ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

Secure File Access Using Biometric Security and Key Share among Cloud

Mayuri Nikam[1] , Priyanka Dupargude[2] , Pooja Patil[3], Dipalee Jadhav[4] , Rajashree Dongare[5]

B.E Scholar, Dept. of Computer, RMDSSOE, Pune, India[1]

B.E Scholar, Dept. of Computer, RMDSSOE, Pune, India[2]

B.E Scholar, Dept. of Computer, RMDSSOE, Pune, India[3]

B.E Scholar, Dept. of Computer, RMDSSOE, Pune, India[4]

Assistant Professor, Dept. of Computer, RMDSSOE, Pune, India[5]

ABSTRACT: Cloud services are used for storing and retrieving the data. Nowadays, most of the drawbacks in cloud computing is the user authentication problems. The system implements the secret key to enter into the cloud by the user. The secret key is given by the CSP. The user use to store and retrieve the data. For viewing the data biometric authentication is used. The secured biometric authentication technique bridges the gap between the insufficiencies of existing electronic authentication solution. In addition, the decryption key is destructed after the user-specified time. In this system, user's biometric information are encrypted and stored in a database. Advanced Encryption Standard (AES) encryption technique is used to encrypt the biometric information provided by user biometric information and MD5 is used for dynamic secret key sharing are compared with the database where the authenticated user's encrypted information are stored.

KEYWORDS: Biometric authentication, fingerprint, key share, cloud, encryption, decryption.

I. INTRODUCTION

Cloud computing is an emerging technology which allows multi-tenant to request for services and resources from their service providers in an on-demand environment. It is a complex yet resource saving infrastructure for today's modern business needs, providing the means through which services are delivered to the end users via Internet access. In the cloud environment, users can access services based on their needs without knowing how the services are delivered and where the service are hosted. It is a computing model, where resources such as computing power, storage, network and software are abstracted and provided as services on the internet in a remotely accessible fashion. When talking about Internet authentication, in most cases, people are still talking about passwords. One of the biggest problems with current authentication approaches is the existence of too many password account pairings for each user, which leads to forgetting or using the same username and password for multiple sites. A possible solution to this problem can be found in the use of biometrics. Biometric authentication techniques, which try to validate the identity of an user based on his/her physiological or behavioral traits, are already quite widely used for local authentication purposes (for private use), while their use on the Internet is still relatively modest. The main reason for this setting is open issues pertaining mainly to the accessibility and scalability of existing biometric technology. Similar issues are also encountered in other deployment domains of biometric technology, such as forensics, law-enforcement and alike.Department of Defense, or the Department of Homeland Security are expected to grow significantly over the next few yours to accommodate several hundred millions (or even billions) of identities. Such expectations make it necessary to devise highly scalable biometric technology, capable of operating on enormous amounts of data, which, in turn, induces the need for sufficient storage capacity and significant processing power. The first solution that comes to mind with respect to the outlined issues is moving the existing biometric technology to a cloud platform that ensures appropriate scalability of the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

technology, sufficient amounts of storage, parallel processing capabilities, and with the widespread availability of mobile devices also provides an accessible entry point for various applications and services that rely on mobile clients. Hence, cloud computing is capable of addressing issues related to the next generation of biometric technology, but at the same time, offers new application possibilities for the existing generation of biometric systems. However, moving the existing biometric technology to the cloud is a nontrivial task. Developers attempting to tackle this task need to be aware of: the most common challenges and obstacles encountered, when moving the technology to a cloud platform. Cloud computing is a highly active field of research and development, which gained popularity only a few years ago. Since the field covers a wide range of areas relating to all levels of cloud computing (i.e. PaaS, IaaS, and SaaS), it is only natural that not all possible aspects of the field is appropriately covered in the available scientific literature. This is also true for cloud-based biometrics.

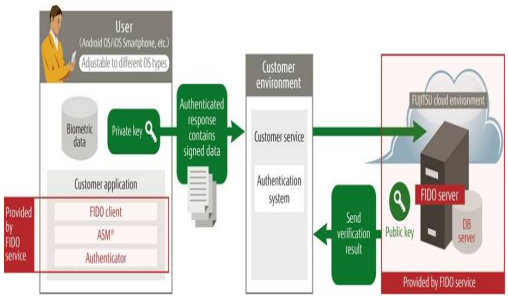

Fig. 1.1 Biometric Authentication Process

II. LITERATURE REVIEW

This paper focuses on leveraging biometric identity to achieve access control in cloud. Biometric possesses a lot of advantages like portability, uniqueness and verification clearness; nevertheless biometric measurements are always noisy. To protect sensitive data along with private key confidential against malicious servers or other external attackers and meet the requirement of removing the biometric noisy property, we exploit and combine techniques of fuzzy identity based encryption (FIBE), biometric measurement, and key insulated encryption [1].

A biometric digital audio watermarking algorithm is presented in this paper. Instead of a constant watermark, a biometric watermark that is unique to an individual is embedded into an audio. Keystroke Dynamics is chosen to stamp the ownership of an individual to the audio file. Constructed biometric template is embedded into wavelet domain by using frequency hopping spread spectrum technique [2].

Recently, computer users can maintain their data and applications on the Internet and in the central remote server by using a technology called cloud computing. It is a kind of technology that allows users to access their personal files from any device provided with Internet services such technology offers even more applications to be utilized without installation. This paper presents a review of basic security challenges consisting of traditional security issues [3].

2.1Data confidentiality between Users and CSP.

- Data owner divides users in groups
- System Encrypts the data of each group with a single symmetric key.
- It gives parts of the symmetric key (KT) to each user of the group.
- CSP computes digest of data by using 128-bit MD5 hash algorithm and then encapsulates the digest and data using the secret shared key.
- This in turn, provides strong data confidentiality and integrity.
- Since, data are encrypted using secret shared key which is known only to respected user group, CSP can't see data even though user's credential comes through it.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

III. PROPOSED SYSTEM

In this scheme, there are basically three entities: Cloud Service Provider (CSP), Fingerprint system and Users.

3.1system architecture

- Client Model
- Server Model

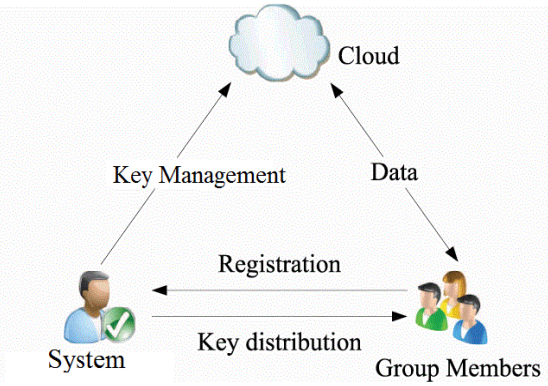

Fig 3.1System Architecture-Key Share

3.2 Proposed Algorithm

1. AES Algorithm:Advanced Encryption Standard (AES) encryption technique is used to encrypt the biometric information provided by user biometric information. Proposed system uses AES algorithm to encrypt the file uploaded by authenticated user. It provides security to high sensitive data.

2. MD5 Algorithm: In proposed system MD5 is used for dynamic secret key sharing are compared with the database where theauthenticated user's encrypted information are stored.The MD5 algorithm is a widely used hashfunction producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities.

3.3 How does process takes place-

Step1: Each new user must register in the system.
Step2: Log-In using credentials and thumb impression.
Step3: User can upload any document file.
Step4: Any another user can request for uploaded file.
Step5: All users must enter their secret key.
Step6: If all keys are matched then only requested user can get access for that file successfully.
Step7: If fails, repeat from step 5.

3.4 Client server Module

CSP is authorized person to assign signature to user. The CSP can able to view the users list and user files which uploaded by the user individually. This CSP is not possible to view the files containing information they can able to view names alone.The user must have to enter all the details in the application in the registration purposes. Once it is completed, user will receive the authentication code for the user ID. After successful registration user can access all document.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

3.5 Finger Print Authentication

The finger print authentication module, and user must upload the finger image for the further entry process after completion of the electronic key validation. Once the finger image was uploaded by the user it will compare with previous finger image when it time of the registration purposes along with during login period.

3.6 Key Share Mechanism

Data confidentiality between Users and CSP will increase using key share mechanism.Data owner divides users in groups. System Encrypts the data of each group with a single symmetric key. It gives parts of the symmetric key to each user of the group. CSP computes digest of data by using 128-bit MD5 hash algorithm and then encapsulates the digest and data using the secret shared key. This in turn, provides strong data confidentiality and integrity.Since, data are encrypted using secret shared key which is known only to respected user group. If anyuser one of them is unable to enter shared key then the file will not b decrypted for requested user. CSP can't see data even though user's credential comes through it.

3.7 Windows GUI:

Our Application is user friendly and platform independent means its can run on any platform or any operating system.

IV. CONCLUSION

Cloud based biometric services have an enormous potential market value and as such attract research and development groups from all around the world. In this paper some directions on how to move existing biometric technology to a cloud platform were presented. Issues that need to be considered when designing cloud-based biometric services have been presented and a case study, where a cloud fingerprint service was developed and integrated.As part of our future work we plan to migrate more secure key modalities to the cloud and, if possible, key share cloud-based biometric solution.

REFERENCES

[1] Ruhul Amin, R. Simon Sherratt, Fellow, IEEE, Debasis Giri,SK Hafizul Islam, Muhammad Khurram Khan, Senior Member, IEEE, "A Software Agent Enabled Biometric Security Algorithm for Secure File Access in Consumer Storage Devices," IEEE Transactions on Consumer Electronics Volume: 63, Issue: 1, February 2017 .
[2] Pengfei Hu Huansheng Ning Tie Qiu, "Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things", 2017.
[3] V. Malathi,B. Balamurugan, s. Eshwar, "Achieving Privacy and Security Using QR Code by Means of Encryption Technique in ATM," IEEE Trans. Consumer Electron., vol. CE-46, no. 4, pp. 958– 961, Nov. 2016.
[4] 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," IEEE Trans. Consumer Electron., vol. CE-46, no.4, pp. 992–993, Nov. 2016.
[5] F.-Y. Yang, T.-D. Wu, and S.-H. Chiu, "A secure control protocol for USB mass storage devices," IEEE Trans. Consumer Electron., vol. CE56, no. 4, pp. 2339–2343, Nov. 2010.
[6] B. Chen, C. Qin, and L. Yu, "A Secure Access Authentication Scheme for Removable Storage Media," Journal of Information & Computational Science.
[7] F.-Y. Yang, T.-D. Wu, and S.-H. Chiu, "A secure control protocol for USB mass storage devices," IET Computers & Digital Techniques, vol. 7, no. 1, pp. 48–55, Jan. 2010.
[8] M.-S. Hwang, and L.-H. Li, "A new remote user authentication scheme using smart cards," IEEETrans. Consumer Electron., vol. CE-60, no. 1, pp. 30–37, Feb. 2007.
[9] E.-J. Yoon, E.-K. Ryu, and K.-Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," IEEETrans. Consumer Electron., vol. CE-50, no. 1, pp. 204– 207, Feb. 2000.
[10] H.-M. Sun, "An efficient remote use authentication scheme using smart cards," IEEE Trans. Consumer Electron., vol. CE-50, no. 1, pp. 204–207, Feb. 2000