**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 4, Issue. 3, March 2015, pg.572 – 577*

**RESEARCH ARTICLE**

# SECURED BIOMETRIC AUTHENTICATION IN CLOUD SHARING SYSTEM

**E. Sasi[1], R. Saranyapriyadharshini[2]**

[1]Computer Science and Engineering, IFET College of Engineering, Villupuram-605 108, India

[2]Computer Science and Engineering, IFET College of Engineering, Villupuram-605 108, India

***Abstract:*** ***The project mainly focus on Secure Storage and Sharing in cloud computing. Cloud services are used for storing and retrieving the data. Nowadays, most of the drawbacks in cloud computing is the user authentication problems. The proposed system implements the electronic key to enter into the cloud by the user. The electronic key is given by the admin. 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. It consists of two levels of authentication such as Fingerprint, and Iris. Those images are compared by the minutia matching algorithm. This algorithm produced efficient image comparison with the percentage levels. Then, implements access control for secure sharing to authenticate for cloud users. The result simulates that, the data stored in the cloud is secured.***

***Keywords: Biometric authentication, Iris image, fingerprint***

## 1. 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 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.

## 2. PROBLEM DESCRIPTION

To introduce a dynamic authentication with sensory information for the access control systems. By combining sensory information obtained from onboard sensors on the access cards as well as the original encoded identification information, we are able to effectively tackle the problems such as access card loss, stolen, and duplication. Our solution is backward-compatible with existing access control systems and significantly increases the key spaces for authentication.

### 2.1 Problem solution

The cloud security is provided by biometric techniques are used such as Iris authentication and fingerprint. Although these biometric authentication methods such as fingerprint, and iris are able to provide personal identification, they have high infrastructure cost and access privileges which cannot be transferred among trusted users.Electronic key is

generated uniquely for an individual user. It is the combination of the data's like encoded information and the ID of the user. The advantage of the proposed system is the electronic key is verified at each time in authentication and finger print & iris verification is highly increases the efficiency of authentication.

## 2.2 Biometric Authentication

Biometric recognition systems represent pattern recognition systems, capable of recognizing individuals based on their physiological or behavioural traits. These traits are considered to be unique to each individual and unlike knowledge or token-based security mechanisms cannot be forgotten, lost or stolen. The most common traits used for biometric recognition are: faces, fingerprints, irises, palm-prints, speech etc. Designing biometric services in cloud emphasize that a decision has to be made with respect to which components of the biometric system should be moved to the cloud and which implemented locally.

This authentication process use the following in proposed system:

- Finger Print as image
- Iris as image

Biometric is the authentication process which is used for the security purpose. The biometrics like fingure print and iris images are used in the proposed system. We are using the minute matching algorithm for comparing the images.

As the first step in the biometric process is, we use fingure print images. An analysis was done between the user's image and the hacker's image. The algorithm is used here for comparing the images. If the hacker tries to view the data it will return that,' the authentication is failed'.

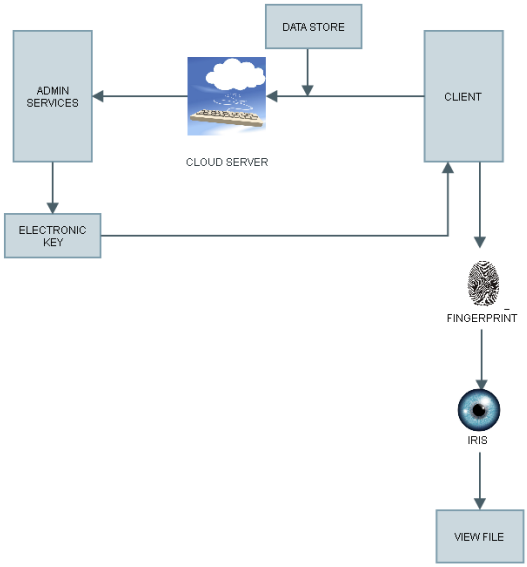
The second step in the biometric process is, we use iris images. This process only compares the image and returns the authentication.

# 3. PROPOSED SYSTEM

The cloud security is provided by biometric techniques are used such as Iris authentication and fingerprint. Electronic key is generated uniquely for an individual user. It is the combination of the data's like encoded information and the ID of the user .Electronic Key is verified at each time in authentication. Finger Print & Iris verification is highly increase efficiency of authentication.

### 3.1 System Architecture




## 3.2 Minutiae Matching Algorithm

Minutiae points from both the input and template imagesare extracted using the algorithm. The algorithmprovides the following two outputs:

(a) A set of minutiaepoints, each characterized by its spatial position andorientation in the fingerprint image.

(b) Local ridge informationin the vicinity of each minutiae point. The two setsof minutiae points are then matched using a point matchingalgorithm.

The algorithm first selects a reference minutiaepair (one from each image) and then determines the numberof corresponding minutiae pairs using the remaining set ofpoints. The reference pair that results in the maximum numberof corresponding pairs determines the best alignment.

# 4. MODULE DESCRIPTION

## 4.1 Admin Module

The admin can able to view the users list and user files which uploaded by the user individually. This admin is not possible to view the files containing information they can able to view names alone.

## 4.2 User Module

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.

### 4.3 Finger Print Authentication

The finger print authentication module , an 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 a time of the registration purposes along with during login period.

### 4.4 Iris Authentication

The iris Authentication module , an user must upload the iris image for the further entry process after completion of the finger print validation. Once the iris image was uploaded by the user it will compare with previous iris image when it is uploaded at a time of the registration purposes along with during login period.

### 4.5 Electronic Key Validation

Theelectronic key validation module, electronic key is combination of the user ID provided by the server and the sensory data provided by the admin. Every time when an user comes to login purposes an initial authentication is electronic key validation.

### 4.6 View Files Module

The module, after completed successfully of all authentication process in our application the main application will process and then scan user can able to add his documents at the same time at the same time view all the previous documents too.

## 5. 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 with the e-learning framework Moodle was described as well. As part of our future work we plan to migrate more biometric modalities to the cloud and, if possible, devise a multi-modal cloud-based biometric solution.

## REFERENCES

[1] Y. Shu, Y. Gu, and J. Chen, "Sensory-Data-Enhanced Authentica- tion for RFID-Based Access Control Systems," Proc. IEEE Ninth Int'l Conf. Mobile Ad Hoc Sensor Systems (MASS), 2012.
[2] A. Juels, "RFID Security and Privacy: A Research Survey," IEEE J. Selected Areas Comm., vol. 24, no. 2, pp. 381-394, Feb. 2006.
[3] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," Proc. Fifth Int'l Conf. Pervasive Computing, pp. 144-161, 2007.
[4] M. Burmester, T.V. Le, B.D. Medeiros, and G. Tsudik, "Uni- versallyComposable RFID Identification and Authentication Protocols," ACM Trans. Information and System Security, vol. 12, no. 4, article 21, 2009.
[5] J. Kong, H. Wang, and G. Zhang, "Gesture Recognition Model Based on 3D Accelerations," Proc. IEEE Fourth Int'l Conf. Computer Science & Education (ICCSE), 2009.

[6] S. Mitra and T. Acharya, "Gesture Recognition: A Survey," IEEE Trans. Systems, Man and Cybernetics, vol. 37, no. 3, pp. 311-324, May 2007.
[7] S. Zhou, Q. Shan, F. Fei, W.J. Li, C.P. Kwong, P.C.K. Wu, B. Meng, C.K.H. Chan, and J.Y.J. Liou, "Gesture Recognition for Interactive Controllers Using MEMS Motion Sensors," Proc. IEEE Fourth Int'l Conf. Nano/Micro Engineered Molecular Systems (NEMS), 2009.
[8] T. Park, J. Lee, I. Hwang, C. Yoo, L. Nachman, and J. Song, "E-Gesture: A Collaborative Architecture for Energy-Efficient Gesture Recognition with Hand-Worn Sensor and Mobile Devices," Proc. Ninth ACM Conf. Embedded Networked Sensor Systems (SenSys), 2011.
[9] A.P. Sample, D.J. Yeager, P.S. Powledge, A.V. Mamishev, and J.R. Smith, "Design of an RFID-Based Battery-Free Program- mable Sensing Platform," IEEE Trans. Instrumentation and Measurement, vol. 57, no. 11, pp. 2608-2615, Nov. 2008.
[10] M. Buettner and D. Wetherall, "An Empirical Study of UHF RFID Performance," Proc. ACM MobiCom, 2008.
[11] A.P. Sample, D.J. Yeager, and J.R. Smith, "A Capacitive Touch Interface for Passive RFID Tags," Proc. IEEE Int'l Conf. RFID, 2009.
[12] N. Saxena and J. Voris, "Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model," Proc. Sixth Int'l Conf. Radio Frequency Identification: Security and Privacy Issues, vol. 6370, pp. 2-21, 2010.
[13] D. Ma and N. Saxena, "A Context-Aware Approach to Defend against Unauthorized Reading and Relay Attacks in RFID Systems," Security and Comm. Networks, doi: 10.1002/sec.404, Dec. 2011.
[14] A. Czeskis, K. Koscher, J.R. Smith, and T. Kohno, "RFIDs and Secret Handshakes: Defending against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), 2008.
[15] N. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. Campbell, "A Survey of Mobile Phone Sensing," IEEE Comm. Magazine, vol. 48, no. 9, pp. 140-150, Sept. 2010.