ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 5, Issue 11, November 2017**

# Two-Factor Data Protection: Enhances Confidentiality of the Data

Syed Saad[1], Sarika Bagade[1], Rahul Singh[1], Akshay Sidral[1], Prof. Vandana P. Tonde[2]

Dept. of Information Technology Sinhgad Institute of Technology, Lonavala, Savitribai Phule Pune University, Pune, India[1, 2].

**ABSTRACT:** This paper introduces the new novel two-factor data security protection solution with new way of revocability. Besides previous systems, our system sender only needs to know about the identity of receiver to encrypt data and to send through a cloud storage server. No other information like receiver keys or its certificate is needed to know to sender. We achievesuch data protection by security device revocability.The receiver needs to possess two things in order to decrypt the cipher text. 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 cipher text without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any cipher text. This can be done by the cloud server which will immediately execute some algorithms to change the existing cipher text to be undecryptable by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text at any time.

**KEYWORDS:** Two-factor, factor revocability, security, cloud storage

## I. INTRODUCTION

Cloud computing is emerging technology which enables universal, adoptable, on-demand access to shared data. Cloud increases its storage capacity and decreases the cost of processing. Data is stored in pools of storage which are generally hosted by third parties in cloud.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 any time. 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 toencryptor to use only the public information (e.g., public key or identity of the receiver) to generate a cipher text 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. We proposed enhanced data protection with two-factor encryption in which sender only need to know about receiver identity and receiver must have two things to decrypt data one is private key and other is security device. We are going to propose the device revocability if receiver device is stolen or lost.

In a normal asymmetricencryption, there is a single secret key corresponding to a public key or an identity. The decryption of cipher text only requires this key. The key is usually stored inside either a personal computer or a trusted 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 happens in 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 key without letting the key owner know. In the physical security aspect, the computer storing a user decryption key may be used by another user when the original computer user (i.e. the key owner) is away. Therefore, there exists a need to enhance the security protection.

The concept of two-factorencryption, which is one of the encryption trends for data protection, has been spread into some real-world applications, for example, full disk encryption with Ubuntu system, AT&T two factor encryption for Smart phones, electronic vaulting and druva cloud-based data encryption. However, these applications suffer from a potential risk about factor revocability that may limit their practicability. A flexible and scalable two-factor encryption mechanism is really desirable in the era of cloud computing. That motivates our work.

## II. LITERATURE SURVEY

The paper [1] explained a two-factor data security protection mechanism with factor revocability for cloud storage system. This system is based on 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 any time. Our proposed system will provide 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 cipher text without either piece.This system 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 cipher text will be updated automatically by the cloud server without any notice of the data owner.

Paper [2] presented a proxy-based storage system for fault-tolerant multiple-cloud storage called NCCloud, which achieves cost-effective repair for a permanent single-cloud failure. In our system we are also going to present NCCloud, a proxy-based, multiple-cloud storage system that practically addresses the reliability of today’s cloud backup storage. NCCloud not only provides fault tolerance in storage, but also allows cost-effective repair when a cloud permanently fails. NCCloud implements a practical version of the functional minimum storage regenerating (FMSR) codes, which regenerates new parity chunks during repair subject to the required degree of data redundancy. Our FMSR code implementation eliminates the encoding requirement of storage nodes (or cloud) during repair, while ensuring that the new set of stored chunks after each round of repair preserves the required fault tolerance. Our NCCloud prototype will show the effectiveness of FMSR codes in the cloud backup usage, in terms of monetary costs and response times. Disadvantage of [2] Cloud server can access information of user as he acts as a proxy server.

Whereas paper [3]a new unidirectional single-hop Identity-Based Conditional Proxy Re-Encryption (IBCPRE) scheme that not only captures the property of IBPRE (i.e. identity-based re-encryption), but also supports conditional re-encryption.

Disadvantages of paper [3] as proxy-based re-encryption technique is presented thus Cloud server can access information of user as he acts as a proxy server.

Paper [4] introduced new security models that remove this assumption for both certificate less signature and encryption schemes. In a certificate less cryptosystem, a Key Generation Center (KGC) is involved in issuing user partial key to user whose identity is assumed to be unique in the system. The user also independently generates an additional user public/secret key pair. Cryptographic operations can then be performed successfully only when both the user partial key and the user secret key are known. Knowing only one of them should not be able to impersonate the user that is carrying out any cryptographic operations as the user. There are two types of attacks that are generally considered in certificate less cryptography:

**Type I -** Key Replacement Attack. A third party tries to impersonate a user after compromising the user secret key and/or replacing the user public key with some value chosen by the third party. However, it does not know the user partial key.

**Type II -** Malicious KGC Attack. The KGC, who knows the partial key of a user, is malicious and tries to impersonate the user. However, the KGC does not know the user secret key or being able to replace the user public key.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Disadvantages of paper [4]that the encrypted 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.
Paper [5] introduced and makes concrete the concept of certificate less public key cryptography (CL-PKC), a model for the use of public key cryptography which avoids the inherent escrow of identity-based cryptography and yet which does not require certificates to guarantee the authenticity of public keys.A certificateless public-key signature (CL-PKS) scheme that is based on a provably secure ID-PKC signature scheme of efficient identity based signature schemes based on pairings. In general, a CL-PKS scheme can be specified by seven algorithms as Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Sign and Verify. These are similar to the algorithms used to define a CL-PKE scheme.
Whereas paper[6] explained a fully functional identity-based encryption scheme based on bilinear maps between groups.The security of the system is based on a natural analogue of the computational Diffie-Hellman assumption. Based on this assumption the system shows that the new system has chosen cipher text security in the random oracle model. Using standard techniques from threshold cryptography of Secure Distributed Key Generation for Discrete-Log Based Cryptosystems and Self-delegation with controlled propagation -or-What if you lose your device then the PKG in our scheme can be distribute so that the master-key is never available in a single location. Unlike common threshold systems, we show that robustness for our distributed PKG is free. Identity-based encryption is to help the deployment of a public key infrastructure. An identity-based encryption scheme E is specified by four randomized algorithms as Setup, Extract, Encrypt and Decrypt.

## III. EXISTING SYSTEM APPROACH

In previous systems like double encryption, this splits the secret key into two parts, if the user has lost his security device, then his/her corresponding cipher text in the cloud cannot be decrypted forever. That is, the approach cannot support security device update/revocability. The sender needs to know the serial number/public key of the security device, in additional to the user’s identity/public key. That makes the encryption process more complicated. In the case of identity-based encryption, the concept of “identity-based” has been totally lost as the sender needs to know not only the identity but another serial number.
Disadvantages of Existing System are as follow:

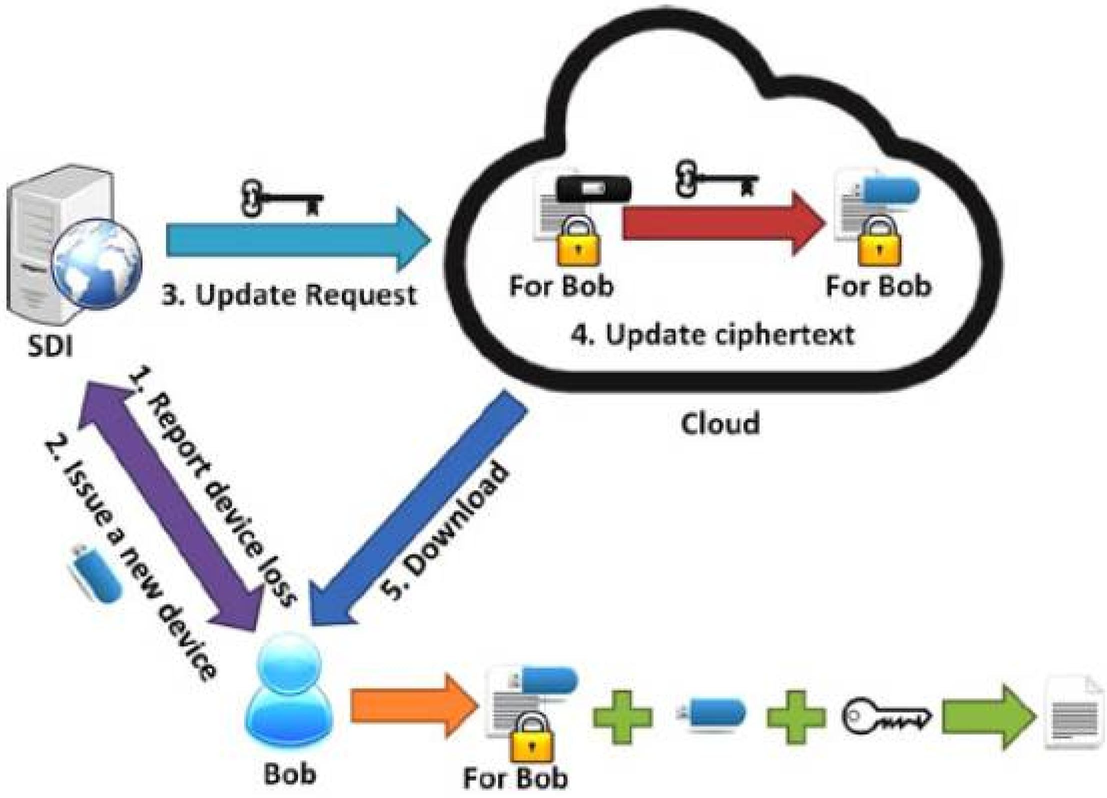
- If the user has lost his security device, then his/her corresponding cipher text in the cloud cannot be decrypted forever.
- The sender needs to know the serial number/ public key of the security device, in additional to the user’s identity/public key.
- The lack of revocability for encryption factor limits the flexibility of the system.

## IV. PROPOSED SYSTEM APPROACH

In this paper, we study the problem of providing better and secure data protection in cloud.Our system is based on an IBE (Identity-based encryption)-based mechanism. In this, the sender only needs to know the identity of the receiver in order to send an encrypted data (cipher text) to him/her. No other information of the receiver (e.g., public key, certificate etc.) is required. Then the sender will send the cipher text to the cloud where the receiver can download it at anytime. Our system willprovide two-factor data encryption protection.In order to decrypt the data stored in thecloud, the user needs to possess two things. First, the user needs to have his/her secret key which will be 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 cipher text without either piece.
Advantages of our proposed systems are as:

- To provide better security protection.
- Allows factor of revocability.
- Data sender is allowed to encrypt the data withknowledge of the identity only.
- Our solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that if device is stolen or lost data can’t be access by others.

The proposed system architecture is shown in Figure (1) :



Z

Figure 1: System Architechture

## V. CONCLUSION

In this paper we introduced the two-factor data securityprotection 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. We showed how our system enhances the confidentiality of the data and also offers the revocability of the device so that once the device is revoked; the corresponding cipher text will be updated automatically by the cloud server without any notice of the data owner.

## REFERENCES

[1] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, Senior Member,“Two-Factor Data Security ProtectionMechanism for Cloud Storage System”, IEEE Transaction on computer, JUNE 2016
[2]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. Comput., vol. 63, no. 1, pp. 31–44, Jan. 2014.
[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 Proc. 15th Int. Conf. Inf. Security Cryptol., 2012, pp. 231–246.
[4] 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. 302–311.
[5] S. S. Al-Riyami and K. G. Paterson, “Certificate less public key cryptography,” in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003, pp. 452–473.
[6] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in Proc. 21st Annu. Int. Cryptol. Conf., 2001, pp. 213–229.