includes system initialization, user registration for existing user, file upload, user revocation, registration for new user and file download.

D. Registration for Existing User

This operation is performed by user, the group manager and the cloud. First of all, the user sends IDi, pk,v1 as a request to the group manager, where IDi is the identity of the user, pk is the public key used in the asymmetric encryption algorithm, Such as ECC, ac is the account user used to pay for the registration, which is related to the identity of the user, and v1∈Z∗q is a random number selected by the user. On receiving the request, the group manager then chooses a random number r∈Z∗q and computes R=e (P, P) r, U=(r+γ·v1·f (pk‖ac‖IDi)) ·P. At last, the group manager sends U, R to the user for verification

Then the verification is performed by user through checking the equation R·e(v1·f(pk‖ac‖IDi) ·P, W) =? e (U, P). The user sends the v2∈Z∗qis a random number, AENC () is a asymmetric encryption algorithm, such as and messaged, v2, AENCsk (IDi, v1, ac) to the group manager after successful verification, where sk is the corresponding private key to the public key pk used in the asymmetric encryption algorithm.

The group manager compares the received IDi message with the identity IDi computed by decrypting AENCsk (IDi, v1, ac). In addition, the group manager verifies if the decrypted number v1 is equal to the random number v1 in the first step. After successful verifications, the group manager generates the message KEY as follows when the IDi message matches the identity in the first step

E. File Upload

The operation of file upload is performed by users and group managers. Then the group member encrypts (IDdata, C1, C2,

C, data) with his private key Bi, where data is the real time stamp. At last, the group member sends EncBi (IDdata, C1, C2, C,tdata) to the group manager. After getting this message EncBi(IDdata,C1,C2,C,tdata), the group manager decrypts it and gets (IDdata,C1,C2,C), then the group manager checks the legal group members in his local storage space and if Bi is the private key of a legal user, then the group manager constructs fp(x)=∏mj=1(x−Vj)=∑mi=0aixi(modq) and the exponential function{W0,…,Wm}={Ga0,…,Gam}. After that, the group manager selects a random re-encryption key Kr and constructs EK={Kr·W0,…,Wm}. Finally, the group manager encrypts cipher-text CE={C1,C2,C}Kr with the re-encryption key and sends {DF=(IDgroup,IDdata,CE,EK,tdata),σDF} to the cloud, where tdata is the time that the data file is uploaded and σDF=γf1(DF) is the signature of the group manager for the data file.

7. SECURITY ANALYSIS

A .Chaotic maps

The serial and parallel versions of Baker map substitution algorithms are implemented. We selected the parameter values to be as follows: [10]

number of partitions (D)=8,

number of baker iterations (n)=5, and

number of total iterations (m)=9.

B. Diffusion Process Experiment

In the same way, the serial and parallel versions of Chen's diffusion algorithms are implemented. We selected parameter values to be as follows,

- logistic map initial value of (l−1)=0.3,
- the initial pixel value (p ′−1)=10, and
- The number of total iterations (m)=9.

The experiments are performed using different number of parallel cores (2, 4, 8, 16, and 32), respectively to experiment the effect of increasing the number of parallel cores on the performance of the proposed algorithm.

C. 3PAKE

It is well-known that images are different from texts in many aspects, such as highly redundancy and correlation, the local structure and the characteristics of amplitude–frequency. As a result, the methods of conventional encryption cannot be applicable to images.

When the A and B communicate for the first time, key is exchanged in this following manner [8]

A→B RQA=A, gx, H (A, gcs2,pwa)

A chooses a random value x from Zq* and calculates g*x, g*xs and the hash value. Then it sends a request RQA to B.

B→S RQA, RQB=B, gyH (B, gys, pwb)

B chooses a random value y from Zq∗ and calculates gy, and the hash value. B sends its request RQB along with RQA to server

S→B

AKB=A,gx,H(A,B,gx,gys,pwb), {T}gysAKA=B,gy.H(B,A,gygxs,pwa),{T}gxs

1. B→AAKA

   Upon receiving the packets, B calculates the hash value and verifies AKB. If verified, B sends AKA to A and calculates the session key as k= (gx)y=gxy. The value of key along with T is stored in the database by B.

2. A verifies AKA and calculates the session key value as k= (gy) x=gxy. The value of key along with T is stored in the database by A.

For the consecutive session establishment between the same clients A and B i.e. phase 2, the concept of reusability of session keys comes into account for which following approach is decided.

First, the information which needs to be maintained at both the clients is:

1. The timestamp sent by server

8. CONCLUSION

The main aim of this approach was to reduce the time required to establish a session by reusing the key value for consecutive sessions between the same pair of users. The users should be able to reuse their secret key value saving on time and costly computations needed for key generation. Experimental results show that the key establishment time was reduced significantly for a series of few executions when key was not calculated in every run. As the technology keeps advancing, systems are becoming more secure. If new attacks are found, counter-measures to prevent the attack are also developed. So owing to the security measures and the fact that key is not travelling through the network even once, it is a fair idea to reuse the key value for a certain period to avoid the complex calculations and faster connection between the users. Concepts of session reuse are employed in SSL/TLS communication where the

abbreviated handshake takes less time when previous session is resumed. Reusability can also be used for any application which uses symmetric cryptography.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "A view of cloud computing", Commun. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[2] Cryptographic Cloud Storage - Microsoft Research Seny KamaraKristin LauterProceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010,136-149,vol 6054,Publisher Springer.

[3] Zhongma Zhu "A secure anti collusion mechanism for dynamic groups in cloud"IEEE Volume: 27, Issue: 1, Jan. 1 2016)

[4] E. Goh, H. Shacham, N. Modadugu, D. Boneh, "Sirius: Securing remote untrusted storage", Proc. Netw. Distrib. Syst. Security Symp., pp. 131-145, 2003.

[5] Shucheng Yu ; Cong Wang ; Kui Ren ; Wenjing Lou Achieving Secure, Scalable, and Fine-grained Data Access Control in cloud computing

[6] R. Lu, X. Lin, X. Liang, X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing", Proc. ACM Symp. Inf. Comput. Commun. Security, pp. 282-292, 2010.

[7] The Attack on Mona: Secure Multi-owner Data Sharing for DynamicGroups in the CloudZhongma Zhu; Zemin Jiang; Rui Jiang2013 International Conference on Information Science and Cloud Computing CompanionYear: 2013Pages: 213 - 218Cited by: Papers (4)Year: 2015

[8] Session key reusability using 3-PAKE in symmetric key cryptographyShivani Bhatia; Rahul V. Anand2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI)Year: 2015

[9] A novel crypto system with key entrenched cipherS. Kiran; R. Pradeep Kumar Reddy; N. Subramanyan2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)Year: 2017

[10] Improving the speed of chaotic-maps-based image encryption using parallelizationAmany Elrefaey; Amany Sarhan; Nada M. El-Shennawy2017 13th International Computer Engineering Conference (ICENCO)Year: 2017

Authors

M.S.Bennet Praba., M.E ,Assistant Professor,SRM Institute of Science and Technology.She used to guide us in each and every possible way and help us with clarifying our doubts.By this we like to show our gratitude and respect towards her.

K.M.Hari Nikhil.(RA1411003020246) ,Student **,**SRM Institute od Science and Technology

C.Manoj Kumar(RA1411003020253),Student,SRM Institute of Science and Technology

G.Dharani Krishna(RA1411003020245),Student,SRM Institute of Science and Technology