Designing Secured User Authentication System by Using Biometrics

Nikita M. Agashe[1] Prof. Sonali Nimbhorkar[2]
[1,2]Department of computer Science and Engineering
[1,2]G. H. Raisoni College of Engg. Nagpur, India.

Abstract— As the security of the web based application are very important and major concern of today's world is security. Each and every fields demands the highest security but in most of the authentication system security is been given by username with their password. Apart from it doesn't provide as security as biometric techniques provides. Biometric application ensures more security for authentication process than proving the username and password. Here it points user verification and the session management to verify continuously presence of logged in users and also protect the system from attacks and hijacking. Also improves the security and usability of session by using authentication and verification of user identity with desired biometric traits.

Keywords: Authentication, Multi modal Biometric, Security, verification

I. INTRODUCTION

As we all know that security is very serious concern now days because of increase in the rate of major attacks which leads to the session hijacking, misuse of computer resources, and malicious use of the confidential information. All these are the today's major problems which we all are facing in our life. Basically the most of authentication procedure for a system is based on the usernames and their respective passwords. As this authentication procedure is not that efficient as biometrics techniques are. Now what exactly the biometrics means? Biometric is a word which is typically consist of two terms. First one is bio that is life and another one is metric which means measurement. Hence by using the biometric traits like fingerprint, eye, face, palm, voice, hand, etc we can protect our system from unethical use by unauthorized persons. The working of the biometric system is been shown below

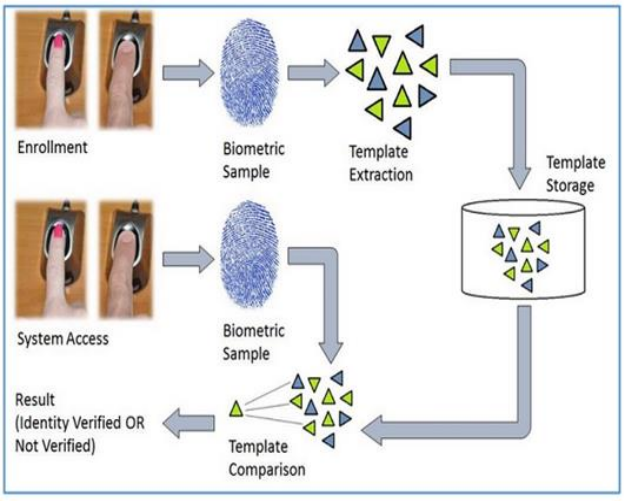

Fig. 1: Basic working of Biometric System

These are 4 basic steps of biometric system which are shown below-

1) Acquire real time sample image of individual from sensor
2) Extraction of features from image
3) Comparison of real time image with stored one.
4) Display the result of decision

Hence for detecting the unethical or malicious use of the several computer resources from hackers and unauthorized user, biometric techniques are used which basically substitute an authorized user with the unauthorized one and enhances the security of the system.

II. PROPOSED METHODOLOGY AND DISCUSSION

For Secure User Identification and Verification system includes respective following modules-

Module 1 :- Fusion Module

In this fusion module, the fusion of biometric data of the user that is eye template with the system is being done by using appropriate method that is the Kalman filter.

Module 2 :- Verification of Authenticate users

In this second module of project, the detection of the eye from face, the template generation as well as the matching of the template i.e. current images of user with the image of the authorized user which is stored in system is being done by using very effective methods that are Haar Cascade Feature Classifier and Binarization.

Module 3 :-Data Sharing Module

In this third module of project, the transferring of files in the network that is the internetwork transmission of data can be done by using ECDH Algorithm which renders the security in transmission of data.

A. Proposed Flow Of Project Work:

The proposed flow of project work is shown below

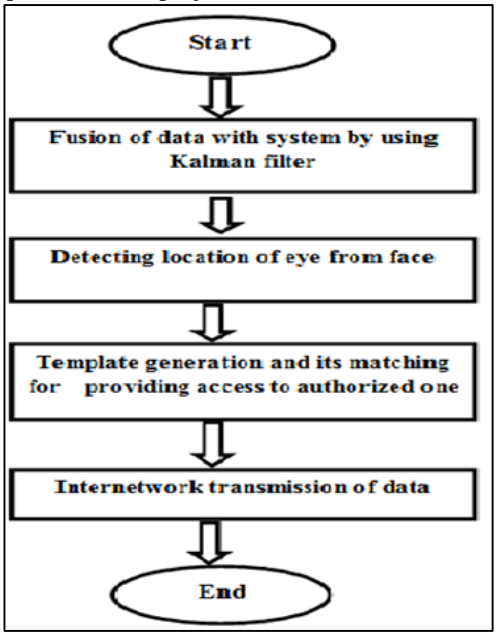

Fig. 2: Flow chart of project work

Working step Secure User Identification and Verification for Wireless Network are as follows:

Step 1: As the session started the sensor device that is web camera gets on and start scanning the face of user. This procedure is called as Feature capturing.
Step 2: Detect the location of eye from the face by using Haar feature-based cascade classifiers and starts scanning the eye of user which continuously which verifies the authorized user and secures the system from session hijacking or from maliciously used by unauthorized person. This phenomenon's involve pre-processing and feature extraction.
Step 3: Images of user's eyes and face can be saved.
Step 4: Template generation and matching:
In this phase of project to verify the identity of the current user is being done by the template generation and matching of the template i.e. matching current images of user with the image of the authorized user which is already stored in the database of system. After matching, only those persons are allowed to access the system whose template is being matched.
Step 5: Internetwork transmission of data:

In this phase of project internetwork transmission of data with Elliptic Curve Diffie Hellman (ECDH) security based algorithm.

Here the transferring of files in the network that is the internetwork transmission of information by using highly secured algorithm that is ECDH, which provides the more security in transmission of data as well as to avoid its delay.

III. Experimental Results and Analysis

The proposed technique has been implemented in dot net programming language and run under Pentium-III (1GHz) machine with 256MB of RAM.

Fig. 3: Sign Up and In page

Figure.3 shows the login page where users can register themselves in the system.

Fig. 4: Detection of eye from face

Figure 4. Shows the detection of location of eye from face i.e. feature extraction.

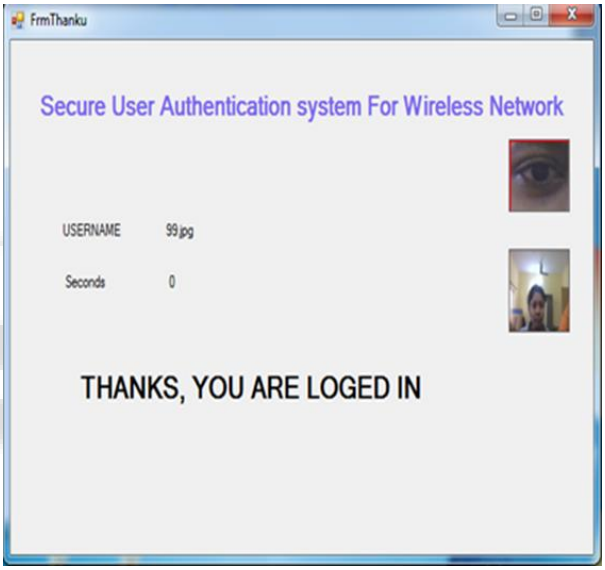

Fig. 5: Authorized user logged in

Here it verifies identity of authorized user as well as shows the time duration for detecting user. After verification and authentication process system provide access to user.

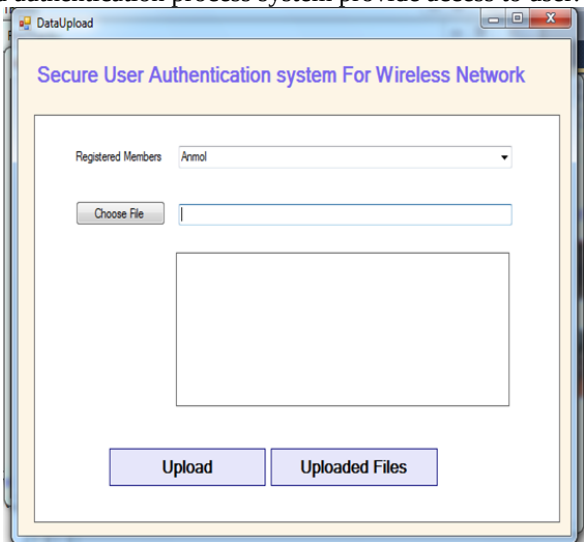

Fig. 6: Page for encryption and decryption of data (communication)

Till the figure 5 shows all about how the authenticate user is being logged in to the system. And this form (Figure- 6) is for the communication purpose in which user can communicate with another party and established a session between them.

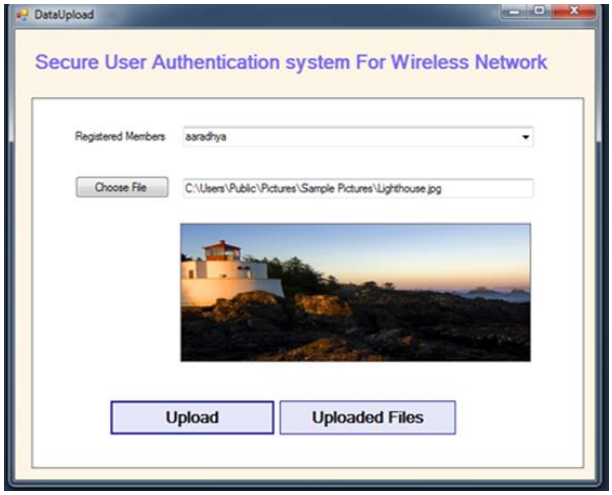

Fig. 7: Form where user entered all detail

This form depict that how the user i.e sender can send image to the receiver. For sending image to the receiver, first of all the user have to select the name of the user to whom he wants to send image and then select the path of the image as shown in the above figure 7. After selecting path of image, the desired image will get display in the form and when user clicked on upload button, the desired image will be send to receiver.

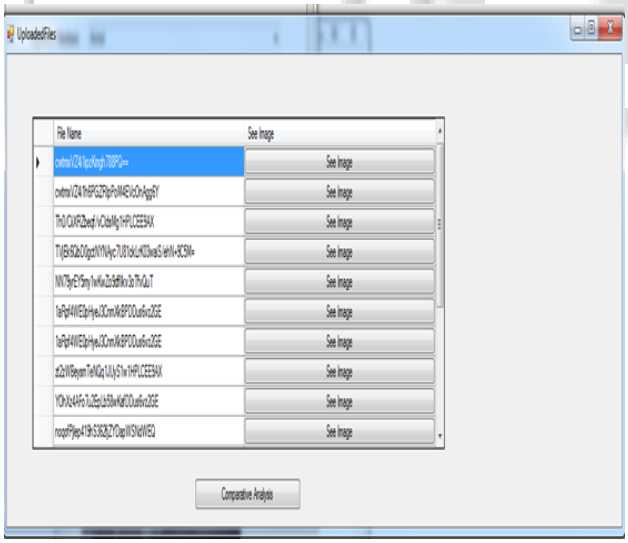

Fig. 8: Form of Uploaded Files

This uploaded form shows each and every transaction which is being done on that system. Here file name and image are in encrypted form

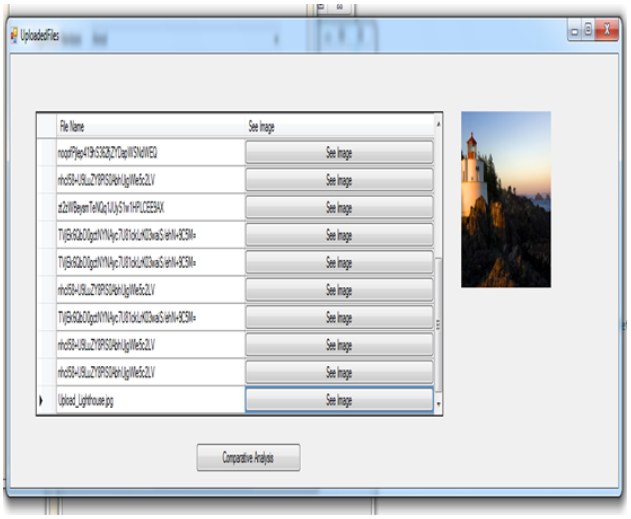

Fig. 9: At receiver side form

Here file name and image will be seen to the receiver. File name and image are in decrypted form.

IV. CONCLUSION

Here presenting approach for continuous user identity verification and session management throughout entire session securely by using biometrics. In the existing system only single verification is being done at the initial phase i.e. login phase due to which there is probability of session hijacking so to avoid the problem of hijacking the session continuous monitoring of users can be done.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1,pp. 4–20, Jan. 2014.

[2] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security", IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp.125–143, Jun. 2013.

[3] X. Suo, Y. Zhu, and G. Owen, "Graphical passwords: A survey", in Proc. Annu. Computer Security Applications, 2012, pp. 463– 472

[4] Zhi Zhou, Student Member, IEEE, Eliza Yingzi Du, Senior Mem-ber, IEEE, N. Luke Thomas, and Edward J. Delp, Fellow, IEEE,"A New Human Identification Method: Sclera Recognition", IEEE transactions on systems, man, and cybernetics part a: systems and humans, vol. 42, no. 3, may 2012

[5] Sandeep Kumar,Terence Sim,Rajkumar Janakiraman and Shen Zhang,"Using Continuous Biometric Verification to Protect Interactive Login Sessions", School of Computing,National University of singapore.

[6] Anil Jain,Kathik Nandakumar and Arun Ross,"score Normalisation in multimodal biometric systems",Pattern Recognition 38(2005)2270 2285.

[7] S. Zhang, R. Janakiraman, T. Sim and S. Kumar, "Continuous Verification Using Multimodal Biometrics", Proc.Second Int'l Conf. Biometrics, pp. 562-570, 2010.

[8] A. K. Jain, S. Prabhakar, and S. Chen, "Combining multiple Matchers for a High Security Fingerprint Verification System", Pattern Recognition Letters, 20(11-13), 1371-1379,1999.

[9] A. K. Jain, S. C. Dass, and K. Nandakumar, "Soft biometric traits for personal recognition systems",LNCS, vol. 3072, pp. 731– 738, 2004.
[10] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics", IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 687–700, Apr. 2011.
[11] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics",Proc. Workshop on Multimodal User Authentication, pp. 131-137, 2013.
[12] Azzini, Stefania Marrara, Roberto Sassi and Fabio Scotti, "A fuzzy approach to multimodal biometric continuous authentication", Fuzzy Optimal Decision Making, vol. 7, pp. 243-256, 2010.
[13] Antonia Azzini and Stefania Marrara, "Impostor Users Discovery Using a Multimodal Biometric Continuous Authentication" Fuzzy System,Lecture Notes In Artificial Intelligence, vol. 5178, Proceedings of the 12th International Conference on Knowledge- Based Intelligent Information and Engineering Systems, Part II, Section II,pp. 371-378, 2009.
[14] Hang-Bong Kang and Myung-Ho Ju, "Multi-modal Feature Integration for Secure Authentication", International Conference on Intelligent Computing, pp.1191-1200, 2012.
[15] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Andrea Bondavalli,, "Continuous and Transparent User Identity Verification for Secure Internet Services", IEEE Transactions On Dependable And Secure Computing, December 2013.

