GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

CLOUD SECURITY: SECURE BIOMETRIC AUTHENTICATION USING PHALANX AND INTERPHALANGEAL LIGAMENTS

P Padma[*1], R Vigneshwar[2], J Senthilkuma[r3], B.Saranya[4] & P.K.Sunitha[5]
[*1,2,3,4&5]Department of Information Technology, Sri Sairam Engineering College Chennai-43, India

ABSTRACT

Cloud Computing refers to providing compute services over the network and storage of data in cloud servers for business purposes. The cloud service providers, commonly referred to as CSPs, store, manage and maintain client data across their data centers located geographically apart and it provides threats of data leak. This research work focuses on the existing authentication schemes, their shortcomings and has proposed a new authentication mechanism that gives better data security. Authentication techniques ensures and helps to confirm a user's identity. The conventional password authentication technique is enough of the oldest and conventional authentication techniques but does not provide enough security. Multifactor authentication methodology uses a combination of multiple authentication techniques including the password so as to ensure more secure authentication. Also since the conventional and traditional authentication techniques like passwords are not able to provide impregnable data security, many research studies turned their focus to behavioral and biometric traits to use them as a validation for providing authentication to the cloud services. The literature survey done as part of the research established that although many researches were done on Palm print as a biometric authentication , focus on the palm prints found in the middle of the phalange bones in the finger have been very little. Despite the fact that the above contention cannot be used as a single standalone authentication technique as the uniqueness of these print-marks is not established, it can be a potent authentication technique when using it in tandem with similar authentication mechanisms. Palm print marks found in between the phalange are characterized by blank spaces in a standard. The characterized spaces may be calculated and estimated using algorithmic procedures to leverage as an extra authentication method to increase security in Cloud services provided by the provider.

Keywords: *Cloud Computing, Authentication, Privacy, Identity.*

I. INTRODUCTION

The term Cloud Computing is generally used to define a model that provides for a demand based access of network to computing resources- specifically Network Servers, Services, Storage, and Applications. On the hindsight, the concept of cloud computing can also be viewed as an advanced and a more mature variation of the data processor services currently relevant in the tech-savvy world today. Most of the IT areas have been impacted by the advent of Cloud Computing.

It provides for sharing of services amongst multiple users across geographies on a massive scale. Therefore, the end user has to be authenticated in order to ensure that each individual user's privacy is protected and trust is established across the cloud network. characterized by a concept referred as CIA. Confidentiality

A which refers to preservation of the data and making the data secure and is highly important in cloud computing because the data is stored on a distributed database and is susceptible to attack; Integrity (I) is the aspect of limiting an individual who does not have the permission or authority to access a data.

TABLE I: Authentication Methods Classification

Authentication	Types
Proof of Knowledge (something a user knows)	Password , PIN Number, User Specific information

Proof-of-Possession (something a user has)	Smart cards, Tokens, Any user related identity verification
Proof of characteristics (Something an user is)	Finger Prints, Facial features, geometry of the hand, eye features

The data integrity is ensured by the use of specific authentication methods which enables the rightful user to access the data and prevents the others from data access. Availability (A) simply means that the data will be made available to the authorized user at all times. User authentication is very much critical in secure cloud computing so that the access to the cloud service can be limited to only those who are authorized the data access that is stored in the cloud data services. (1) The user must be able to be identified by the system using any of the identification methods so as to authenticate the user to access the cloud computing network and services.

Our work is an attempt in having a broad overview of the existing authentication techniques. Initially, with the help of two case study, the study focuses on the data security and privacy concerns in cloud computing. The paper then gradually moves on to the types of authentication and a brief analysis of each type. Thus a comprehensive background study of the biometric based authentication techniques in cloud computing services and a new authentication and a more efficient technique is proposed.

Biometric authentication techniques are classified into two broad types based on physical and behavioral traits. We have studied the major available biometric authentication techniques as part of our study. The existing biometric methods are generally better in terms of security but do have some shortcomings when used as a standalone authentication method. For example, some behavioral biometric techniques have the drawback of being mimicked by attackers. On the other hand, some physical biometric traits need the use of additional hardware to support the effective functioning of the authentication system. In addition, there is a also the possibility that a physical biometric trait may alter over the course of the life due to ageing or some unfortunate incidents. The most robust authentication techniques currently in existence involve the use of more than one biometric trait for authentication and validation of the user.

II. AUTHENTICATION METHODS

The authentication techniques are based on the premise that the user qualifies self as the valid individual to access the data. This is achieved through a authentication mechanism that checks the user for his proof of authenticity. The authentication methods classification is enlisted in the Table 1. The proof authentication is basically of three types - proof of knowledge (the user shows himself as authentic by possessing the knowledge about the secure mechanism), proof of possession (the user is in possession of some particular thing that is used to authenticate him) and the proof of characteristics (the user has a characteristic that is unique to self and is authenticated by it).

The biometric traits fall under the category of proof of characteristics. Compared to the other two types of proofs, the proof of characteristics is more relevant to the user and gives more security because the data is directly from one or more of the user's natural feature. It is difficult to mimicked or hacked into by any other external intruder. The paper does not argue that the biometric authentication technique is better than the other techniques and understands that there are limitations to it. The over-arching idea is that the literature study motivated us to focus on exploring the existing biometric techniques and propose a new biometric technique.

III. PHYSICAL BIOMETRIC AUTHENTICATION

The physical biometric authentication refers to the use of the physical attributes of the individual user as a means of authentication. Some of the widely used physical biometric authentication methods are finger print, palm print, Iris identification, Retinal scanning, Complex eye movement, Hand vascular movement, Face recognition, Ear recognition. Among these widely used techniques the most common is the finger print authentication which holds huge significance owing to its establishment of uniqueness. That is, no two individuals can have the same finger print which is a very good rationale for it to be used in an authentication mechanism. So, we have proceeded to study a proposed finger print based authentic system.

Figure 1. Fingerprint Sample

Figure 1 shows the sample of a finger print that is sampled as a template and stored for authentication. We have studied an existing Finger-Ident authentication system and its mechanism in detail.

The idea here is to understand the existing system so that we can incorporate the findings in our proposed system. A finger print is uniquely identified by ridges, valleys and minutiae found in the fingers. When storing a template of the finger print these are the essential parameters which are extracted and stored for authentication later. Although the concept behind the use of finger prints in authentication systems are straightforward, the efficiency of the finger print authentication mechanism depends on the algorithm that is used. (9) The paper highlights the various aspects in extracting and using the finger print templates.

The existing Finger-Ident system is categorized into the following phases:

- During user enrollment with the service for the first time a biometric template specimen of a particular user is constructed & stored in the system's DB.
- In the second phase, which is the user verification phase, the identity claim of a particular user is verified and authenticated. Registration process captured the biometric data using a finger print reader whereas the subsequent phase, if the quality of the captured finger print sample is evaluated and found to be adequate, then the features are extracted from it and stored as a specified biometric template in the database. Features from the captured biometric data (captured during every authentication) are extracted & analyzed in comparison to those samples stored in the DB. The mechanism to verify is made based on certain procedures involving pattern matching that are embedded as an algorithm, that is the base foundation for the validation of the identity of the corresponding user

We move the biometric engine as well as the biometric database to the cloud.

a) The fingerprint of a given user is first captured using fingerprint scanner (the pre-requisite here is that the scanner libraries that allow capturing fingerprint images are required to be integrated into the local application);
b) The application then communicates with the help of a API with the cloud hosted biometric web service and sends an embedded image to the library containing fingerprint processing which provides the functionality for the cloud service;
c) The transmitted biometric image is processed in the cloud service and the result is finally returned to the local application.
d) HTTPS protocol is used for data transfer.
e) SSL Protocol certificates are used
f) The passwords and other data (such as biometric templates) in the database are encrypted.
g) The access to the cloud-service is protected with the help of a sophisticated 'forty digit' password. The cloud-based service is modularly designed, which makes it a relatively simple task of service upgrade.

IV. BEHAVIOUR BIOMETRIC AUTHENTICATION

The behavioral biometric authentication technique uses the behavioral aspects of an individual user to authenticate him/her in to the cloud database system. It does not use any physical aspect but the studies the behavioral pattern of the individual, stores it and uses it as a means to authenticate. Some of the widely used behavioral biometric authentication techniques are Voice recognition, DNA recognition, Typing Behavior, Body odor, Signature recognition, Mouse movement.

We have taken one of the biometric authentication methods to study in detail - Typing behavior. The paper we have focused on uses the keystroke dynamics as a point of measurement of the user's behavioral identity. The system involves the use of complex algorithms which extracts the keystroke dynamics of the individual user and stores it as a template. The working of the system has been given in brief below along with the behavioral authentication features.

□Continuous – It protects the data after access authentication on a continuous basis.

□Adaptive – It learns the behavior of the user and tries to adapt itself by improving the user's behavioral profile.

□Transparent – The users are restricted from indulging in any sort of software manipulation.

□Non-intrusive – The software does not intrude into the user activities but only focuses on how the user is working.

□Easier to manage & integrate – The software needs minimal or literally no central configuration and administration or additional hardware

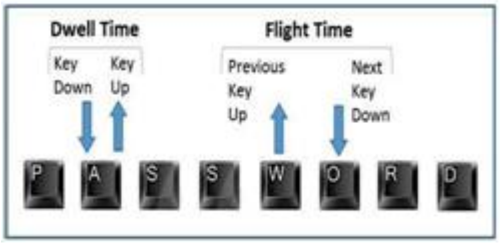

Figure 2: Keystroke Behavior Capturing Process

Registration phase

- Get the event acquisition from mouse, keyboard…
- Extract the action.
- Extract the feature.
- Create the data base for the individual users.

Verification phase

- Get the event acquisition from mouse, keyboard.
- Extract the action.
- Extract the feature.
- Using probability calculation and similarity Match(decision tree) compare the feature with original database

V. PROPOSED AUTHENTICATION SYSTEM

The proposed authentication system intends to use the phalange marks (the print marks between the phalange bones) as a template to authenticate the user to provide him/her access to the cloud data. As discussed earlier, the phalange print authentication technique is not to be used as a stand-alone authentication as its uniqueness is not established despite its high variance among individual human beings. The model is based upon our study of the two other authentication proposals and we have 3 major phases in the implementation of this authentication technique -

Registration phase, Login phase and Verification phase. The process flow in each of the phase is described in a detailed manner below.

The security of template based biometric authentication technology has been challenged because of information leakage and which is limited by the ability of the user to memorize the keys.

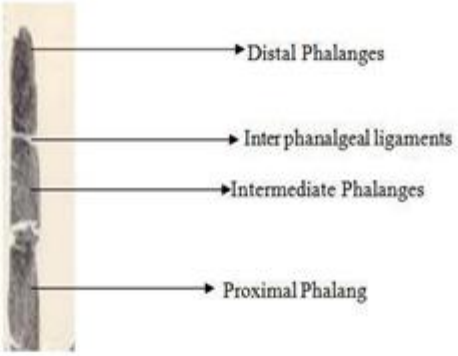

Figure 3: An Overview of the Phalange prints

Registration p2hase

- ✓ Capture Biometric finger image with high dimensional space.
- ✓ Feature of the biometric data is extracted.
  - Get the finger image
  - Calculate the ending and bifurcation of

Allphalange and compute

UID=Number (ending+bifurcation) of all phalanges.

- Identify the space in interphalangeal ligaments
- Generate the bio key **Kkey=mod (UID,Random Prime number**) using their unique ID UID **.**

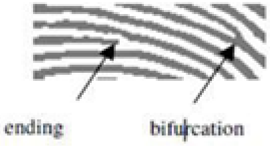

Figure 4: Phalange prints data extraction pattern

- ✓ A unique label for the extracted feature of identification is generated.
- ✓ Post encryption, it is sent to the cloud server authentication center.

Cloud Sever then decrypts the feature captured before encrypting again before storing in the Cloud database

Login phase

- The requisite biometric data point from the user is extracted for authentication.
- The feature that is to be compared for authentication is extracted.
- The label id for identification is calculated and identified.
- Encrypt the extracted template using the standard public key of the cloud server authentication network.
- Post encryption, the extract template is sent to the server side.
- Cloud server then decrypts the feature template.
- Retrieve the encrypted template from the cloud DB.

Verification phase

✓ The retrieval of the template stored in the cloud is assisted by Web API which also acts as a bridge between the user interface and the cloud server.

✓ Using the relevant decryption technique, decrypt the store biometric template.

Take Phalange prints from user
Take Interphalangeal ligament space from data base and generate the Kkey
Compare with original Keys and check for a match.

✓ Depending upon the guidelines set the extracted template is compared with the biometric feature.

✓ The user is authenticated to access the cloud if the templates match.

VI. CONCLUSION

The essence of the paper is to analyze existing biometric cloud authentication methods and propose a biometric authentication mechanism which is expected to be robust and fool proof when used along with another authentication technique. We have done a literature survey of other research works in a detailed manner by studying the various nuances used in the physical biometric as well as behavioral biometric techniques. The study also understands the significance of the data security in Cloud computing wherein authentication is a means to ensure the data security in cloud services. Since cloud computing services are becoming increasingly essential, it is imperative for us to be able to come with user friendly but robust authentication methodologies to achieve high data security. Our study also helped us understand that biometric authentication techniques are more secure and difficult to be manipulated than some of the other traditional techniques. Hence, we intended to propose a solution that is based out of biometric data. Further research about the existing biometric proposals threw light into the fact that the finger print marks in between the phalange bones are not given much importance in the finger print or palm print authentication technique. The finger print and palm print techniques predominantly focus on the print marks on the edges of the fingers, palm and ridges in the palm region. The phalange print marks vary widely among individuals but its uniqueness has not been established. Nevertheless, considering that the phalange marks vary between individuals and the possibility of two people having similar phalange marks being rare, we propose the use of phalange marks as a biometric authentication methodology in combination with another authentication technique. We have rationale that the use of phalange marks will enable for efficient, secure and effective authentication. The scope of the paper also discusses on how the authentication methodology functions through a three phase explanation - Registration phase, Login phase and Verification phase. In the future scope of work, we plan to focus on implementing the authentication model in a prototype environment and test whether our rationale that this authentication technique will be more effective and secure holds good.

REFERENCES

1. *A survey of password attacks and comparative analysis on methods for secure authentication. Authored by Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider. 2012, World Applied Sciences Journal.*
2. *Keystroke dynamics-based user authentication using long and free text strings from various input devices authored by Pilsung Kang, Sungzoon Cho. 2014, Elsevier.*
3. *On Mouse Dynamics as a Behavioral Biometric for Authentication. Zach Jorgensen, Ting Yu. s.l. : ACM Digital Library, 2011. 6th ACM Symposium on Information, Computer and Communications Security.*
4. *On Continuous User Authentication via Typing Behavior. Joseph Roth, Xiaoming Liu, Dimitris Metaxas. 2014, IEEE TRANSACTIONS.*
5. *Providing Authentication by Using Biometric Multimodal Framework for Cloud Computing. R. Parimala, C. Jayakumar. 2015, Indonesian Journal of Electrical Engineering.*
6. *Problems and Promises of Using the Cloud and Biometrics. Boult, Abdullah A. Albahdal and Terrance E. s.l. : IEEE, 2014. 11th International Conference on Information Technology: New Generations.*
7. *Biometric Matching and Fusion System for Fingerprints from Non-Distal Phalanges. Mehmet Kayaoglu, Berkay Topcu, Umut Uludag. s.l. : arXiv preprint, 2015.*
8. *A Literature Study on Finger Knuckle Matching. Sivaranjani, Yamini C, Jackulin Durairani. 2014, INTERNATIONAL JOURNAL FOR RESEARCH IN EMERGING SCIENCE AND TECHNOLOGY.*

9. *A Comparative Study on Fingerprint Matching Algorithms for EVM. D. Ashok Kumar, T. Ummal Sariba Begum. s.l.: Science and Education Publishing, 2012.*
10. *The cloud Computing security Secure User Authentication Technique. Ahmad,S&Ehsan,B.2013.IJSER,4,2166-217.*
11. *[11]User Authentication through typing biometrics features.Signal Processing,IEEE Transaction .53,851-855.Araujo,L.C.Sucupra, L.H.Lizarraga,M.G.Ling.2005.*
12. *Secure biometric template generation for multi-factor Authentication. Pattern Recognition 48,458 -472.Khan, S.H,Akbar M,A.Shahzad,F, Faroo O.M&Kahn,Z.2015/.*