ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

MULTIMODAL BIOMETRIC AUTHENTICATION IN CLOUD COMPUTING USING FINGERPRINT, FINGER VEIN AND PALM VEIN MODALITY

DHIVYAPRABHA.E[1], KALPANA.P[2], ASMITHA SHREE .R[3]

[1,2,3] ASSISTANT PROFESSOR, COMPUTER SCIENCE ENGINEERING, SRI KRISHNA COLLEGE OF TECHNOLOGY, COIMBATORE, TAMILNADU. INDIA.

Abstract: Now a days cloud computing is the most wanted method to share and store information. When it comes to confidentiality and security of private data in cloud storage need to be improved. Two factor authentication is the best technique used to protect the data, currently. Yet, we need to move for advanced technologies like biometric systems to provide high level security. Biometrics can be implemented as unimodal (single human characteristics) or multimodal (two or more human characteristics). Unimodals are not efficient because human characteristics are not constant and it is not an error free modal. Hence we are moving to Multimodal biometrics which will improve reliability of biometrics authentication when a unimodal technology cannot satisfy a required reliability. This paper is an analysis on Bio plug-in SDK device which contains three human parameters combined for authentication: (1) finger print modal (2) finger vein model and (3) palm vein modal.

KEYWORDS: unimodal, multimodal and bio plug-in SDK.

I. INTRODUCTION

Since the technologies are expanding every day, securing the personal data also became more risky. Biometric authentication is the only way to provide high level security for data stored in cloud. Unimodal Biometric authentication produces various errors like noisy data, intra class variations, non-universality, spoof attacks, and distinctiveness. To obtain accurate recognition, biometric technology with multiple human characteristic comparisons is the one which will give high authentication with the help of personal identification protocols. The inputs are either from a single device or multiple devices for measuring multiple human characteristics. Number of device is not a constrain, Biometric traits will remain independent from each other, so no need of combined mathematical equation among the characteristics.

Authentication	Types
Proof-of-Knowledge (something you know)	Passwords, PIN, Phone Number, etc.
Proof-of-Possession (something you have)	Smart cards, Tokens, Driver's license, PKI Certificates.
Proof-of-characteristics (Something you are?)	Finger Prints, Hand Geometry, Facial Image, Iris, Retina, Voice, Signature patterns.

Table 1. Authentication types

Hence high accuracy is resulted. Table 1 shows the authentication types.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

In this paper we are going to analyze drawbacks of unimodal biometric systems, proposed work, conclusion and future scope of this technology.

II. BACKGROUND

Biometric multimodal system has been analyzed by some researchers. Abdullah A. Albahdal and Terrance E. Boult (2014) revealed the major problems in systems, (1) confidentiality of user's biometric data (i.e. if a user's fingerprint is compromised it cannot be changed and the user cannot use it in the future for authentication purposes), (2) lake of matching accuracy and tradeoffs between FAR (False Accept Rate) and GAR (Genuine Accept Rate), (3) trust issue in remote biometric authentication. Also they explained to overcome those problems by using multimodal biometric authentication with a systematic procedure. There are few examples for the multimodal biometric system development such as, web-based multimodal biometric authentication application by Ghada Al-Hudhud, Eman Alarfag , Shahad Alkahtani, Afnan Alaskar, Basmah Almashari, and Hanna Almashari (2015), Authentication of E-Learners Using Multimodal Biometric Technology by S.Asha and Dr.C.Chellappan (2008), A New Biometric-based Security Framework for Cloud Storage by Ihsen Nakouri, Mohamed Hamdi and Tai-Hoon Kim (2017), A survey on Biometric Based Authentication in cloud computing by P. Padma and Dr. S. Srinivasan (2016). In this paper we are experimenting a new multimodal biometric system which consist the combination of finger print modal, finger vein modal and palm vein modal. Where finger print is a general biometric characteristic used commonly and finger vein and palm veins are the new characteristic which will result in really high level accuracy and safety. Because finger print may be damaged or can be faked whereas finger vein and palm veins cannot be set as fake. All were scanned by using a single device to reduce the cost.

III. PROBLEM DEFINITION

The problems analyzed in biometric authentication systems are; thefting of biometric details, little changes in biometric parameter are common those are not acceptable, once a biometric parameter is used for an user means it cannot be changed for any reason, duplicate parameters used means cannot find that and mismatches may occur in case of some situations like damage or scratches in finger etc. In overall, efficiency of multimodal system is better than unimodal systems yet it needs to be improved. Accuracy also not high in existing multimodal systems. Accessibility challenges like voice recognition and retina identification for respective disabled people and poor quality of the given biometric sample will lead to the failure of the system. To overcome all the problems discussed above, this multimodal system contains biometric parameters of finger print, finger vein and palm vein combined in a single device to produce authentication at it is peak level. Because finger and palm veins cannot be replaced by a fake one and all human beings will have uniqueness in these parameters basically.

IV. PROPOSED SOLUTION

Biometric parameters, Bio-Plugin servers and authentication mechanism of the Bio-Plugin SDK are discussed below.

(1) Biometric Parameters

(a)Finger print

Finger print is one of the most unique parameters in humans which cannot be same for anyone. Due to this uniqueness it is used for authentication purpose to provide high security for cloud data. The finger print scanner will determine whether the given finger image is matched with the stored image or not. Finger print will be saved in terms of binary code, not as an image. The code cannot be recovered as an image, hence no chance for duplication. But there are some drawbacks like dry skin, wet skin and damaged skin will affect the accuracy. Hence we are adding some more parameters for accuracy and security purposes.

(b)Finger vein

By capturing images of the vein patterns inside the finger we can authenticate the data, because they are inside the human body. It is impossible to remake or duplicate the finger vein. Finger vein modal scans the inner surface of the skin to scan the vein pattern that is feasible by causing near-infrared light through the finger. Hemoglobin absorbs the sunshine and offers the image of veins on a CCD camera. The authentication accuracy is a smaller amount than 0.01% for the FRR (False Rejection Rate), less than 0.0001% for

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

the way (False Acceptance Rate), and 0.33 for the FTE (Failure to Enroll). Constant vein patterns indicate the distinctiveness of the technology once even among identical twins and stay constant through the adult years. Through the optimized Bio-Plugin server, the 1: N identification happens at a rate of 8,000 templates/second.

(c)Palm vein

Palm vein scanners have to be compelled to undergo the skin surface issues like Xeroxes, roughness, wet or scarring with a high tolerance. To neglect these surface issues non-intrusive contactless authentication scanner is employed to scan the palm vein image. To register a picture the palm vein detector wants hand and blood flow of the user. Therefore identification accuracy during this technique is 100 percent. It is often enforced in 1:1 and 1: N matching environments. Palm vein modal has no physical restrictions, 100 percent accuracy all the time, no privacy risk and reasonable additionally.

(2) Bio-Plugin Servers

(a) Bio-Plugin App server

To Replace Biometric SDK Integration into Windows-based Software. (Figure 1)

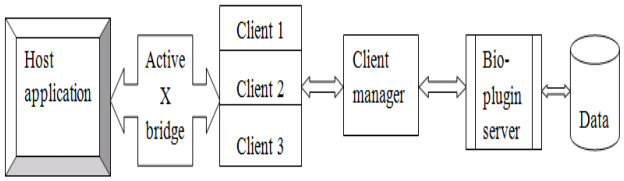

Fig. 1 Bio-Plugin App server

Supports a wide variety of development environments such as: C/C++, Delphi, Foxpro, Java, VB, Clarion, and PowerBuilder.

(b) Bio-Plugin Webserver

To Replace Biometric SDK Integration into Web-based Software. (Figure 2)

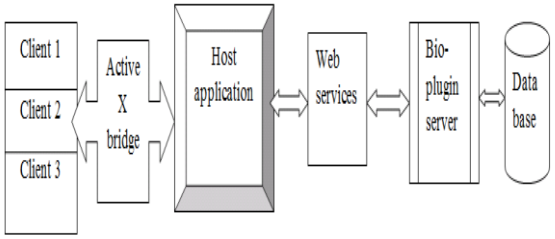

Fig. 2 Bio-Plugin Web Server

(3) Cloud Authentication Mechanism

This section explicitly focuses on establishing how the bio- metric template is embedded in the cloud computing structure to ensure authentication. The entire authentication mechanism using bio-metric in Cloud can be broadly classified into 3 phases– the Registration phase, Log-in phase and the Verification phase.(Sudhan and Kumar, 2015) The registration phase is the initial phase wherein a user who prefers to use the Cloud service registers his biometric details with the cloud computing server. The login phase immediately succeeds the registration phase and is the phase wherein the biometric feature to facilitate access to Cloud is captured and verification for authentication is initiated. The actual authentication takes place in the verification phase.

(a) Registration Phase

In registration phase (figure.3), biometric details are collected which are going to be used for authentication. After quality checking, biometric data feature extraction, unique label generation the feature is encrypted by using a public key and sent to the cloud server. Finally, the feature is decrypted and again encrypted by the cloud server before storing into the cloud

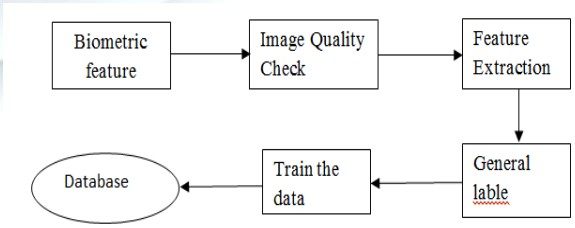

Fig. 3 Registration Phase

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

(b)Login Phase

In login phase (figure.4), the registered biometric feature and scanned image will be compared for authentication. The user's feature is extracted and label id is calculated for identification. The extracted feature is encrypted in the cloud server by a public key. Finally the cloud sever decrypts the feature template and obtain the encrypted template from the database.

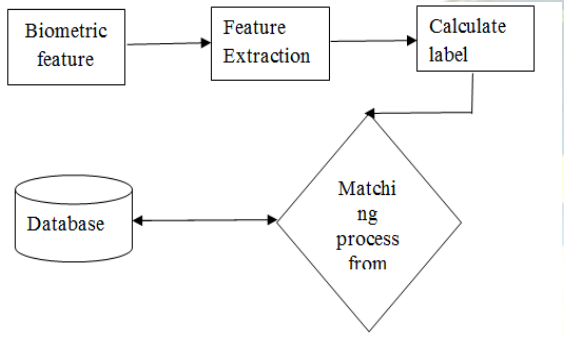

Fig. 4 Login Phase

(c) Verification Phase (sub phase within the Login Phase)

Web API links the user interface and cloud server also helps to retrieve the stored templates in cloud. It retrieves and decrypts the stored template in the cloud server by using suitable decryption technique. It compares the stored template and extracted feature, if match found means user is allowed to access or else the user will be terminated.

V. ANALYSIS

All low level biometric SDKs will leads to a disadvantage of tight embedding of image. From the analysis (Table 2) we are showing that bio- plugin is better than biometric SDK in all the cases.

Parameter	Biometric SDK	Bio-Plugin
Product Structure	DLLs; it's the building block of the system	high- performance multi-modal biometric identification engine was developed completely
Development Time	8-12 months	Within 24 hours
System Dependencies	Host software depends on biometric SDK DLLs. Constant recompile code is needed.	No dependencies on system.
Documentation	Some information for development environment may not be available.	M2SYS supports various development environments and can provide sample code. Examples include: C++, VB, .NET, Delphi, PowerBuilder, Java, Clarion, and web applications.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

Support	Minimal vendor support only, for remaining user is the responsible.	Automatic support from the development engineer for integration and developing environment.

Table 2. Comparison between Biometric SDK and Bio-Plugin

VI. CONCLUSION

This paper is an analysis regarding providing high level authentication for cloud storage information by using multimodal biometric system. The physical characteristics of biometric parameters aren't correct all the time and biometric system isn't a slip free methodology. To avoid these issues we tend to analyze a multimodal biometric system with three human characteristics that are; finger print, finger vein and palm vein. All parameters are captured by one compact. Hence it's reasonable in terms of price and compact in size conjointly. Time interval to investigate these biometric parameters is moderate. Finger print are often faked in some cases, finger vein may pretend terribly seldom however once it involves future parameter palm vein cannot be faked and appropriate for everybody while not exceptions. With the mix of those 3 parameters authentication accuracy is 100 percent and security level in it's peak. In future the process speed is often increased more and a few additional parameters (iris scanning, tissue layer scanning, heart beat functioning and voice recognition etc.) are often hooked up for additional protection.

REFERENCE

[1]. AHMAD, S. & EHSAN, B. 2013. The Cloud Computing Security Secure User Authentication Technique (Multi Level Authentication). IJSER, 4, 2166-2171.

[2]. ARAÚJO, L. C., SUCUPIRA, L. H., LIZARRAGA, M. G., LING, L. L. &YABU-UTI, J. B. T. 2005. User authentication through typing biometrics features. Signal Processing, IEEE Transactions on, 53, 851-855.

[3]. BABAEIZADEH, M., BAKHTIARI, M. & MOHAMMED, A. M. 2015. Authentication methods in cloud computing: A survey. Research Journal of Applied Sciences, Engineering and Technology, 9, 655-664.

[4]. BARRON, C., YU, H. & ZHAN, J. Cloud computing security case studies and research. Proceedings of the World Congress on Engineering, 2013. 1- 6.

[5]. DARVE, N. R. & THENG, D. P. Comparison of biometric and non- biometric security techniques in mobile cloud computing. Electronics and Communication Systems (ICECS), 2015 2nd International Conference on, 2015. IEEE, 213-216.

[6]. KHAN, S. H., AKBAR, M. A., SHAHZAD, F., FAROOQ, M. & KHAN, Z. 2015. Secure biometric template generation for multi-factor authentication. Pattern Recognition, 48, 458-472.

[7]. LI, H., DAI, Y., TIAN, L. & YANG, H. 2009. Identity-based authentication for cloud computing. Cloud computing. Springer.

[8]. MANASA, N., GOVARDHAN, A. & SATYANARAYANA, C. 2014. Fusion of Multiple Biometric Traits: Fingerprint, Palm print and Iris. Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations. Springer.

[9]. PFLUG, A. & BUSCH, C. 2012. Ear biometrics: a survey of detection, feature extraction and recognition methods. Biometrics, IET, 1, 114-129.

[10]. ROTH, J., LIU, X. & METAXAS, D. 2014. On continuous user authentication via typing behavior. Image Processing, IEEE Transactions on, 23, 4611-4624.

[11]. SINGH, M. & SINGH, S. 2012. Design and implementation of multi-tier authentication scheme in cloud. International Journal of Computer Science Issues (IJCSI),9.

[12]. SUDHAN, S. K. H. H. & KUMAR, S. S. 2015. An Innovative Proposal for Secure Cloud Authentication using Encrypted Biometric Authentication Scheme. Indian Journal of Science and Technology, 8.

[13]. YASSIN, A. A., JIN, H., IBRAHIM, A. & ZOU, D. Anonymous password authentication scheme by using

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

digital signature and fingerprint in cloud computing. Cloud and Green Computing (CGC), 2012 Second International Conference on, 2012. IEEE, 282-289.

[14]. ZISSIS, D. & LEKKAS, D. 2012. Addressing cloud computing security issues. Future Generation computer systems, 28, 583-592.

[15]. ZIYAD, S. & KANNAMMAL, A. 2014. A Multifactor Biometric Authentication for the Cloud. Computational Intelligence, Cyber Security and Computational Models. Springer.

BIOGRAPHY

Dhivyaprabha E. received the B.Tech degree in Information Technology from Vivekanandha Institute of Engineering and Technology for Women, Tamilnadu and the M.E degree in Computer and Communication from Sri Sairam Engineering College, Tamilnadu, in 2011 and 2013 respectively. Since then she has been with Sri Krishna College of Technology, Coimbatore, Tamilnadu as an Assistant Professor in the Department of Computer Science and Engineering. Her research interest includes Cloud Computing Security and Data Analytics

Kalpana P. Received the B.E degree in Computer Science from P.S.R Engineering College, Tamilnadu in 2011 and the M.E degree in Computer Science from Sri Krishna College of Engineering and Technology, Tamilnadu in 2013. She is Currently working as an Assistant Professor in Sri Krishna College of Technology, Tamilnadu. Her research interests are in Data mining and Cloud Computing.

Asmitha Shree R. is an Assistant Professor at Sri Krishna College of Technology, Tamilnadu. She received the bachelor's degree in Information Technology from Sri Krishna college of Engineering and Technology, Coimbatore, in 2013 and completed Master's degree in Computer Science Engineering Technology from Sri Krishna college of Engineering and Technology, Coimbatore, in 2015. Her research interest includes wireless *ad-hoc* networks, wireless sensor networks and cloud computing.