ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Data Security for Cloud Storage by Using Two-Factor Data

[1] Nimmaraju Rajesh
[1] Department of Computer Science, Siddartha Institute of Engineering and Technology
Ibrahimpatnam, Rangareddy, Telangna.

***Abstract* – 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**

INTRODUCTION

Cloud storage is a model of networked storage system where data is stored in pools of storage which are generally hosted by third parties. There are many benefits to use cloud storage. The most notable is data accessibility. Data stored in the cloud can be accessed at any time from any place as long as there is network access. Storage maintenance tasks, such as purchasing additional storage capacity, can be offloaded to the responsibility of a service provider. Another advantage of cloud storage is data sharing between users.
If Alice wants to share a piece of data (e.g. a video) to Bob, it may be difficult for her to send it by email due to the size of data. Instead, Alice uploads the file to a cloud storage system so that Bob can download it at anytime. Despite its advantages, outsourcing data storage also increases the attack surface area at the same time. For example, when data is distributed, the more locations it is stored the higher risk it contains for unauthorized physical access to the data. 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 protect 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 gained access to the cloud, as the data has been encrypted, the adversary cannot get any information about the plaintext. Asymmetric encryption allows the encryptor to use only the public [2] information (e.g. public key or identity of the receiver) to generate a ciphertext while the receiver uses his/her own secret key to decrypt. This is the most convenient mode of encryption for data transition, due to the elimination of key management existed in symmetric encryption.

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 [6], 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

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, March 2018

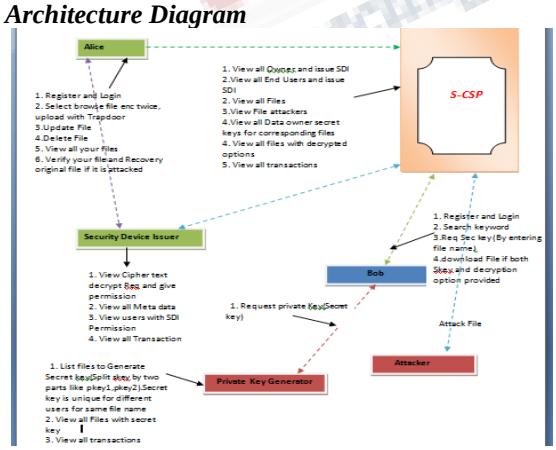
identity of the receiver in order to send an encrypted data (ciphertext) to him/her. No other information of the receiver (e.g. public key, certificate [3] etc.) is required. Then the sender sends the ciphertext to the cloud where the receiver can download it at anytime.

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.

Architecture Diagram



Modules:-

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

MODULES DESCRIPTION:

1.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 [4] 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.

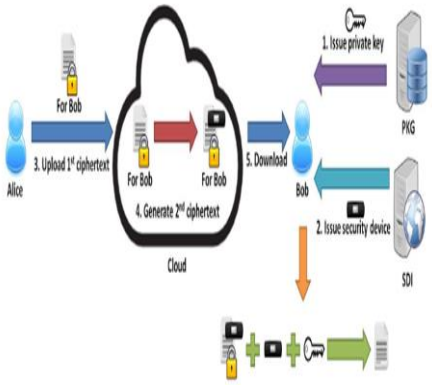
2. Cryptosystems with Online Authority

Mediated cryptography [1] 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

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, March 2018

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.



3.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.

Update Ciphertext After Issuing a New Security Device

4. 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.

LITERATURE SURVEY

1. Simultaneous Hardcore Bits and Cryptography against Memory Attacks.

Authors: A. Akavia, S. Goldwasser, V. Vaikuntanathan.
Cryptography Secure Against Memory Attacks.
A particularly devastating side-channel attack against cryptosystems, termed the "memory attack", was pro-
posed recently. In this attack, a significant fraction of the bits of a secret key of a cryptographic algorithm can be measured by an adversary if the secret key is ever stored in a part of memory which can be accessed even after power has been turned off for a short amount of time. Such an attack has been shown to completely compromise the security of various cryptosystems in use, including the RSA cryptosystem and AES.We show that the public-key encryption scheme of Regev (STOC 2005),and the identity-based encryption scheme of Gentry, Peikert and Vaikuntanathan(STOC 2008) are remarkably robust against memory attacks where the adversary can measure a large fraction of the bits of the secret-key, or more generally, can compute an arbitrary function of the secret-key of bounded output length. This is done without increasing the size of the secret-key, and without

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, March 2018

introducing any complication of the natural encryption and decryption routines.

2. Certificateless Public Key Cryptography

Authors: Sattam S. Al-Riyami and Kenneth G. Paterson

The main difficulty today in developing secure systems based on public key cryptography is not the problem of choosing appropriately secure algorithms or implementing those algorithms. Rather, it is the deployment and management of infrastructures to support the authenticity of cryptographic keys: there is a need to provide an assurance to the user about the relationship between a public key and the identity (or authority) of the holder of the corresponding private key.In a traditional Public Key Infrastructure (PKI), this assurance is delivered in the form of certificate, essentially a signature by a Certification Authority (CA)on a public key [1]. The problems of PKI technology are well documented, see for example [16]. Of note are the issues associated with certificate management,including revocation, storage and distribution and the computational cost of certificate verification. These are particularly acute in processor or bandwidth-limited environments [9].Identity-based public key cryptography (ID-PKC), first proposed by Shamir[22], tackles the problem of authenticity of keys in a different way to traditional PKI. In ID-PKC, an entity's public key is derived directly from certain aspects of its identity. Private keys are generated for entities by a trusted third party called a private key generator (PKG). The first fully practical and secure identity-based public key encryption scheme was presented in [5]. Since then, a rapid development of ID-PKC has taken place, see [18] for a brief survey. It has also been illustrated in [8, 18, 24] how ID-PKC can be used as a tool to enforce what might be termed "cryptographic work-flows", that is, sequences of operations (e.g. authentications) that need to be performed by an entity in order to achieve a certain goal.

3. A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero.

Authors: Shi-Feng Sun, Man Ho Au, Joseph K. Liu

We initially study the necessary properties and security requirements of Ring Confidential Transaction (RingCT) protocol deployed in the popular anonymous cryptocurrency Monero. Firstly, we formalize the syntax of RingCT protocol and present several formal security definitions according to its application in Monero. Based on our observations on the underlying (linkable) ring signature and commitment schemes, we then put forward a new efficient RingCT protocol
(RingCT 2.0), which is built upon the well-known Pedersen commitment, accumulator with one-way domain and signature of knowledge (which altogether perform the functions of a linkable ring signature). Besides, we show that it satisfies the security requirements if the underlying building blocks are secure in the random oracle model. In comparison with the original RingCT protocol, our RingCT 2.0 protocol
presents a significant space saving, namely, the transaction size is independent of the number of groups of input accounts included in the generalized ring while the original RingCT suffers a linear growth with the number of groups, which would allow each block to process more transactions.

4. Malicious KGC attacks in certificate less Cryptography.

Authors: Man Ho Au,Jing Chen,Joseph K. Liu

Identity-based cryptosystems have an inherent key escrow issue, that is, the Key Generation Center (KGC) always knows user secret key. If the KGC is malicious, it can always impersonate the user. Certificate less cryptography, introduced by Al-Riyami and Paterson in 2003, is intended to solve this problem. However, in all the previously proposed certificate less schemes, it is always assumed that the malicious KGC starts launching attacks (so-called Type II attacks) only after it has generated a master public/secret key pair
honestly. In this paper, we propose new security models that remove this assumption for both certificate less signature and encryption schemes. Under the new models, we show that a class of certificate less encryption and signature schemes proposed previously are insecure. These schemes still suffer from the key escrow problem. On the other side, we also give new proofs to show that there are two generic constructions, one for certificate less signature and the other for certificate less encryption, proposed recently that are secure under our new models

5. Divertible Protocols and Atomic Proxy Cryptography

Authors: Matt Blaze Gerrit Bleumer Martin Strauss

First, we introduce the notion of divertibility as a protocol property as opposed to the existing notion as a language property. We give a definition of protocol divertibility that applies to arbitrary 2-party protocols and is

compatible with Okamoto and Ohta's definition in the case of interactive zero-knowledge proofs. Other important examples falling under the new definition are Blind signature protocols [5] . We propose a sufficiency criterion for divertibility that is satisfied by many existing protocols and which, surprisingly, generalizes to cover several protocols not normally associated with divertibility (e.g., Diffie-Hellman key exchange). Next, we introduce atomic proxy cryptography,in which an atomic proxy function,in conjunction with a public proxy key,converts ciphertexts (messages or signatures) for one key into ciphertexts for another. Proxy keys, once generated, may be made public and proxy functions applied in untrusted environments. We present atomic proxy functions for discrete-log-based encryption, identification, and signature schemes. It is not clear whether atomic proxy functions exist in general for all public-key cryptosystems. Finally, we discuss the relationship between divertibility and proxy cryptography.

CONCLUSION

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.

REFERENCES

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In TCC,volume 5444 of Lecture Notes in Computer Science, pages 474–495.Springer, 2009
.

[2] 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.

[3] 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.

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang. Malicious kgc attacks in certificateless cryptography. In ASIACCS,pages 302–311. ACM, 2007.

[5] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In K. Nyberg, editor, EUROCRYPT,volume 1403 of LNCS, pages 127–144. Springer, 1998.

[6] 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.

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

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

[9] R. Canetti and S. Hohenberger. Chosen-ciphertext secure proxy re-encryption. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson,editors, ACM Conference on Computer and Communications Security,pages 185–194. ACM, 2007.

[10] H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang. Nccloud: A network-coding-based storage system in a cloud-of-clouds. IEEE Trans. Computers, 63(1):31–44, 2014.