Volume 6, Issue 9, September 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Session Management using Continuous Authentication in Internet Services: A Survey

Jennifer Lathakumari Wilson[1], Dr. Lata Ragha[2]
[1] P.G. Student, Dept. of Computer Engineering, Terna Engineering College, Navi Mumbai, Maharashtra, India
[2] H.O.D, Dept. of Computer Engineering, Terna Engineering College, Navi Mumbai, Maharashtra, India

Abstract— Security is a very important aspect, whether it may be personal or commercial usage. Our traditional systems have passwords for login to avoid unwanted users from logging into the system. Conventional computer systems authenticate users only at the initial log-in session, which can be the cause of a critical security flaw. To resolve this problem, systems need continuous user authentication methods that continuously monitor and authenticate users based on some biometric trait(s). Such problems are identified probably when user takes a short break or when the user may not have logged out due to some reason. This is a critical issue as far as security is concerned 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. In this paper we describe the development of a continuous authentication systems which uses biometric subsystems for face recognition, keystroke recognition, fingerprint recognition, use of heart beat rate and body temperature for maintaining the session. Also a comparative study is done among these systems to evaluate which system works better for continuous authentication.

Keywords— Biometrics, continuous authentication, session, face recognition.

I. INTRODUCTION

Security is an important feature for any kind of distributed environment. Mostly people perceive computer security in a corporate or business context. Companies often store a lot of very 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 that important for home computer users. Computer systems mostly open itself to intrusion risks like hacking, data breaching, etc. by internet activities. 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 [9]. 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 [7]. 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- or 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 have to reenter 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[10]. 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. LITERATURE SURVEY

1) Using continuous biometric verification to protect interactive login sessions [1].

This paper uses the combination of digital camera-based face verification with a mouse-based fingerprint reader. The main objective is to build a multi-modal biometric feedback mechanism into the operating system so that verification failure can automatically lock up the computer.

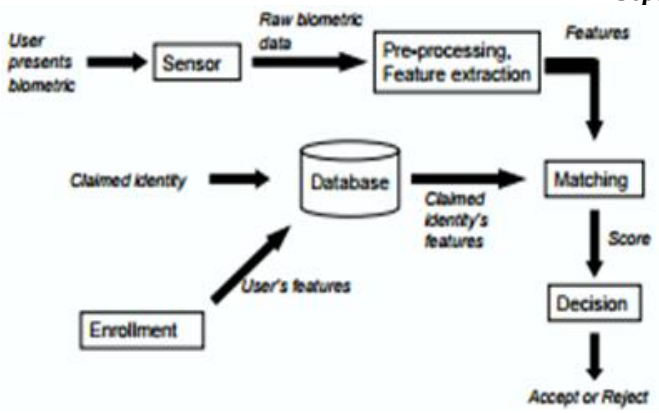

Fig 1: Biometric verification process.

Working:

In this system the user's biometric features are entered into the database during the enrollment phase. Then during the continuous verification the user first presents the biometric data. This data is then preprocessed. In case of fingerprint, a matching algorithm is used to compute the similarity score between the input and the biometric already stored in the database. In case of face verification, the viola-jones face detector algorithm is used. Then the integration of biometric observations across modalities and time is done using Hidden Markov model. Finally this biometric feedback is integrated into the operating system.

Drawbacks:

- If the OS integrated feedback mechanism fails, it can make way for illegal user access.
- Verification using fingerprint-enabled mouse decreases the usability.

2) Continuous Verification using Multimodal Biometrics [2].

This system presents the use of two biometric modalities: face and fingerprint and it can be extended to use more modalities. Also this paper has proposed new metrics for measuring the performance of the system.

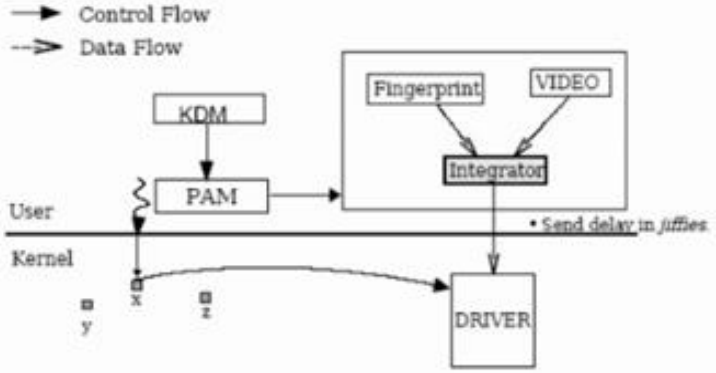

Fig 2: Architecture of continuous verification system integrated into the OS

In this system the user logs in at the console using the kdm session manager, kdm authenticates the user using a password. Then it starts the face and fingerprint verification. Once the integrator has the user-id of the logged in user, it loads the biometric profile corresponding to the user and starts acquiring biometric observations using the video and fingerprint. The integrator is the central coordinating entity that combines verification results and communicates the value of P_{safe} to the kernel. The viola-jones face detector algorithm is used for face verification. Finally the continuous verification system is integrated into the operating system. This paper uses false accept rate and false reject rate and additional performance metrics: time to correct reject, probability of time to correct reject and usability.

Drawbacks:

- Failure in the inbuilt feedback system may lead to access by imposter.
- Usability of system is affected because there is less transparency.

3) Wearable Authentication Device for Transparent Login in Nomadic Applications Environment [3].

In this paper a wearable authentication device (a wristband) is presented for a continuous user authentication and transparent login procedure in web applications. By wearing the authentication device, the user can login transparently through a wireless channel and can transmit the authentication data to computers by just approaching them. Here fingerprint is used for authentication using the wristband and to ensure that the person is wearing the device, it measures continuously his vital signs (skin temperature and heart rate) along with body capacitance and acceleration. The heart rate of the user could be obtained from the pulse oximeter output. The received signal strength of the wireless connection offered an inexpensive and simple way to implement the transparent login by estimating the range between the user and a terminal.

Drawbacks:

- ❖ Temperature and heartbeat is been sensed for continuing the session, which is not a personal identity thus leading to imposter access of sensitive data.

4) Investigating the Discriminative Power of Keystroke Sound and provide authentication [4].

This paper uses the method of keystroke for recognizing a legal user. Using digraphs a virtual alphabet is learned from keystroke sound segments. Then the digraph latency within the pairs of virtual letters along with the other statistical features is used to generate match scores. The resultant scores are used to indicate the similarity between two sound streams. If the computed similarity score is high then the user can continue the session otherwise he/she is found to be an imposter and logged out of the system.

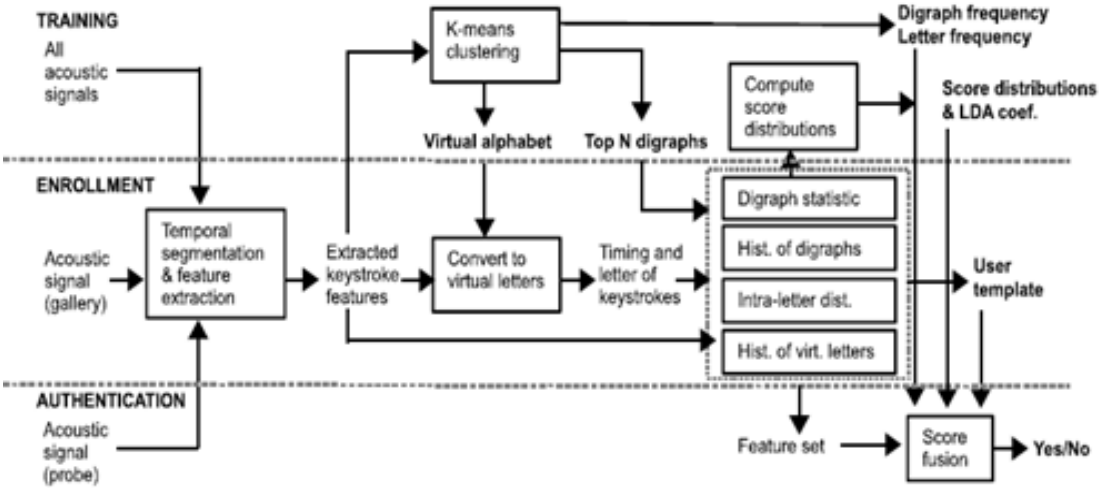

Fig 3: Architecture of a biometric authentication system based on keystroke sound.

Keystroke sound algorithm:

This system uses pattern matching algorithm that takes gallery sound stream and probe sound stream as inputs and returns a similarity score between them. The gallery sound stream has its features pre-computed and stored as a user template during the enrollment stage. The probe sound stream is produced by the current user of the system who has to be recognized. There are three different stages of operation for the system: training, enrollment and authentication. In the training stage a set of pre-recorded sound streams from multiple subjects is used to learn the various parameters of the algorithm suitable for the given environment. In the enrollment stage a new subject types a pre-defined text while the system records the sound stream. It then estimates when keys were pressed, extracts the features from the stream, and creates and stores a user template for the subject. Finally in the authentication stage the system extracts features from the sound stream in real-time and, after a sufficient length of time, compares them with the user template of the claimed identity to output a similarity score. If the computed similarity score is high enough, the subject is accepted and can continue operating the computer. Otherwise the subject is deemed an impostor and logged out of the system.

- *Temporal segmentation and feature extraction*: In temporal segmentation the time at which keystroke occurs is estimated. It is based on the energy of the keystroke which lies between the frequencies 400Hz to 12kHz and after this feature is extracted using 32 channels of Mel-scale filter bank which results in 256-dimensional vector f_i.
- *Virtual alphabet via clustering*: This step estimates the letter/label pressed at each keystroke. Each label is called a virtual letter, the collection of which is called a virtual alphabet. Each virtual alphabet is learned using K-means clustering.
- *Compute, fuse scores and authentication*: Four important scores are computed, they are digraph statistic, histogram of digraphs, histogram of virtual letters and intra-letter distance. These four scores are reduced to a single score function S through linear discriminate analysis (LDA). Then a simple threshold τ is used to classify the user as genuine when $S>\tau$.

Drawbacks:

- ❖ The current database is constrained in the number of subjects, single keyboard, consistent typing environment, and single day of collection.
- ❖ There is no understanding of the susceptibility of the current system to attacks.
- ❖ Keystroke can also be done by illegal user as the system lacks in identifying keystrokes using supervised learning or context sensitive threshold.

5) Continuous and Transparent User Identity Verification for Secure Internet Services [5]

This paper proposes a secure protocol for perpetual authentication through continuous user verification. The protocol determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user. The system uses face verification for continuous authentication [8].

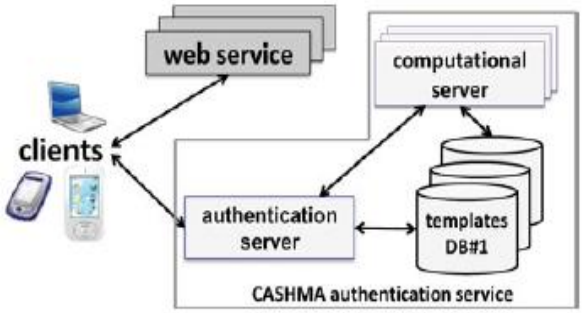

Fig 4: Overall view of CASHMA architecture.

The CASHMA authentication service [6] includes an authentication server, a set of computational servers and databases of templates that contain the biometric templates of the enrolled users. Clients acquire the biometric data (the raw data) corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server as part of the authentication procedure towards the target web service. A client contains sensors to acquire the raw data and the CASHMA application which transmits the biometric data to the authentication server.

The authentication server verifies the user identity, and grants the access if the user is enrolled in the CASHMA authentication service and if the acquired biometric data match those stored in the templates database associated to the provided identifier. In case of successful user verification, the CASHMA authentication server releases an authentication certificate to the client, proving its identity to third parties, and includes a timeout that sets the maximum duration of the user session. The client presents this certificate to the web service, which verifies it and grants access to the client. The CASHMA application operates to continuously maintain the session open. It transparently acquires biometric data from the user, and sends them to the CASHMA authentication server to get a new certificate. Such certificate, which includes a new timeout, is forwarded to the web service to further extend the user session.

Drawbacks:

- The qualities of images are not considered very specifically.
- During low light conditions the application may fail to detect legal user due lack of quality.

Table 1: Comparison Table

Year	Authors	Method used	Shortcomes
2005	T. Sim, S. Zhang, R. Janakiraman and S. Kumar [1].	Face and fingerprint sensor enabled mouse and an in-built mechanism placed in the operating system.	Failure of device may lead to illegal user access.
2007	T. Sim, S. Zhang, R. Janakiraman and S. Kumar [2].	Face and fingerprint sensor enabled mouse.	User needs to interact with the system continuously
2008	S. Ojala, J. Keinanen and J. Skytta [3].	Wristband	Other person can also access account by using wristband.
2015	Joseph Roth, Xiaoming Liu, Arun Ross and Dimitris Metaxas [4].	Keystroke Sound	Illegal user can also make keystroke sound and get access to the user's data.
2015	Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Agnelo Marguglio and Andrea Bondavalli [5].	Face recognition	Image quality and Lighting conditions are not considered

We have discussed various methods of continuous authentication using applications, biometric recognition systems, etc. Each system uses some biometric data for the purpose of continuous authentication. The use of biometric data in these systems ensures that only the legal users access his/her data, as biometric data identifies the user personally. Some systems still have some drawbacks like lacking in usability, system failure, image quality, etc. Thus these factors should be considered while designing the new systems.

III. CONCLUSION

Our survey covers the methods used for continuous authentication. From the above survey we have learned that each system has made use of biometric data for the purpose of continuous authentication. The biometric data is selected in such a way so as to improve the usability of the user and reduce user's interaction with the system. Thus with such systems we can assure that data is being protected from imposters access. There is also a need to consider the environmental factors like low light, which can be improved by using an efficient algorithm that alleviates this problem.

REFERENCES

[1] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," Proc. 21st Ann. Computer Security Applications Conf. (ACSAC '05), pp. 441-450, 2005.

[2] 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.

[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for Transparent Login in Nomadic Applications Environment," Proc. Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.

[4] Joseph Roth, Xiaoming Liu, Arun Ross and Dimitris Metaxas, "Investigating the Discriminative Power of Keystroke Sound and provide authentication," IEEE Trans. Information Forensics and Security, vol. 10, no. 2, pp. 333-345, Feb. 2015.

[5] 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.

[6] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.

[7] 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.

[8] A. Ceccarelli, A. Bondavalli, F. Brancati, and E. La Mattina, "Improving Security of Internet Services through Continuous and Transparent User Identity Verification," Proc. Int'l Symp. Reliable Distributed Systems (SRDS), pp. 201-206, Oct. 2012.

[9] 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.

[10] BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.

