BI SECURITY MECHANISM FOR CLOUD STORAGE

V.SRAVAN KUMAR
Mtech(Computer Science and Engineering)
Institute Of Aeronautical Engineering
Dundigal Hyderabad
Email id : vasalasravankumar585@gmail.com

YERRAGUDIPADU SUBBARAYUDU
Asst Professor(Computer Science And Engineering)
Institute Of Aeronautical Engineering,
Dundigal ,Hyderabad
Email Id - Subbu.Iare@Gmail.Com

Abstract

In this paper, a two-factor data security protection mechanism with factor revocability for cloud storage system is proposed. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the cipher text. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the cipher text without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any cipher text. This can be done by the cloud server which will immediately execute some algorithms to change the existing cipher text to be un-decrypt able by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text at any time. The security and efficiency analysis show that our system is not only secure but also practical.

Introduction:

Cloud storage is a model of network storage system which is stored in pools of storage which are generally hosted by third parties. There are many benefits to use cloud storage system. The most notable is data accessibility and data access at any time and any place there is a network access. Another advantage of cloud storage is data sharing between users.

By sharing storage and networks with many other users it is also possible for other unauthorized users to access your data. This may be due to mistaken actions, faulty equipment, or sometimes because of criminal intent.

A promising solution to offset the risk is to deploy encryption technology. Encryption can the protect data as it is being transmitted to and from the cloud service. In a normal asymmetric encryption, there is a single secret key coresponding to public key or an identity of receiver. The decryption of cipher text only requires this key. The key is usually stored inside either a personal computer or trusted server and may be protected by a password. Unfortunately, connected with the world through the internet, the computer / server may suffer

from potential risk by hackers. The secret key can be compromised by some attackers who can access the victim's personal data stored in the cloud system. Therefore, there exists a need to enhance the security protection an analogy is e-banking security. Many e-banking applications require a user to use both a password and a security device (two factors) to login system for money transfer.

The security device may display a one-time password to let the user type it into the system or it may be needed to connect with the computer (e.g., through USB or NFC). The purpose of using two factors is to enhance the security protection for the access control. As cloud computing becomes more mature and there will be more applications and storage services provided by the cloud, it is easy to for e see that the security for data protection in the cloud should be further enhanced. They will become more sensitive and important, as if the e - banking analogy. Actually, w e have noticed that the concept of t w o –security key encryption, which is one of the encryption trends for data protection, one has been spread into some real-world applications, for example, full disk encryption with Ubuntu system,

- AT&T two factor encryption for Smart phones,
- Electronic vaulting and druva—cloud-based data encryption.
- However, these applications suffer from a potential risk about factor revocability that may limit their practicability.

Literature Survey

Identity-based Encryption with Efficient Revocation

Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority.

Unidirectional Chosen-Cipher text Secure Proxy Re-Encryption

In 1998, Blaze, Bleumer, and Strauss proposed a cryptographic primitive called proxy re-encryption, in which a proxy transforms – without seeing the corresponding plaintext – a cipher text computed under Alice's public key into one that can be opened using Bob's secret key. Recently, an appropriate definition of chosen-cipher text security and a construction fitting this model were put forth by Canetti and Hohen Berger.

Mediated Certificate less Cryptosystem for the Security Of Data In Public Cloud

Security is a serious issue in cloud computing. Encryption is the solution for the security in cloud. There are many encryption techniques. Each one has its own merits and demerits. In the case of identity based encryption it is free from security mediator, predefined keys are there, and have the problem of key escrow and certificate revocation.

Methodologies:

Existing System

As cloud computing becomes more mature and there will be more applications and storage services provided by the cloud, it is easy to foresee that the security for data protection in the cloud should be further enhanced. They will become more sensitive and important, as if the e-banking analogy. Actually, we have noticed that the concept of two keys encryption, which is one of the encryption trends for data protection, has been spread into some real-world applications, for example, full disk encryption with Ubuntu system, AT&T two keys encryption for Smartphones, electronic vaulting and druv—cloud-based data encryption. However, these applications suffer from a potential risk about factor revocability that may limit their practicability.

The existing approach is Double encryption and this is not a flexible approach because, if the user has lost his security device, then his/ her corresponding ciphertext in the cloud cannot be decrypted forever! That is, the approach cannot support security device update/revocability. Splitting Secrete Key into two parts is also one of the existing approaches. This approach may achieve the security goals in the cloud. However, note that the security of a normal encryption scheme cannot be guaranteed if part of the secret key has been exposed. The security is only guaranteed if the whole secret key has not been exposed to the adversary.

Drawbacks of the Existing System

The sender needs to know the serial number/ public key of the security device, in additional to the user's identity/public key. That makes the encryption process more complicated.

The security of the existing system is still guaranteed if the leakage of the secret key is up to certain bits such that the knowledge of these bits does not help to recover the whole secret key.

Proposed System

To overcome the existing system drawbacks, in this proposed work we used Identity Based Encryption Algorithm (IBE) to develop a novel two security keys protection mechanism for data stored in the cloud. Our mechanism provides the following nice features: 1) Our system is an IBE (Identity-based encryption)- based mechanism. That is, the sender only needs to know the identity of the receiver in order to send an encrypted data (ciphertext) to him/her. No other information of the receiver (e.g., public key, certificate etc.) is required. Then the sender sends the ciphertext to the cloud where the receiver can download it at anytime. 2) Our system provides two-factor data encryption protection. In order to decrypt the data stored in the cloud, the user needs to possess two things. First, the user needs to have his/her secret key which is stored in the computer. Second, the user needs to have a unique personal security device which will be used to connect to the computer (e.g., USB, Bluetooth and NFC). It is impossible to decrypt the ciphertext without either piece. 3) More importantly, our system, for the first time, provides security device (one of the factors) revocability. Once the security device is stolen or reported as lost, this device is revoked. That is, using this device can no longer decrypt any ciphertext (corresponding to the user) in any circumstance. The cloud will immediately execute some algorithms to change the existing cipher text to be un-decryptable by this device. While, the user needs to use his new/replacement device (together with his secret key) to decrypt his/her ciphertext; this process is completely transparent to the sender.

Advantages of Proposed System:

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.

1. The cloud server cannot decrypt any ciphertext at any time

Role based access control:

1. System Architecture:

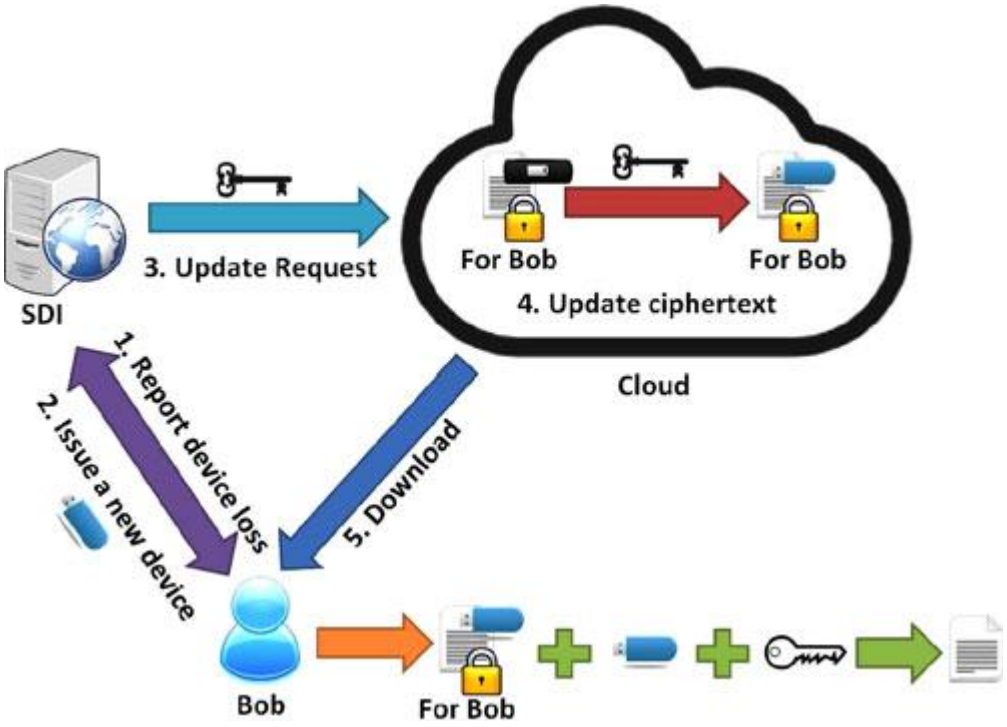

Fig1 : Update ciphertext after issuing a new security device

2. Architecture Work flow:

Setup phase: The setup phase generates all public parameters and master secret key used throughout the execution of system. The public parameters are shared with all parties participating into the system (including data sender/receiver, cloud server and a PKG), while the master secret key is given to the PKG.

Key and device issued phase: A SDI and a PKG will respectively generate a security device and a secret key for a registered user ID in secure channel such that the user can combine the security device with the secret key to recover message from its encrypted format.

First-level ciphertext generation phase: a data sender encrypts a data under the identity of a data receiver, and further sends the encrypted data to the cloud server.

Second-level ciphertext phase: After receiving the first level ciphertext of a data from the data sender, the cloud server generates the second-level ciphertext.

Device updated phase: Once a device of a user needs to be updated due to some incidences (e.g., it is either lost or stolen), the user first reports the issue to the SDI. The SDI then issues a new device for the user.

Ciphertext updated phase: The SDI notifies the cloud server to update the ciphertext of the user by sending a special piece of information.

Data recovery phase: A data receiver uses a decryption key and a device to recover the **data**

MODULES

In this implementation we have 5 Modules,

1. Private Key Generator (PKG)
2. Security Device Issuer
3. Sender
4. Receiver
5. Cloud Server

Module Description:

Private Key Generator: It is a trusted party responsible for issuing private key of every user.

Security Device Issuer (SDI): It is a trusted party responsible for issuing security device of every user.

Sender: She is the sender (and the creator) of the ciphertext. She only knows the identity (e.g., email address) of the receiver but nothing else related to the receiver. After she has created the ciphertext, she sends to the cloud server to let the receiver for download.

Receiver: He is the receiver of the ciphertext and has a unique identity (e.g., email address). The ciphertext is stored on cloud storage while he can download it for decryption. He has a private key (stored in his computer) and a security device (that contains some secret information related to his identity). They are given by the PKG. The decryption of ciphertext requires both the private key and the security device.

Cloud server: The cloud server is responsible for storing all ciphertext (for receiver to download). Once a user has reported lost of his security device (and has

obtained a new one from the PKG), the cloud acts as a proxy to re-encrypt all his past and future ciphertext corresponding to the new device. That is, the old device is revoked.

Performance study

We show the running time comparison and practical communication comparison in table 1 and 2 respectively.

The experimental results are same how similar to the theoretical ones. Our system needs extra running time in device generation and update.

- In practical, if we make security device as USB disk and deliver it to a registered user by mail/in person, there is no needs for paying the price for communication cost in the metrics of "security device size" and "cost in cipher text update".

TABLE-1

Computation Comparison (Running Time in Second)

Scheme	[2]	[20]	Ours
Secret Key Generation	0.007311	0.003123	0.007311
Security Device Generation	_	_	0.00614
Ciphertext Generation	0.049203	0.027515	First-level Ciph:0.010380 Second–level ciph:0.026214
Ciphertext Update	_	0.055677	0.065312
Device update	_	_	0.006606

Data Recovery (from Orginal Ciph.)	0.018146	0.036948	0.049095
Data Recovery (from updated ciph.)	_	0.021569	0.032797

TABLE-2 Communication comparison (length of size in bit)

Schemes	[2]	[20]	Ours
Secret Key Size	160	160	320
Security Device Size	_	_	640
OriginalCiphertextSize	480	1,504	1600
Update ciphertext Size	_	1,504	2144
Cost in Ciphertext Update	_	320	320

- From table (1) we see that our running time is nearly the same as that of [20] and meanwhile, our system outperforms (20) and (2) in encryption.
- In the communication cost, our scheme suffers from the largest price in "update Ciphertext Size" due to a reason that the scheme outputs a pairing in the update phase.
- However, state that the price is only an approximately 50percent increase from that of [20] in the name metric, which is an acceptable increment.

Conclusions:

In this paper, a novel two-factor data security protection mechanism for cloud storage system is developed, in which a data

sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use both his/her secret key and a security device to gain access to the data. 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 cipher text 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.