|| Volume 2 ||Issue 12 ||JULY 2017||ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Three Factor Data Sharing Mechanism for Cloud Storage System

Ms. Swati R. Vibhute

ME CSE,EES College of Engineering Aurangabad, Maharashtra, India

***Abstract*— The goal of this system is to provide data security protection mechanism for cloud storage system with three factors. Security is the most important factor for data storage and transmission. In this system it allows a sender to send a message in encrypted form to the receiver with the help of cloud server. The sender only needs to know the identity of the receiver but there is no need to other information. The receiver needs to control two things in order to decrypt the cipher text. The first factor is his/her secrete key stored in the computer. The second is personal device which is unique, connected to the computer.**

As we know that cloud computing is a pure internet based service which is permit to its users for store large amount of data on cloud and use whenever the required from anywhere ,any part of world using any terminal. Also cloud computing is another facility is data sharing and access remotely. As the data stored in cloud is expose to different attacks by hackers or unauthorized users and it is becomes very difficult to maintain security and privacy of data. So the solution provided by this situation is to our system is "Three factor Security "for data. In this system we protect data by using all three factors of authentication, data security, privacy and verification at the same time. In this paper we use figure print and 3DES algorithm to protect confidentiality, privacy of stored data in cloud.

Keywords:-Three-factor, factor revocability, security, cloud storage.

I INTRODUCTION

Cloud storage means "the huge amount of data will be stored online" in the cloud. In a company or organizations the stored data in cloud is accessible from connected multiple resources and distributed resources that contains a cloud. But day by day cloud storage security is a Challenging task for organizations. Cloud storage is a model of data storage in which the digital data is stored in logical pools and physical storage spans multiple servers and physical environment is owned by a hosting company. Cloud computing is invented by Joseph Carl Robnett Licklider in the 1960s with his work on ARPANET to connect people and data from anywhere at any time. With the development of cloud computing, Data security problem becomes more and more important in cloud computing. This paper introduces the third factor authentication process for data sharing mechanism for cloud storage. CompuServe offered its consumer users a small amount of disk space that could be used to store any files they chose to upload in 1983. AT&T launched Persona Link Services, an online platform for personal and business communication and entrepreneurship in 1994. In a Cloud Computing it provides the way to share distributed resources and services which belong to different organizations or sites. So the cloud computing share distributed resources via network in the open environment thus it makes security problems. In this method some important security mechanism including authentication, encryption and decryption are provided in Cloud Computing system. The following figure 1.1 shows that the data stored on cloud in encrypted format.

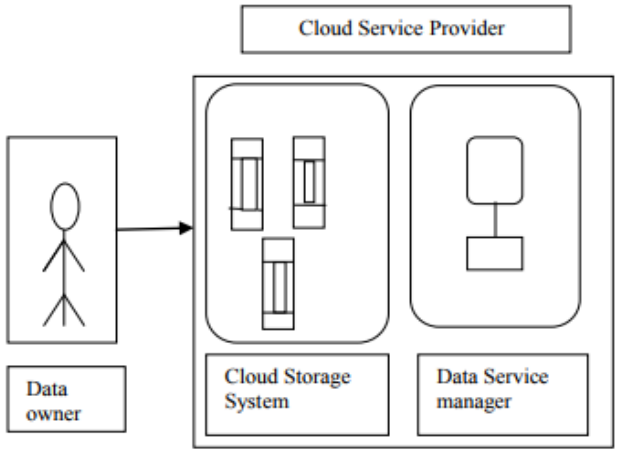

Figure 1 Data stored on cloud in encrypted format

What are authentication factors?

An authentication factor is an independent category of credential used for identity verification. The three most common categories are often described as something you know (the knowledge factor), something you have (the possession factor) and something you are (the inherence factor). For systems with more demanding requirements for security, location and time are sometimes added as fourth and fifth factors.

Two-factor authentication (2FA)

Two-factor authentication is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical

token, such as a card, and the other is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as something you have and something you know. A common example of two-factor authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it. Including those two elements makes it more difficult for someone to access the user's bank account because they would have to have the physical item in their possession and also know the PIN.

According to proponents, two-factor authentication can drastically reduce the incidence of online identity theft, phishing expeditions, and other online fraud, because stealing the victim's password is not enough to give a thief access to their information.

In this model a two-step authentication process one is incorporated, the login password authentication mechanism and with another authentication phase of an addition of digital fingerprint mechanism to enhance the authentication process implemented using overcome the following password vulnerabilities. AES algorithm is used for encryption of data and messages shared by users for data privacy.

II LITERATURE SERVEY

Data security on cloud storage system is the challenging task in the enterprises and company.So the main problem is that how to provide the security on data on cloud. So to overcome the data security problem on cloud storage and provide more security we have studied some cases. Here by referred some previous work related with data security protection mechanism for cloud storage system.

Joseph K.Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang et al June 2016 [2] propose a two factor data security mechanism with factor revocability for cloud storage system. This approach helps to provide the data security protection mechanism foe cloud storage is in two factors which a data sender is allowed to encrypt the data with knowledge of the identity of receiver only while the receiver is required to use both his /her secret key and a security device to gain access to the data.

Yogesh Kale and Archana Patankar et al June 2014[3] they have focus on tacking security issues of authentication, privacy of user data.In this paper two schemes are used.

i) Registration and authentication mechanism scheme.

ii) Storing and accessing own data Scheme.

Divya Sarswat and Dr.Pooja Tripathi et al May 2015[4] proposed a two factor authentication approach is employed for the authentication and authorization of the client to increase the confidentiality and integrity of the data .OTP to authenticate user and MD5 hashing for hiding information.AES encryption technique is used for data storing in cloud.

Adi Akavia, Shafi Goldwasser and Vinod Vaikuntananthan [5] this paper focus on public key and identity based encryption schemes that are secure against memory attacks.

III RELATED WORKS

In this propose system registration mechanism, the user is verified with 3 factor verification. This system introduces an advance improvisation in sharing mechanism of data on cloud. This system includes a third factor to authentication and triple encryption technique for secure storage in cloud. System focuses on detailed explanation of proposed system which helps in tacking security issues of authentication, privacy of user data. The username and password pair is common authentication method which allow only authenticated user to upload and access data but it not protect data from cloud vendor. Also data travel on network in plain text format so it is vulnerable to attack. Following fig.4.1 shows that the registration mechanism of proposed system.

Authentication factor 1:

In this client has to provide username and password which client has entered at the time of registration.

Authentication factor 2:

i. In this level CSP send OTP on clients registered Email-id

ii. In this level CSP send OTP on clients registered Mobile no.

Authentication factor 3:

By using Finger print Scanner scan the finger print of user.

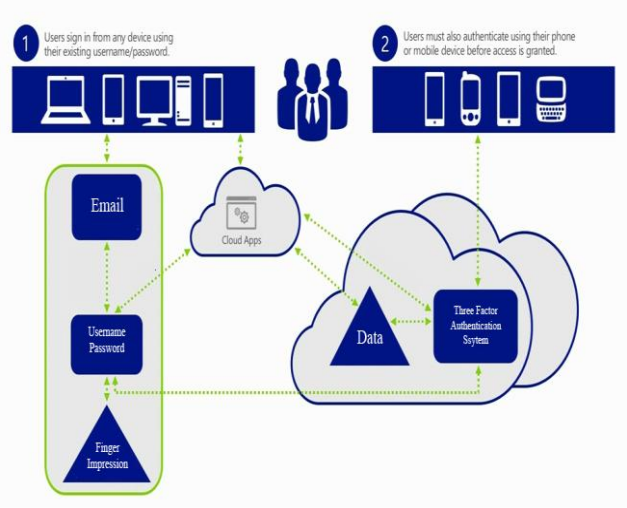

Figure 2 Proposed system registration mechanism

IV CONCLUSION

This paper is focus on a new approach in the form of third factor authentication method to provide data privacy and security mechanism for cloud storage. This paper also discussed access control and data integrity, confidentiality, availability, and privacy technologies. Cloud storage systems are moving towards unlimited bandwidth, capacity, and processing power, and data must be securely accessible anytime and anywhere.

Because of changing demands, existing technology cannot ensure the privacy and security of data stored in the cloud. Further research needs to be done on scalability of secure storage and secure storage management in a large, complex cloud.

Storage devices are provided by a number of different service providers and shared by a large number of users. Frequent equipment deployment, data operations, and data access make the cloud a dynamic environment. Cloud data storage and management therefore needs to be safe but also highly scalable.

ACKNOWLEDGMENT

It is my great pleasure in expressing sincere and deep gratitude towards my guide Prof. V S Karwande. I am also thankful to Head of Department of Computer Science and Engineering, Prof. R. A. Auti for providing me various resources and infrastructure facilities. I also offer my most sincere thanks to Principal of Everest College of Engineering, Aurangabad, my colleagues and staff members of computer science and Engineering department, Everest college of Engineering, Aurangabad for cooperation provided by them in many ways.

REFERENCE

[1]. Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, Senior Member, IEEE.“Two-Factor Data Security Protection Mechanism for Cloud Storage System.”June 2016.

[2]. Y. Kale, A.Patankar, “Enhanced Data Security Mechanism on Cloud Using
Two-factor Authentication, Data Encryption and Key Sharing Mechanism” 15 June 2014 Pune.

[3]. A. Akavia. S.Goldwasser, and V. Vaikuntanathan“Simultaneous Hardcore Bits and Cryptography against Memory Attacks.” 2009.

[4]. A.Boldyreva, V. Goyal, V.Kumar “Identity-based Encryption with Efficient Revocation “2008.

[5]. Prveenkumar, J.Patil, “Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases”.

[6]. J.Shao & Z. Cao,”Multi-use unidirectional identity-based proxy re encryption from hierarchical identity-based encryption**”,** Info.Sci. 2012.

[7]. Vijay Varadharajan, Senior Member, IEEE, and Udaya Tupakula, Member, IEEE. IEEE Transactions on Network And Service Management**,”** Security as a Service Model for Cloud Environment”**,**Vol. 11, No. 1, March 2014 .

Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and