Data Security Protection Mechanism of Two Factors for Cloud Storage System

Mrs. Mukul P. Jagtap.

Lecturer
Computer Engineering Department

***Abstract*—In this paper, a two factor data security is proposed with factor revocability for cloud storage systems. In this system the sender sends an encrypted message to the receiver via a cloud storage server. Only the identity of receiver needs to be known by the sender. The identity information includes receiver's public key or certificate. The receiver requires to know only two things to decrypt the ciphertext i.e. first it requires his/her secret key stored in the computer and second a unique personal security device that connects to the computer. Without this information it is impossibleto decrypt the ciphertext. If in case, the security device is stolen or lost then it cannot be used again to decrypt any ciphertext (the device is revoked). For this faulty device the cloud server will execute some algorithms and convert the stored ciphertext in the device to un-decryptable text. The sender is aware of this entire process. With this transparency, it can be concluded that our system is not only secure but also practical.**

***IndexTerms*—Two Factor, Security, Cloud Storage, Revocability**

I. INTRODUCTION

Cloud storage is a model used for data accessibility. Data stored in the cloud is accessible atany time from any place as long as there is a network access. Another advantage of cloud storageis data sharing between users. Despite of above advantages outsourcing data storage increases thepossibility of attack at the same time. A promising solution to reduce the risk of attack is to deploy encryption technology.

ENHANCED SECURITY PROTECTION is a solution.In a normal asymmetric encryption,there is a single secret key corresponding to a public key or an identity. The decryption of ciphertext only requires this key. The key is usually stored inside either a personal computer or atrusted server, and may be protected by a password. The security protection is sufficient if the Computer server is isolated from an opening network. Unfortunately, this is not what happensin the real life. When being connected with the world through the Internet, the computer/server may suffer from a potential risk that hackers may intrude into it to compromise the secret keywithout letting the key owner know. In the physical security aspect, the computer storing a userdecryption key may be used by another user when the original computer user (i.e. the key owner)is away (e.g., when the user goes to toilet for a while without locking the machine). In an enterpriseor college, the sharing usage of computers is also common. For example, in a college, a publiccomputer in a copier room will be shared with all students staying at the same floor. In thesecases, the secret key can be compromised by some attackers who can access the victims personaldata stored in the cloud system. Therefore, there exists a need to enhance the security protection.

II. LITRATURE SURVEY

In [1], the certificate less cryptosystem is introduced. It combines the merits of identity-based cryptosystem and traditional public-key infrastructure.In [2], encryption or signature verification requires the knowledge of both the public key and user identity. In [3], the concept of Certificate-Based Cryptosystem(CBC) is introduced. In [4], the concept is almost the same as CLC, except that the partial secret key given by the KGC is a signature of the identity and the public key of the user by the KGC. Due to the similarities, CBC faces the same disadvantages as CLC mentioned above. In [5], the mediated cryptography was introduced for the purpose of revocation of public keys.In [6], the Security Mediated Certificateless(SMC) cryptography is introduced. 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.

In [7], the paradigm of key-insulated cryptography was introduced. A long-term key is storedin this device, while a short-term secret key is kept by users on a powerful but insecure device where cryptographic computations take place. Different from our concept, key-insulated cryptosystem requires all users to update their key in every time period. 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.

III. SYSTEM OVEVIEW

Double Decryption

In this technique the encryption process is executed twice. First encrypt the plain text with the public key of the user. Second re-encrypt it using public key or serial number of the security device. While decrypting, the security device decrypts first, this partially decrypted ciphertext is the passed to the computer which uses users secret key to decrypt it again. If one of them doesn't agree to decrypt, then the process of decryption remains incomplete.

Split the Secret Key in two parts

The first part is stored in the computer while the second part is embedded into a security device. Similar to the above approach, without either part one cannot decrypt the ciphertext. This security approach cannot be completely guaranteed. The security is only guaranteed onlyif the whole secret key has not been exposed to the adversary. There exists another cryptographic primitive called \leakage-resilient encryption. In this technique the leakage of a few bits of secret key is considered normal.

Some real-world systems, such as ATT and druva, also leverage two-factor encryption techniquesto protect message from being leaked to malicious users. However, their techniques suffer from a potential practical risk. Below we take druva system as an example. In a druva system, a message is first encrypted under a user key k1, and next uploaded to a cloud server. The user key k1 is further encrypted by another user key k2, and stored in the server as well. The key k2is held by the user. When retrieving the message, the user needs to use k2 to recover k1 which is further used to recover m. It is undeniable that this message-key-encrypt mechanism is much better than the mode only using a single key to encrypt an outsourced data, and storing the ciphertext along with the key in the server. Nevertheless, this mechanism suffers from a potential risk in practice (which we have mentioned previously): once the user loses the key k2, all data of the user stored in the cloud cannot be retrieved. The lack of revocability for encryption factor limits the flexibility of the system.

The system proposes a fine-grained two factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the following properties (1) It can compute some lightweight algorithms, e.g. hashing and exponentiation and (2) it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside. In this paper, we propose a fine grained two factor access control protocol for web-based cloud computing services, using a lightweight security device.

The protocol used supports fine-grained attribute-based access which provides a great exibility for the system to set different access policies according to different scenarios. At the same time , the privacy of the user is also preserved. The cloud system only knows that the user processes some required attribute, but not the real identity of the user. To show the practicality of our system, we simulate the prototype of the protocol.

IV. SYSTEM ARCHITECTURE

The mechanisms framework is demonstrated in fig 1 and fig 2 below. When a new system user, say Bob, joins our system, a PKG will issue a private key, and SDI will issue a security device to him. Both the private key and the security device are necessary for recovering a data from its encrypted format. In ordinary data sharing, a data sender, say Alice, first encrypts the sharing data under the identity of a data receiver, say Bob, and next uploads the ciphertext to the cloud server. Here we refer to this ciphertext as first-level ciphertext. After receiving the first-level ciphertext from Alice, the cloud server then turns the ciphertext to become a second-level ciphertext for the corresponding security device belonging to Bob. Bob then downloads the second level ciphertext from the cloud, and next recovers the data from its encrypted form by using his private key and security device.

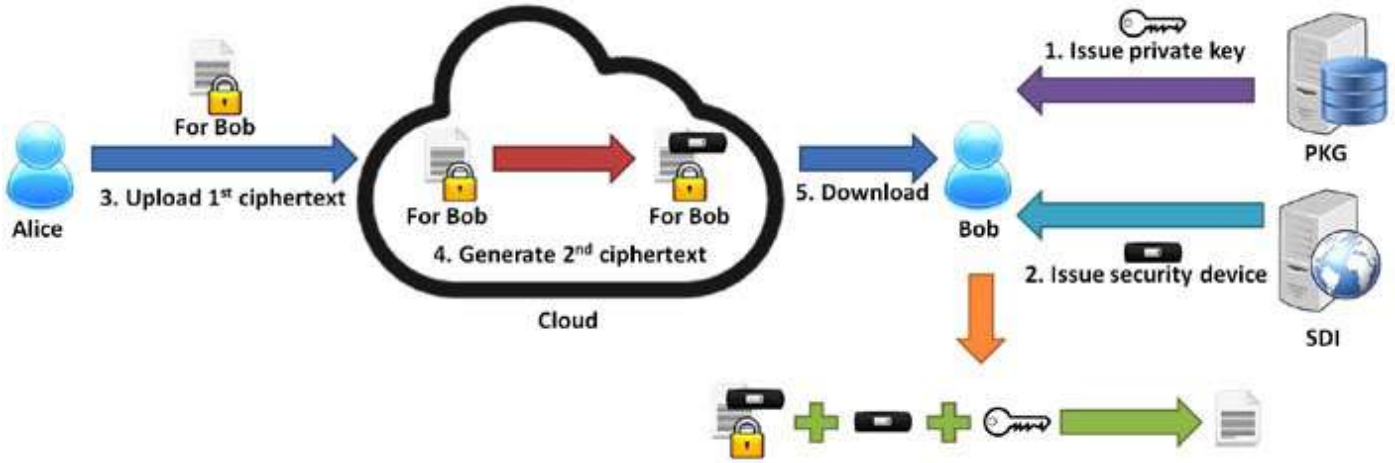

Figure 1- Ordinary Data Sharing.

When the security device of Bob is either lost or stolen, Bob first reports the issue to the SDI. The SDI then issues a new security device to Bob, and meanwhile, it sends a request of updating Bobs corresponding ciphertext along with a special key to the cloud server. The cloud server updates the ciphertext of Bob under an old security device to the ones under a new device. However, it does not gain access to the underlying data in the update process. Here Bob is allowed to download and recover the data by using his private key and new security device.

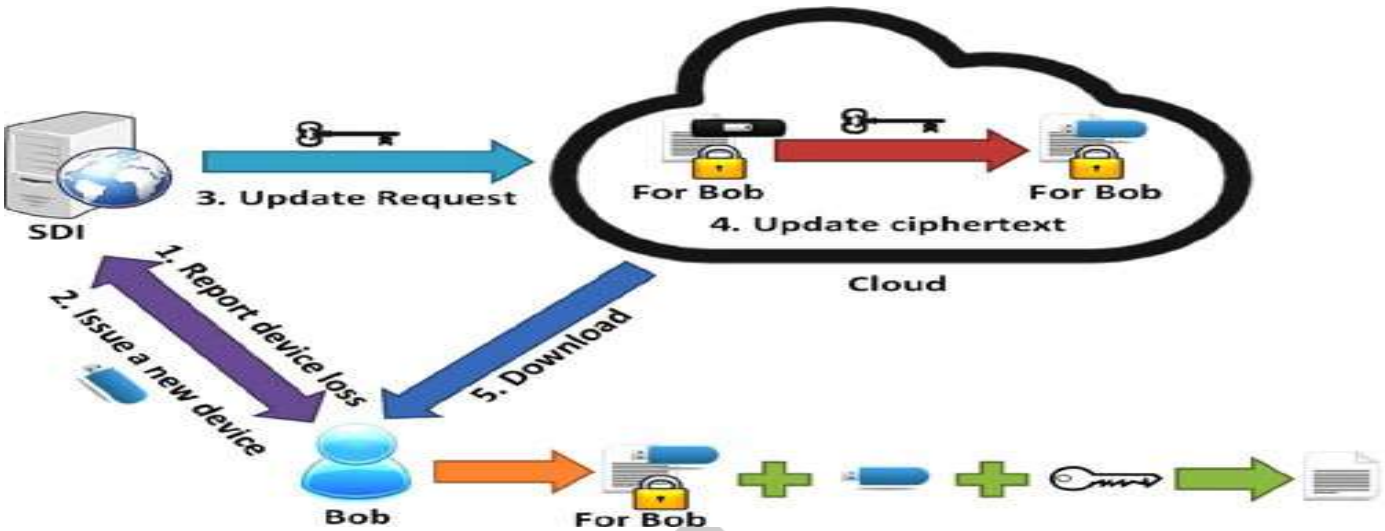

Figure 2- Update Cipher text after issuing a new Security Device.

In 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. And in Second-level ciphertext generation phaseafter receiving the firstlevel ciphertext of a data from the data sender, the cloud server generates the second-level ciphertext.

V. CONCLUSION

In this paper, a novel two-factor data security protection mechanism for cloud storage system is introduced. In which a data sender is allowed to encrypt the data with knowledge of the identityof a receiver only. The receiver is required to use both his/her secret key and a security device to gain access to the data. This 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 correspondingciphertext will be updated automatically by the cloud server without any notice of the dataowner.

VI. REFERENCES

[1] S. S. Al-Riyami and K. G. Paterson, \ Certificate less public key cryptography," in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003, pp. 452473.

[2] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, \Malicious KGC attacks in certificate less cryptography, in Proc. 2nd ACM Symp. Inf., Comput. Commun. Security, 2007 pp. 302311.

[3] C. Gentry, \Certificate-based encryption and the certificate revocation problem, in Proc. Int. Conf. Theory Appl. Cryptographic Techn, 2003, pp. 272293.

[4] 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. 7992.

[5] D. Boneh, X. Ding, and G. Tsudik, \Fine-grained control of security capabilities, ACM Trans. Internet Techn., vol. 4, no.1, pp. 60 82, 2004

[6] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, \Security-mediated certificateless cryptography, in Proc. 9th Int. Conf. Theory Practice Public-Key Cryptography, 2006, pp. 508524.