RESEARCH PAPER

Computer Science

Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

A Novel Combined Biometrics Method for Restricted Web Services Access Via Mobile Phone

KEYWORDS

Biometric recognition, mobile phones, web-based access.

Thamarai Selvi. V

D/O G.vasudevan, No.18,Veeraperumal Iyyangar Street, Uthiramerur, Kancheepuram District, Pin-603406.

ABSTRACT *Biometric Technology is one of the most secured methods for accessing restricted web services in accordance with recent trends. The existing architecture used in a personal computer (PC), allows a multiplatform biometric web access. The proposed application allows a mobile phone to be used as a biometric-capture device. It is different from using the biometrics in personal computer (PC). It is impossible to use the same technologies that can be used to capture biometrics in PC platforms. The problem of capturing and sending the biometrics to the web server via PC is very easy to solve using embedded applications in the web pages. The main contribution will be in - the way of capture and later it's recognition that can be performed during a standard web session. And it also overcomes the limitation of the web-browser(s) in present mobiles. Combined biometrics increases the security level and ease of access of the web services.*

I. INTRODUCTION

A Web service is a set of related application functions that can be programmatically invoked over the Internet. Web services allow buyers and sellers all over the world to discover each other, connect dynamically, and execute transactions in real time with minimal human interaction. Web services technology can be implemented in a wide variety of architectures, can co-exist with other technologies and software design approaches, and can be adopted in an evolutionary manner without requiring major transformations to legacy applications and databases.

"Web Services are encapsulated, loosely coupled, contracted functions offered via Standard protocols" where "Encapsulated" means the implementation of the function is never seen from the outside. "Loosely coupled" means changing the implementation of one function does not require change of the invoking function. "Contracted" means there are publicly available descriptions of the function.

The main characteristics of proposal with regard to the state of the art are Simplicity, Low Cost, Multiplatform, Multibiometrics and Secure.

Low cost

The same architecture for biometric web applications can be used both in PC and mobile. Then, the differences at the server side are minimal, irrespective of whether the access is via PC or mobile device, thereby reducing the cost to migrate or adapt an existing web application to mobiles.

Multiplatform

There are almost no differences for accessing the server services via PC or via mobile.

Multibiometrics

II. SYSTEM ARCHITECTURE

In mobile banking, security is one of the issues which are faced by both developer and a user. Fig 1 shows system architecture for mobile banking by using a biometric recognition. In biometric recognition the biometric acquisition and biometric up loader is done at the client side capturing engine. Captured biometrics is passes to the web server. In server side captured data features extracted and stored in template database. Biometric recognition will be done by comparing the captured data with stored data. If the data is matched with stored data means user will allow accessing the mobile banking.

User recognition is usually performed just before accessing the controlled service (i.e., login time); however, some authors propose the interesting concept of transparent authentication [2], [5], [6], i.e., to recognize the user during the run time.

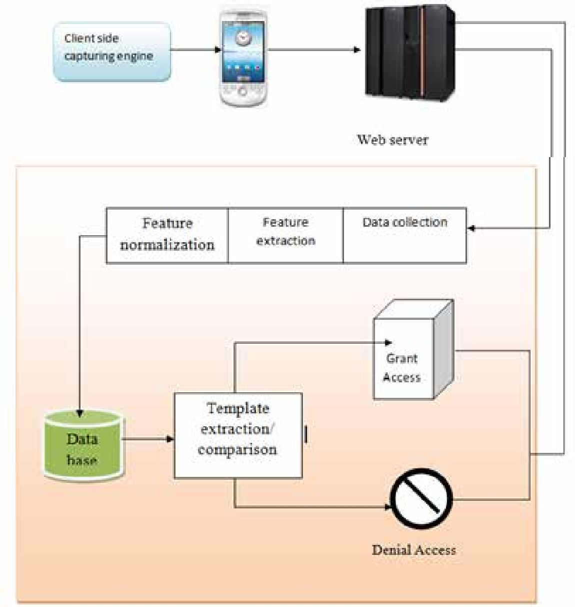

Fig. 1. System Architecture for mobile banking

The modules of the proposed architecture are allocated mainly on the server, looking for greater system security, upgrade control and avoiding computation limitations.

A. Client registration and ID generation

On the client side, the biometric acquisition software is deployed. The architecture proposes to leave only the data-capturing module on the client side, with the rest of the modules at the server side. This means that the applications developed need no special memory or processing requirements, since the main computer load falls on the execution of a web navigator and standard mobile devices (e.g., touch screen, microphone, camera, etc.) are used to capture the biometrics. Client Registration (user details, image, signature) from mobile end where the images are converted to Hash Code format as a sign of user's privacy and stored at the back end of server which in turn creates account id and user id for the respective client. The images at the server end are in turn stored as file formats.

B. User Login and feature extraction

Biometric Capturer takes in charge of calling and managing the mobile capture devices and a biometric up loader is in charge of sending the biometric data to the server and managing this uploading. A Client makes a login using his account id and user id, and the server performs a validation using his details. The Biometric Capturer captures the client's image and passes on to the server.

C. Password, IMEI No. Authentication

The password and IMEI Number Authentication will be done at the server end. The IMEI Number will be stored at the back end of the mobile's application during the time of registration process. During this stage of validation, the IMEI Number stored in the application, the mobile's IMEI Number and the password are sent to the server for the server end's validation process.

D. Signature verification and e-banking

The next level of authentication will be Signature Storage and Signature Verification which is in turn stored as Norm and Digest files in the Server end. After the validations are done, the server forwards you to the Home Page of the Bank. A balance check and a transfer of some amount to some other's account can be done in this process. The Server makes a login to deposit some amount for the particular user in his account for the above process to occur (Balance Check, Transfer of Amount).

E. Face detection and recognition

The main base of the project falls under the domain of SYSTEMS, MAN and CYBERNETICS which deals with face recognition and face detection. Java software is used to validate Face Recognition Technique. Inputs to the recognition are image 1, image 2, and path of the directory where the output file will be written. Both the faces will be compared, recognized and the output will be written inside the corresponding directory.

III. ALGORITHMS

Base64 algorithm
Dynamic time warping algorithm
Structure similarity index algorithm

A. Base64 algorithm

Base64 encoding schemes are commonly used when there is a need to encode binary data. An stream of bytes, into a stream of 64-printable characters. Base64 encoding is used to convert binary data into a text-like format that allows it to be transported in environments. Base64 encoding takes the original binary data and operates on it by dividing it into tokens of three bytes. A byte consists of eight bits, so Base64 takes 24bits in total. These 3 bytes are then converted into four printable characters. Like the same way Base64 decode schemes are performed.

IV. IMPLEMENTATIONS

Based on the system architecture system has been developed for the Mobile Banking by using different biometrics in mobile phone(e.g face recognition, signature verification).

Signature verification: The online-signature system is designed to replace the password for accessing to a remote site by the user's signature. The different system engine/modules have been implemented as follows.

Client side: A system has been developed to enable multi device authentication from both PC-like and Mobile-like web browsers. For this biometric, a touch screen in the mobile is required, since it is used to capture the signature. For capturing the signature data from the PC-like browser, a Java Applet, which captures signatures locally, and then, sends them to the server has been developed.

Server side: Apache web server with the Tomcat application server is used to design a server side. The server modules for capture and preprocessing have been developed in the hypertext-processor (PHP) programming language, and the verification engine was written in Java.

Face Recognition: This application allows services/local data of the mobile device to be accessed after authentication by face, although the biometric recognition is performed remotely. Captured face has been stored in the database. Images which is stored in the database and the input image are convert into gray code. Gaussian window is created for given grid size and standard deviation. It is used when the quality of images are compared. During authentication captured face has been compared with the stored templates by using the structure similarity index algorithm.

IMEI No. Authentication: This application allows user to register the details. Along with user detail mobile phone IMEI No. has stored in the back end. In authentication process before signature verification IMEI No. has been verified. Each user have only one account and user will access the account by the same mobile which is used to registration process.

V. CONCLUSION

The primary goal of this project is using the mobile phone has biometric capture devices. Using the mobile phone has biometric capture devices reduces the usage of separate capture devices. In this paper, the problem of using biometric user authentication during a standard web session when a mobile phone is used has been successfully approached. The technological problem of capturing the biometric with the mobile phone, sending it to the web server, and, after user authentication, allowing or rejecting the user's continuation with the web session in the same way this had been performed using password authentication.

REFERENCE

[1] M. Martinez-Diaz, J.Fierrez, J.Galbally, and J.Ortega-Garcia, "Security Management for Mobile Devices by Face Recognition," in Proc. 19th Int. Conf. Pattern Recogn., Dec. 2008, pp. 1–5. | [2] A. Hadid, J. Y. Heikkil¨a, O. Silven & M. Pietik. "Face And Eye Detection For Person Authentication In Mobile Phones Inf. Manage. Comput. Secur., vol. 15, no. 3, pp. 214–225, 2007. | [3] X. Chen, J. Tian, F. Wang."A Secured Mobile Phone Based On Embedded Fingerprint Recognition Systems" vol. 24, no. 7, pp. 519–527, 2005. | [4] R. M. Godbole and A. R. Pais, "Secure and efficient protocol for mobile payments," in Proc. 10th Int. Conf. Electron. Commerce, 2008, pp. 1–10. | [5] D. S. Jeong, H.-A. Park, K. R. Park, and J. Kim, "Towards mobile authentication using dynamic signature verification,"Lect. Notes Computer. Science.,vol. 38, pp. 457–463, 2005.