Design and Modeling of Real Time Multimodal Biometric Authentication System

Sanjay Kumar, Surjit Paul and Dilip Kumar Shaw

1Department of Computer Science and Engineering, NIT Jamshedpur, India
2Department of Computer Application, NIT Jamshedpur, India

Abstract: Authentication is a major challenge for accessing different web-based applications, information exchange, communicating people, conducting e-business and performing financial operations, access to system like ATM, Wi-Fi etc. Biometrics based authentication could be used to prevent unauthorized access to these systems. Multi-modal biometric authentication system could be used to further strengthen the security by overcoming the limitations imposed by unimodal biometric authentication system. This paper aimed to design and model the multimodal biometric authentication system for secured access to different web applications through WLAN. The proposed system is designed using UML (Unified Modelling Language) diagrams.

Keywords: Unimodal, Multi-Modal, Biometric System, WLAN, UML, Authentication

Introduction

Authentication is the process of verifying the identity of the claimant. Biometric systems are becoming popular day by day to identify claimant by measuring his/her physiological or behavioral characteristics. The biometric characteristics are unique in nature which cannot be misplaced, stolen, forgotten, guessed, or easily forged. Despite of these inherent advantages, biometric systems have some limitations. For example a person's finger may be changed sizes or form/pattern over time and the fingerprint scanner does not take this into consideration, for face, the image quality, image size, face angle and processing and storage are the biggest hurdle whereas with iris recognition technology that is the equipment is very expensive. The multimodal biometric authentication system using different biometric traits provide added advantage over the conventional authentication system.

Biometrics, together with encryption can be capable of providing better security for web access, e-commerce and m-commerce (Teodoro and Serrao, 2011). But despite all these measures, hackers and attacker still penetrate into organization’s records leading to violation of people’s information rights. For secured web application access through WLAN is the biggest challenge for the researchers. To deal the security problem of web application is that it requires implementing security at various layers like, network, internet, transport and application. Our proposed work deals with the application layer security. In our system, each web application present in the local server needs an additional level of authentication using multimodal biometric authentication system. First of all all users who want to access the web application using Wi-Fi required to enroll themselves. Once the enrollment has been done, to access the web application by the users, they required to pass through authentication process by providing their credentials as per requirement of different web applications. In our proposed system, we have introduced four levels of authentication for different web applications. Advance Authentication Server (AAS) verifies the user’s credentials with the stored credentials for each and specific level. Based on matching, the server either grants access permission to web application to the authenticated user or access is denied.

The rest of the paper is organized as follows; section II deals the problem statement; section III deals the proposed system architecture, Section IV introduces the proposed system design using UML; Section V deals application layout and finally section VI deals with conclusion and future work.

Related Work

Teodoro and Serrao stated that the National Institute of Standards and Technology (NIST) had a National Vulnerability Database (NVD), which has over 4000
biometric traits, individual can be distinguished easily as physically present at the point of identification; physiological or behavioral characteristics. This method providing full proof security for web access, e-commerce being decrypted and be used to gain access to the application illegally (Okafor and Ogbuabor, 2013). Biometrics, together with encryption is capable of providing full proof security for web access, e-commerce and m-commerce (Niham, 1995). Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: The person to be identified is required to be physically present at the point of identification; identification based on biometric techniques obviates the need to remember a password or carry a token (Uddin et al., 2011). Due to inherent property of biometric traits, individual can be distinguished easily and become a choice for authentication which will provide high level of security. Use of multiple biometric indicators for identifying individuals, so-called multimodal biometrics, has been shown to increase accuracy (Jain et al., 1999; Ross and Jain, 2001; Uddin et al., 2011) and would decrease vulnerability to spoofing while increasing population coverage. It has been proved that the use of multimodal biometric traits of individuals can achieve a higher accuracy than the use of a single biometric (Kumar and Zhang, 2006; Bouchaffraa and Amira, 2008; Chang et al., 2003; Uludag et al., 2004).

Problem Statement

There are different web applications hosted in different servers. Web application access through username and password is no more secure due to attacks. We required developing a secured system to access different web application by any user. Users have to connect with Advanced Authentication Server (AAS) through Access Point (AP) in order to access web applications. The AAS facilitates enrollment and authentication for users. Biometrics is widely used for identification and verification of the users. The web applications can be secured by incorporating different levels of security parameters based on confidentiality of the particular web application. AAS incorporates an additional level of security mechanism based on biometric traits to access the web applications. It does preprocessing, feature extraction, template generation, template encryption, decryption and matching. Users enroll during enrollment phase and are authenticated during authentication phase. During enrollment biometric traits with user information are stored in the database. During the authentication, AAS verifies the biometric traits of the user with the decrypted stored template. If match is found then user get permission from AAS to access the web application otherwise access is denied. By incorporating multi modal biometric authentication scheme in the web application, security of the web application can be ensured and the security breaches i.e., man in the middle attack, masquerading, sniffing etc. can be minimized.

System Architecture

The Fig. 1 shows the proposed system architecture for accessing the web applications hosted in different web servers in LAN. The architecture consists of three basic blocks i.e., client, web server and AAS. Different web applications can be hosted in different web servers in LAN. Based on sensitiveness of information contained in different web applications, different level of security can be assigned to access these applications. Client may be a personal computer, laptop or mobile stations through which users want to access the hosted web applications in LAN. The AAS consists of two main modules i.e., enrollment and authentication. For accessing these web applications, users have to first register themselves to the AAS using enrollment module. After getting registered from the AAS, as per requirement to access the web application, the client can initiate the access request to AAS. AAS uses matching module to match the biometric traits provided by the user during authentication with the registered user credentials during enrollment. Figure 2 shows the modules present in the proposed multimodal biometric authentication system. The Table 1 shows the security levels assigned to different web applications. The web application 1 requires level1 authentication using username and password, the web application 2 requires level 2 authentication using username, password and fingerprint, the web application 3 requires level 3 authentication using username, password, fingerprint and face and web application 4 requires level4 authentication using username, password, fingerprint, face and iris. The different web servers hosting different web applications, AAS consists of enrollment and authentication modules, mobile stations are connected through the Wi-Fi access point (AP). In order to access these web applications, first of all users have to enroll themselves into AAS. After getting authentication from AAS, users can access the web application hosted in the server. The AAS can be accessed through wireless LAN.
Fig. 1. Architecture of the Proposed System

Multimodal Biometric Authentication System

- Enrollment
- Authentication
- Web

Fig. 2. System Modules

Fig. 3. Enrollment and Authentication Phases of the System
Table 1. Level wise authentication of the proposed model

<table>
<thead>
<tr>
<th>Authentication level</th>
<th>Level1</th>
<th>Level2</th>
<th>Level3</th>
<th>Level4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Password</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Thumb</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Face</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Iris</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Web Application</td>
<td>Website 1</td>
<td>Website 2</td>
<td>Website 3</td>
<td>Website 4</td>
</tr>
</tbody>
</table>

The working steps of enrollment and authentication phases are shown in the Fig. 3.

Enrollment

Client request for enrollment to the AAS. AAS provides the enrollment form to the user. User provides his/her username and password along with biometric traits like fingerprint, face and iris. For providing fingerprint, face and iris optical finger print scanner, digital camera, iris scanner respectively can be used. The captured biometric templates will be preprocessed using median and Gaussian filtering techniques. After processing, feature extraction for different biometric traits will be done. For fingerprint minutia based features are extracted; for face different Eigen faces will be generated from the face images; for iris Hough transformation will be used for segmenting iris then it will be normalized using Daugman’s rubber-sheet algorithm. After submitting the enrollment form, AAS server encrypts the user password and biometric templates using different symmetric key algorithms like AES, Blowfish and RC4 and will be stored into template database. Finally AAS will provide an enrollment successful message to the user.

Authentication

During authentication, the authentication form will be provided to the client as per the authentication level used for the web application. User provides his/her credentials in the authentication form as per the security level of the web application. For authentication level 1, the username and password provided by the user will be hashed with salt and will be matched with hashed password stored in the database. For authentication based on level2 to level4, user provides his/her biometric traits using the biometric scanners. The input biometric templates are preprocessed and feature will be extracted. After feature extraction template will be generated and will be matched with decrypted template of the user stored in the database during enrollment. If match will be found then user will be granted access by AAS and is redirected to the corresponding web application.

During different levels user authentication are performed as given below:

Level-1 Authentication

AAS matches the username and password of the claimed identity with hashed password generated using password along with salt stored in the database shown in Fig. 4.

Level-2 Authentication

In Level2, the web application requires username, password pair and thumb for authentication by AAS. If the username and password are matched as per level1 and also thumb templates are matched with the decrypted template of the encrypted thumb template stored in the database during enrollment as shown in Fig. 5. If both are matched then only user is authenticated by the AAS and corresponding web application is loading in the browser.

Level-3 Authentication

In Level3, the web application requires username, password pair, thumb and face for authentication by AAS. If level1 and level2 authentication are successful then face template is matched with the decrypted template of the encrypted face template stored in the database during enrollment as shown in Fig. 6. If both are matched then only user is authenticated by the AAS and corresponding web application is loading in the browser.

Level-4 Authentication

In Level4, the web application requires username, password pair, thumb, face and iris for authentication by AAS. If level1, level2 and level3 authentication are successful then iris template is matched with the decrypted template of the encrypted iris template stored in the database during enrollment as shown in Fig. 7. If both are matched then only user is
authenticated by the AAS and corresponding web application is loading in the browser.

The total authentication time to access web applications hosted in the server with different level of security are expressed by the equations given below:

\[
\begin{align*}
\text{Level 1: } & \text{TAT}^1 = \text{TMHPi} \\
\text{Level 2: } & \text{TAT}^2 = \text{TAT}^1 + \text{TDT}_{\text{thumb}} + \text{TMT}_2 \\
\text{Level 3: } & \text{TAT}^3 = \text{TAT}^2 + \text{TDT}_{\text{face}} + \text{TMT}_3 \\
\text{Level 4: } & \text{TAT}^4 = \text{TAT}^3 + \text{TDT}_{\text{iris}} + \text{TMT}_4
\end{align*}
\]

where, \( \text{TAT}^1, \text{TAT}^2, \text{TAT}^3 \) and \( \text{TAT}^4 \) are the Total authentication time for level1, level2, level3 and level4 respectively. \( \text{TMHPi} \) = Time to match the hashed password. \( \text{TDT}_{\text{thumb}}, \text{TDT}_{\text{face}} \) and \( \text{TDT}_{\text{iris}} \) are template decryption time for thumb, face and iris respectively. \( \text{TMT}_2, \text{TMT}_3 \) and \( \text{TMT}_4 \) are template matching time for corresponding levels.

Database Structure of the proposed system in MySQL is shown in Table 2.

![Diagram of Level 1 Authentication using Hashed Password with Salt](image1)

![Diagram of Level 2 Authentication using Thumb Impression](image2)
Table 2. Database Structure of the proposed system

<table>
<thead>
<tr>
<th>Field</th>
<th>Data type</th>
<th>NULL</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>RegNo</td>
<td>Int (11)</td>
<td>No</td>
<td>Primary key</td>
</tr>
<tr>
<td>StudName</td>
<td>Varchar (30)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>Varchar (30)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>Varchar (1)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Dob</td>
<td>Varchar (15)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>email</td>
<td>Varchar (30)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td>Varchar (256)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>photo</td>
<td>mediumblob</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>facephoto</td>
<td>mediumblob</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>leftirisphoto</td>
<td>mediumblob</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>rightirisphoto</td>
<td>mediumblob</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Encryption_type</td>
<td>mediumblob</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Fig. 8. Enrollment and Authentication Steps

Fig. 9. Class Diagram
Fig. 10. Use Case Diagram

Fig. 11. Sequence Diagram of Enrollment

Fig. 12. Sequence Diagram for Authentication
Fig. 13. Home Page

Fig. 14. User Enrollment Interface

Fig. 15. Screenshot of Level 1 Authentication
Proposed System Design

From the problem statement we have identified five classes and one interface from the different candidate classes. The corresponding class diagram, use case diagram and sequence diagram are designed for the proposed system using Unified Modeling Language (UML) (https://www.gliffy.com/uses/uml-software/). It is a general-purpose, developmental, modeling language and is de facto standard of designing in the field of Software engineering. The Fig. 9 to Fig. 12 shows the respective diagrams of the proposed system.

Proposed Application Layout

The proposed system is developed in java, JSP and servlet technology. The screenshots of enrollment and authentication are shown in the Fig. 13 to Fig. 16.

Conclusion and Future Work

Most of the systems are designed based on unimodal. Very few systems are designed based on
multi-modal authentication system using fusion approach. Also, most of the systems are based on internet whereas the proposed system is multi-modal with different security levels assigned to web applications access through WLAN. Here, in the proposed model there is flexibility of assigning security based on sensitiveness of the web application. According to the security assignment to the web application, user can access these web applications either by minimum one biometric trait or maximum three biometric traits along with username and password. The proposed system has facility to be used as unimodal as well as multi-modal system. The proposed model is object oriented based designed and is modeled using UML diagrams. The system interfaces are developed using java, JSP, opencv and servlet technology. Different biometric scanners and their software development kit can be used to develop the system. During enrollment, different symmetric key encryption technique like AES, Blowfish and RC4 can be used. Use of encryption and decryption technique during enrollment and authentication will be tested and its performance analysis will be judged in future. Also, best preprocessing and feature extraction and template generation technique will be explored.

Acknowledgement

The authors feel greateful to the anonymous reviewer for their valuable comments and suggestions to improve the quality of paper and would like to thank them from core of the heart.

Author’s Contributions

Sanjay Kumar: Conceptualization, Design and Analysis Drafting and Critical revision.

Surjit Paul: Implementation, Drafting and Revision.

Dilip Kumar Shaw: Drafting the Manuscript and Revision.

Ethics

After publication of the paper, if we learn any sort of errors that changes the interpretation of the research findings, We are ethically obligated to promptly correct the errors in a correction, retraction, erratum or by other means.

References

DOI: 10.1016/j.patcog.2007.06.033

DOI: 10.1109/TPAMI.2003.1227990

https://www.gliffy.com/uses/uml-software/


DOI: 10.1109/TIP.2006.875214


DOI: 10.1007/3-540-45344-X_52


DOI: 10.1109/JPROC.2004.827372

***