Three Factor Data Security Protection Mechanism For Cloud Storage System

Gowtham .V[1], Kathiravan .S[2], Mrs. P. Nirmala Deve[3], Mrs. R.K. Kapilavani[4]
[3, 4]Assistant Professor
[1, 2, 3, 4] Prince Shri Venkateshwara Padmavathy Engineering College, Ponmar.

Abstract*- In this paper we propose a three-factor data security protection mechanism for cloud storage system. The first factor is the public and private keys of each user. The second factor is the secret key which is sent from the cloud and the third factor is a security device. This system provides a way to send the encrypted data to a receiver through a cloud storage server. Initially the sender encrypts the data using receiver's public key and in cloud it is again encrypted using an AI program which is automatically performed in cloud. The receiver needs three things in order to decrypt the data, the security device, the secret key and his own private key. Decryption of data is not possible without either piece. Moreover, if security device is lost or stolen, it is revoked. When any unauthorized access is detected, the cloud server automatically changes the encryption algorithm. This process is not known to the sender. This enhances the security of the existing system.*

Keywords- Three factor, AI program, security device

I. INTRODUCTION

Generally, a cloud refers to the “internet” that is used to connect the end-points of a transmission. It can also be called as a network cloud. The cloud can also be used as a storage medium. There are many benefits in using cloud storage system. One of the important benefit is the data accessibility. Any amount of data can be stored in a cloud and data can be accessed until there exists a network connection. As cloud space is a public storage, anyone can access data at anytime. There may be some security issues which could be overcome by adopting some secure methodologies.

Despite its advantages, outsourcing data storage also increases the attack surface area at the same time. By sharing storage and networks with many other users it is also possible for other unauthorized users to access your data. A novel solution for the offset risk is to deploy encryption technology. By using encryption technology, the data being transmitted can be secured from the intruders. As the encryption is performed corresponding ciphertext is being generated which is not directly understandable by the intruders. The most convenient mode of encryption is Asymmetric encryption as the need of key management in symmetric encryption is eliminated.

IDENTITY BASED ENCRYPTION

Identity based encryption (IBE) is a primitive of ID-based cryptography. It is a type of public key encryption, in which the public key of a user is some unique information about the identity of the user. This means that the sender can encrypt the data using receiver's name or email address as a key. The receiver can decrypt the data using the key sent by the central authority, which is to be trusted as it generates secret keys for every user. This system allows any party to generate a public key from a known identity values as an ASCII string. A trusted third party- Private Key Generator (PKG), generates the corresponding private keys. It provides master key using which the parties may encrypt without prior distribution of keys between individual participants.

The major advantage of this technique is that if there are only finite number of users, the third party's secret can be destroyed only after all the users have been issued with the keys. Moreover, IBE eliminates the need for a public key distribution infrastructure. The authenticity of the public key are guaranteed. As the Private Key Generator generates private keys for users, it can decrypt messages without authorization. This implies that IBE systems cannot be used for non-repudiation.

1.1 Some Naive Approaches

We discuss some naïve approaches for enhancement of security protection and explain why they are not the best candidate to achieve the goal of flexibility

Double encryption:

Initially the sender encrypts the data that is to be sent to the receiver. The data is encrypted using the public key of the receiver. The encrypted data is sent to the cloud, where it is temporarily stored. In the cloud an automatic encryption is done using an AI program which uses IBE scheme. The decryption key is automatically sent to the receiver through message passing system (Gmail, OTP, etc.).

It seems that this approach may achieve the goal but there exists some practical issues. For example,

If the secret key sent via Gmail is stolen (hacked) by the intruder and as the public key is known to everyone, it is possible to decrypt the data easily.

Security Device:

The security device adds one more layer of security. When the user needs to download the data, first he need to enter the device key which is uniquely provided for each user as they request. The device will be provided by the Security Device Issuer (SDI) only after the authentication of each user. If the security device is stolen then the user can no longer use the old device key to access the data. Again this seems to achieve our goal. This methodology can be applied in the places where the secrecy of information need to be maintained.

1.2 Our Contributions

In this paper, we propose a novel three-factor security protection mechanism for data stored in the cloud. Our mechanism provides the following features:

1) Our system is an IBE(Identity Based Encryption) based mechanism. It means that the sender only needs to know the identity of the receiver. The sender uses the public key of the receiver to encrypt the data. Then the sender transmits the encrypted data to the cloud.
2) Our system provides three-factor data encryption protection mechanism. In order to decrypt the data stored in the cloud, the user needs to possess two things, one is his/her private key and the secret key sent from the cloud. Without the either piece it is impossible to decrypt the data.
3) A security device is provided to each user when they want to access the data from the cloud. Also, security device revocability is provided which is done when the device is stolen or lost. The cloud will immediately change the encryption scheme and the new key is sent to the user. This process is not known to the sender.
4) The cloud server cannot decrypt the ciphertext at anytime.

II. RELATED WORK

We first review some solutions which may contain similar functionalities. We will further explain why they cannot fully achieve our goal.

2.1 Distributed and concurrent access to cloud database

This architecture combines the cloud database services with the data confidentiality and the possibility of executing concurrent operations on encrypted data. This serves as the first solution that supports the client to directly connect to the encrypted cloud database. In this they have used Secure DBaaS which provides confidentiality, scalability, elasticity and eliminates the use of trusted third proxies.

Secure DBaaS uses two types of metadata: Database metadata and Table metadata, which are used to secure the encrypted data in the cloud. A master key is associated with every client so that the concurrency is achieved.

The present version of the Secure DBaaS prototype supports PostgreSQL, MySql and SQL Server relational databases. This architecture can be used to provide services to large amount of users concurrently.

2.2 Privacy preserving public auditing system

In this a privacy-preserving public auditing system is used to provide security to the data stored in the cloud. In this they introduce a TPA (Third Party Auditor) to check the integrity of the outsourced data and be worry free. The main problem discussed in [2] is how to tackle the privacy-preserving third party auditing independent of data encryption.

As a solution we utilize the technique of public key based homomorphic linear authenticator which enables TPA to perform auditing with demanding local copy of data and it reduces the computation and communication overhead. The public auditing scheme consists of four algorithms: KeyGen, SigGen, GenProof, Verify Proof. Here they have proposed two basic solutions:

i. MAC- based solution: Used for authentication of the data

ii. HLA-based solution: Supports public auditability

Thus this system may concurrently handle multiple auditing upon different user’s delegation.

2.3 Two factor data security in cloud storage system

This system proposes a two factor data security mechanism with factor revocability for cloud storage system. The cloud storage enhances the data accessibility at anytime anywhere as long as there is network access. To enhance the security protection the following are considered:

1. Double Encryption: The plaintext is encrypted using public key and again encrypted with a random key generator of a unique security device.
2. Split the secret key into two parts: The first part is stored in computer while second part is embedded into security device. But there exist problems such as if any part of secret key is known to attacker, data can be decrypted easily. So this technique is not useful. They used another method called Leakage-Resilient encryption (LRE), which guarantees security even if some amount of secret key is leaked. To decrypt data user needs two things:

    i. His own secret key
    ii. unique personal security device.

2.4 Dynamic audit services for outsourced storages in clouds

This system proposes a dynamic audit service for verifying the integrity of an untrusted and outsourced storage. In this the audit services uses fragment structure, random sampling and index-hash table. The security audit enables trace-back and analysis of any activities including data accesses, security breaches and so on. A proof of concept prototype is implemented to evaluate the feasibility and viability of proposed approaches. Main operations used in audit services are:

1) Tag Generation: client uses secret key to prepare a file.
2) Periodic sampling audit: using interactive proof protocol solution for random sampling is achieved.
3) Audit for dynamic operations: In practical applications this architecture can be constructed into a virtualization infrastructure which implements HDFS concepts.

2.5 Ciphertext policy for attribute based encryption

In this, the system combines the homomorphic encryption algorithm with traditional CP-ABE algorithm which ensure ciphertext retrieval and also reduces the retrieval time. CP-ABE algorithm usually performs the following: setup, encrypt, keygen and decrypt. The basic idea is traditional CP-ABE algorithm and factoring homomorphic encryption algorithm combined to achieve a searchable ciphertext. First users encrypt the plaintext using homomorphic encryption. Then using CP-ABE it is again encrypted using homomorphic key. Finally, homomorphic key cipher and ciphertext of message combined to produce final ciphertext document. So this ensures more security. This concludes that using CP-ABE access control scheme, users can retrieve the needed data from the file which is stored in the cloud and do not need to download ciphertext.

III. OVERVIEW

3.1 Proposed System

Inspired by [7], we propose a three factor data security protection mechanism for cloud storage system. Before going to the system, let’s see the entities involved in the system.

- Security device issuer: The main role of SDI is to issue a device whenever the user requests for it. The device is issued only after checking the credentials of the user.
- Cloud server: It is mainly used to store ciphertext and has the capability to revoke the device once it is found to be lost.
- Sender: He/ She is the initiator of the process. The sender transmits the encrypted data to the cloud.
- Receiver: It is the recipient of the ciphertext. It can be decrypted using private key of the receiver..
- Private key generator: It is third party which provides unique private key for each user.

Now let us discuss the mechanism of our system illustrated in fig.3.1. This system describes a novel three factor security protection mechanism for data stored in the cloud. The system is based on IBE.

Identity based encryption (IBE) is a primitive of ID-based cryptography. It is a type of public key encryption, in which the public key of a user is some unique information about the identity of the user. This means that the sender can encrypt the data using receiver’s name or email address as a key. The receiver can decrypt the data using the key sent by the central authority, which is to be trusted as it generates secret keys for every user. This system allows any party to generate a public key from a known identity values as an ASCII string. A trusted third party- Private Key Generator (PKG), generates the corresponding private keys. It provides master key using which the parties may encrypt without prior distribution of keys between individual participants. The three factors are:

- Encryption of plaintext using public key of the receiver
- The automatic encryption in the cloud using an AI program and
- The security device for each user

This enhances the security of the existing system. In order to decrypt the ciphertext the user needs three things: his/her private key, shared key and the device key. Without either piece the decryption is impossible. The cloud server cannot decrypt the ciphertext at anytime.

3.2 Detailed Process

The process starts with the sender. Initially the data is encrypted using the public key of the receiver. Whenever a user creates an account, a private key is generated. The private key is unique for each user.

The sender transmits the encrypted data to the cloud.

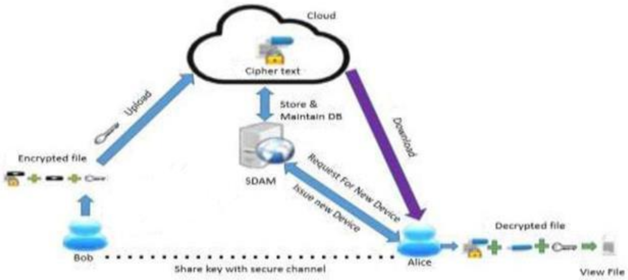

Fig.3.1. Overall architecture diagram

In the cloud an automated encryption is performed using an AI program. From a set of encryption algorithms, a random algorithm is chosen and the data is encrypted. Once the encryption is performed the key is sent to the receiver. Then the receiver request for a security device to SDI. The Security device issuer verifies the user credentials and then the device is issued to the receiver. The receiver must possess three things in order to decrypt the data. First, the device key which opens the device and shows the list of files in the cloud. Then to download the file the receiver must enter the shared key sent from the cloud and finally, his/her private key is used to decrypt the final ciphertext.

IV. CONCLUSIONS

Various techniques are available to provide security for cloud storage data. Among them, three-Factor Data Security Protection mechanism only provides confidentiality of the data and revocability for cloud data by using secret key and unique personal device. The efficiency and security analysis show that the system is secure as well as practically implemented.

V. FUTURE ENHANCEMENT

Our solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked, the corresponding ciphertext will be updated automatically by the cloud server without any notice of the data owner. Furthermore, we presented the security proof and efficiency analysis for our system.

REFERENCES

[1] J. Shao and Z. Cao. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. Information Sciences, 206(0):83 – 95, 2012.

[2] Luca Ferretti , Michele Colajanni and Micro Marchetti. Distributed, concurrent and independent access to encrypted cloud databases. IEEE Transactions on Parallel and Distributed systems, 2013.

[3] V. Varadharajan and U. K. Tupakula. Security as a service model for cloud environment. IEEE Transactions on Network and Service Management, 11(1):60–75, 2014.

[4] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for secure cloud storage. IEEE Trans. Computers, 62(2):362–375, 2013.

[5] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou. Toward secure and dependable storage services in cloud computing. IEEE T. Services Computing, 5(2):220–232, 2012.

[6] A. Akavia, S. Goldwasser and V. Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks, in Proc. 6th Theory Cryptography Conf., 2009, pp. 474–495.

[7] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jlianghua Liu and Yang Xiang. Two factor data security protection mechanism for cloud storage system. IEEE Transactions on Computers, 65(6), June 2016.

[8] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, “Certificate based (linkable) ring signature,” in Proc. Inf. Security Practice Experience Conf., 2007, pp. 79–92.

[9] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An and C. Hu. Dynamic audit services for outsourced storages in clouds. IEEE Transactions on Services Computing, 6(2), April 2013.

[10] M. Blaze, G. Bleumer and M. Strauss, Divertible protocols and atomic proxy cryptography, in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1998, pp. 127–144.

[11] A. Boldyreva, V. Goyal, and V. Kumar, Identity-based encryption with efficient revocation, in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426.