Session Management in Internet Services using Continuous Authentication

Jennifer Lathakumari Wilson
Department of Computer Engineering,
PG student, Terna Engineering College,Navi Mumbai, University of Mumbai
Dr. Lata Ragha
Department of Computer Engineering,
Faculty of Terna Engineering College,Navi Mumbai, University of Mumbai

Abstract — Security is a very significant aspect, whether it may be for an individual or commercial usage. Our existing systems have passwords for login to avoid illegal users from logging into the system. Traditional computer systems authenticate users only during initial log-in session, which can be the cause of a critical security flaw. To alleviate this problem, continuous user authentication methods should be used continuously to monitor and authenticate users based on some biometric traits. These kinds of problems are identified mostly when user takes a short interval or when the user may not have logged out due to some reason. This is a very important issue in terms of security concerns especially for systems holding confidential information. Due to advancement in technology some online services have started using biometric data instead of username and password for the purpose of login. The CASHMA architecture has the functionality of both continuous and transparent authentication. This architecture has focused less on the image quality and authentication during low light conditions. Thus we proposed a methodology that uses face biometrics in the management of sessions. The proposed system can continuously authenticate the user without his/her interaction. The system focuses mainly on the facial features and the environmental conditions especially during low light for verifying the user during authentication.
***Index Terms* — Biometrics, Continuous authentication, Session, CASHMA architecture.**

I. INTRODUCTION

Security is a significant feature for any kind of online environment. Mostly people can view computer security in a corporate or business context. Companies often store a lot of sensitive information electronically, including trade secrets, customer lists and extensive corporate documents, both finished and those in progress. The importance of computer security is important in these contexts but not very important for home PC users. Computer systems are vulnerable to intrusion attacks like data breaching, hacking, etc. by internet access and various other technical ways. Web services are used to provide easy accessible services over a network. To be successful in business scenarios, web services need to be suitable for secure communication. The security factors like authentication, authorization, confidentiality and integrity should be considered for the usage of web services. Authorization grants access to specific resource based on the user's designation, authentication ensures that it is the legal user who makes use of the service, authorization grants access to specific resource based on the user's designation, confidentiality helps in keeping the information secure and private allowing access to the specific user and integrity makes sure that the data or information remains unaltered during the transmission by digitally signing the message thus providing non-repudiation.

There are several ways to identify oneself: by means of something you know (like a password), something you have (like an ID card) or something you are (their identity). The aim of biometrics is to recognize a person based on his/her identity, the characteristics through which a person is identified should therefore be unique, not change significantly over a reasonable amount of time and each person should have these characteristic [2]. A few examples of characteristics that are used in biometrics are finger-print or palm print, face, veins in a finger or palm, DNA, gait, iris, ear and voice [3]. Some of these are easier to collect than others, which makes some of these characteristics more usable than others. To get a DNA sample one would have to extract blood or saliva on some device, neither of which is usually desirable. When a person logs in on a computer, this person is identifying him/herself to the computer. A person needs to do this only once to gain access, this is referred to as static authentication. In contrast to static authentication there is also continuous authentication, which continually identifies the user. Since it is undesirable for a person to re-enter a password or rescan an ID card every minute, it would seem that biometrics offer the best authentication method for this problem. The use of biometrics

provides better usability by reducing the interaction of user with authentication service and also has the assurance that it is the legal user accessing the service [4]. Continuous authentication is useful in a situation where a user should be able to leave his or her system for a certain amount of time without having to log out or fearing that someone who is not authorized could use the system.

II. RELATED WORK

In [5], a biometric verification system is used which is multi-modal in nature and is used to detect the physical presence of the client logged in a computer. In this approach initially the user logs in using a powerful authentication procedure. After the user logs in, the session can be continued by multi-modal biometric verification of face by face recognition system and finger print sensing using fingerprint-reader-enabled mouse. One important mechanism used in this system is, the multi-modal feedback mechanism which is build inside the operating system is in such a way that if there is any verification failure, it leads to automatic locking of the computer. In this system user interaction is needed thus preventing transparency in authentication and also in case of failure of the feedback mechanism, it may lead to illegal user access. A similar approach is presented in [6] where a fingerprint sensor enabled mouse and a face detector is used. At the initial step of authentication the user logs in using a proper authentication process and for continuing the session, a multi-modal biometric verification system is used to verify the user who is having access to the computer. In case of failure in verification the system locks the computer or delays the access of the service till the user is verified as a legal one. To use this system there is need of user interaction to continue the session.

In [7], a wearable wristband which acts as an authentication device for continuous and transparent authentication is used by the user to login. In this system this device enables the login to be done transparently via a wireless channel and does the transmission of biometric data to the computers by staying within the specific range. The initial step of authentication is done by verification of fingerprint and the session is continued by verifying the presence of user by using the skin temperature and the body capacitance. In order to continue the session even an illegal user can make use of the wearable authentication device since only body functionalities of human is considered rather than considering biometric data. In [8] a method to recognize the user with keystroke sound is used. Discriminative power of keystroke sound in the context of a continuous user authentication application is analyzed. Based on the concept of digraphs used in modeling keystroke dynamics, a virtual alphabet is first learned from keystroke sound segments. Next, the digraph latency within the pairs of virtual letters, along with other statistical features is used to generate match scores. The resultant scores are indicative of the similarities between two sound streams, and are fused to make a final authentication decision. Disadvantage is that exact identity of the valid user cannot be verified.

III. PROPOSED METHODOLOGY

A. Architecture of Proposed System:

The system consists of a CASHMA application, CASHMA server, a web service, database of templates and the client who uses the web service through the CASHMA application. The system architecture is shown in the figure 3.1

- **Client:** The client contains sensors (webcam) to acquire the raw data, and the CASHMA application which transmits the biometric data to the authentication server.
- The **CASHMA authentication server** includes:
  i) An authentication server, which interacts with the clients.
  ii) A set of high-performing computational servers that perform comparisons of biometric data for verification of the enrolled users.
  iii) Databases of templates that contain the biometric templates of the enrolled users (these are required for user authentication/verification).
- **Web services:** The various services that use the CASHMA authentication service and demand the authentication of enrolled users to the CASHMA authentication server. These services are potentially any kind of Internet service or application with requirements on user authenticity. They have to be registered to the CASHMA authentication service, expressing also their trust threshold.

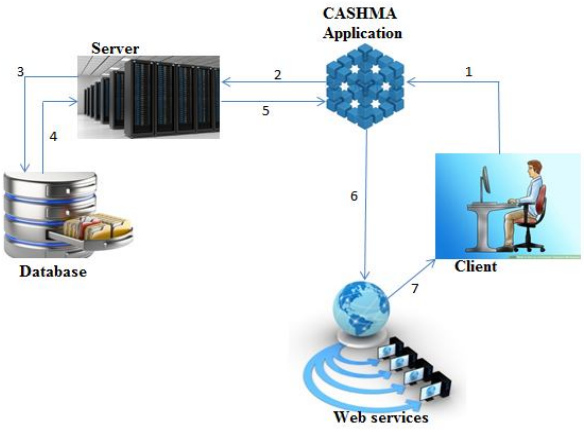

Figure 3.1: Architecture of Proposed system

B. Continuous authentication protocol:

1. Registration Phase:

- The user opens the CASHMA application for registration and enters his name, password, sites to be accessed via the CASHMA application and 10 images of his/her face.
- This data acquired by the CASHMA application is sent further to the server to register the user.
- The data received at the server is stored in the database, which is used during verification during user login.

2. Initial Phase:

- Initially the client logs in using CASHMA application.
- The CASHMA application sends the details (username, Password, site to be accessed and image) of the user to the server.
- The server verifies with the details of user database and if yes/no it notifies the server about it.
- If it is the legal user the server sends a certificate to the CASHMA application.
- The CASHMA application sends it to the web service/ website to be accessed.
- Finally the user gets access of the web service.

3. Continuous authentication phase

- After the initial login procedure is done, the user accesses the web service.
- In the background the CASHMA application for every 2 minutes updates the session timeout by authenticating the user by sending the image of the user to server.
- Similarly the server verifies with the database and sends certificate to update session timeout if it is a legal user.

C. Algorithm for face detection and face recognition

The system uses OpenCV libraries for face detection and face recognition, where Local Binary Pattern is used as face recognizer and uses haar classifier for face detection.

1. Face Detection

To detect faces, images must be 'grabbed' by the web camera. The faces are to be detected from the image, which is done by using the frontal face cascade classifier. OpenCV uses Viola Jones algorithm [9] for face detection. The algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then it extracts features from it. For this, haar features are used. Each feature is a single value obtained by subtracting sum of pixels under white rectangle from sum of pixels under black rectangle. All possible sizes and locations of each kernel are used to calculate plenty of features. For each feature calculation, we need to find sum of pixels under white and black rectangles. The integral image simplifies

calculation of sum of pixels. Here the same windows applying on same area of face or any other place is irrelevant. Thus the best features out of 160000+ features are selected. It is achieved by Adaboost. This is done by applying each and every feature on all the training images. For each feature, it finds the best threshold which will classify the faces to positive and negative. The features with minimum error rate are selected, which means they are the features that best classifies the face and non-face images. Each image is given an equal weight in the beginning. After each classification, weights of misclassified images are increased. This process is continued. Then new error rates and new weights are calculated. The process is continued until required accuracy or error rate is achieved or required number of features is found. Final classifier is a weighted sum of these weak classifiers. The weak classifier classify the image, together with others to forms a strong classifier. Their final setup had around lesser features (eg. 6000 features from more than16000 features). In order to reduce the time consuming process of applying 6000 features to a single image. A simple method is used to check if a window is not a face region. If it is not then it discards it and will not process it again. For this they have introduced a Cascade of classifiers, which groups the features into different stages of classifiers and apply one-by-one. The first few stages will contain very less number of features If a window fails the first stage, it is discarded else it passes, the second stage of features and continue the process. The window which passes all stages is a face region.

2. Face Recognition:

The next step after locating a face inside of an image is the recognition of it. The recognition is the process of identifying a face inside of a set of previously learned faces. OpenCV provides three methods of face recognition: Eigenfaces, Fisherfaces and Local Binary Patterns Histograms (LBPH)[10]. The LBPH method takes a different approach than the Eigen faces method. LBPH performs well even when variations in different factors are present, such as pose, viewpoint, facial expressions, time (when the pictures are made) and illumination (lightening changes). In LBPH each images is analyzed independently, while the Eigen faces method looks at the dataset as a whole. The LBPH method characterize each image in the dataset are characterized locally and when a new unknown image is provided, we perform the same analysis on it and compare the result to each of the images in the dataset. The way which we analyze the images is by characterizing the local patterns in each location in the image. The frame is normalized and added as a template to LBP Face Recognizer.

IV. IMPLEMENTATION

A. Implementation details and modules:

- Registration Form: The user has to initially register with the cashma application in order to avail the facility provided by the cashma service. The user during registration submits the details username, password, the site to access through cashma application and a set of maximum 10 images to the cashma application. These details are submitted to the cashma server where it is stored in the database is shown in figure 4.1.

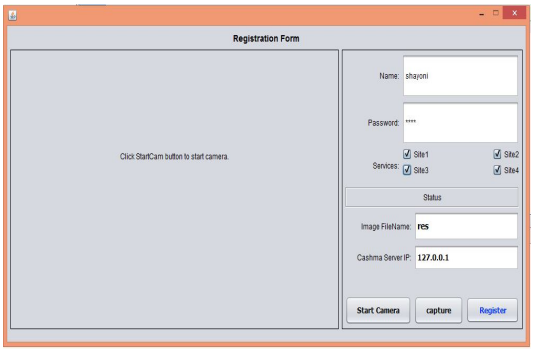

Figure 4.1: Registration Form

- Login form: During the login phase the user has to enter the username, password, site and the face image for authentication is shown in figure 4.2.
- Session open and login Ok notified: Once the user submits his/her details the server checks with the details stored in the database if it is verified the user gets access to the site and is allotted a session timeout of 2 minutes.

- Login failed no person detected notified: In case no face is detected in the camera the session expires thus logging off out of the session.
- Login failed imposter detected notified: When a person other than the legal user is detected the session logs off and thus preventing imposter accesses the account.

Figure 4.2: Login Form

- Session logged out and imposter detected notified: When the imposter tries to login, he is denied to access the account thus showing the following webpage in figure 4.3.

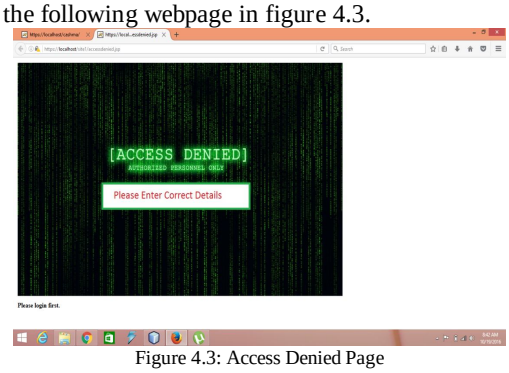

Figure 4.3: Access Denied Page

- Confidence level of person during login displayed: The legal person is authenticated based on his/her confidence level. The confidence level is set to a threshold value. If the value exceeds the threshold the person is rejected from accessing the site. The confidence level is displayed in the background is shown in figure 4.4.

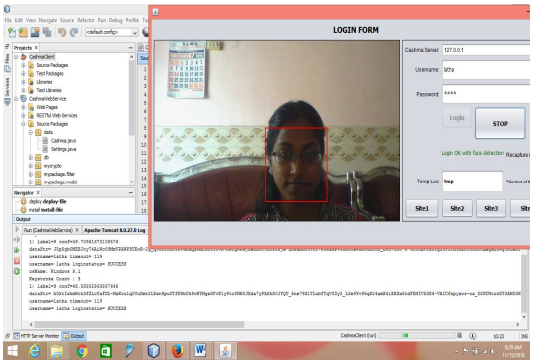

Figure 4.4: Confidence Level Displayed

B. Result analysis in terms of confidence level

The analysis on 20 samples is performed and the recognition percentage of each person is calculated considering the confidence level of the user. The following are certain values obtained from confidence level used to decide the system's performance and its thus proving to be better than the CASHMA architecture which is our existing system.

Best match rate obtained: 28.01

Moderate match rate obtained: 45.21
Worst match rate obtained within threshold value: 62.68
False Match Rate: 0
Recognition rate: 89.99%
Memory of data: 55-130kb

V. CONCLUSION

Biometric authentication systems provide a secure way of verifying the user as a legal one. This method of using biometrics for information security prevented enormous amount of imposter access to accounts containing sensitive data. As these systems had only single time verification of the user, it led to imposter access after the user logins the account without user's concern. Thus to overcome this problem continuous authentication systems were introduced which used biometrics as authentication parameter. Finally there were problems where the user had to interact with the system each time to refresh the session timeout. These all drawbacks were overcome in the CASHMA architecture.

The CASHMA architecture was proposed with the goal to have continuous as well as transparent authentication. This system worked well with good client satisfaction. Few drawbacks were identified. The system does not consider the image quality of user and is unable to perform successfully during low light conditions. Thus we have proposed a system which has overcome the drawbacks of the traditional CASHMA architecture. As per result analysis, our proposed method has zero false match rate and the memory required for each image is only 55-150kb. Thus the performance of the system is better than the traditional CASHMA architecture, as per analyzed results, when compared in terms of false match rate and memory requirement.

REFERENCES

[1] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Agnelo Marguglio and Andrea Bondavalli, "Continuous and Transparent User Identity Verification for Secure Internet Services", IEEE Trans. Dependable and Secure Computing, vol. 12, no. 3, pp. 270-283, June. 2015.
[2] 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.
[3] Koichiro Niinuma and Anil K. Jain, "Continuous User Authentication Using Temporal Information", Proc. SPIE 7667, Biometric Technology for Human Identification VII, 76670L (April 14,2010); doi:10.1117/12.847886.
[4] BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.
[5] 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.
[6] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "using continuous biometric verification to protect interactive login sessions", Proc. 21st Annual Computer security Applications Conf. (ACSAC '05), pp. 441-450, 2005.
[7] S. Ojala, J. Keinanen, and J. Skytta, "Wearable AuthenticationDevice for Transparent Login in Nomadic Applications Environment," Proc. Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.
[8] Joseph Roth, Xiaoming Liu, Arun Ross, and Dimitris Metaxas, "Investigating the Discriminative Power of Keystroke Sound", IEEE Transactions on Information Forensics and Security, VOL. 10, NO. 2, February 2015.
[9] http://docs.opencv.org/trunk/d7/d8b/tutorial_py_face_detection.html
[10] http://www.pyimagesearch.com/2015/12/07/local-binary-patterns-with-python -opencv/