International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

Continuous User Authentication Using CASHMA System

Sarala Hasare[1] , Rashmi Rachh [2]
[1]*Department of CSE , PG Centre VTU Balagavi*
[2]*Department of CSE , PG Centre VTU Balagavi*

Abstract— Session management in distributed Internet service is traditionally on the basis of username and password, biometrics until explicit logouts or session timeout occurs. But there is chance of misusing session as length of its timeout is more. To overcome from this from problem re-authentication came into existence, where the user needs to reenter his credentials again and again, which is an overhead. In order to overcome the above problems, continuous user authentication using Context Aware Security by Hierarchical Multilevel Architectures (CASHMA) system is being used. This system provides secure authentication over the Internet, by continuous authentication with the help of multi-modal biometric, where in multiple biometric traits are used and only one at a time is given to the system. In this system, user authentication verification is a continuous process instead of onetime occurrence and user credentials are acquired transparently. In this project username along with fingerprint biometric are used to authenticate user during login phase and face biometric is used for continuous authentication during working session.

Keywords— Security, Authentication, Biometric, Continuous user authentication, CASHMA.

I. INTRODUCTION

Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, item, nation, or organization. Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm. Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, protective barriers, locks, access control protocols, and many other techniques. Three main elements are there to physical security. First, barriers can be placed were high possible attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes, and water sprinklers. Second, surveillance and notification systems can be put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras. Third, methods can be implemented to catch attackers and to recover quickly from accidents, natural disasters or fires.

In today's era, almost every single organization uses a computer and has a computer network to send, receive and store information. Whether it's sending emails, storing documents, or serving information through a web server, it is very important to focus on security, especially if your network contains sensitive, confidential and personal information.

Definition of computer security: "The protection afforded to an atomized information system in order to attain the applicable objective for preserving the integrity, confidentiality and availability of information system resources".

- Confidentiality: It makes sure that confidential data is not made available to unauthorized user.
- Integrity: It makes sure that data and system information can be changed only by authorized user.
- Availability: It makes sure that data and system must be available to the authorized user as and when he need.

In some security field only confidentiality, integrity and availability (CIA) are not enough to provide sufficient degree of security; two more security objectives are being added to provide the complete picture of security; such as authenticity and accountability.

- Authenticity: It is the process by which identity of the user will be verified for which they claim to be. This will be done on the bases of access control. Access control identifies the identity of user based on user credentials like username, password and some biometric traits; which helps user to have access to the allotted system resources.
- Accountability: Users are assigned with responsibilities in order to indicate something that user has done and something that user supposed to do [1].

1.1 NEED FOR AUTHENTICATION

There are amazing opportunities, which will be provided by both inter and intra network. To have access to these opportunities without proper access control, it will results in several types of attacks, which are explained bellow.

Loss of Privacy: Confidential data traversed through the Internet will be read by unauthorized user.

Loss of Data Integrity: Confidential data traversed through the Internet will be changed by unauthorized user.

Authentication Credentials:

Authentication is the process by which identity of the user is verified. The identity will be verified on the bases of proofs provided by the user like ID card which include unique ID number and photo or user biometric information like finger print, retina scan, face scan etc these are called credentials of the user. Authentication credentials fall into three categories:

Something you know: While authenticating, parties which involve in authentication must share a secrete key. For example, static password belongs to this category.

Something you are: While authenticating, physical presence of the user will be presented; such as finger print, retina scan, face scan etc.

Something you have: A token or a card will be used for authentication; such as driving license, identity card etc.

1.2 SINGLE SHOT USER AUTHENTICATION

Secure user identity verification is essential in majority of Information and Communication Technologies (ICT) frameworks. User verification frameworks are customarily on the basis of username and password, and user identity will be verified only during login time, no further verifications are carried out at the time of working session, and sessions will be closed by logouts or timeouts.

As cyber attacks are increasing, security is the major concern in web based applications, biometric systems provide solutions for this kind of problems [2-3]. Here it make use of biometric data instead of username and password, at the same time misuse of biometric data is also increasing it will not promises an adequate level of security especially in financial sectors such as banking [4-5].

Single authentication verification by using username and password as well as biometric solution is normally formulated as “single shot “, in which identity of the user is verified only at the login stage. Once the identity of the user is verified then the authorized user can have access to the system resources only for fixed period of time i.e. until explicit logout or timeout. As this approach is based on single verification, the user identity will be constant over whole session. Consider a scenario: Suppose a user is logged into the system with his/her credentials like username and password or biometric data, after successful login if he/she kept his system open in the work place for a while; at that time there is possibility of impersonating the authorized user and can access to sensitive data (i.e. personal data). This issue is even trickier with regards to cell phones; where in the cell phone can be easily stolen while the session for a particular user is active, allowing unauthorized user to have access to sensitive data. In this scenario the user identity can be easily misused [6-7]. A solution to this issue is to use session with very short timeouts and user should periodically request his/her

credentials again and again but this system has a problem that it results in overhead for user even though the user is authorized one; still he/she has to re-authenticate.

1.3 MULTIMODAL BIOMETRIC AUTHENTICATION

One solution to the above problem is to use multimodal biometric system with continuous authentication, here in the users identity is verified in a continuous process instead of onetime occurrence [8]. An issue with customary biometric system is that single biometric trait can be forged; to avoid this issue biometric authentication process relay on multimodal biometric trait [9]. At last, the use of biometric authentication allows sensitive data to be obtained transparently, i.e. without explicitly informing the user, which is crucial to ensure better service usability. Here they have been introduced few cases of transparent securing of biometric information. Face can be gained while user is situated in the front of the camera, yet not intentionally for the procurement of biometric information; i.e. the user might read a printed SMS or watching a movie on a cell phone. Voice can be acquired when the user talks on the phone or with other individuals close-by if the microphone dependably catches background. Keystroke information can be obtained at whatever point the user type on the keyboard, for instance, when composing an SMS, chatting, or browsing the Internet. This methodology is different from the customary authentication forms, where the username/password is asked for just once at the login time. Such conventional authentication processes weakens ease of use for improved security, and have no solutions for forgery or taking of password.

Another methodology has been exhibited in this system for user session management is on the basis of "context aware security by hierarchical multilevel architectures (CASHMA)" system [10]. CASHMA system can able to operate securely on variety of web applications including high security demand services like online banking and can also used on variety of client devices like PC, smart phones etc.

The rest of the paper is organized as follows. Principle component analysis (PCA) algorithm and system architecture are explained in section II; implementation is presented in section III. Results are presented in section IV. Conclusions are described in section V.

II. PROPOSED SYSTEM

A. Principal Component Analysis (PCA) Algorithm –

Face is a complex multidimensional structure and needs a good computing technique for recognition. Here, face recognition is interpreted as a two-dimensional recognition problem; face recognition is done by Principal Component Analysis (PCA). Face images are projected onto a face space that encodes best variation among known face images. The face space is defined by eigenface which are eigenvectors of the set of faces, which may not correspond to general facial features such as eyes, nose, and lips. The eigenface approach uses the PCA for recognition of the images. The system performs by projecting pre extracted face image onto a set of face space that represents significant variations among known face images. Face will be categorized as known or unknown face after matching with the present database. If the user is new to the face recognition system then his/her template will be stored in the database else matched against the templates stored in the database. The variable reducing theory of PCA accounts for the smaller face space than the training set of face.

Algorithm: Principal Component Analysis (PCA)

1. Calculate the mean of the input face images.
2. Subtract the mean from the input images to obtain the mean-shifted images
3. Calculate the eigenvectors and eigenvalues of the mean-shifted images
4. Order the eigenvectors by their corresponding eigenvalues, in decreasing order
5. Retain only the eigenvectors with the largest eigenvalues (the *principal components*)
6. Project the mean-shifted images into the eigenspace using the retained eigenvectors

B. SYSTEM ARCHITECTURE-

The CASHMA system architecture consists of CASHMA service, client, and web service. All components are connected by communication channel is shown in Fig 1.
CASHMA service consists of

1. Authentication server: It provide interface to the client.
2. Computational server: It is responsible for comparison of biometric trait with the enrolled user for verification of user's identity.
3. Data base of templates: All the enrolled biometric templates will be stored in database.

Web service can be any Internet service or an application that require a user authenticity. So these services must be registered to CASHMA service. Similarly for user who wants to access these web services they must also be registered to CASHMA service. While registration user need to provide his/her credential information like username and fingerprint biometric data, and this information will be stored in the templates database at authentication server and later this information can be used by authentication server, in order to authenticate user while accessing web service.
Finally the client can be any user devices like laptop, Smartphone's, desktop PC's or tablet etc. The client acquire user's credentials like username and fingerprint biometric data and send this information to CASHMA service, in order to authenticate user to access the target web service. The client consists of

1. Sensor to get the biometric data
2. CASHMA application which send out the biometric data to the authentication server.

The CASHMA service compares these received credentials with the stored templates to provide authentication to user when he/she logged into access the web service. So it helps to identify the identity of the user during login time. Next, during working session identity of the user is verified by continuously capturing the user facial information through webcam. Here authentication server task is, for given image or a sequence of scenes identify the people in the scene, this can be accomplished by the use of the Principle Component Analysis (PCA) algorithm. PCA algorithm will generates a set of eigenfaces on big set of images representing different human faces.

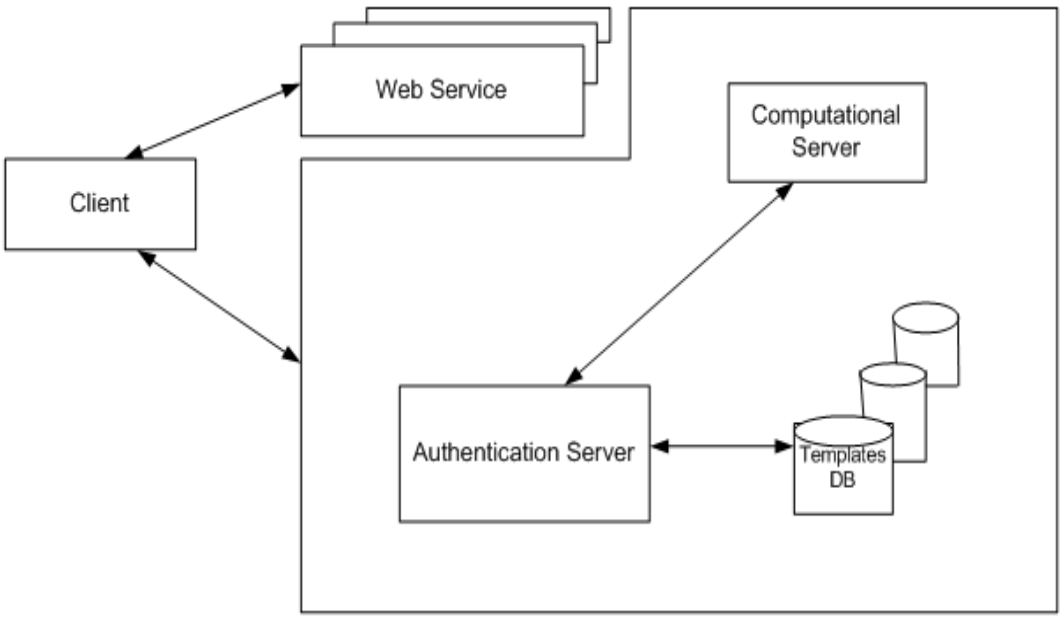

Fig. 1 Architecture of CASHMA system [12]

Modules are shown in the diagram are:

Client: this module is responsible for sending authentication credential. Authentication server can communicate internally with the computational server.

Authentication server: authentication server communicates with both template database and computational server for storing and accessing biometric data based on ID's.

Web service: this module sends the request to CASHMA service and also processes the client request.

Template DB: this module represents data base for storing the client data. Authentication server can directly interact with template DB.

III. IMPLEMENTATION

There are two phases for successful use authentication such as initial phase and Maintenance phase. Fig 2 shows the initial phase and Fig 3 shows Maintenance.

Initial phase:

1. The user send a request to the web service in order to access its service; then web service send a replay back to the user saying that get certificate from CASHMA service.
2. User will make use of CASHMA application and send his credentials to the CASHMA service for requesting certificate. To perform stronger authentication; user send different biometric data to CASHMA service at time t_0.
3. The CASHMA service will verifies the received data and perform the user authentication by providing certificate. Here it has two cases.

Case 1: If the identity of the user is not verified (i.e. global trust level < trust threshold g_{min}), then some other biometric data is required (step 1) till the trust threshold g_{min} is satisfied.

Case 2: If identity of the user is verified successfully, the CASHMA service will generates the certificate for user indicating that user is authenticated successfully. It calculates timeout for the user session, here T_0 will be the initial timeout, and set the timestamp with the certificate with expire time is $T_0 + t_0$. Then CASHMA send certificate to the client, then it forward to web service for accessing web service.

4. The web service get the request from client along with certificate, then verifies the certificate. If the certificate is not expired then web services allow user to access its services until time $T_0 + t_0$.

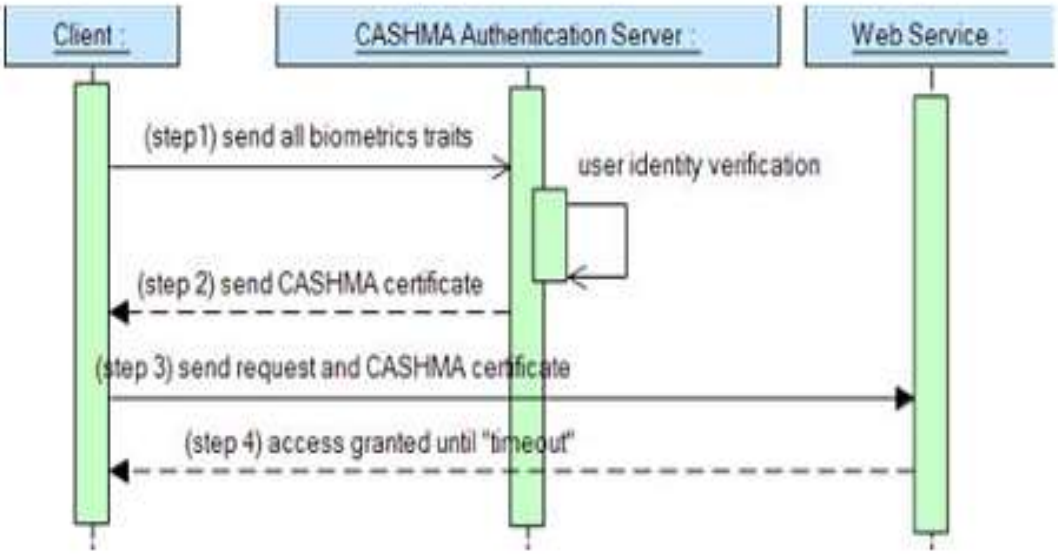

Fig. 2 Initial phase in case of successful user authentication [12]

Maintenance phase:

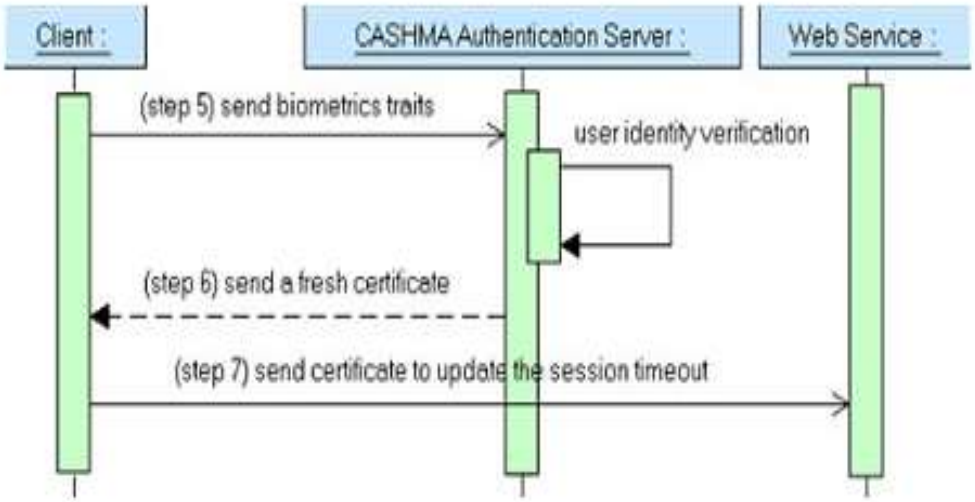

Fig 3 Maintenance phase in case of successful user authentication [12]

At time t_1 user should get the fresh biometric data, and send this biometric data to CASHMA service. This biometric trait will be taken transparently, that is without knowing to the user. This process is shown in step 5.

5. The CASHMA service get the biometric trait such as facial information from client and verifies it with the templates stored in it database. The data base considered here will be text file. Once the match occurs then CASHMA will start generation a certificate for requested user, then it computes the timeout and attach it with the certificate then forward to the client indicating that the user is legitimate. If the user is verified successfully, the CASHMA will use an algorithm that adaptively calculates new timeout, T_i will be the length of the time out, the session will expire at $t_i + T_i$ and CASHMA will creates and sends this certificate to the user.

6. The user at client get this certificate and send it to the web service; the web service verifies this certificate base on timestamp attached with it and allow the client to access its web service until session timeout occur i.e. till $t_i + T_i$.

IV. RESULTS

In this chapter, the implementation results of the project are shown in the form of snapshots. First both CASHMA service and web service must be started. User can start accessing web service by providing certificate taken from CASHMA service. So as to do this, user must be register with CASHMA service before start accessing web service.

CASHMA Server: User Authentication

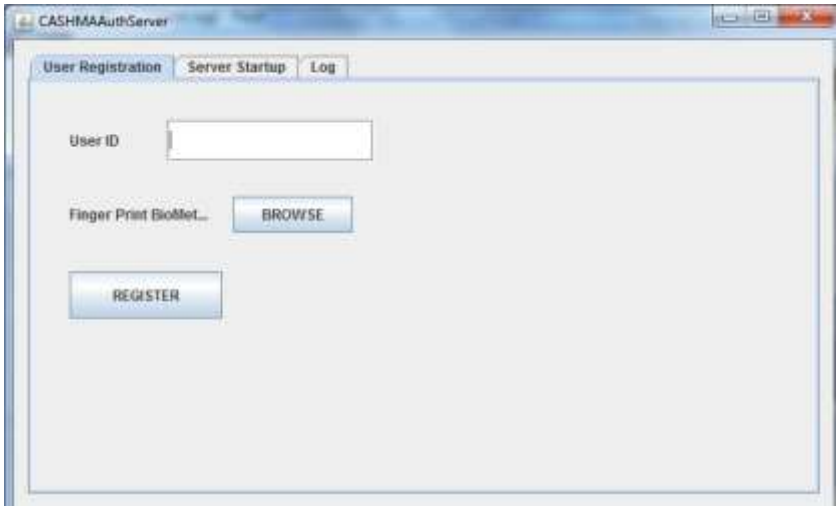

Fig. 4 CASHMA authentication service for user authentication

User who wants to use CASHMA service for their authentication, first they must register with CASHMA service. While registration they must provide his credential information such as user Id (or username) and finger print biometric information. Once he registered successfully then his/her credential information will be stored into database template such as text file. Snapshot given in Fig. 4 shows the user registration process.

CASHMA Server: Server Setup

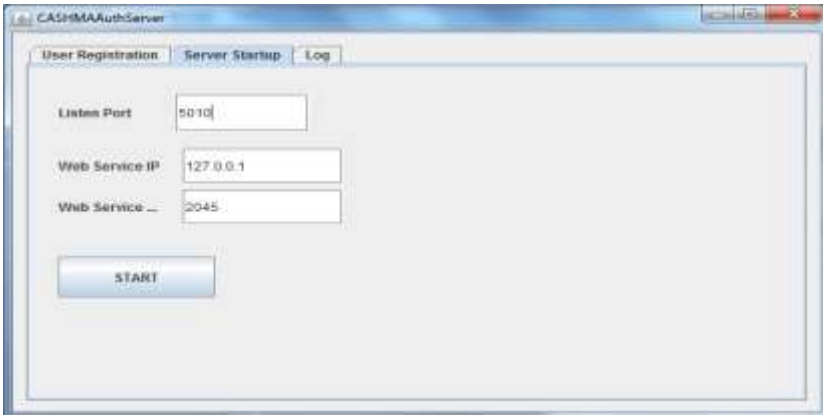

Fig 5 CASHMA authentication service for web service setup

Any web service wants to make use of CASHMA service for their security purpose; they must be registered with CASHMA service. To accomplish this task the CASHMA service need to establish a secure connection setup with the web service, for this CASHMA service specify the listen port number of its own, IP address of web service and port number on which web service is going to listen. This process is shown in Fig. 5

CASHMA Server: Log Record

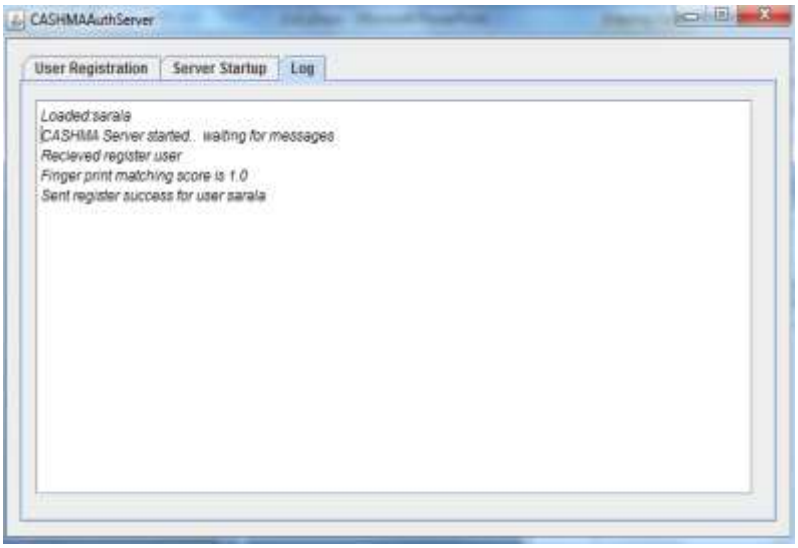

Fig. 6 User registration log record.

User registration log record for CASHMA service is shown in Fig 6. It keeps record of all users who have been registered into CASHMA service.

Temperature Service:

Fig. 7 Temperature web service.

Web services can be ranging from simple to high security demand services such as online banking, ecommerce etc. Temperature service is a simple web service is being considered in this project is shown in Fig 7 it calculates a temperature value for given a city name. These values will be random in nature. To accomplish this task user need to provide city name along with certificate issued from CASHMA service to the temperature service. Then temperature web service will first check the certificate to know that whether it is expired or not with the help of timestamp attached with certificate. If it is expired then the temperature web service will not provide services to that user, and

send a message back to him indicating that, to bring certificate from CASHMA service. Otherwise web service can provide service to user until certificate expires.

Temperature Service: Log Record

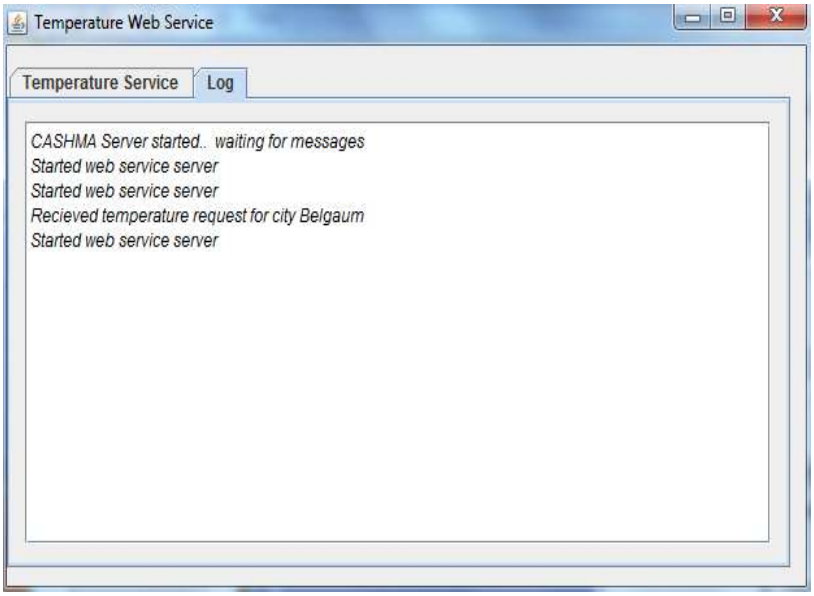

Fig 8 Temperature web service with log

Log record for temperature web service is shown in Fig. 8. Information such as whether the CASHMA server is started or not, whether the temperature web service is started or not and for which city user is requesting for temperature.

Client Portal: User Authentication

Fig. 9 Client portal for user authentication

To access the web service, user need to authenticate to web service. This can be done by sending user credentials such as username and fingerprint information of the user to CASHMA service, if

user is new to the system then first he need to register with CASHMA service which is described in CASHMA service module. CASHMA service will verify his credentials with stored templates, once match occur it generates a certificate with timestamp and send back to user. Then user can use this certificate to authenticate with temperature web service by clicking authenticate button shown in Fig. 9. Here web service will check whether certificate is expired or not by seeing timestamp attacked with it. If it has not expired; web service allow user to access the service, at the same time webcam starts capturing user facial information for further authentication.

Client Portal: Service Access When User is in Front of the Webcam:

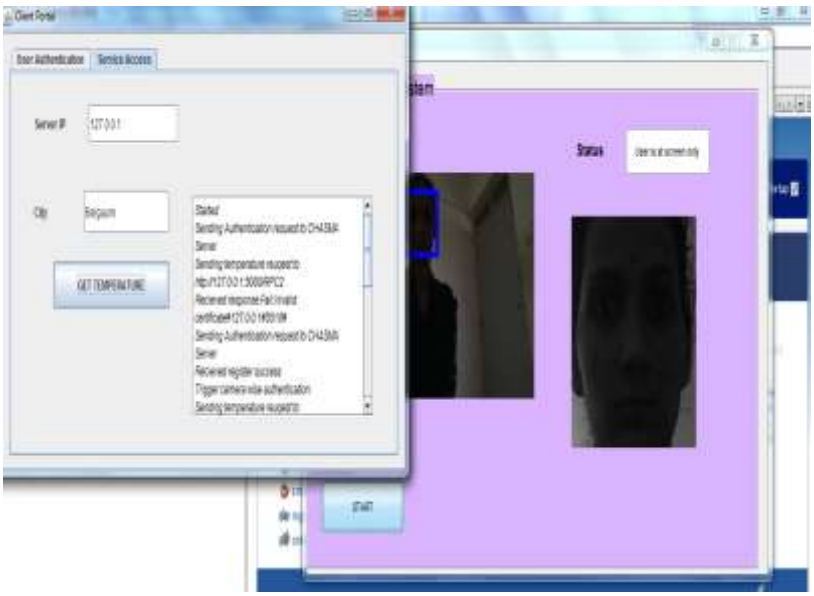

Fig 10 Authentication success when user is physically present in front of the camera.

In this project a simple temperature web service will be considered. Once user is authenticated with web service, he/she can have access to the web service by providing city name. Here temperature value will be calculated at random. User keeps accessing web service as along as he/she is physically present in front of webcam is shown in Fig 10.

Client Portal: Service Access when User goes out from the Webcam:

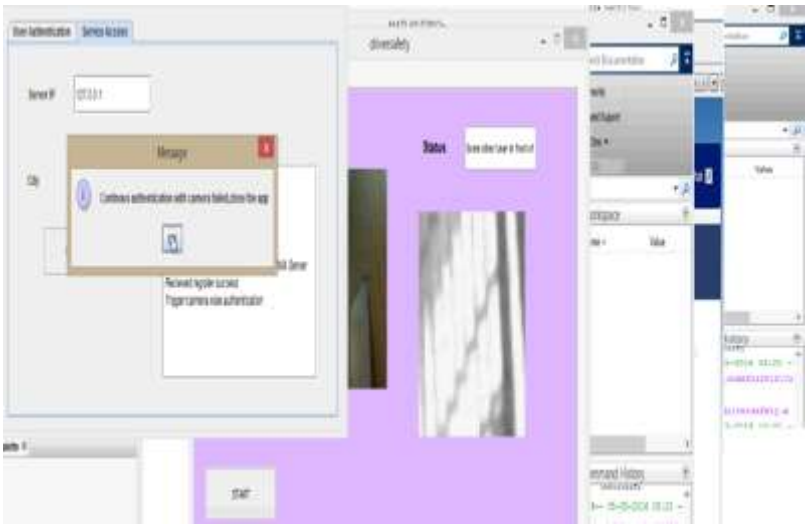

Fig 11 Authentication failed when the user is physically absent.

When user goes out or some other user came and starts accessing the web service then it will stop providing web service and it will send a pop up message that "continuous authentication with camera failed, close the application", is as shown in Fig. 11

V.CONCLUSION

This project implemented multimodal biometric system for authentication to ensure high level security. It uses CASHMA system. Identity of the user is being verified in two stages by acquiring credential in continuous and transparent manner. As this system is continuous and transparent; it helps to provide guaranteed secure authentication hence it can be applied to high security demand service like online banking and E-commerce etc.

REFERENCE

1. William Stallings Fifth Edition.
2. C. Roberts, "Biometric Attack Vectors and Defences," Computers & Security, vol. 26, no. 1, pp. 14-25, 2007.
3. U. Uludag and A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622-633, 2004.
4. S.Z. Li and A.K. Jain, Encyclopedia of Biometrics. First ed., Springer, 2009.
5. T.F. Dapp, "Growing Need for Security in Online Banking: Biometrics Enjoy Remarkable Degree of Acceptance," Banking & Technology Snapshot, DB Research, Feb. 2012.
6. A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.
7. L. Allano, B. Dorizzi, and S. Garcia-Salicetti, "Tuning Cost and Performance in Multi-Biometric Systems: A Novel and Consistent View of Fusion Strategies Based on the Sequential Probability Ratio Test (SPRT)," Pattern Recognition Letters, vol. 31, no. 9, pp. 884-890, 2010.
8. L. Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?" Proc. Workshop on Automatic Identification Advances Technologies (AutoID '99) Summit, pp. 59-64, 1999.
9. BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.
10. CASHMA- "Context Aware Security by Hierarchical Multilevel Architectures2005.
11. T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.
12. Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, and Andrea Bondavalli, Member, IEEE "Continuous and Transparent User Identity Verification for secured Internet services", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3, MAY/JUNE 2015.

