Two Factor Data Protection Security Mechanism for Cloud Storage System

Priyanka Pawar[1], **Vrushali Ranmalkar[2]**

[1]Pune University, Vishwabharti Academy's College of Engineering Ahmednagar,

[2]Pune University, Vishwabharti Academy's College of Engineering, Ahmednagar.

Abstract

We propose a two-factor data security protection system with factor revocability for cloud storage system. This system allows a person or sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to recognize the identity of the receiver but no other information (like as its certificate or its public key). The receiver needs to possess two things in order to decrypt the cipher text. The first one is her/his secret key saved in the computer. The second thing is a unique personal security device which attach to the computer. It is impossible to decrypt the cipher text without either piece. More important thing, once the security device is lost or stolen, this device is revoked. It cannot be used to decrypt any cipher text. This can be completed by the cloud server which will immediately execute few algorithms to change the existing cipher text to be un-decryptable by this device. This process is totally transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text at any time. The efficiency and security analysis show that our system is not only practical but also secure.

***Keywords*:** *two factor, factor revocability, security, cloud storage.*

I. INTRODUCTION (*HEADING 1*)

Cloud storage system is a model of networked storage system where data or information is stored in pools of storage which are hosted by third parties. There are lots of benefits to use cloud storage. The most notable is data accessibility. Data stored in the cloud system can be accessed at any time from any place as long as there is network access. Storage maintenance tasks, like as purchasing additional storage capacity, can be offloaded to the responsibility of a service provider. And another benefit of cloud storage is data sharing between users. If Alice (person) wants to share a piece of data (e.g. a video) to Bob (person), it may be difficult for her to send it by email because of the size of data. Instead, Alice uploads the file of the video to a cloud storage system so that Bob can download it at any time from any place.

Despite its advantages, outsourcing data storage also increases the attack surface area at the same time. For e.g., when data is shared, the more locations it is stored the higher risk it contains for unauthorized physical access to the data. By distributing storage and networks with other users it is also possible for other unauthorized users to access your data. This may be due to faulty equipment, mistaken actions, or sometimes because of criminal intent. A promising solution to offset the risk is to deploy encryption technology. Encryption can secure data as it is being transmitted to and from the cloud service. It can further protect data that is stored at the service provider. Even there is an unauthorized adversary who has increased access to the cloud, as the data has been encrypted ,the adversary cannot know any information about the plaintext. Asymmetric encryption allows the encryptor to use only the public information(example. identity of the receiver or public key.) to generate a cipher text while the receiver uses her/his own secret key to decrypt. This is the most convenient way of encryption for data transition, due to the elimination of key management existed in symmetric encryption.

II Literature Survey

A. Cryptosystems with Two Secret Key

There are two types of crypto-systems that require two secret keys for decryption. They are certificate less crypto-system and certificate based cryptosystem. Certificate less cryptosystem (CLC) was first known in [1] and further improvements can be seen in [2]. It combines the merits of traditional public-key infrastructure (PKI) and the identity- based cryptosystem (IBC). In a Certificate less crypto-system, a user with an identity chooses 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. Signature verification or encryption requires the knowledge of both the user identity and the public key. 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 signature or the encryptor verifier still needs to know the user public key. It is less convenient than identity based cryptosystem where only identity is required for signature verification or encryption. Similar to certificate less cryptosystem (CLC), another primitive called certificate- based cryptosystem (CBC) was introduced in [3]. Further Further variants may include [4]. The logic is almost the same as CLC, except that the partial secret key given by the KGC (which is called the certificate) is a signature of the identity and the public key of the user by the KGC. (Note that in certificate less cryptosystem, the partial secret key given by the KGC is just the signature of the identity of the user.) Due to the similarities, CBC faces the same disadvantages as CLC mentioned above.

B. Cryptosystems with Online Authority

Mediated cryptography was first introduced in [5] 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 certificate less (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.

C. Cryptosystem with Security Device

The paradigm of key-insulated cryptography was introduced in [6]. There is a physically-secure but computationally-limited device in the system. A long- term 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 present 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 decryption algorithm or signing does not require the device anymore within the same time period. While our logic does require the security device every time the user tries to decrypt the ciphertext. Furthermore, there is no key updating required in our system. Thus we do not require any synchronization within the whole system.

D. Cryptosystem with Revocability

Since our system is an IBE-based mechanism, we below introduce IBE-based systems supporting revocability. The first revocable IBE is proposed by Boneh and Franklin [7], in which a ciphertext is encrypted under an identity id and a time period T , and a non- revoked user is issued a private key skid,T by a PKG such that the user can access the data in T . Boldyreva, Goyal and Kumar [8] proposed the security notion for revocable IBE. To achieve adaptive security, Libert and Vergnaud [9] proposed a revocable IBE scheme based on the combination of attribute-based encryption and IBE. Recently, Seo and Emura [11] formalized a revised notion for revocable IBE. Since its introduction, there are many variants of revocable IBE, such as [10]. The premise of a revocable IBE system is mainly related to a time period: next the decryption rights of the next time period relies on a secret token (for the next time period) issued by PKG and a current time period key. However, this premise yields inconvenience once the current time period key is lost. Another cryptosystem supporting revocability is proxy re-encryption (PRE). Decryption rights delegation is introduced in [12]. Blaze, Bleumer and Strauss [13] formally defined the notion of PRE. To employ PRE in the IBE setting, Green and Ateniese [14] 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, [14] is the most efficient one without loss of revocability. We state that leveraging [14] can only achieve one of our design goals, revocability, but not two-factor protection.

Conclusion

In this project, we introduced a novel two factor data security protection system for cloud storage system, in which a data sender is confess to encrypt the data with information of the identity of a receiver only, while the receiver is required to use both her/his 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 take back, the corresponding ciphertext will be updated automatically by the cloud server without any notice of the data owner. Furthermore, we introduced the security proof and efficiency analysis for our system.

References

[1]. S. S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In ASIACRYPT, volume 2894 of Lecture Notes in Computer Science, pages 452–473. Springer, 2003.

[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 ASIACCS, pages 302–311. ACM, 2007.

[3]. C. Gentry. Certificate-based encryption and the certificate revocation problem. In EUROCRYPT, volume 2656 of Lecture Notes in Computer Science, pages 272–293. Springer, 2003.

[4]. M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen. Certificate based (linkable) ring signature. In ISPEC, volume 4464 of Lecture Notes in Computer Science, pages 79–92. Springer, 2007.

[5]. D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techn., 4(1):60–82, 2004.

[6]. Y. Dodis, J. Katz, S. Xu, and M. Yung. Key-insulated public key cryptosystems. In EUROCRYPT, volume 2332 of Lecture Notes in Computer Science , pages 65–82. Springer, 2002.

[7]. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In CRYPTO ’01, volume 2139 of LNCS, pages 213– 229. Springer, 2001.

[8]. A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In P. Ning, P. F. Syverson, and S. Jha, editors, ACM Conference on Computer and Communications Security, pages 417–426. ACM, 2008.

[9]. B. Libert and D. Vergnaud. Adaptive-id secure revocable identity- based encryption. In M. Fechlin, editor, CT-RSA, volume 5473 of Lecture Notes in Computer Science, pages 1–15. Springer, 2009.

[10].A. Sahai, H. Seyalioglu, and B. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In R. Safavi- Naini and R. Canetti, editors, CRYPTO, volume 7417 of Lecture Notes in Computer Science, pages 199–217. Springer, 2012.

[11].J. H. Seo and K. Emura. Efficient delegation of key generation and revocation functionalities in identity-based encryption. In E. Dawson, editor, CT-RSA , volume 7779 of Lecture Notes in Computer Science , pages 343–358. Springer, 2013..