Journal of Computer Science

Original Research Paper

Real-Time Multimodal Biometric User Authentication for Web Application Access in Wireless LAN

[1]Sanjay Kumar, [1]Surjit Paul and [2]Dilip Kumar Shaw

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

Article history
Received: 29-07-2017
Revised: 01-08-2017
Accepted: 25-09-2017

Corresponding Author:
Sanjay Kumar
Department of Computer Science and Engineering, NIT Jamshedpur, Jharkhand, India
Email: sanjay.cse@nitjsr.ac.in

Abstract: Web applications store trustworthy information and can be accessed online through wired or wireless network. Authentication is one of the major challenges to access these web applications. With varying level of sensitive data stored in web application, the concept of level of authentication can be introduced using biometric traits. This paper proposes biometric-based multi-modal authentication system with four levels of securities. Level 1 uses user name and password only; Level 2 uses fingerprint with user name and password; Level 3 uses fingerprint and face with user name and password; Level 4 uses fingerprint, face and iris with user name and password.

Keywords: Trustworthy, Authentication, Biometric, Security, Multimodal

Introduction

Due to advancement of web technology, it is possible to design and develop web application that can fulfill the customer demand 24×7. These web applications are used to store the commercial, personal, military and information related to government etc. and can be access online. To access this information in real time a proper verification or authentication method is required. The various approaches used for authentication are as follows:

- Possession: The use of identity card
- Knowledge: The use of PIN and password
- Inherent: Biometric traits like physiological or behavioral

The first two approaches are widely used. However the tokens such as ID cards can be stolen lost or duplicated. For the second approach, one needs to remember lengthy and complex passwords which area difficult task. Further, in these two approaches, a person identity is verified or authenticated based on what he/she knows or possesses rather than who he/she is. Due to these reasons the first two approaches are susceptible to fraudulent attack. Biometric, an emerging technology can be used to establish identification or verification of users through two types of inherent biometric traits like physiological traits (finger- print, face, iris etc.) or behavioral traits (voice, gait, signature etc.). It also requires the person to be present during time of authentication. Also, due to uniqueness of the biometric traits, they cannot be stolen, guessed, forgotten or easily forged. To provide better security to the web applications, biometrics traits can be encrypted further.

The unimodal biometric authentication system uses only one physiological or behavioral trait for authentication along with username and password. Each unimodal biometric authentication system has certain limitations due to following reasons: Noise involved in sensor data, lack of universality and individuality in selection for user authentication. To overcome the limitations of unimodal biometric authentication system, multimodal biometric authentication system can be devised to enhance the level of security by incorporating multiple biometric traits.

The proposed multimodal system uses biometric traits like fingerprint, face, iris, along with user id and password. Using these biometrics traits, four levels of authentication are introduced. To access web application containing less sensitive information Level 1 authentication is used whereas level 4 is used for web application containing most sensitive information. Level 1 uses user id and password; Level 2 uses fingerprint with user id and password; Level 3 uses fingerprint and face with user id and password; Level 4 uses fingerprint, face and iris with user id and password. To increase the security, biometric traits is further encrypted using AES algorithm.

Rest of the paper is organized as follows: Section 2 Background work is introduced, Section 3 introduced the proposed work; Section 4 introduced the implementation of the proposed work, Section 5 deals

with Experimental Evaluation and section 6 deals with conclusion and future work.

Related Work

Recently the Wireless LAN (WLAN) communications has become one of the fastest growing sectors in telecommunication and network industry. The wireless network provides many advantages over the wired networks. However, the management of such wireless network proves to be challenging. Due to increase in the web application attacks, highly reliable and convenient personal identification and verification technology are vital in our society today (Fry and Dunphy, 2009). The ancient Babylonian conducted business transaction by pressing the tips of their fingertips into clay (Lee and Gaensslen, 2001). The use of fingerprint as a valid means of identification was formally accepted by the law-enforcement agencies in the early 20th century (Šošević *et al*., 2013). Even two samples of biometric data gathered from the same person are never the same, due to sensor noise, aging and imperfect acquisition conditions (Jain *et al*., 2004). Therefore, there is always a possibility of biometric system error. There are two types of recognition errors in fingerprint biometrics: False accept rate and false reject rate. Fingerprint identification system performance is measured in terms of its False Accept Rate (FAR) and False Reject Rate (FRR). If a non-matching pair of fingerprints is accepted as a match, it is called a false accept while if a matching pair of fingerprints is rejected by the system, it is called a false reject (NIST, 2000; Merati, 2011). It has been reported (Jain *et al*., 1998) to the U.S. Congress that approximately two percent of the population does not have a legible fingerprint and therefore cannot be enrolled into a fingerprint biometrics system. Multimodal biometrics is a possible solution for improving biometric system precision (Jain *et al*., 2008). In multimodal biometrics, different modalities are taken simultaneously in order to determine user's identity. Biometric data is irrevocable (Zhang *et al*., 2009). Some algorithms for revocable biometrics exist, but they seriously affect verification precision. Therefore, there is a need for extra layer of security, because if an attacker compromises raw biometric data, it cannot be replaced. The identification and matching process takes less than one second to complete (Jain *et al*., 1998). This depends on the environment where the system is hosted as there are many factors that delay the execution of the program such as bridge in network transmission. The system determines the users identity by comparing the match score to a threshold set by the administrator (Jain *et al*., 2005; Ratha *et al*., 2007; 2001). To secure access of web pages a prototype of biometric based authentication system based on hand geometry is used (Jain *et al*., 1998). The security issues, a set of security automated tools and methodology are discussed in each stage of SDLC (Teodoro and Serrao, 2011). Fingerprint based student monitoring system is developed using Java technology and MySQL to evaluate the performance and evaluation of biometric based web application (Okafor and Ogbuabor, 2013). A real time multimodal biometric authentication system using java for secure access to internet banking web page based on password and fingerprint (Cătălin *et al*., 2015).

Proposed Work

Security is a one of the major concern for all types of application access stored in a server either in wired or wireless network. Single level security is not sufficient in today's scenario as it can be easily breakable due to advancement of parallel computing systems. The level of security can be enhanced by adding different biometric traits in authentication level for web applications stored in web server. In the proposed work we have devised multimodal biometric authentication system architecture for web application as shown in Fig. 1.

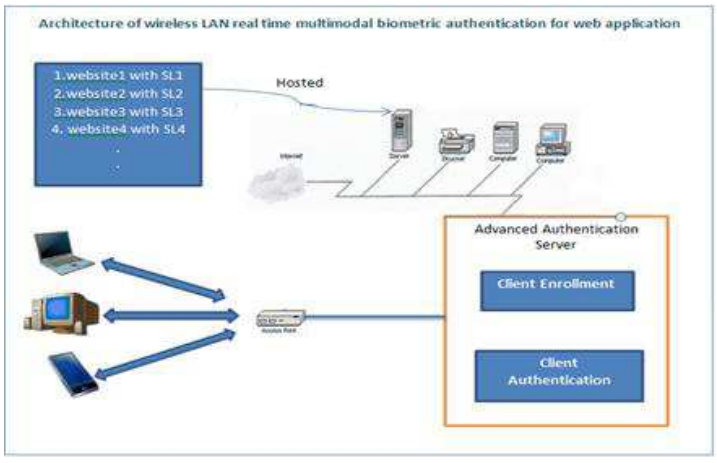

Fig. 1. Proposed system architecture

In the proposed architecture, web applications hosted in the server or servers in a wireless LAN can be accessed through wireless client after its authentication by Advance Authentication Server (AAS). The proposed scheme consists of two phases i.e., enrollment and authentication.

Enrollment Phase

In this phase, an enrollment center is used at the client end to enroll the user. During enrollment, raw biometric data of the user is acquired using the sensor. To capture fingerprint, Mantra MFS100, a high quality USB electronic fingerprint sensor is used; to capture face, Logitech Camera is used; and for iris 3M Cogent scanner is used. The scanned version of biometric image is sent to AAS for further preprocessing and feature extraction to get standard template from raw image. The standard templates is further encrypted through AES encryption technique and stored in database along with client's unique id. Figure 2 shows the enrollment steps.

Preprocessing and Feature Extraction

In the preprocessing step, raw biometric template of fingerprint, face and iris is passed through the Median/Gaussian filter to remove the noise and to enhance the quality of the image. For generating thumbprint template: Minutia based feature extraction technique is used, for face template: OPENCV haarcascaded classifier technique is used and for iris template: Hough transformation is used for iris localization and Doughman Rubbersheet algorithm is used for iris normalization. Figure 3 shows the preprocessing and feature extraction steps used by AAS.

Authentication Phase

During authentication phase, a data sample of the user claiming an identity is acquired after passing through appropriate sensors. This data sample is referred to as query sample. These query samples are passed through preprocessing and feature extraction module to acquire the salient features. These salient extracted features must be same with those extracted features at the time of enrollment. The features of the query sample are compared with the decrypted information of a claimed identity. The process of comparison of query sample with the decrypted template stored at the time of enrollment and the output score of the process is referred to as matching and matching score respectively. The type of the matching score is either similarity or distance expressing the similarity or dissimilarity of the query sample to the stored template. The decision of accepting or rejecting the identity claim is made by comparing the matching score with the threshold. For fingerprint matching the optimized threshold calculated as 14000; for face the optimized threshold is calculated as 10; and for iris optimized threshold is calculated as 30.

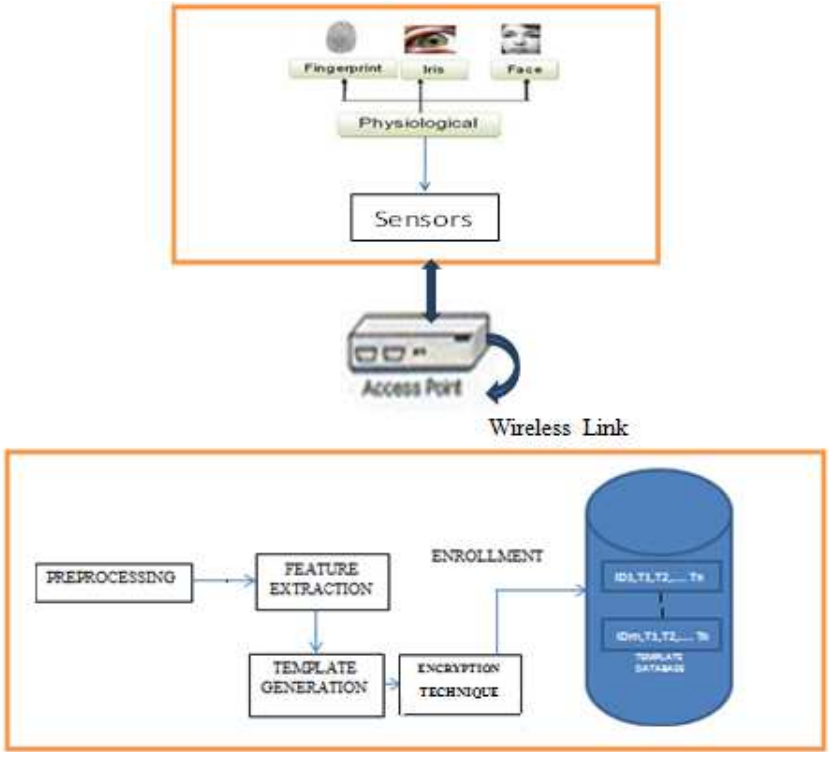

Fig. 2. Advance Authentication Server (AAS)

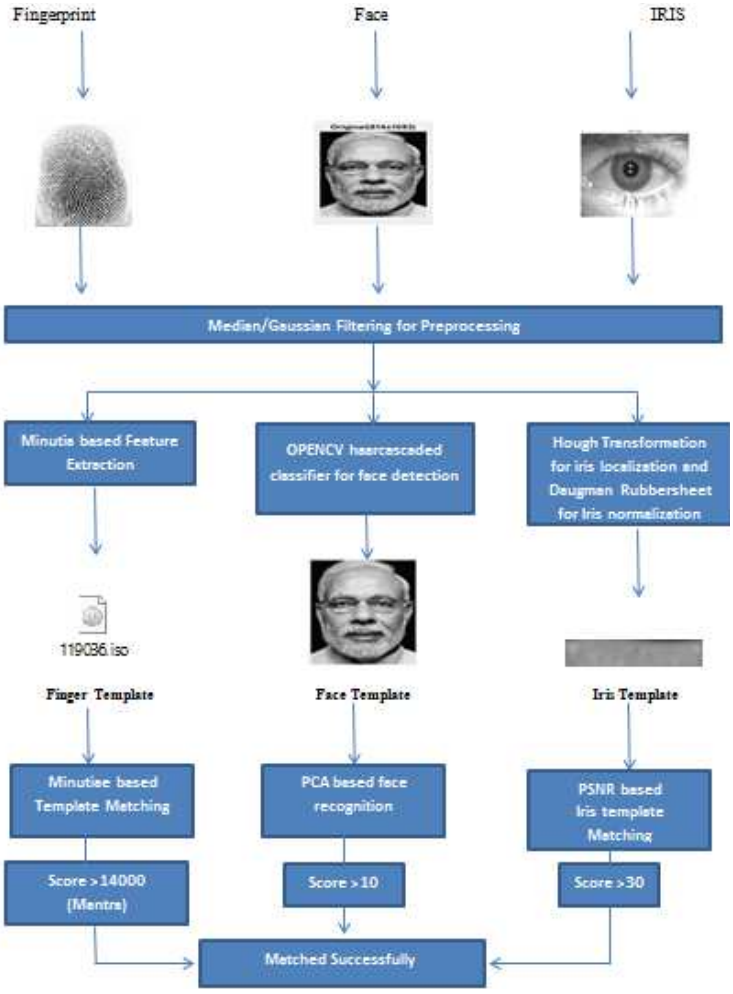

Fig. 3. Preprocessing and feature extraction technique

Advance Authentication Server does enrollment and authentication process. It grants access to authenticated users.

The proposed model uses four level of authentication. 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. Figure 4 shows the authentication using user name and password.

Level-2 Authentication

To access web application using Level-2 requires matching of thumbprint along with user id and password one by one by AAS. For each case, thump print along with user id and password of the claimed identity is matched with the decrypted stored claim identity during enrollment. For thumb print, minutia based template matching is used. If both are matched successfully then only user is authenticated by the AAS and corresponding web application is loaded in the browser.

Level-3 Authentication

To access web application using Level-3 requires matching of thumbprint, face along with user id and password one by one by AAS. For each case, thump print, face along with user id and password of the claimed identity is matched with the decrypted stored claim identity during enrollment. For face matching, PCA based face recognition algorithm is used. If all three are matched successfully then only user is authenticated by the AAS and corresponding web application is loaded in the browser.

Level-4 Authentication

To access web application using Level-4, requires matching of thumbprint, face, iris along with user id and password one by one by AAS. Here, thump print, face,

iris along with username and password of the claimed identity is matched with the decrypted stored claim identity during enrollment. For iris, PSNR based iris template matching is used. If all four are matched successfully then only user is authenticated by the AAS and corresponding web application is loaded in the browser. Figure 5 shows the level wise authentication process.

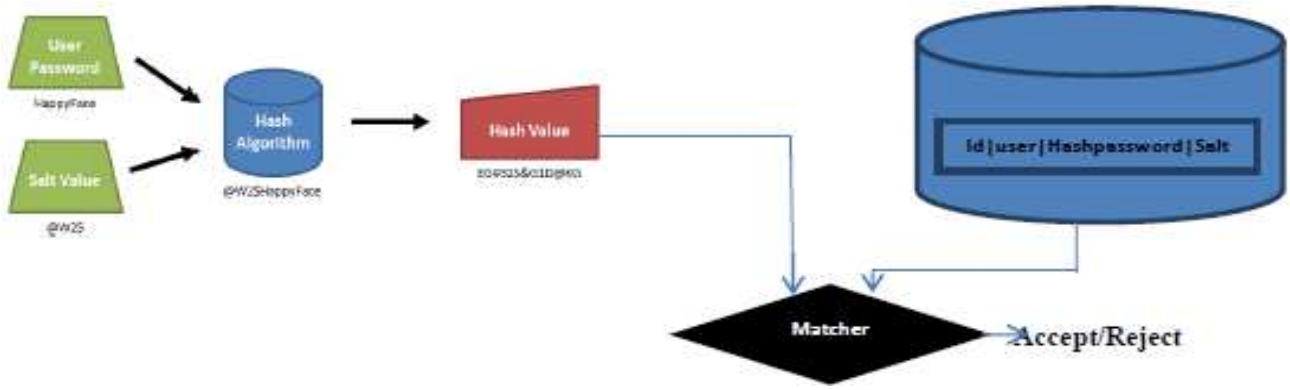

Fig. 4. Authentication using hashed password using salt

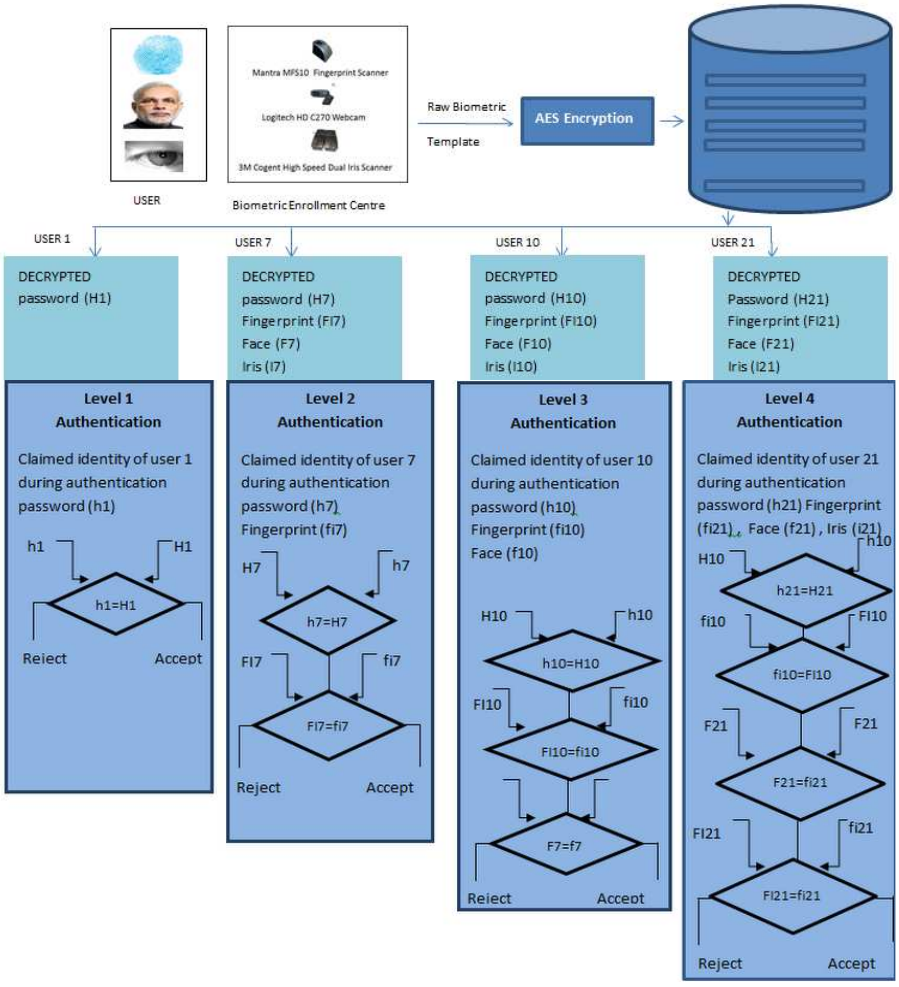

Fig. 5. Enrollment and level wise authentication

Implementation

This section deals with the technologies used and screenshots of the implemented system.

Technologies Used

Java Technology

It is used to develop client and *server* side interface. Remote method invocation is used to access different distributed methods present in the server interface.

JSP & Servlet Technology

It is used to develop web application interface to access the web applications present in the server. Web applications require different level of authentication.

MySQL Database

Using MySQL database, user enrollment details are stored, which is used during the authentication phase.

Screenshots of the Implemented System

The different screen shots for enrollment and authentication of users for different levels of user authentication are shown in below figures from Fig. 6-4.

Level-1 Authentication

In Level-1 authentication, user has to enter only their username and password credentials into the authentication interface. If their credentials do not match then it shows "invalid credential" message otherwise it will show the message "you are authenticated" and redirect to corresponding web application as depicted in the below figures.

Level-2 and Level-3 authentication methods uses thumb and face biometric traits for authentication. In Level-4 authentication we are using three physiological biometric traits i.e., thumb, face and iris for user authentication along with username and password. The screen shots for Level-4 are as shown below.

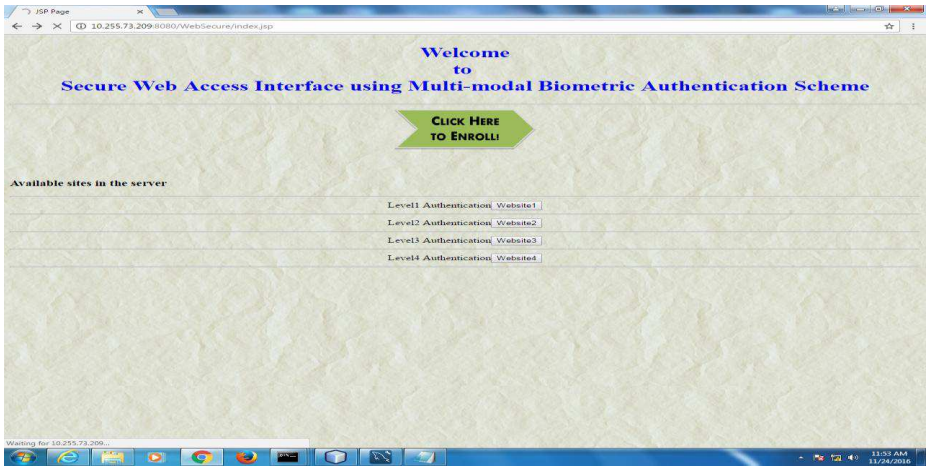

Fig. 6. Screenshot of the authentication server interface

Fig. 7. Screenshot of user enrollment interface

Fig. 8. Screenshot of Level 1 authentication

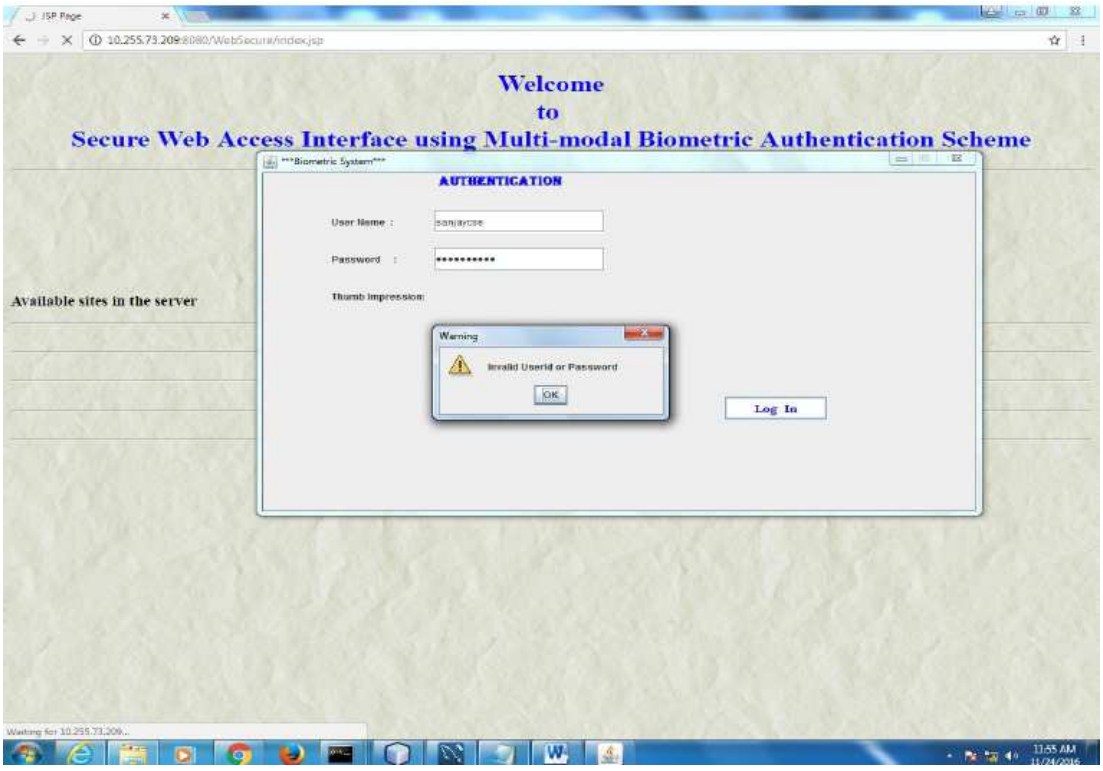

Fig. 9. Screenshot of invalid user authentication

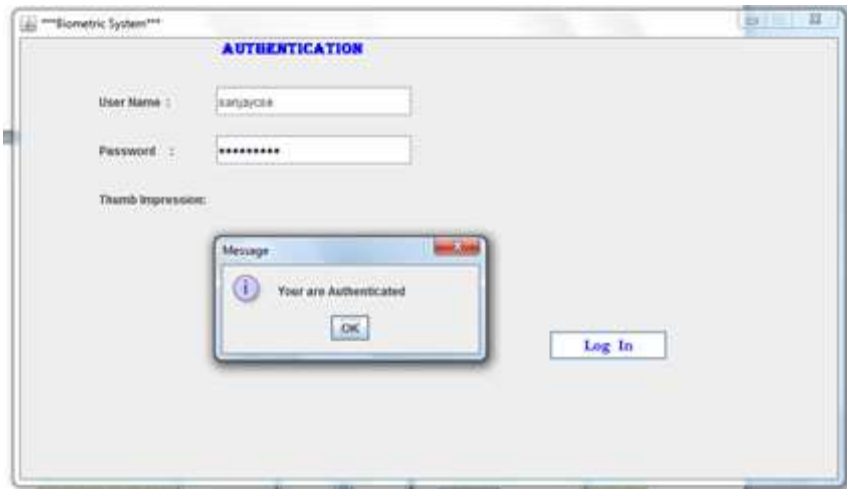

Fig. 10. Screenshot of successful authentication in Level 1

Fig. 11. Screenshot of redirected web application

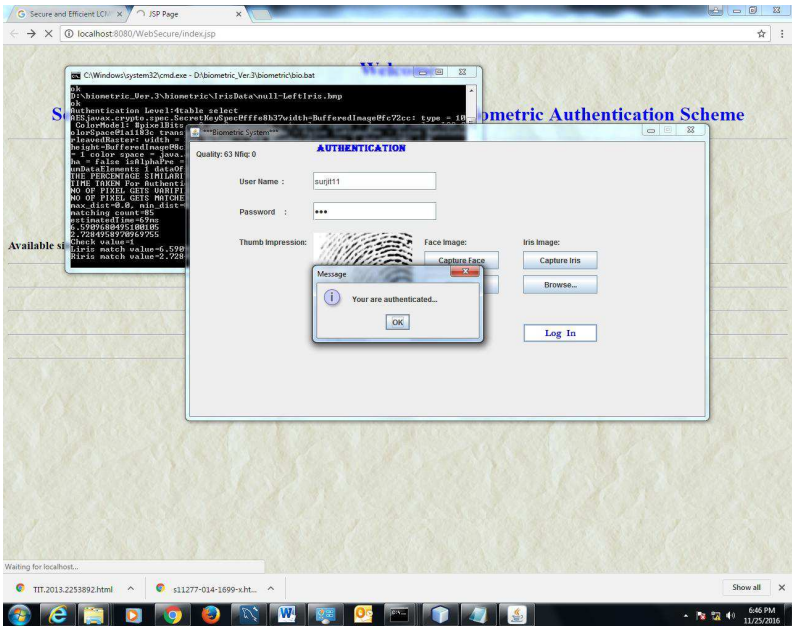

Fig. 12. Screenshot of successful authentication in level 4

Fig. 13. Screenshot of redirected web application

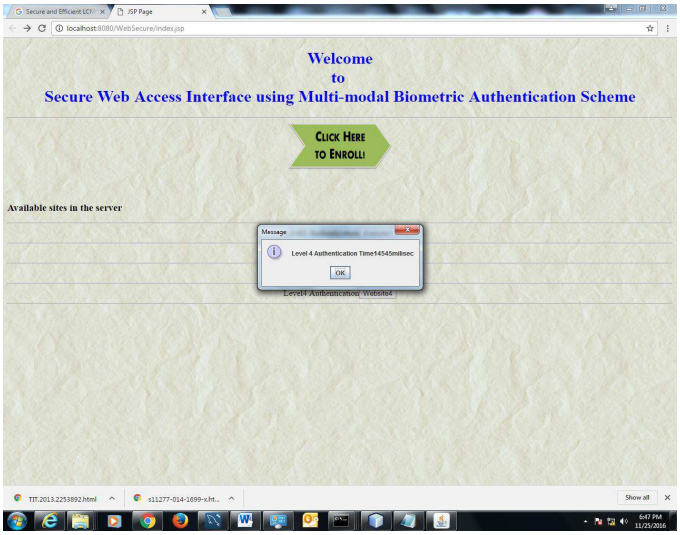

Fig. 14. Screenshot of authentication time in Level 4

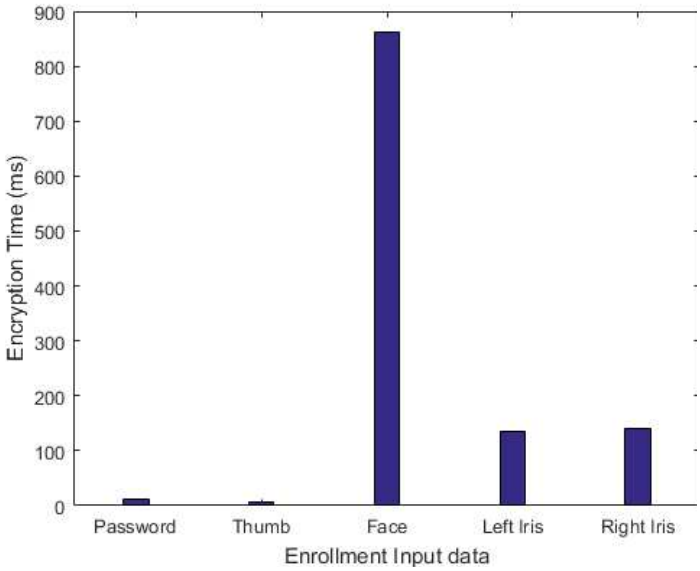

Fig. 15. Encryption time of biometric template during enrollment

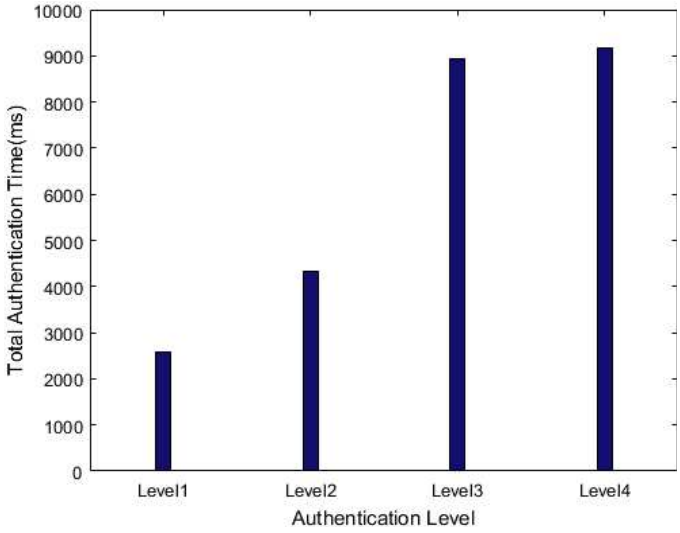

Fig. 16. Computation time Vs level of authentication

Experimental Evaluation and Result

Time required to access web applications hosted in the web servers using four level of authentication can be expressed using following equations:

$$Level\,1 : TAT1 = TMHPi \tag{1.1}$$

$$Level\,2 : TAT2 = TAT1 + TDTthumb + TMT2 \tag{1.2}$$

$$Level\,3 : TAT3 = TAT2 + TDTface + TMT3 \tag{1.3}$$

$$Level\,4 : TAT4 = TAT3 + TDTiris + TMT4 \tag{1.4}$$

Where:

*TAT*1, *TAT*2, *TAT*3 and *TAT*4	=	The Total authentication time for level1, level2, level3 and level4 respectively
TMHPi	=	Time to match the hashed password
TDTthumb, *TDTface* and *TDTiris*	=	Template decryption time for thumb, face and iris respectively
*TMT*2, *TMT*3 and *TMT*4	=	Template matching time for thumb, face and iris

Authentication time (in milliseconds) for four level of authentication is shown in Table 1 and 2 shows the Encryption time and their corresponding graph are shown in the Fig. 15 and 16 respectively.

During enrollment 100 users were enrolled, whose biometric traits like finger print, face and iris were captured and stored in the MySQL database. The screenshot of the records of sixteen users are shown in Fig. 17.

Performance of the Purposed System

The system performance of the proposed biometric based multimodal system can be done using mathematical based performance evaluation and graphical based performance evaluation.

Mathematical Based Performance

The authentication of the biometric system can be represented by a decision function and can be expressed as:

$$D(x) = \begin{Bmatrix} accept & if\ s(x) > \Delta \\ reject & otherwise \end{Bmatrix} \tag{1.5}$$

where, Δ is the threshold score value and $s(x)$ is the matching score obtained by the comparison of template generated during authentication phase with the decrypted template of the encrypted template stored in the database during enrollment.

During decision making process, two most common types of error may occur are: False Acceptance (FA) Error and False Rejection (FR) Error. FA Error may occurs when system falsely accept the imposter (A person claiming an identity other than their own) whereas FR Error may occurs when the system falsely rejects the claimant's (Genuine user) during authentication. The normalized version of FA and FR are known as FAR and FRR respectively. They are often used in the performance analysis and are defined as:

$$FAR(\Delta) = \frac{FA(\Delta)}{N^i} \tag{1.6}$$

$$FRR(\Delta) = \frac{FR(\Delta)}{N^c} \tag{1.7}$$

where, FA and FR give total no of counts for false accepted access and false rejected access respectively; and N^i and N^c represent total number of imposter and client access.

FAR and FRR are the functions of threshold Δ and can be expressed in terms of class distribution of matching score. Let $f_C(s)$ = $Pr(S=s|Client)$ and $f_I(s)$ = $Pr(S=s|Imposter)$ be the probability density function of client and imposter scores respectively. The *FAR* and the *FRR* of the biometric system may be expressed as equation 1.8 and 1.9:

$$FAR(\Delta)=P(S\geq\Delta|Imposter)=\int_{\Delta}^{\infty} f_I(s)ds \quad (1.8)$$

$$FRR(\Delta)=P(S<\Delta|Client)=\int_{-\infty}^{\Delta} f_C(s)ds \quad (1.9)$$

For finding the better result in biometric system, two types of notations True Acceptance (TA) and True Rejection (TR) are used. TA means claims made by clients are correctly accepted whereas *TR* means claims made by imposter are correctly rejected.*TAR* is also known as GAR. *TAR* and *TRR* can be expressed as follows:

$$TAR(\Delta)=P(S\geq\Delta|Imposter)=\int_{\Delta}^{\infty} f_C(s)ds \quad (1.10)$$

$$TRR(\Delta)=P(S<\Delta|Imposter)=\int_{-\infty}^{\Delta} f_I(s)ds \quad (1.11)$$

The relationship between *GAR* and *FRR* can be expressed as follows:

$$GAR(\Delta)=P(S\geq\Delta|Client)=1-FRR(\Delta) \quad (1.12)$$

Graphical Based Performance Evaluation

In order to set the threshold value for fingerprint, face and iris scanner at which the *FAR* and *FRR* are found to be minimum, two types of curve known as Receiver Operating Characteristics (ROC) Curve and Detection Error Trade-off (DET) Curve are used. ROC curve shows the relationship between *FAR* and *GAR* whereas DET shows the relationship between *FAR* and *FRR*. The ROC curve enables to set threshold values Δ for different biometric traits at the intersection point of FAR and FRR curves with respect to different threshold values. The DET curve provides the trade-off between the two types error (False Acceptance and False Rejection), which enables the user to select the threshold according to the system requirements. For testing purpose, we have taken number of imposter (Ni) = 20 and number of client (Nc) = 100. Figure 18, 20 and 22 show the ROC curve for fingerprint, face and iris respectively. Figure 19 shows the threshold value for fingerprint, which is equal to 14000. Figure 21 shows the threshold value for face, which is greater than 31 and Fig. 23 shows the threshold value for iris, which is greater than 11. Figure 24-26 shows the DET curves of fingerprint, face and iris respectively.

Table 1. Authentication time in various level of authentication using AES 128 bit

Authentication level	*TMHPi*	*TDTthumb*	*TDTface*	TDTiris	*TMT*	TAT
1	2579 ms	NIL	NIL	NIL	NIL	2579 ms
2	2579 ms	10 ms	NIL	NIL	1749 ms	4338 ms
3	2579 ms	10 ms	1609 ms	NIL	4733 ms	8931 ms
4	2579 ms	10 ms	1609 ms	74ms	4902 ms	9174 ms

Table 2. Encryption time of different biometric traits using AES 128 bit technique during enrollment

Encryption technique	Password hashed time	Thumb encryption time	Face encryption time	Left Iris Encryption time	Right Iris Encryption time	Total time for encryption
AES 128 bit	13 ms	7 ms	862 ms	135 ms	140 ms	1157 ms

RegNo	StudName	Address	Gender	Dob	email	password	photo	facephoto	leftirisphoto	rightirisphoto	encryption_type
119032	s Kumar	nit	M	26/10/1978	sk	MmdncW44bGtzaTNkdWRhYTk5OGRmZzJrMmb…	BLOB	BLOB	BLOB	BLOB	Blowfish
119033	S Kumar	nit	M	24/11/1991	sk20	MmNuZmRxYzY4Z2VmcmczZGpqN2ljYmE3cHZe1…	BLOB	BLOB	BLOB	BLOB	RC4
119034	Surjit	nit	M	20/10/1973	surjit2015	NXJuMWhkNmcyb3RwZmgxMm4zMzM3bWE0bG…	BLOB	BLOB	BLOB	BLOB	AES
119035	surjit	nit	M	22/12/1974	spaul29	NmwxNnZqM2ZzOXE1MGdhYTBuYThrMTZnZ2lYK…	BLOB	BLOB	BLOB	BLOB	AES
119036	surjit	nit	M	21/11/1969	spaul007	NWprbXNlMHJucjRmNnI3ZzE2M2EyOXRrZmVoz…	BLOB	BLOB	BLOB	BLOB	AES
119037	surjit	nit	M	24/9/1972	surojit	cDM3NXE1bDRsZjhjYXA4c2xjNnFldGdsdW21xwj…	BLOB	BLOB	BLOB	BLOB	AES
119038	Mohit Kumar	NIT	M	30/10/1997	mohit	MWF1ZWNma2RrMTJlcjk4N2cxN2hrYjd0OTeQjF…	BLOB	BLOB	BLOB	BLOB	Blowfish
119039	Mohan	NIT	M	25/10/1974	mohan	NDdpdmpoOG8yaDgwMTBuYzMydnY5M2U4ZPk…	BLOB	BLOB	BLOB	BLOB	AES
119040	Amit Kumar	NIT	M	25/9/1975	amit	M250djd1YzJmNjI3MTJlcnV2Y3RqZTc5NjAYt014…	BLOB	BLOB	BLOB	BLOB	RC4
119041	Jagdish Singh	NIT Jamshedpur	M	29/11/1976	jagdish	N2dvZ2Eyb25qNXJsaTA5bGswaGNzcGtrMnZa1…	BLOB	BLOB	BLOB	BLOB	AES
119042	Sumitra Prad…	nit jsr	F	16/9/1969	sumitra	MmVoYW5qczZsOWI1Nm50cTZjOG1mMHNpNDY…	BLOB	BLOB	BLOB	BLOB	AES
119043	Sunil Gaur	NIT jsr	M	6/5/1972	sunil	M3U1NW50czhlam8xOXVycmp1am8zczFqaDTls8…	BLOB	BLOB	BLOB	BLOB	AES
119044	Aditya Singh	NIT Jsr	M	3/12/1994	Aditya	NHA4YzVlOHY4bzllNzg4ZTdtc2xyZXNyb2L1yb69…	BLOB	BLOB	BLOB	BLOB	AES
119045	Amit Negi	NIT jsr	M	23/10/1991	amit	aWowcWVqczFvbDVmbm8xYjI3anR2Z2U0bbuak…	BLOB	BLOB	BLOB	BLOB	AES
119046	nihar	nit	M	23/11/1998	nihar	MjNqaDZxaWs3ZDJxdjZxZGFndG9hdDlvY2aSqP…	BLOB	BLOB	BLOB	BLOB	AES

Fig. 17. Screenshot of the MySQL database of the enrolled users

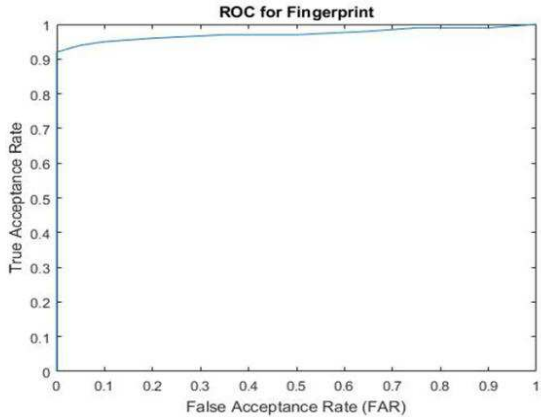

Fig. 18. ROC for fingerprint

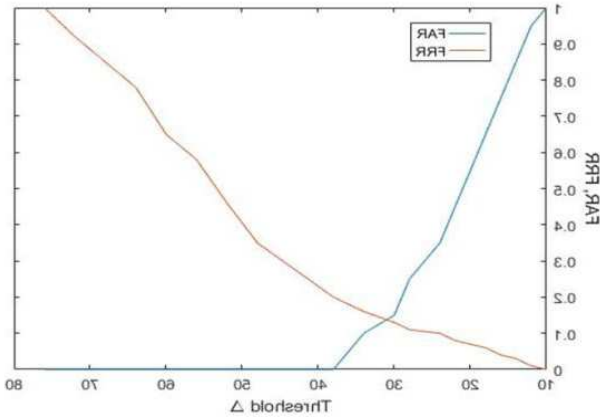

Fig. 21. FAR and FRR versus threshold for ace

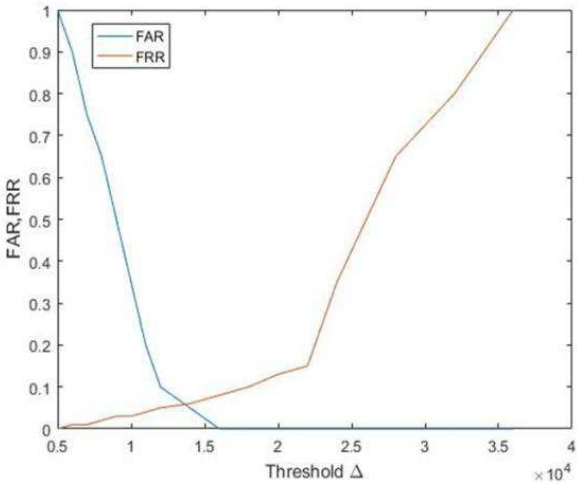

Fig. 19. FAR and FRR versus threshold for fingerprint

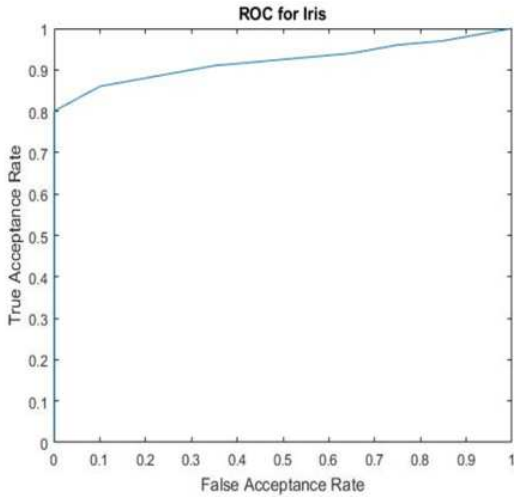

Fig. 22. ROC for iris

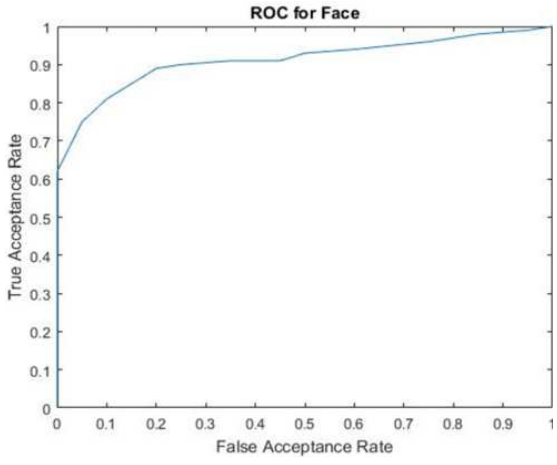

Fig. 20. ROC for face

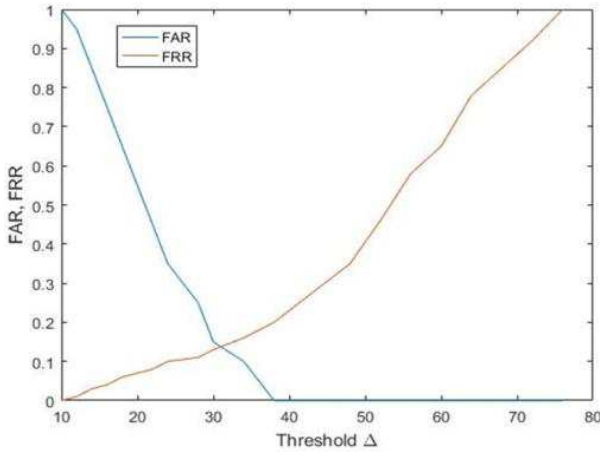

Fig. 23. FAR and FRR versus threshold for iris

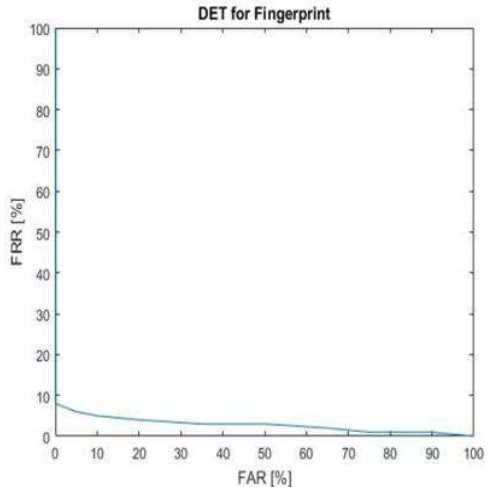

Fig. 24. DET curve for fingerprint

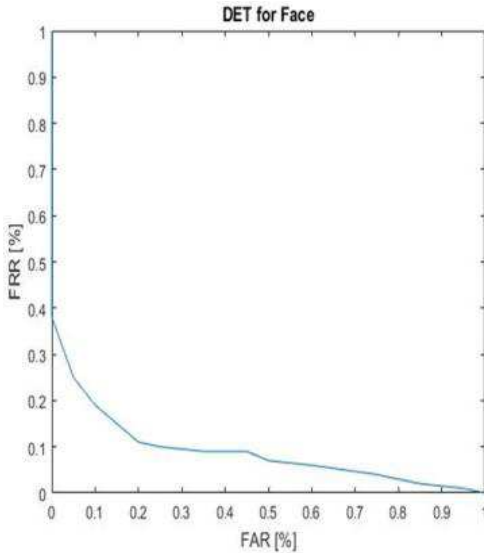

Fig. 25. DET curve for face

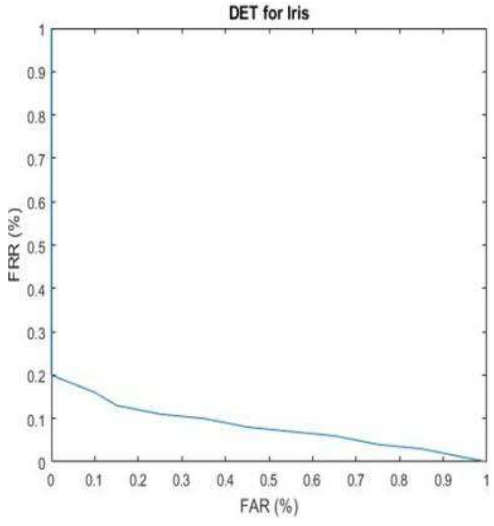

Fig. 26. DET curve for iris

Conclusion and Future Work

In our proposed multi-modal biometric authentication system, concept of multi-level security i.e., Level1, 2, 3 and 4 are employed. In Level1, we have used hashing of password with salt using Hashed MAC (HMAC) and SHA, to further strengthen the security of the password. For the other levels, we have used biometric traits like thumb print, face and iris. From the graph it is apparent that as the level of authentication increases the level of security as well as authentication time also increases. The ROC enables the user to select a threshold that best meets system requirement graphically. The DET curve provide the trade-off between the two types of error (FAR and FRR) which enables the user to select the threshold according to system requirement. The lower the DET curve the better the performance. With varying level of security, people will prefer to do e-transactions, e-commerce and m-commerce securely.

For future work: Different chaotic encryption algorithms can be employed for biometric templates security; the developed model can be extended for securing websites access through internet; the developed model can be implemented as mobile application for secure authentication; the proposed system can be developed as firmware in router to implement device level security.

Acknowledgement

The authors feel greateful to the anonymous reviewer for their valuable comments and sugessions 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: Execution, 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

Cătălin, L., V.G. Găitan and V. Lupu, 2015. Security enhancement of internet banking applications by using multimodal biometrics. Proceedings of the IEEE 13th International Symposium on Applied Machine Intelligence and Informatics, Jan. 22-24, IEEE Xplore Press, Herlany, Slovakia. DOI: 10.1109/SAMI.2015.7061904

Fry, J. and A. Dunphy, 2009. Biometric student identification: Practical solutions for accountability and security in schools.

Jain, A.K., A. Ross and S. Prabhakar, 2004. An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol., 14: 4-20. DOI: 10.1109/TCSVT.2003.818349

Jain, A.K., A. Ross and U. Uludag, 2005. Biometric template security: Challenges and solutions. Proceedings of the 13th European Signal Processing Conference, Sept. 4-8, IEEE Xplore Press, Antalya, Turkey, pp: 1-4.

Jain, A.K., K. Nandakumar and A. Nagar, 2008. Biometric template security. EURASIP J. Adv. Signal Process., 2008: 1-17. DOI: 10.1155/2008/579416

Jain, A.K., S. Prabhakar and A. Ross, 1998. Biometric-based web access. Trans. Institute Brit. Geographers.

Lee, H. and R. Gaensslen, 2001. Advances in Fingerprint Recognition. 2nd Edn., S.l.: CRC Press, Taylor and Francis Group.

Merati, A. 2011. Multi-modal biometric authentication with cohort-based normalization. PhD Theses, Centre for Vision, Speech and Signal Processing, Faculty of Engineering and Physical Sciences, University of Surrey, UK.

NIST, 2000. Summary of NIST standards for biometric accuracy, tamper resistance and interoperability. Report to the United States Congress.

Okafor, F.O. and G Ogbuabor, 2013. Performance and security evaluation of biometric-based web application. West Afr. J. Industrial Acad. Res.

Ratha, N.K., J.H. Connell and R.M. Bolle, 2001. Enhancing security and privacy in biometricbased authentication systems. IBM Syst. J., 40: 614-634. DOI: 10.1147/sj.403.0614

Ratha, N.K., S. Chikkerur, J.H. Connell and R.M. Bolle, 2007. Generating cancelable fingerprint templates. IEEE Trans. Pattern Analysis Machine Intelligence, 29: 561-572. DOI: 10.1109/TPAMI.2007.1004

Šošević, U., I. Milenković, M. Milovanović and M. Minović, 2013. Support platform for learning about multimodal biometrics. J. Universal Comput. Sci., 19: 1684-1700.

Teodoro, N. and C. Serrao, 2011. Web application security: Improving critical web-based applications quality through in-depth security analysis. Proceedings of the International Conference on Information Society (i-Society), Jun. 27-29, IEEE Xplore Press, London, UK.

Zhang, D., F. Song and Y. Xu, 2009. Advanced Pattern Recognition Technologies with Applications to Biometrics. 1st Edn., Book News Inc., ISBN-10: 1605662003, pp: 366.