BIOMETRIC AUTHENTICATION FOR A MOBILE PERSONAL DEVICE FOR ACCESING WEB SERVICES

[1]Akash Kanshal, [2]Pankaj Kr Giri, [3]Dr.C.Nalini

[1,2]*Student*

Computer Science Department, Bharath University

Chennai, India

k.akash008@gmail.com

pankajcse019@gmail.com

[3]Professor

Computer Science Department, Bharath University

Chennai, India

drnalinichidambarfam@gmail.com

ABSTRACT-This paper provides a guidance method using an application that allows a mobile phone to be used as a biometric-capture device. The experimental environment of proposal is that this capture, and later recognition, are performed during a standard web session, using the same architecture that is used in a personal computer (PC), thus allowing a multiplatform (PC, personal digital assistant (PDA), mobile phone, etc.) biometric web access. The main goal of this experiment is to study the Biometric capture and recognition which is done through biometric multiplatform web access, either performed locally in the mobile phone,PDA or remotely in personal computer (PC). The second goal of this experiment is deep analysis of the present mobile web-browser limitations; thus, it is concluded that, it is impossible to use the same technologies for embedded web page in order to capture and send the biometrics are Applet Java, ActiveX controls, Flash technology, Javascript, and Microsoft Silverlight; therefore, new solutions, as shown here, are needed.

Index Terms—Biometric capture, mobile phones, web-based access.

I.INTRODUCTION

This paper focuses on the use of human biometric recognitions for secure access to restricted data/services using mobile phone's web browsers with Internet connection. Biometric-recognition tasks can be splited into two groups: identification, used to determine the identity of a suspect from crime-scenes informations. And verification (i.e. authentication) access places or informations of client.

There are three general categories of user authentication:

1) something you know, such as. passwords and personal-identification numbers (PINs),

2) something you have (such as. tokens), and

3) something you are (such as. biometrics).

The issues of capturing and transmitting the biometrics to the web server via PC is easy enough to solve using embedded applications in the web pages as Applets Java, ActiveX controls, Javascript, Flash technology, or Microsoft Silverlight; in our implementations, Applets have been used. Although, due to the limitations of thosedevices, this solution is further not possible in current personal mobile phones. Hence, a new solution is needed. Regardless of the huge amount of too carefully used applications that can be found, the rate of changing or modifying biometric platforms, the lack of normalization of the capture-device technology and also in communication protocols, as well as social-acceptance drawbacks, are someof the barriers to the popularization of biometric detection.

Some of the highlighted characteristics of our proposal are shown below:

1) *Simplicity*: The first two mobile applications (based on speech and online signature) were developed for the mobiles of Windows platform, and the last one (which is based on face), was also developed for Android in just two more weeks without previous experience in Android development. This is an example of the simplicity of our proposal.

2) *Multibiometrics*. The biometric recognition can be monomodal, i.e., using only one biometric, or merging several biometrics.

3)*Low cost*: Same architectures for biometric web applications can be used both in PC and mobile phones. Then, the differences at the server side are minimized, irrespective of whether the access is via PC or mobile device, results in reduction of cost to migrate or adapt an existing web application to mobiles.

4) *Secure*: Dealing with biometrics, which is a compulsary requirement, is security. Although, this issue is overcome in web technology at the communication layer, with the secure version of the hypertext transfer protocol (see http) protocol.

Physiological, on direct measurementing of a part of ahuman body (such as, iris, fingerprint, face,handshape, etc.) and Behavioral, on indirect measurements and data recieved from an action performed by the client characteristics of the human body (e.g., voice, keystrokedynamics, signature-handwriting, gait, etc.). Thisescalating technology can play a big role inaddressing the prevalent security and informationprotection issues faced by a large variety of everydayapplications.

II.RELATED WORK

Use of the main biometric images have been found: voice, iris, face, signature, fingerprints, keystroke, and gait. An original link to ear recognition can be found. It is not so easy to find an optimised biometric image for practical purposes which are easy, and secure to capture with good recognition quality. The use of various biometric images(i.e., multimodal biometric image) may result as an important fieldwork at present time. Some of the learnings that have been carried out on using the mobile phones; some of them can be seen in (voice, face, and keystroke), (face, voice, keystroke, and fingerprint), (voice and face), and (fingerprint and voice).Although, due to the drawbacks of the mobile devices, this is not a possible solution in current personal mobile phones. Hence, a new solution is needed. User recognition is normally performed just before accessing the controlled service (i.e., login time). Implementing the multimode of authentication using RFID and Fingerprint for accessing the restricted web services (such as Banks and Hospitals). The users provide the Fingerprint image and RFID while in the registration phase. This information (or data) will be stored in the Server for the future purpose of accessing web services. Then the server will divide the fingerprint image into two halfs and save one part in the server itself and provide another part to the user. The Server will check/ compare the RFID and the Fingerprint, later if it authenticates, the web server will be allowed by the server to be used by the user to access the web services.Another important contribution which can be found related with the practical

applications are those which are related with secure-payment systems based upon the mobile-phone systems. Such as, in a modified secure mobile-payment service is said to work efficiently for micropayments, thereby results in reducing the computation and communication for each and every payment. Other amount of interesting references to several payment-system proposals based on mobile devices can be seen. Within these, it should be described, as it proposes using the biometrics (i.e., fingerprint) to verify the user during payment; this recognition system is performed in the mobile phones.

III. EXISTING SYSTEM

In the existing system, it is very difficult to have a bio-metric based authentication in the mobile phones are difficult. Although the Bio-metric based authentication is secure is not developed as such as other security system. Also there is no implantation of the RFID with the Android Smartphone's.

III.1 Disadvantages / Failures

- High cost of changing or modifying biometric platforms.
- The lack of normalization in capture-device technology.
- Communication protocols, as well as social acceptance drawbacks, are all barriers to the popularization of biometric recognition

IV.PROPOSED SYSTEM

In the proposed model, we implement multimode of authentication using RFID and Fingerprint for accessing restricted web services (Banks and Hospitals). The users have to provide the Fingerprint image and RFID while registration phase.

This information will be store in the Server for the future purpose. Then the server will split the fingerprint image into two parts and save one part in the server itself and provide another to the user. The Server will check/ compare the RFID and the Fingerprint, if it authenticates, the server will allow the user to access the web services. This increases the Security.

IV.1 Advantages

- The normalization in capture-device technology is enhanced and improved.
- The problem of capturing and sending the biometric captures to web servers via PC made easy enough to solve using embedded applications in the web pages.
- Reducing the cost of changing or modifying biometrics platforms.
- Same architectures for biometric web applications can be used both in PC and mobile phones, results in reduction of cost to migrate or adapt an existing web application to mobiles.

IV.2 Modification

Apart from the multimode, we encrypt the entire data of access in the data server and the corresponding key is stored in the authentication server only after it authenticates RFID, Fingerprint and Key, then the user is allowed to access the data server.In the proposed model, we implement multimode of authentication using RFID and Fingerprint for accessing restricted web services (Banks and Hospitals).

The users have to provide the Fingerprint image and RFID while registration phase. This information will be store in the Server for the future purpose. Then the server will split the fingerprint image into two parts and save one part in the server itself and provide another to the user. The Server will check/ compare the RFID and the Fingerprint, if it authenticates, the server will allow the user to access the web services. This helps in increasing the Security.

V. IMPLEMENTATION

V.1 Algorithm:

RANDOM NUMBER GENERATION ALGORITHM:

Random number generation algorithm is used to perform a computational task to generate a sequence of number or symbols in a random manner.The many applications of randomness have led to the development of several different methods for resulting random data. Many of these have been seen since very long ago, containing dice, coin flipping, shuffle of the playing cards and many other activities. Due to the mechanical nature of these activities, producing large number of sufficient random numbers (important in statistics) which also requires a lot of work (or time). Thus, results may be collected and then distributed like random number tables. Nowadays, after the event happened of computational random number generators, a fast growing number of government-run lotteries, and other lottery games, are using RNGs instead of other traditional drawing methods. RNGs are also used nowadays to determine the odds of modern slot machines.

V.2 Modules

1) MOBILE USER

2) MAIN SERVER

3) AUTHENTICATION SERVER

4) RFID / FINGER PRINT VERIFICATION

5) WEB SERVER INTERACTION

V.3 Modules Description

V.3.1 MOBILE USER:

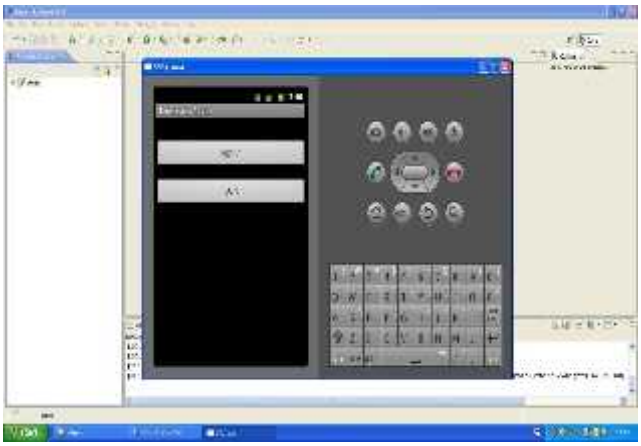
An Android mobile client is an application that access a service made available by a server. The server is often (but not always) on another computer, in which case the client accesses the service by way of a network.

To send the request to the server, the users have to be an registered person in the server. The user have to submit their user name password and another details to the server during the registration phase. All this information is stored in the database via server for future purpose.

V.3.2 MAIN SERVER:

A server is a computer program running to serve the requests of other programs, the "clients". Thus, the "server" performs some computational task on behalf of "clients". The clients either run on the same computer or connect through the network.

Here the Server acts as the main resource for the client. Server is responsible for maintaining all the client information. So the server will process the user's request and get the concerned data from the database.

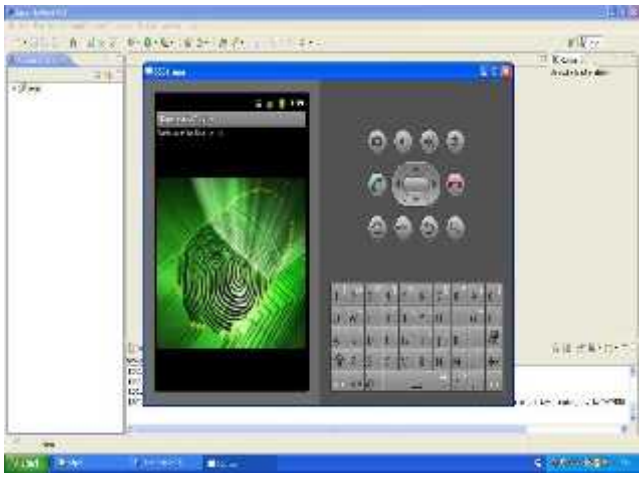


V.3.3 AUTHENTICATION SERVER:

In this module, the entire data of the data server is encrypted and corresponding is stored in Authentication server. The authentication server will verify all the information provided by the user when logging into to the account. When the data is encrypted the hacker is not possible to view the data. This provides more security.

V.3.4 RFID / FINGER PRINT VERIFICATION:

During the registration phase the user RFID and the Fingerprint was obtained by the server and stored in the database. When the user is logging in every time from the Android mobile the user's RFID and Fingerprint will be verified. If the RFID and Fingerprint are not matched the user will not allowed accessing the server.



V.3.5 WEB SERVER INTERACTION:

If the user's RFID and Fingerprints are matched, then the user is requested to enter their Authentication Key. If the key is matched then the user is allowed to access the raw data from the data server.

V.4 Architecture:

Fig: Diagramatic architecture of the system

VI.EXPERIMENT AND RESULT

The experiment is to perform a biometric recognition during a web session, in the time when a mobile phone is used. The biometric-user authentication system can be used to substitute the password or can be used in addition to it. This has already been done for PC, laptop, and other similar platforms, that are related with signature recognition. Analysis of the technologies used for the embedded programs in a web page in order to capture and send the biometrics, followings have been found by us:

1) *Applet Java tests*:

2) *ActiveX control tests*4:

3) *Javascript test*:

4) *Flash tests:*

5) *Microsoft Silverlight test*:

Our first step to the problemis to create the biometric acquisition by using a mobile phone in the same way as with the PC, i.e., using the aforementioned technologies to embed applications in a web page. Having knowledge about the computational restrictions of the mobile devices, a study about the state of the technology in the main mobile-phone platforms and browsers was necessary.

The biometric to the web server based on the current mobile technology is not ready for embedded applications inmobile web browsers. The standard communication protocol are A web browser and internet connection. Where the remote services are accessible via web (e.g. e-banking, ecommerce, e-mail, etc.)As there are different multiplatform mobiles are accessible through different web browsers .the different access devices are personal computers (PCs), laptops, NetBooks, video-game consoles, personal digitalassistants (PDAs) and mobile phones.

A general suggestion to capture biometrics through a mobile device, during a standard web session whichonly can be stored in the server or used with remote (i.e., web service) or local (i.e., mobile data or application).It can also be used for restricted access to local data and/or applications in the mobile device, using remote biometric recognition system.When the biometric templates are already stored in a central database and the authentication is done in the network, the constraints upon the algorithmic complexity become less stringent, and the system modifications becameeasier to implement; these only have an effect on the server and not on the user device.The acquired biometric can only be stored in the server, which plays very important role for remote presence control or for online remote documents "biometric sign". For an example, the Spanish General Post Office uses mobile devices like MC70 handheld mobile computers in order to capture user signature in telegram delivery system, but this capture is performed offline; our proposal would further allow the signature to be sent to the server just in the time when the user receives the telegram, thereby it allows an online-delivery tracing, i.e., it can be known the time and, if the device has a GPS, where the delivery has to be handed in.

VIII. CONCLUSION

A solution can be essentially contains, embedding a web browser on a mobile-phone application, using amodular architecture. By the three different Biometric images that are refined with architecture modules is very simple, veryefficient ideas and are exposed. First, we have shown that there are lots of related works, projects; however, as far as the authors knowledge, none of them have ever approached the biometric recognition system in a mobile environment via the Web.

Secondly, we have shown that the standard solution to approach the problem in a PC platform, using Applets Java, ActiveX controls, Javascript, or Flash technology, doesn't work under the mobile platforms. Therefore, a new alternate solution is needed.

The future stage of the work should be divided into technological problems and basic research. The technological problems to be approached in the future are to implement the proposed solution onanother mobile-phone platforms and to perform very deep study of the communication load and server performance in words of the number of users.With regards to basic researches, multichannel (PC, PDA, mobile phone, etc.) biometric recognition can be used as an interesting problem. There are some studies in biometrics, such as voice or face, but later biometrics, such as signature, face, are still an open problem.

REFERENCES

1) N. L. Clarke and A. Mekala, "The application of signature recognition to transparent handwriting verification for mobile devices," *Inf. Manage. Comput. Secur.*, vol. 15, no. 3, pp. 214–225, 2007.
2) R. L. Kay. (2003). Protecting mobility, IDC White Paper [Online]. Available at: http://www.tsi.enst.fr/∼chollet/Biblio/Articles/Domaines/ BIOMET/IDC/Protecting_Mobility.pdf
3) 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.
4) D. S. Jeong, H.-A. Park, K. R. Park, and J. Kim, "Iris recognition in mobile phone based on adaptive gabor filter," *Lect. Notes Comput. Sci.*, vol. 3832, pp. 457–463, 2005.
5) Q. Zhang, J. N. Moita, K. Mayes, and K.Markantonakis, "The secure and multiple payment system based on the mobile phone platform," presented at Workshop Inf. Secur. Appl., Jeju Island, Korea, 2004.
6) N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones—A survey of attitudes and practices," *Comput. Secur.*, vol. 24, no. 7, pp. 519–527, 2005.
7) K. R. Park, H.-A. Park, B. J. Kang, E. C. Lee, and D. S. Jeong, "A study on iris localization and recognition on

mobile phones," *EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 1–11, 2008.