Secure Cloud Storage Using Novel Authentication Mechanism

D. Janani , V.pandimeena ,S.Vincy priyadharshini, *Mr.S.DILIP KUMAR,M.Tech.,*

Department of Information Technology,

Arasu Engineering Collage, Kumbakonam.

Abstract---*USB connections allow a wide range of different electronic devices to connect to computers, including keyboards, cell phones, chargers, speakers, printers and various electronic devices. Information security is currently a very important topic in computing. Traditional authentication methods based on passwords involve many security problems. In traditional way of using auxiliary devices as an authentication key, it leads to drawback that it cannot be recovered when the auxiliary device would be lost. To overcome the drawbacks and make more efficient than the traditional way of authentication using the auxiliary devices, the new authentication protocol can be created. The conventional way of using the auxiliary devices as an authentication credentials for the cloud server. Without device authentication (unique id of device) user cannot encrypt the file or decrypt the file. The auxiliary device lost can be recovered by enhancing the existing with the password credentials. The auxiliary device can be monitored in the system when it copies any data from the cloud storage. This can be implemented as client and server architecture to monitor the data from the cloud server.*

I. INTRODUCTION

Cloud computing is Internet based development and use of computer technology. In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them. It typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.

The term cloud is used as a metaphor for the Internet, based on how the Internet is depicted in computer network diagrams and is an abstraction of the underlying infrastructure it conceals. Typical cloud computing services provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers.

"Cloud Computing" refers to the use of Internet based computer technology for a variety of services. It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet on a pay-for- use basis, at a fraction of the cost of provisioning a traditional Data center based solution. All the costs associated with setting up a data center such as procuring a building, hardware, redundant power supply, cooling systems, upgrading electrical supply, and maintaining a separate Disaster Recovery site can be passed on to a third party vendor. Since the customer is charged only for computer services used, cloud computing costs are a fraction of traditional technology expenditures.

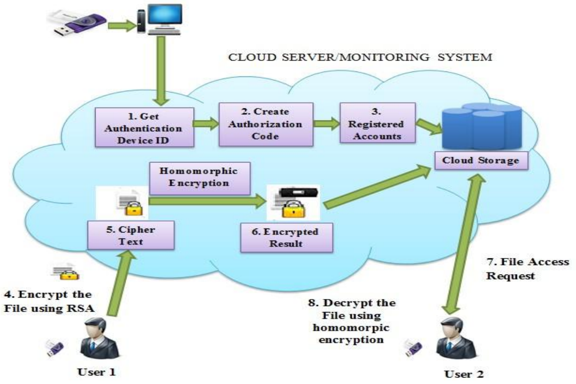
As a metaphor for the Internet, "the cloud" is a familiar cliché, but when combined with "computing," the meaning gets bigger and fuzzier. Some analysts and vendors define cloud computing narrowly as an updated version of utility computing: basically virtual servers available over the Internet. Others go very broad, arguing anything we consume outside the firewall is "in the cloud," including conventional outsourcing.

II. RELATED WORK

We discuss some naïve approaches for enhancement of security protection and explain why they are not the best candidate to achieve the goal of flexibility.

Client System:

In this client system, the files storage area may create with the


CLOUD SERVER/MONITORING SYSTEM
1. Get Authentication Device ID
2. Create Authorization Code
3. Registered Accounts
Cloud Storage
Homomorphic Encryption
5. Cipher Text
6. Encrypted Result
7. File Access Request
4. Encrypt the File using RSA
8. Decrypt the File using homomorpic encryption
User 1
User 2

system authentication credentials registration. The application which provide the UI design to create the authentication details, file uploading and downloading. It also includes the feature of sharing the data with the key aggregation with the auxiliary device. In this system, the user needs to create the profile and their signature of auxiliary devices. That the signature may be recoverable when the user needs to recover from the server.

Server Implementation with monitoring system

The server can be implemented with the features of connecting and binding the specific client application with the authentication credentials. The server may implement with the monitoring system and that system governs the transactions in the data storage. Server management is required to enhance the up-time of servers. Based on the server system, management plans may vary. Yet the bottom line is that proper server management software will guarantee the security and stability of servers throughout its lifespan.

Auxiliary device registration:

The user needs register to their details to the server using the auxiliary device. The auxiliary device unique identification can be retrieved in this module. This unique Id will be stored in the server system. It is recoverable the user authentication credentials will be used for the recovery options.

Auxiliary device usage:Suppose it assume that an authenticated user U□ accesses an important file which is stored in the USB storage device of the U□ and wants to get it from the server too. If an attacker knows that the U□ is the user of the important file then he/she may get the file either steal or by some means. But, it is confirmed that if the attacker does not know the user who are using the important file, then it is extremely hard to capture the important file. Therefore user anonymity is necessary for such type of application and our protocol provides it efficiently. Thus the registered auxiliary may use for the file storage and file retrieval from the server. The data file transactions will be maintained in the server logs.

III. CONCLUSIONS

In this paper, we introduced a novel Authentication 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]. Akavia, S. Goldwasser, and V.Vaikuntanathan, “Simultaneous hardcore bits and cryptography against memory attacks,” in Proc. 6th Theory Cryptography Conf., 2009, pp. 474–495.

[2]. S. S. Al-Riyami and K. G.Paterson, “Certificateless public key cryptography,” in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003,pp. 452–473.

[3]. M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, “Certificate based (linkable) ring signature,” in Proc. Inf. Security Practice Experience Conf., 2007, pp. 79–92.

[4]. M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, “Malicious KGC attacks in certificateless cryptography,” in Proc. 2nd ACM Symp. Inf., Comput. Commun. Security, 2007, pp. 302–311.

[5]. M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Int. Conf. Theory Appl. Cryptographic Techn., 1998, pp. 127–144.

[6]. A.Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426.