ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (343-347), Month: April-June 2014, Available at: www.researchpublish.com

Restricting Unauthorized Access Using Biometrics In Mobile

S.Vignesh*, M.Narayanan#

Under Graduate student*, Assistant Professor#
Department Of Computer Science and Engineering, Saveetha School Of Engineering
Saveetha University, Saveetha Nagar, Thandalam, Chennai-602105.

Abstract: **The use of biometric person recognition for secure access to restricted data /services using a mobile phone with Internet connection have been dealt. Biometrics can be divided into two categories based upon the underlying characteristic they are using: physiological and behavioral. There are three general categories of user authentication: 1) something you know, e.g., passwords and personal-identification numbers (PINs), 2) something you have (e.g., tokens), and 3) something you are (e.g., biometrics). Today, with the advancement of mobile handsets and wireless networking, mobile devices have both the network access and computing capacity to provide users with a diverse range of services (e.g, secure payment , e-banking, e-commerce (better: m-commerce), etc.).Then, a very popular device, with increasing functionality and access to personally and financially sensitive information; therefore, the requirement for additional and/or advanced authentication mechanisms is essential.**

Keywords: **Biometrics, network access, authentication mechanism, personal identification number.**

I. INTRODUCTION

The mainstay of this project is to present an application that allows a mobile phone to be used as a biometric-capture device. The main contribution of our proposal is that this capture, and later recognition, can be performed during a standard web session, using the same architecture that is used in a personal computer (PC).

The use of biometric person recognition for secure access to restricted data /services using a mobile phone with Internet connection have been dealt. Biometrics can be divided into two categories based upon the underlying characteristic they are using: physiological and behavioral. There are three general categories of user authentication: 1) something you know, e.g., passwords and personal-identification numbers (PINs), 2) something you have (e.g., tokens), and 3) something you are (e.g., biometrics).

Today, with the advancement of mobile handsets and wireless networking, mobile devices have both the network access and computing capacity to provide users with a diverse range of services (e.g, secure payment, e-banking, e-commerce (better: m-commerce), etc.). We have, then, a very popular device, with increasing functionality and access to personally and financially sensitive information; therefore, the requirement for additional and/or advanced authentication mechanisms is essential.

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 proposal of this project is to present a novel mobile-phone application architecture to capture and send the biometric to the web server based on the use of an embedded web browser. The current mobile technology is not ready for embedded applications in mobile web browsers; however, it is prepared for our solution, which is very easy and effective, as will be seen.

II. SYSTEM ANALYSIS

2.1 Existing System

Many commercial and research efforts have recently focused on this subject. However, in spite of the great amount of particular applications that can be found, the cost of changing or modifying biometric platforms, the lack of normalization in capture-device technology, and communication protocols, as well as social-acceptance drawbacks, are all barriers to the popularization of biometric recognition.

The dominant approach on current control access is via password or PIN, but its weaknesses are the most clearly documented: if it is easy to remember, it is usually easy to guess and hack into, but if it is difficult to attack, it is usually difficult to remember; hence, a lot of people write them down and never change them. The problem with tokens is that they authenticate their presence, but not the carrier; they can be easily forgotten, lost, or stolen, and, as it happens with the credit cards, can be fraudulently duplicated. As a result, biometry appears as a good solution, which is generally used, in addition to the previous authentication methods, to increase security levels.

2.2 Proposed System

The main contribution of our proposal is that this capture, and later recognition, can be performed during a standard web session, using the same architecture that is used in a personal computer (PC). Today, with the advancement of mobile handsets and wireless networking, mobile devices have both the network access and computing capacity to provide users with a diverse range of services.

The main characteristics of our proposal with regard to the state of the art are Simplicity, Low Cost, Multiplatform, Multi biometrics and Secure. A lot of works/applications can be found that focus on the use of biometry with mobile devices; however, as far, none of them show a similar system to the one in this paper: a general proposal to capture biometrics by means of a mobile phone during a standard web session. This capture can only be stored in the server or used with remote (i.e., web service) or local (i.e., mobile data or application) restricted access.

III. REQUIREMENT SPECIFICATIONS

3.1 Introduction

The requirements specification is a technical specification of requirements for the software products. It is the first step in the requirements analysis process it lists the requirements of a particular software system including functional, performance and security requirements. The requirements also provide usage scenarios from a user, an operational and an administrative perspective. The purpose of software requirements pecification is to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface, hardware and software requirements. It defines how the client, team and audience see the project and its functionality.

3.2 Hardware and Software Specification

1) Hardware Requirements

- Hard Disk: 80 GB and above.
- RAM: 1 GB and above.
- Processor: Pentium III and above.
- Mobile Phone with Wi-Fi Access and Java Support.
- Wi-Fi Router.

2) Software Requirements

- Java 1.6.0_24
- Tomcat 7.0.12
- Struts 1.2
- Matlab Compiler Runtime(MCR) 7.6

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (343-347), Month: April-June 2014, Available at: www.researchpublish.com

- J2ME Wireless Toolkit

3.3 Technologies Used

1) Java

It is a Platform Independent. Java is an object-oriented programming language developed initially by James Gosling and colleagues at Sun Microsystems. The language, initially called Oak (named after the oak trees outside Gosling's office), was intended to replace C++, although the feature set better resembles that of Objective C.

IV. SYSTEM DESIGN

4.1 Architecture Diagram

It gives the basic architecture of the developing project

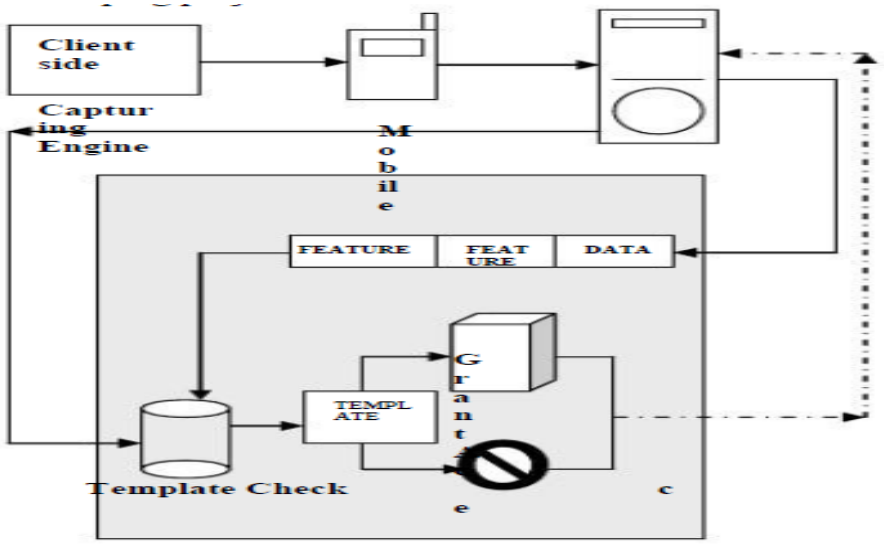

Figure. 4.1 Architecture Diagram

V. SYSTEM IMPLEMENTATION

5.1 Module Explanation

1) Server Design

The server side contains the main parts of the functionality of the proposed architecture. In our first module we deal upon accessing the Server Tier designing part of our project. We deal on working with Tomcat Server and designing our web pages using Struts.

On the client side, the biometric acquisition software is deployed. Our architecture proposes to leave only the data-capturing module on the client side, with the rest of the modules at the server side. Http// 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. We perform Client Registration from our mobile end to connect it to our server which in turn creates account id and user id for the respective client.

2) User Login and Image Capturing Engine

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.

3) Feature Extraction

This module collects the raw biometric data and prepares them for processing by the verification engine. This is based on biometric data supplied by the server-side capturing engine, and it generates the feature vectors. In addition to obtaining the features vector or sequence of feature vectors, it is usual to perform further geometric transformations. The database contains information from the users of the system (i.e., user's database subsystem) and their biometric templates (i.e., user's templates subsystem).

The matcher compares the information received against the template of the client stored in the database, thereby generating a numeric comparison score. The Score-normalization is to improve the system performance or to use a universal decision threshold. From the comparison of the score with a decision threshold, this determines whether the user is accepted or rejected and is, thus, granted or denied access to the system or protected services and transmits the output back to the client.

VI. CODING AND TESTING

6.1 Coding

Once the design aspect of the system is finalizes the system enters into the coding and testing phase. The coding phase brings the actual system into action by converting the design of the system into the code in a given programming language. Therefore, a good coding style has to be taken whenever changes are required it easily screwed into the system.

6.2 Coding Standards

Coding standards are guidelines to programming that focuses on the physical structure and appearance of the program. They make the code easier to read, understand and maintain. This phase of the system actually implements the blueprint developed during the design phase. The coding specification should be in such a way that any programmer must be able to understand the code and can bring about changes whenever felt necessary.
Some of the standard needed to achieve the above-mentioned objectives are as follows:

1. Program should be simple, clear and easy to understand.
2. Naming conventions
3. Value conventions
4. Script and comment procedure
5. Message box format
6. Exception and error handling

6.3 Test Procedure

1) System Testing

Testing is performed to identify errors. It is used for quality assurance. Testing is an integral part of the entire development and maintenance process. The goal of the testing during phase is to verify that the specification has been accurately and completely incorporated into the design, as well as to ensure the correctness of the design itself. For example the design must not have any logic faults in the design is detected before coding commences, otherwise the cost of fixing the faults will be considerably higher as reflected. Detection of design faults can be achieved by means of inspection as well as walkthrough.

Testing is one of the important steps in the software development phase. Testing checks for the errors, as a whole of the project testing involves the following test cases:

- Static analysis is used to investigate the structural properties of the Source code.
- Dynamic testing is used to investigate the behavior of the source code by executing the program on the test data.

VII. CONCLUSION

In this proposed system the problem of using biometric user authentication during a standard web session when a mobile phone is used has been successfully approached. It has focused on 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.

First, it has been shown that there are several related works, projects, and commercial applications; however, as far as the authors knowledge, none of them have approached the biometric recognition in a mobile environment via the Web. Second, it has proved that the standard solutions to approach the problem in PC platforms, using Applets Java, ActiveX controls, Javascript, or Flash technology, do not work under mobile platforms. Therefore, a new alternative is needed.

A solution has been shown that basically consists of, instead of embedding an application in the web page, embedding a web browser in a mobile-phone application, using a modular architecture to develop the biometric web application. Three different implementations of this simple, but very effective, idea have been shown, with one allowing the password to be substituted by the signature in a web access to a restricted service, and the others allowing a restricted access to local data and/or applications in the mobile phone, using remote voice/face recognition via the Web. The main characteristics of our proposal are that 1) it is free of charge to the user (he/she only needs to download the application), 2) there is no difference with regard to access by means of a PC, even more, it is easier, as the user does not need to key the URLs, 3) the server modification and mobiles multiplatform-application development costs are very low.

The future lines of the work can be divided into technological and basic research. The technological problems to be approached in the future are to implement the proposed solution in other mobile- phone platforms and to perform an in-depth study of the communication load and server performance in terms of the number of users. With regard to basic research, multichannel (PC, PDA, mobile phone, etc.) biometric recognition is an interesting problem.

There are studies in biometrics, such as voice or face, but other biometrics, such as signature, 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.