

Two Component Information Security Fortification Method in a Distributed Storage Framework using Cloud

^[1] Mr. Mallesh HL ^[2] Prof. Pavithra H
^[1] M.Tech Student ^[2] Assistant Professor,
^{[1][2]} Department of CSE, R.V. College of Engineering [RVCE], Bengaluru-59
^[1] hmallesh2010@gmail.com, ^[2] pavithrah@rvce.edu.in

Abstract: This paper proposes two-factor authentication for the data stored in the cloud with revocability option. In our system, sender sends an encrypted message to the receiver through cloud server. The sender needs to know only Identity of the receiver but no other information like public key or certificate etc. To decrypt a cipher text, the receiver should possess two things. First one is secret key of the receiver stored in the computer system and second one is some hardware device, which is unique, that is connected to the computer. Cipher text cannot be decrypted without having these two things. But if the hardware device like pen drive or USB device is lost or stolen, then cipher text can never be decrypted and this hardware device is cancelled to decrypt any cipher text. Our system is secure as well as practical. We can use a new hardware device to decrypt the cipher text together with the secret key.

I. INTRODUCTION

There are so many advantages, to store the data in the cloud. Data hosted in the cloud storage [1] server can be accessed at any time from any place. Cloud users can get any amount of additional resources [2] any time that will be provided by cloud service provider. No risk of data maintenance. Data sharing between users is very easy.

There are so many disadvantages also, if we store the data in the cloud. As long as data is stored in the third party physical storage device, there is no security for data stored in the cloud server.

Many users are connected to the cloud server every day so that, any entity or user can get access to cloud data stored in the cloud server. Malicious cloud users can access any information stored in the cloud server, it is difficult to predict malicious cloud user because the number of users are connected to the cloud every day.

How to protect data in the cloud means, cloud data is usually protected by using asymmetric encryption. Asymmetric encryption [5] allows the sender to use only the public key or Identity of the receiver to generate a cipher text. Receiver should possess his/her own secret key to decrypt.

But the risk in protecting data in the cloud server is anybody can hack the secret key stored in the personal computer or a trusted server. This personal computer or a trusted server may be protected by a password. In an open network, this works best.

But today is an Internet age. In this internet age, every computer is somehow connected to another computer through networks. Therefore, so many chances required for the hacker to compromise the secret key. Therefore, there is a need to enhance a security protection. That is why; we are using two-factor authentication process which is flexible and scalable in the cloud computing era.

II. RELATED WORK

Here, we discuss some of the presented method to give the security for the cloud storage.

Double encryption: In this method, the plain text is encrypted using a public key or identity of the user. Again this cipher text is encrypted using some hardware device like pen drive. To decrypt, we first put hardware device, which will decrypt the cipher text once [4]. Finally, secret key of the receiver is used to decrypt to get the original plain text. We should have these two things to encrypt as well as decrypt (Secret key and hardware device). This disadvantage of this method is, if the hardware device is lost or stolen, then it is not possible to decrypt the cipher

text forever because, this method does not support revocability or new hardware device update.

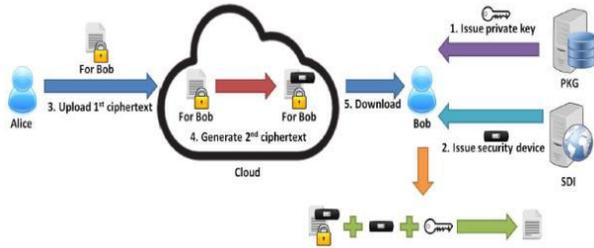


Fig 1: Existing system

The above figure 1 demonstrates the existing method to secure the cloud storage.

Split the secret key into two parts: In this method split secret key into two parts. First part is stored in the computer and second part is embedded into a security hardware device, then the drawback is that again without either part, one cannot decrypt the cipher text and also, if the device is lost, anybody who is having that device can break into the computer where the other part of the key is stored and he/she can decrypt all cipher text [3].

III. PROPOSED METHOD

Our system is Identity Based Encryption mechanism (IBE mechanism). Sender need to know only the Identity of the receiver to send encrypted data. In order to decrypt the data present in the cloud, the receiver need to do following things: where he/she should provide secret key which is stored in the computer and should have unique security hardware device, which will be connected to computer. It is impossible to decrypt the cipher text without either of these two things (either secret key or security device).

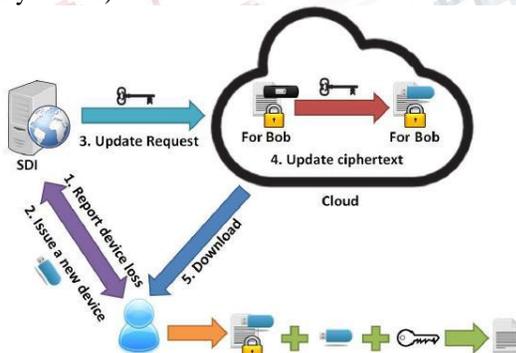


Fig 2: Proposed System

Our security hardware device can be revocable; the cloud server at any time cannot decrypt any cipher text itself. Our approach or method provides flexible security mechanism for the data stored in the cloud server.

IV. EXPERIMENTAL RESULTS

This section gives details of the experiment carried out to provide the two factor security for the cloud by means of Eclipse Juno IDE.

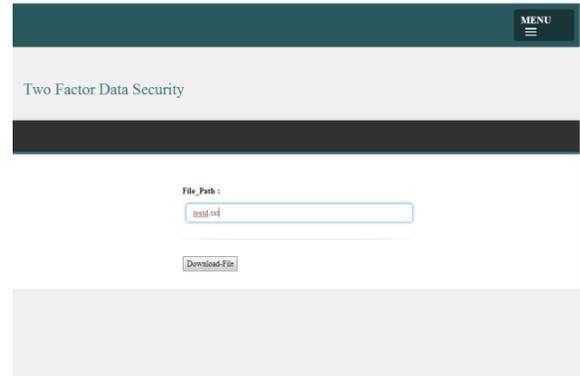


Fig 3: File download

The above screenshot shows the File downloading step. Here we have to mention the Filename.

The fig 4 shows actual File downloading from the Amazon cloud server. This file is downloaded and stored locally.



Fig 4: Downloading file from Amazon cloud server

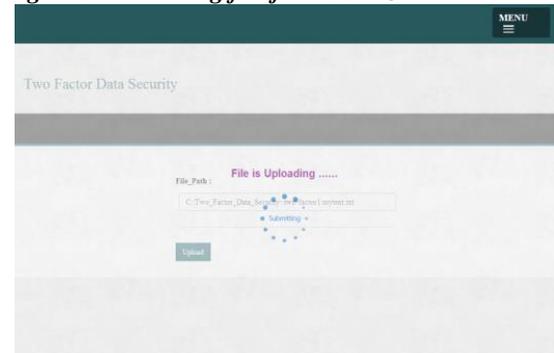
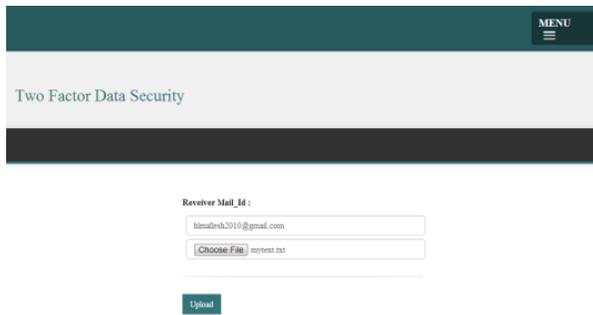


Fig 5: File uploading to the Amazon cloud server

The fig 5 shows the actual File Uploading to amazon cloud server. This file is encrypted twice and stored in the cloud server.



Two Factor Data Security

Receiver Mail_Id :
himalresh2010@gmail.com
Choose File mytest.txt
Upload

Fig 6: File Upload

The fig 6 shows the File Uploading step. It requires a receiver's email Id and File name to upload.

V. CONCLUSION

In this paper, a novel two-factor authentication for the data stored in the cloud server is introduced. Data is encrypted twice using the Identity of the receiver as well as security hardware device. The receiver uses both the security hardware device and a secret key, to decrypt the data twice.

Confidentiality of the data is enhanced in our project and also the revocability of the security hardware device is revoked, the corresponding cipher text will be updated with the new hardware device, without the knowledge of the sender, by the cloud server. Multiple revocability is not possible, one file can be sent to one receiver only. Multiple files cannot be sent to one receiver or multiple receivers.

REFERENCES

- [1] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for secure cloud storage. *IEEE Trans. Computers*, 62(2):362–375, 2013.
- [2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou. Toward secure and dependable storage services in cloud computing. *IEEE T.Services Computing*, 5(2):220–232, 2012.
- [3] 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.
- [4] 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.

[5] 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