ANALYSIS OF MULTILEVEL BIOMETRIC AUTHENTICATION SYSTEM

(NIKHIL VARMA, JUNED BAGWAN, NILESH BASUTKAR, VIKRAM WANKHADE)
GUIDED BY - PROF. BHAGYASHREE PATLE

(DEPARTMENT OF COMPUTER ENGINEERING, SKN-SITS COLLEGE OF ENGINEERING,

SAVITRIBAI PHULE PUNE UNIVERSITY, INDIA)

ABSTRACT

In the time of overall surge of data being created and used in day to day life, from the simplest things like making a call to more complicated and security intensive tasks like online transactions the need of full proof yet easy to use security system is becoming more of a need than a choice. Now a days keeping data secure is very big issue. There is lack of strong authentication system which can provide security to confidential data. A 3D image can be used for the authentications as it gives more accuracy. We can also use the gestures for the doing the authentication for users. Multilevel Biometric Authentication System uses the several levels and each level is different which makes it more secure and reliable. In our system we have added three levels for user to be able to access the system. Once user is able to access the system, we also provide him with the encryption option for the data he is going to use and store after completing these three stages successfully. We are using AES algorithm for this.

Keywords: *Biometric authentication, AES, 3D, Face Detection, Multi-level, Encryption.*

INTRODUCTION

These days, a growing number of users store and manipulate important and sensitive information online, everything we do on the Web or Mobile devices produce a massive amount of data. Therefore we needed to find out more secure and easy-to-use authentication methods, with the increase in exploitation of data the necessity to keep this data secure increases. Previously, passwords and PINs are the most widely-used authentication methods for gaining access to PCs, mobile devices and online accounts, and they are well-understood.

There are series of application like e-commerce transactions, such applications requires more reliable personal recognition schemes for individuals which are requesting their services. However the traditional authentication systems are having large number of complex passwords and is preferred for users having multiple accounts, users typically resort to using options of a simple password, which puts users at high risk if it is compromised. Although, researchers have long been working on a wide range of biometric traits of several major categories (e.g. hard and soft biometrics, the static biometrics, the activity-related ones etc.), only specific modalities have been proven sufficient to support robust and accurate recognition performance up to now, i.e. fingerprint-, palm print-, iris, face- and to an extent gait recognition [1].

The traditional text password can be easily get prone to shoulder-surfing attacks by just observation of password entry or any smudge attacks, by observation of residue its touch-based password or stroke gesture entry. As a likely solution to the

previously mentioned problems, we present a biometric authentication method that uses 3D face, in-air hand gestures and key to authenticate the user. Instead of depending on the user's information of a secret, biometric authentication systems, such as proposed system can enhance security of data by directly using the distinct physical features of a the real user and examining behavioural characters of the genuine user during the authentication process. As biometrics, proposed system uses different points on the user's face and hand (fingertip positions and hand centre).

Developed system uses password and key as its first level of authentication. This will allow the user to choose his own key. The next level use the user's in-air hand gestures to provide next level of authentication security. In this case user can put his own unique hand gesture for authentication at the time of registration. The third level of the system focus on users face including depth. In this level we are extracting details of the user's face along with depth of the features from each other. Compared to other face recognition systems being used in other authentication mechanisms it gives much better results. This will provide system with additional level of advanced security. The system will take 22 points in case of hand gesture and 72 points with respect to face recognition and then do the computation work on it. The system developed is going to be used for a standalone network along with cloud based system.

DEVELOPED SYSTEM

As shown in the below diagram our system consists of a software application and a RealSense camera. Using this we have developed a system which is a 3 level based biometric authentication system. The three levels are – login with id and password, then a gesture input from the user and third and final stage is face detection. Once user registers with login id and unique gesture along with his face, he has to just remember the login id as gestures are very easy to be remembered and we do not need to actually remember them[2].

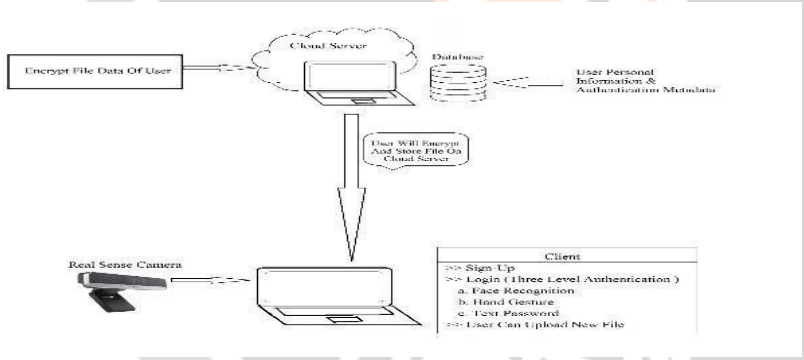

Fig: System Design

Every time the user has to access his data he has to login using the id and the unique gesture he registered at the time of creating his profile. Once he clears these two stages he has to go for face detection. After he clears that he has access his data which is stored in the system in the encrypted form. We are using AES algorithm to encrypt the data. For storing the data we are not using any database as it becomes difficult to process the data in real time. We are using the concept of Serialization.

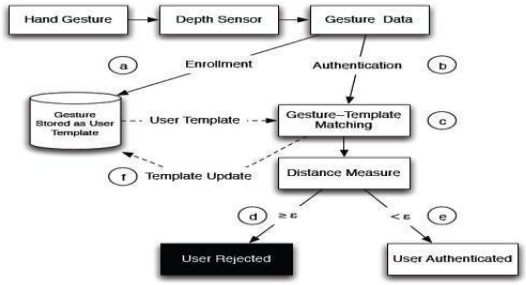

Fig: Conceptual Overview

The Actual process of whole system is as shown in the figure below. When we input the hand gesture for the first time, it is stored as a user template and for the further times the gesture is compared with that template for matching. If the template is matched after getting the distance and other details of the gesture, user is authenticated else user is rejected.

ANALYSIS

OLD SYSTEM: Traditionally there always has been one technique of authentication which is Login and password combination. But with the vastness of the penetration of Internet and computers into our daily lives this system is not enough to give us the required security. It can't protect the transactions where money is involved or which are too classified to be known by others than the legitimate owners for the simple reason that this system can be broken up by the hackers and intruders very easily. To solve this problem different technique were tried for example giving more than one password, OPTs etc, but they are not yet full proof. The more security to be provided the more complex the stages became. User had to remember many things which was cumbersome on his part. Keeping all this in mind the new system was designed to overcome all the bad aspects of this system.

NEW SYSTEM: In the development of Multilevel Biometric Authentication System we used combination of hardware and software sophistications. While designing levels of authentication we envisioned a system which will be easy to use for the user yet provide high level of security to the data being stored [3].

In the first level we implemented normal login Id/password method which is used in most of the conventional systems and to which normal used is accustomed. Other two stages were designed keeping in mind that they should increase security but not at the cost of complicating the procedures. So in the second stage Gesture Recognition, we are taking a unique gesture from the user at the time of registration. It is scientifically proven that it is nearly impossible to copy a particular gesture made by a person by another person. Even if the intruder succeeds through these two stages he will be stopped at the third stage which is impossible to pass though if you are not a genuine user. In the third stage users face is taken as an input through a camera. This stage differs from other face recognitions in a way that its a 3D-face recognition with 72points given out by the camera. This is very much accurate compared to its counterparts. Even for second stage, this same depth sensing camera is used which gives 22 coordinates. Once a user successfully enters in the system by passing these 3 stages, he has option of either Uploading a file to the web server or downloading the files previously uploaded. These files are encrypted using AES algorithm. Key for this algorithm is taken from combination of outputs of three levels of authentication, so user does not need to remember the key too [4].

In this way we designed a whole new system by combining three authentication stages to give the best possible security along with maintaining the simplicity of it so that even normal user is able to use it without much difficulty.

TEST CASES

We are using unit testing for testing the system we have developed. The objective in unit testing is to isolate a unit and validate its correctness. Automation approach is efficient for achieving the objectives of this testing and it enables the many benefits.

Following test cases were performed on the system developed.

Test Case Objective	**Expected Results**	**Status (Pass/Fail)**
Leave all fields as blank and click Log-in button	By leaving all fields as blank and on click Login button then mandatory symbol (*) should appear in front of Username and	Pass

	Password fields	
Enter Invalid Username	By entering invalid Username then an error message should appear as " Please Enter Valid Username "	Pass
Enter valid Username	It should allow the user to proceed	Pass
Enter password	The password field should display the encrypted format of the text typed as (****)	Pass
Enter wrong password	By entering invalid password then an error message should appear as " Please Enter Correct Password"	Pass
Enter Correct password	It should allow the user to proceed	Pass
Correct Inputs	It should lead the user to the respective page	Pass
Check for Validation / Error Messages on all the Screen	Validation error messages Shall be displayed properly at correct position	Pass
Check for all the Fields Label on all Forms	Field labels Shall be standard e.g. field accepting users first name should be labelled properly as First Name	Pass
Check text on all pages for spelling and grammatical errors	All Spelling Shall be Correct and without Grammatical Errors	Pass
Check functionality of buttons available on all pages	All Buttons on the Forms should be Functional	Pass
Check all the Fields on the Page/ Forms	All fields on page (e.g. text box, radio options, dropdown lists) shall be aligned properly	Pass
Check if correct data is getting saved in database upon successful page submit	Correct data shall be saved in database	Pass

Check values for columns which are not accepting null values	Enter Null/ Empty Values into database	Pass

Checkfordata integrity	Data shall be stored in single or multiple tables based on design	Pass
Check if page load time is within acceptable range	Page shall be loaded within acceptable time range	Pass
Check CPU and memory usage under peak load condition	CPU and memory under peak load shall be loaded within acceptable time range	Pass

CONCLUSION

The Biometric security Systems are the systems which uses the physical characteristics of a person like finger print, hand geometry, face , voice and iris. These systems overcomes the drawbacks of the traditional computer based security systems which are used at the places like ATM, passport, payroll, drivers' licenses, credit cards, access control, smart cards, PIN, government offices and network security. The biometric security systems have been proved to be accurate and very effective in various Applications. The biometric features can be easily acquired and measured for the processing only in the presence of a person. Hence these systems are proved highly confidential computer based security systems. This system recovers the drawbacks of previous systems by means of the newly developed stages for securing of the data.

FUTURE ENHANCEMENTS

This system can be used along with other more accurate systems such as Retina Detection to develop a more secured system. It can be shifted to web based application for remote user. Levels of authentications can be modified. Enhanced Security algorithms can be added which will allow us address data protection issues in a better way. This system can be also implemented as a mobile application. Overall this can be swapped with the applications such as AppLock services which aren't as efficient as this.

REFERANCES

[1] "AirAuth: A Biometric Authentication System using In-Air Hand Gestures", Sven

G. Kratz, Md Tanvir, CHI Extended Abstracts 2014: 499-502.

[2] "The Scheme of 3-Level Authentication Mechanism for Preventing Internal

Information Leakage", Sang-Pil Cheon, Jung-Min Kang, Min-Woo Park, Jung-Ho Eom, 2014 IEEE.

[3] "A Multimodal Biometric Recognition

System Based on Fusion of Palmprint, Fingerprint and Face", Sheetal Chaudhary , Rajender Nath, 2009 ICARTCC.

[4] "A Study of Encryption Algorithms

(RSA, DES, 3DES and AES) for Information Security", Gurpreet Singh, Supriya, April 2013 International Journal of Computer Applications.