iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10182

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

Two-Factor Data Security Protection Mechanism for Cloud Storage System

Mahesh K[1], Dr. Shiva Murthy G[2]
[1]*Computer science and engineering,* [2]*HOD, Department of Computer Science VTU-CPGS Muddenahalli, Chickkaballapura, India*

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.

Keywords:* *factor revocability, two-factor, security, cloud storage, encrypt, decrypt

I. INTRODUCTION

Cloud storage [6], [7], [14], [10] 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. 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 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.

II. OVERVIEW

In our two factor data security protection system, we have the following entities:

Private key(PKG) :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 (Alice): 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 (Bob): He is the receiver of the ciphertext and has a unique identity (e.g. email address).

The ciphertext is stored on a 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

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

III.RELATED WORK

In view of the expiration or reveal of user's private credential (or private key) in a realistic scenario, identity-based encryption (IBE) schemes with an efficient key revocation mechanism, Boldyreva,V et al. [2] presented an RIBE scheme from lattices by combining two Agrawal. IBE schemes with the subset difference (SD) method. This scheme is secure against adaptive identity- time attacks in the standard model under the learning with errors (LWE) assumption. Key-insulated cryptography is a crucial technique for protecting private keys. To strengthen the security of key-insulated protocols, Hanaoka, Hanaoka and Imai recently introduced the idea of parallel key-insulated encryption (PKIE) where distinct physically-secure devices (called helpers) are independently used in key updates. Their motivation was to reduce the risk of exposure for helpers by decreasing the frequency of their connections to insecure environments. J. H. Seo *et al. [5]* showed that it was non-trivial to achieve a PKIE scheme fitting their model and proposed a construction based on the Boneh-Franklin identity-based encryption (IBE) scheme. The security of their system was only analyzed in the idealized random oracle model. Dodis et al. [13] provided a fairly efficient scheme which is secure in the standard model (i.e. without random oracles). To do so, first show the existence of a relation between PKIE and the notion of aggregate signatures (AS) suggested by Boneh. Then describing the random oracle-free construction using bilinear maps. Thus, our contributions are both on the concrete side, namely the first realization of parallel key-insulated encryption without the random oracle idealization, and on the conceptual side revealing the relationships between two seemingly unrelated primitives.

A. *Following are the list of objective of the project work*

1) To design and develop only sender needs to know the identity of the receiver in order to send an encrypted data (ciphertext) to him/her.
2) To design and develop two-factor data encryption protection. In order to decrypt the data stored in the cloud.
3) To develop and design 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

IV.MODULES

A. *Cryptosystem 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 identity based 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.

B. *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.

C. *Cryptosystem with Security Device*

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 current time period.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

D. 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.

V. SYSTEM ARCHITECTURE

Framework

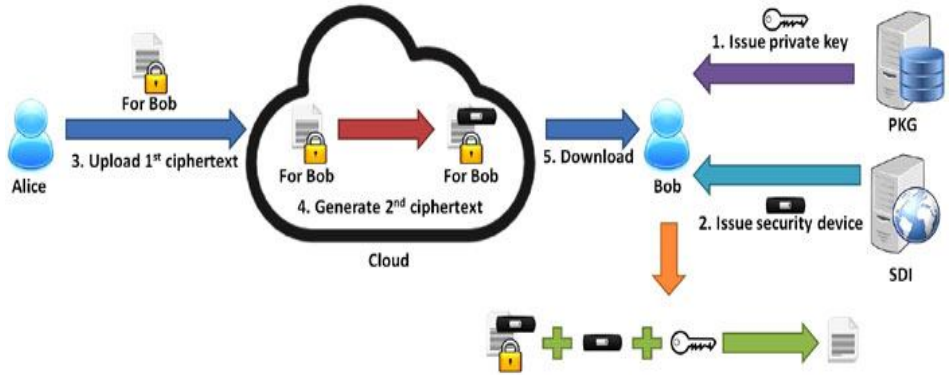


Fig 1: Ordinary Data Sharing

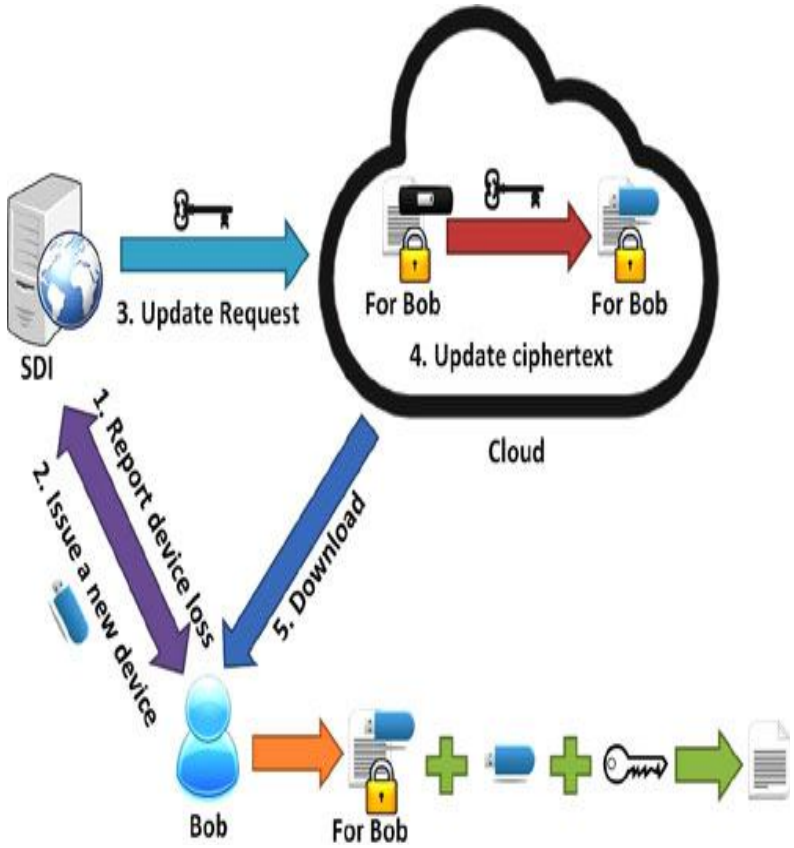


Fig 2: Update Ciphertext after issuing a new security device

VI. CONCLUSIONS

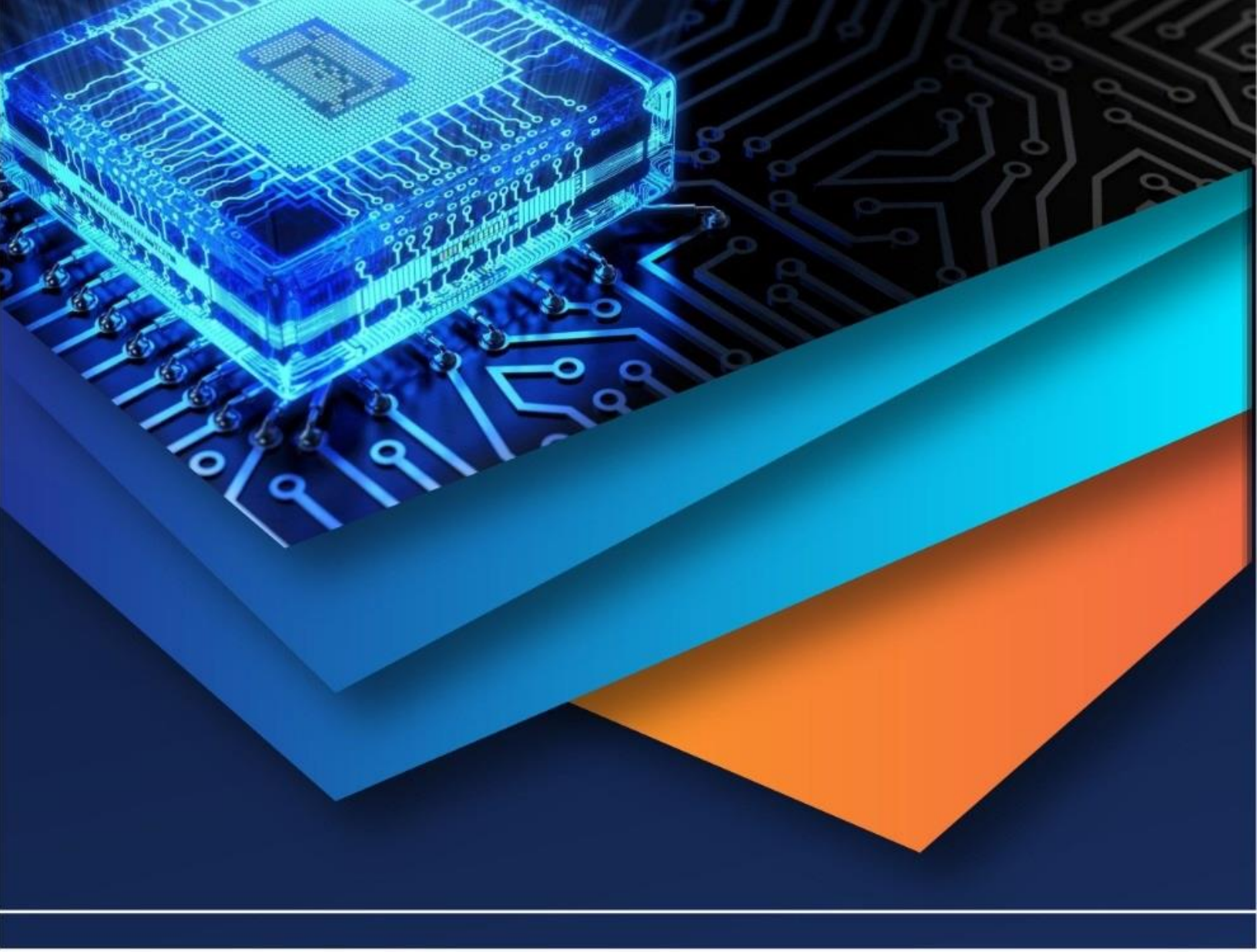
In this Paper we proposed a novel two-factor data security protection mechanism for cloud storage system, in which a data sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use both his/her secret key and a security device to gain 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.

VII. ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to Dr.Shiva Murthy G HOD, Department of Computer Science and Engineering, Visvesvaraya Institute of Advanced Technology. Who gave me the golden opportunity to do this wonderful project on the topic (Two Factor Data Security Protection Mechanism for Cloud Storage System), which also helped me in doing a lot of research and I came to know about so many new things I am really thankful to him. And, secondly I would also like to thank my parents who helped me a lot in finalizing this project within the limited time frame.

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] 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
[3] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang. A cca-secure identity-based conditional proxy re-encryption without random oracles. In T. Kwon, M. -K. Lee, and D. Kwon, editors, ICISC, volume 7839 of LNCS, pages 231–246. Springer, 2012.
[4] A. Sahai, H. Seyalioglu, and B. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption, 2012.
[5] 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
[6] V. Varadharajan and U. K. Tupakula. Security as a service model for cloud environment. IEEE Transactions on Network and Service Management
[7] H. Wang. Proxy provable data possession in public clouds. IEEET.Services Computing, 6(4):551–559, 2013
[8] . Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C. Hu. Dynamic audit services for outsourced storages in clouds. IEEE T. Services Computing, 6(2):227–238, 20
[9] Q. Tang, P. H. Hartel, and W. Jonker. Inter-domain identity-based proxy re-encryption. In M.Yung, P. Liu, and D. Lin, editors,Inscrypt, volume 5487 of Lectu Notes in Computer Science, pages 332–347. Springer, 2008.
[10] J. K. Liu, F. Bao, and J. Zhou. Short and efficient certificate-based signature.In Networking Workshops, volume 6827 of Lecture Notes in Computer Science, pages 167–178. Springer,2011.
[11] T. Matsuo. Proxy re-encryption systems for identity-based encryption.In Pairing '07, volume 4575 of LNCS, pages 247–267. Springer, 2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY