**Two-Factor Data Security Protection Mechanism for Cloud Storage System**

**Abstract**

In this paper, we propose a two-factor data security protection mechanism with factor revocability for cloud storage system. 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 ciphertext. 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 ciphertext without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any ciphertext. This can be done by the cloud server which will immediately execute some algorithms to change the existing ciphertext to be un-decryptable by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any ciphertext at any time. The security and efficiency analysis show that our system is not only secure but also practical.

**EXISTING SYSTEM**

This is the most convenient mode of encryption for data transition, due to the elimination of key management existed in symmetric encryption. 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.

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-factor encryption, which is one of the encryption trends for data protection1, has been spread into some real-world applications, for example, full disk encryption with Ubuntu system, AT&T two factor encryption for Smartphones2, electronic vaulting and druva - cloud-based data encryption3. However, these applications suffer from a potential risk about factor revocability that may limit their practicability.

**Proposed System**

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.

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.

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 ciphertext 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.

The cloud server cannot decrypt any ciphertext at any time. We provide an estimation of the running time of our prototype to show its practicality, using some benchmark results. We also note that although there exist some naive approaches that seem to achieve our goal, that there are many limitations by each of them and thus we believe our mechanism is the first to achieve all the above mentioned features in the literature.

### IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**MODULE DESCRIPTION:**

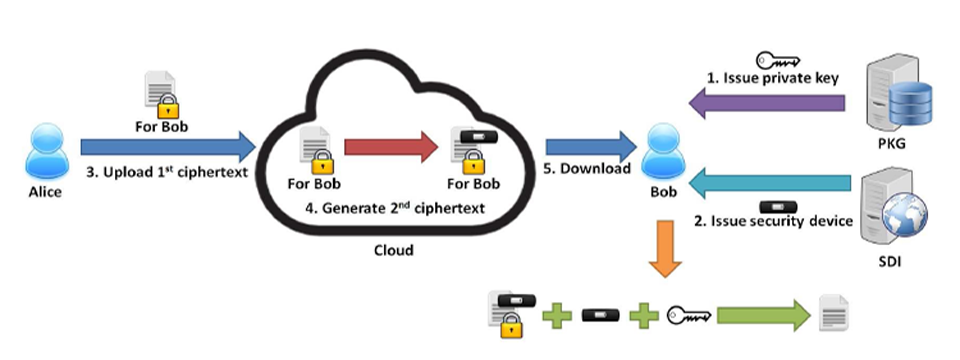
1. Cryptosystems with Two Secret Keys
2. Cryptosystems with Online Authority
3. Cryptosystem with Security Device
4. Cryptosystem with Revocability

**Cryptosystems with Two Secret Keys**

There are two kinds of cryptosystems that requires two secret keys for decryption. They are certificateless cryptosystem and certificate-based cryptosystem. Certificateless cryptosystem (CLC) was first introduced in further improvements can be found. It combines the merits of identitybased cryptosystem (IBC) and the traditional public-key infrastructure (PKI). In a CLC, a user with an identity chooses his own user secret key and user public key. At the same time the authority (called the Key Generation Centre (KGC)) further generates a partial secret key according to his identity. Encryption or signature verification requires the knowledge of both the public key and the user identity. On the opposite, decryption or signature generation requires the knowledge of both the user secret key and the partial secret key given by the KGC. Different from the traditional PKI, there is no certificate required. Thus the costly certificate validation process can be eliminated. However, the encryptor or the signature verifier still needs to know the user public key. It is less convenient than IBC where only identity is required for encryption or signature verification.

**Cryptosystems with Online Authority**

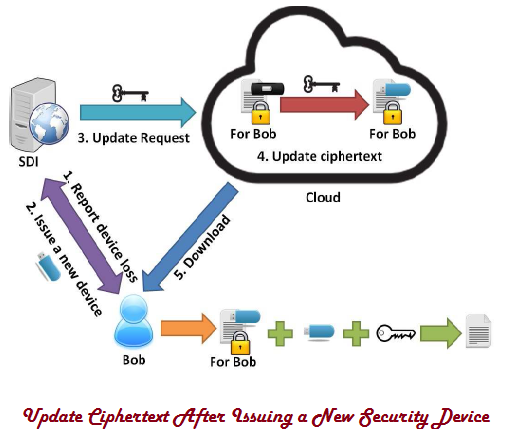
Mediated cryptography was first introduced for the purpose of revocation of public keys. It requires an online mediator, referred to a SEM (SEcurity Mediator), for every transaction. The SEM also provides a control of security capabilities. If the SEM does not cooperate then no transactions with the public key are possible any longer. In other words, any revoked user cannot get the cooperation from the SEM. That means revoked users cannot decrypt any ciphertext successfully. Later on, this notion was further generalized as security mediated certificateless (SMC) cryptography. In a SMC system, a user has a secret key, public key and an identity. The user secret key and the SEM are required to decrypt a ciphertext or sign a message. On the opposite side, the user public key and the corresponding identity are needed for signature verification or encryption. Since the SEM is controlled by the revocation authority, the authority can refuse to provide any cooperation for revoked user so that no revoked user can generate signature or decrypt ciphertext. Note that SMC is different from our concept. The main purpose of SMC is to solve the revocation problem. Thus the SME is controlled by the authority and it has to be online for every signature signing and ciphertext decryption. Furthermore, it is not identity-based. The encryptor (or signature verifier) needs to know the corresponding public key in addition to the identity. That makes the system less practical and looses the advantages of using identity-based system.



**Cryptosystem with Security Device**

There is a physically-secure but computationally-limited device in the system. A longterm key is stored in this device, while a short-term secret key is kept by users on a powerful but insecure device where cryptographic computations take place. Short term secrets are then refreshed at discrete time periods via interaction between the user and the base while the public key remains unchanged throughout the lifetime of the system. The user obtains a partial secret key from the device at the beginning of each time period. He then combines this partial secret key with the one from the previous period, in order to renew the secret key for the current time period.

Different from our concept, key-insulated cryptosystem requires all users to update their key in every time period. It may require some costly time synchronization algorithms between users which may not be practical in many scenarios. The key update process requires the security device. Once the key has been updated, the signing or decryption algorithm does not require the device anymore within the same time period. While our concept does require the security device every time the user tries to decrypt the ciphertext.



**Cryptosystem with Revocability**

Another cryptosystem supporting revocability is proxy re-encryption (PRE). Decryption rights delegation is introduced in Blaze, Bleumer and Strauss formally defined the notion of PRE. To employ PRE in the IBE setting, Green and Ateniese defined the notion of identity-based PRE (IB-PRE). Later on, Tang, Hartel and Jonker proposed a CPA-secure IB-PRE scheme, in which delegator and delegatee can belong to different domains. After that there are many IB-PRE systems have been proposed to support different user requirements. Among of the previously introduced IB-PRE systems, is the most efficient one without loss of revocability. We state that leveraging can only achieve one of our design goals, revocability, but not two-factor protection.

# System Configuration

# H/W System Configuration:

# Processor - Pentium –III

Speed - 1.1 Ghz

RAM - 256 MB(min)

Hard Disk - 20 GB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

# S/W System Configuration:

* Operating System :Windows95/98/2000/XP
* Application Server : Tomcat5.0/6.X
* Front End : HTML, Java, Jsp
* Scripts : JavaScript.
* Server side Script : Java Server Pages.
* Database : Mysql
* Database Connectivity : JDBC.

**CONCLUSIONS**

In this paper, we introduced a novel two-factor data security protection mechanism for cloud storage system, 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 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.