Providing Authentication by Using Biometric Multimodal Framework for Cloud Computing

R. Parimala[1] C. Jayakumar [2]

[1] *PhD Research Scholar, Bharathiar University, Coimbatore, India*
Assistant Professor, S.S.K.V College of Arts and Science for Women, Kanchipuram
[2] *PhD Research Supervisor, Bharathiar University, Coimbatore, India*
Professor, CSE Department, RMK Engineering College, Kavaraipettai

Abstract - As Cloud Computing has been spreading widely, users and service providers enables to use resource or service cheaply and easily without owning all the resource needed. However, Cloud Computing has some security issues such as virtualization technology security, massive distributed processing technology, service availability, massive traffic handling, application security, access control, and authentication and password. User authentication among them requires a high-guaranteed security. Identification of humans through their characteristics and traits is referred as biometrics. It is used in the area where authentication of individual or to have supervision upon individuals in a group. Each and every individual have unique biometric characteristic which cannot be forgotten, stolen or lost. But in token based or knowledge based security mechanism there are chances that it can be lost or stolen. The following the most commonly used biometric authentication and recognition trait: faces, fingerprints, irises, palm-prints, speech etc. This paper comprehensively reviews multimodal recognition using ear pattern and finger print data, it is concluded that further research should investigate fast and fully automatic ear-finger print multimodal systems robust to occlusions and deformations.

***Keywords* – Multimodal Biometrics, Ear pattern, Finger print. Security, Authentication.**

I. INTRODUCTION

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user *knows*, something the user *has*, and something the user *is*. Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority. Security research has determined that for a positive authentication, elements from at least two, and preferably all three, factors should be verified.[2] The three factors (classes) and some of elements of each factor are:

- the knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question, or pattern)
- the ownership factors: Something the user has (e.g., wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token)
- the inherence factors: Something the user **is** or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

II. BIOMETRIC SYSTEMS

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain *et al.* (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication. Universality means that every person using a system should possess the trait. Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm. Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets. Performance relates to the accuracy, speed, and robustness of technology used. Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

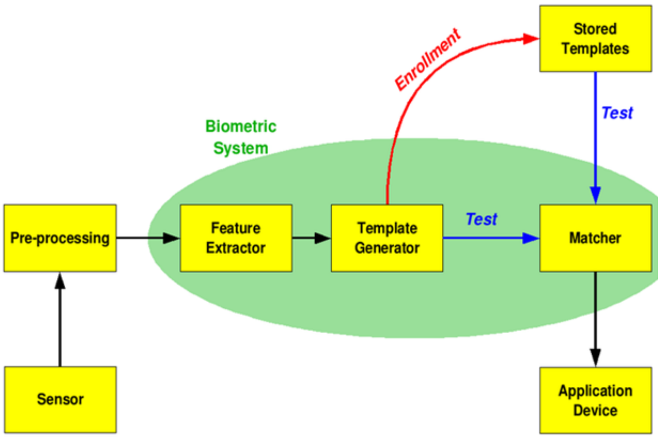


Fig.1: Simplified block diagram of biometric verification and identification.

The block diagram (Fig.1) illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

III. FINGER PRINT RECOGNITION

The functionality of the existing local version of the FingerIdent system can be divided into two main categories: user verification (enrollment*)*, during which a biometric template of a given user is constructed and stored in the system's database, and
ii) user identification during which the identity claim of a given user is validated.

The registration process uses a fingerprint reader to capture the (biometric) fingerprint data. In the next phase the quality of the captured sample is evaluated and if it is found to be adequate, the system extracts features from it and stores them in the form of a biometric template in the database. During the verification process features from the captured "live" fingerprint are again extracted and compared to those stored in the database. The comparison is made based on pattern matching procedures, which form the foundation for the validation of the identity claim. An illustration of both function is shown in Fig.1.

To reach the goal of devising a cloud-based biometric service , one needs to migrate the presented functionality of the local FingerIdent system to the cloud and provide the necessary infrastructure for accessing the biometric service. Details on this procedure are given in the next section.

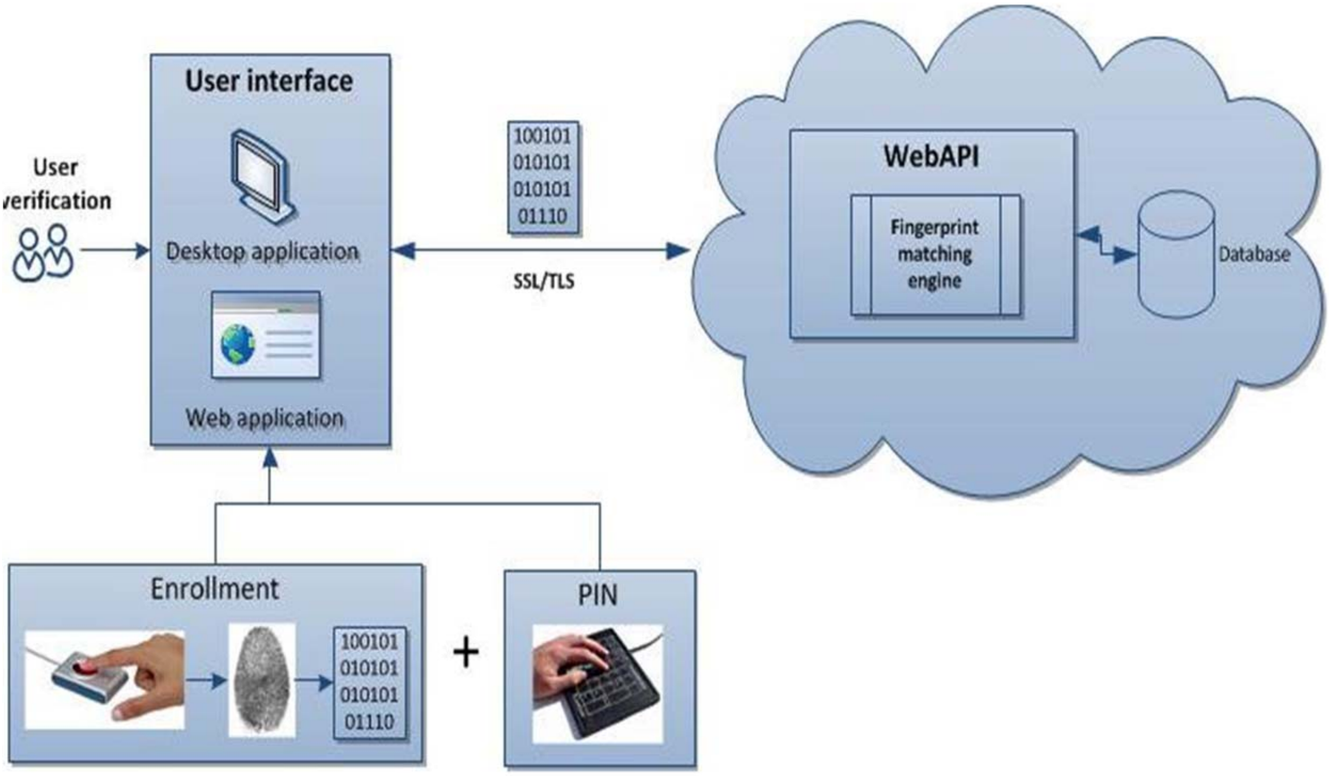


Fig.2: Scheme of the biometric verification system in the cloud

A. Designing Cloud biometric services

A review of some existing market solutions in the field of biometrics in the cloud showed some common points between the solutions. All solutions operate on the principle of the client-server model. Client on the user's computer is responsible for capturing biometric sample and sending it to the server, where matching process is executed. For the safety of network traffic between client and server security protocols are used. Verification process is done using the following scenario (Figure 2): First, fingerprint is captured via fingerprint scanner. Scanner libraries that allow you to capture the image must be integrated into the application (web, desktop). Application communicates with API, which is hosted in the cloud. Encoded image is sent to the fingerprint processing library via API. Image is then processed in the cloud and results are sent back to the application.

Solution is modularly designed, thus upgrading is possible. Our API solution could be used for other biometric modalities, also in the context of multi -modal person authentication.

B. Authentication data fusion and data security

With data fusion we want to integrate multiple data derived from different authentication processes into useful representation. We combine authentication data from desktop application and data obtained from other web applications, such as Moodle. Security of our solution is provided on different levels, the most important of these are: The use of HTTPS protocol for data transfer, encryption of passwords and other data in the database , access to cloud services is protected with a complex 40-digit password. However, in future work we want to implement additional security mechanisms, both in terms of storage and data transfer.

C . Moodle with fingerprint verification

To demonstrate the effectiveness of the presented solution and to provide a proof-of-concept, the e-learning environment Moodle [3] is augmented with biometric authentication capabilities by integrating it with the cloud-based fingerprint verification service. Since Moodle is also designed modularly, the biometric authentication procedure is implemented as an additional (optional) authentication scheme, which can complement the existing procedures and provide an additional level of access security. A block diagram of the integration is shown in Fig.3.

The main problem faced during integration is the compatibility of various fingerprint readers with different browsers. Each manufacturer of fingerprint readers offers their own protocols and libraries to access the corresponding hardware. A standard is not yet available.

The solution developed in the scope of this case study uses an ActiveX component to access the hardware. ActiveX components are officially supported only on Internet Explorer, which represents a weakness in the implementation. As future work, an extension of the presented solution is planned, so it can work with other popular browsers, such as Firefox, Opera or Chrome too After the integration of the fingerprint authentication service into the Moodle framework, the screen was modified to account for t functionality. The result of this procedure is shown in Fig. 4. Note how the added biometric authentication functionality seamlessly integrates into the existing framework.

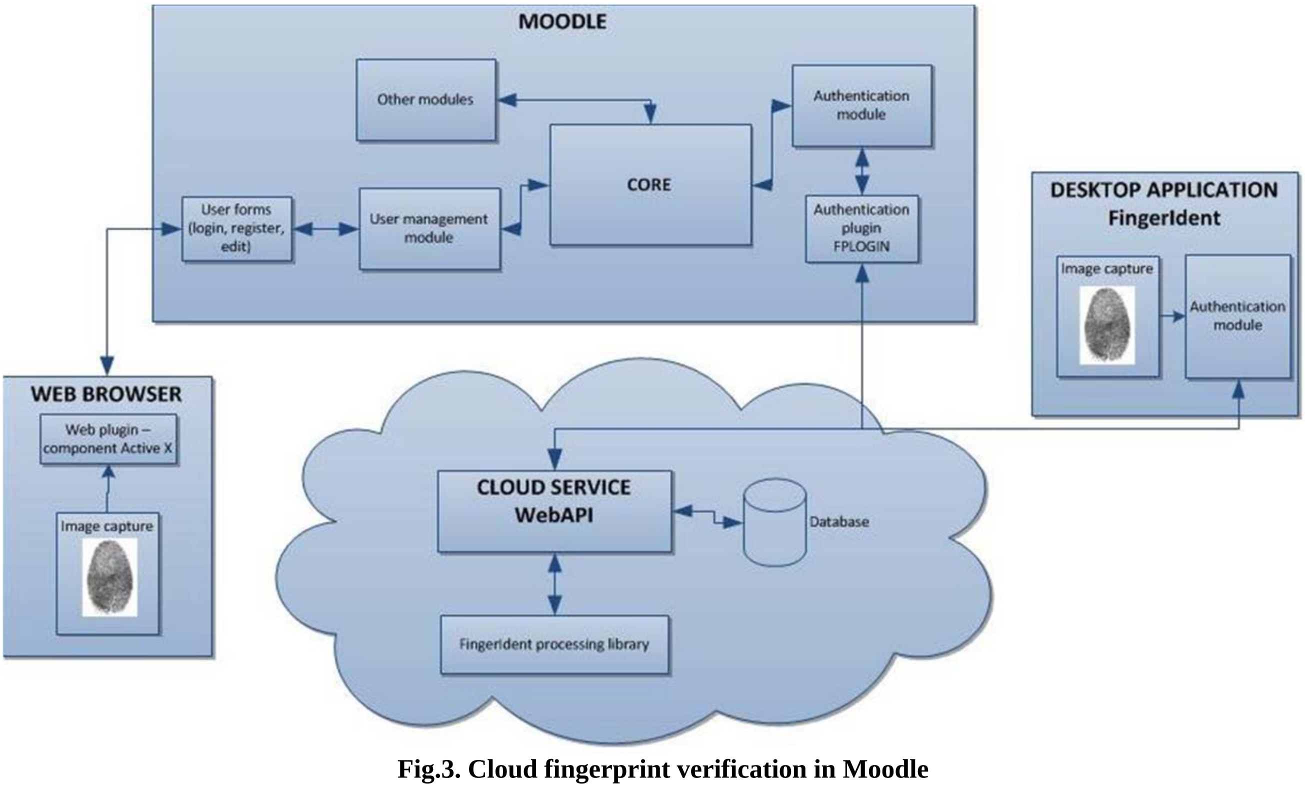
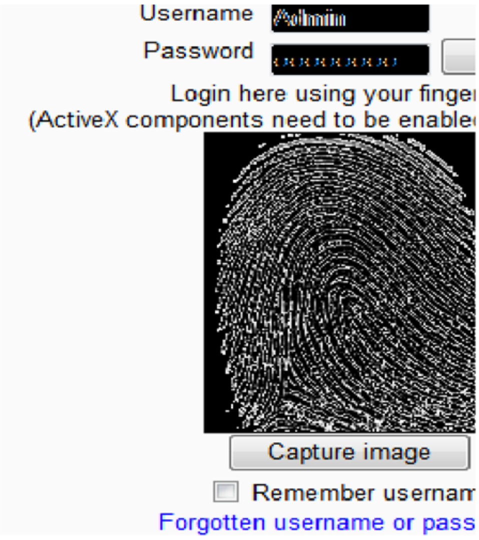


Fig.3. Cloud fingerprint verification in Moodle



Login here using your finge
(ActiveX components need to be enable

Fig.4: Customized Moodle login

IV. Ear Segmentation

First of all ear images and finger print data were collected. Next color normalization was applied because of the lighting conditions of individual images of the ear. The image acquisition system captures ear as a larger portion of image that also contains data from immediately surrounding ear region. Thus, prior to performing segmentation and feature extraction it is necessary to localize only that portion of the image that contains antihelixes, crus of helix, concha and tragus of the ear as shown in Fig.5,i.e.external ear. Here, the idea which is ear images can be seen as a composition of micro-patterns was taken which can be well described by fusion of two techniques such as DWT (using haar wavelet) and GLCM, into account. Afterwards, in order to get the features user can adjust the location of ear center. Then, those features were combined with DWT (using haar wavelet) and GLCM. The results of previous steps give representation of ear. Next to increase the accuracy of authentication system, the solid judgment on authenticating users can be achieved by a fusion of multiple sub authentication systems.

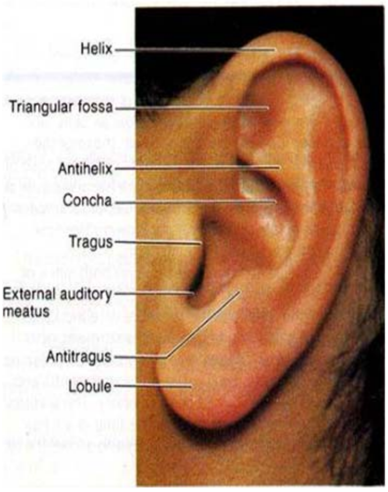


Fig 5: The surface anatomy of the auricle of the ear

In this experiment color image cannot be taken. That is why this image has to be converted into gray scale image by using the function 'rgb2gray'. Then the centroid of the image was found. Then the image was cropped as depicted in the following Fig.6

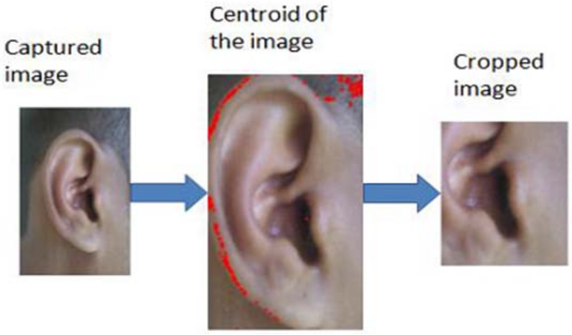


Fig.6: The process of cropping the image with respect to the centroid

A .*Discrete Wavelet Transform (DWT)*

A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. It captures both frequency and location information. For an input represented by a list of 2^n numbers, the Haar wavelet transform may be considered to simply pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale: finally resulting in (2^n-1) differences and one final sum. The Haar wavelet's mother wavelet function $\Phi(t)$ can be described as $\Phi(t) = \{ \; 0 \leq t \leq 1$, otherwise.

B. *Gray-Level Co-Occurrence Matrix (GLCM)*

GLCM is a tabulation method of how often different combinations of grey levels occur in image neighborhoods. Key components in creating the GLCM are the direction (E,W,N,S,NE,NW,SE,SW) and distance between the reference pixel and neighbor pixel.

After manipulating, we have got four matrices as follows:

A – Auxiliary matrix } approximation co-efficient matrix
H – Horizontal matrix
V – Vertical matrix
D – Diagonal matrix
Afterwards we have to calculate the mean and variance of all four matrices as depicted above.

C. **Deriving Statistics from a GLCM**

After creating the GLCMs, several statistics can be derived from them using the 'graycoprops' function. These statistics provide information about the texture of an image. The following table lists the statistics which can be derived.

Table 1: The statistics which provide information about the texture of an image.

Property	Description
Contrast	It measures the intensity contrast between a pixel & its neighbor over the whole image.
Correlation	It measures how correlated a pixel is to its neighbor over the whole image.
Energy	It returns the sum of squared elements in the GLCM.
Homogeneity	It measures the closeness of the distribution of elements.

V. Conclusion

In this paper, an up-to-date review of existing approaches for two promising biometric traits, the ear and the fingerprint are described. Techniques involving data acquisition, detection, representation and multimodal recognition with these two modalities are categorized and analyzed, thus providing the reader with a comprehensive overview of the research field. It is found that many solutions have been proposed with unimodal approaches and most of them report quite high recognition and low error rates in a controlled scenario, however, they suffer a significant decrease in accuracy in the presence of pose and expression variations and occlusions. Although it is perceived that the accuracy and robustness can be increased with fusion of ear and fingerprint, very few such approaches have been proposed. The identification and discussion of the underlying problems and challenges in this paper imply that significant further research should be performed in the area of developing fast and fully automatic ear-fingerprint multimodal systems using low-cost acquisition devices and with a data or feature level of fusion.

References

[1] H. Sieger, N. Krischnik, and S. Moller, "POSTER: User Preferences for Phones", *proceeding of 6th Symposium on Usable Privacy and Security.*

[2] A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *Transactions on Circuits and Video Technology* vol. 14, no. 1, pp. 4-20, 2004.

[3] E. Kohlwey, A. Sussman, J. Trost, and A. Maurer, "Leveraging the Cloud Meeting the performance requirements of the Next Generation Biometric Systems," in *the IEEE World Congress on Services* 2011.

[4] V. Štruc and J. Žganec " Recognition Technology for Biometrics service," in: *pp. 68-75, 2012.*

[5] J. Bule and P. Peer, "Fingerprint Verification as a Service in KC CLASS," in: 2012, pp. 76-82, 2012.

[6] The KC Class project http://www.kc-class.eu/,

[7] D. Gonzales Martinez, F.J. Gonzels Castano, E. Argones Rua, J.L. Ala Castro, D.A. Rodriguez Silva, "Secure Crypto-Biometric System for Cloud Computing," in: *Internationa Securing Services on the Cloud.*

[8] H. Vallabhu and R.V. Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution," *International Journal of Soft Computing and Engineering, vol. 2, no. 4, pp. 163.*

[9] S. Suryadevara, S. Kapoor, S. Dhatterwal, R. Naaz and A. Sharma, "Tongue New Prospects of Cloud Computing Security," in: *International Conference on Information and Network Technology*, vol. *4, 2011.*

[10] S.N.S. Raghava, "Iris Recognition on Handoop: a Biometrics System Implementation on Cloud Computing," in: *Proceedings of IEEE CCIS,*

[11] C. Senk and F. Dotzler, "Biometric Authentication as a Service for Enterprise Identity Management Deployment: A Data Protection Pers" *International Conference on Availability, Reliability and Security.*

[12] E. Kohlwey, A. Sussman, J. Trost "Leveraging the Cloud for Big Data Biometrics: Meeting the Performance Requirements of the Next Generation Biometric Systems" *Congres on Services*, pp. 597

[13] D.M. Dakhane and A.A. Arokar, "Data Secuity in Cloud Computing for Biometric Application," *International Journal of Scientific & Engineering Research*, vol. 3, no. 6, pp. 1

[14] Cloud computing use case discussion group, "Cloud Computing Use Cases: White Paper" available from: http://cloudusecases.org 05.12.2012.

[15] Homepage of the Animetrics cloud recognition solution 37 (2013) 115–122 121 *Privacy*, vol. 10, pp. 22-27, 2012. *IEEE Technology*, for Big Data Biometrics: *Proceeding of Services*, pp. 597-601.

Authors

Dr. C. Jayakumar
Ph.D Research Supervisor, Bharathiar University, Coimbatore, India
Professor, CSE Department, RMK Engineering College, Kavaraipettai, Ponneri.

Ms. R. Parimala
Ph.D Research Scholar, Bharathiar University, Coimbatore, India
Assistant Professor, S.S.K.V College of Arts and Science for Women, Kanchipuram