ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 11, May 2016

International Conference on Innovations in Engineering and Technology (ICIET'16)

6th & 7th April 2016

Organized by

K.L.N. College of Engineering and Technology, Madurai, Tamil Nadu, India

# Design and Analysis of Continuous and Transparent User Identity Verification for Secure Internet Service

Dr Ch Venkatramana Reddy[1], Dr Vijay Reddy Madireddy [2]

Associate Professor, Head Department of CSE, RamanandaTirtha Engineering College, Nalgonda, India[1]

Associate Professor, Department of CSE, RamanandaTirtha Engineering College, Nalgonda, India[2]

**ABSTRACT:** Protection of the net based services is actually become major concern right now a days. Secure user authentication is fundamental and important very in the majority of the systems User authentication systems are usually based on pairs of password and username and confirm the identity of the end user just at login phase. We check out the constant user verification for the protected online services with biometrics in the consultation management No checks are actually carried out during working sessions, that are terminated by an explicit logout or perhaps expire after an idle task phase of the user However an individual verification move is currently deemed enough, as well as the identity of a user is actually regarded as immutable during the whole session. Furthermore, the fixed measurements of the consultation timeout may effect on the enhancing of the service as well as consequent customer satisfaction. This paper explores promising options provided by using biometrics in the managing of sessions. A secure protocol is actually defined for perpetual authentication through constant user verification.

**KEYWORDS***:* Security, Web Servers, Mobile Environments, Authentication.

## I. INTRODUCTION

User authentication is very crucial for the computers as well as network system security. Lately, awareness based methods (e.g., passwords) along with token-based techniques (e.g., smart cards) are actually the most favored techniques. However, these techniques are having a selection of security flaws. For instance, passwords can be shared, stolen, and forgotten easily [1, 2].Similarly, the clever cards may be shared, stolen, duplicated, or perhaps may lost. To overcome these issues, a selection of login authentication techniques like textual, graphical passwords and biometric authentication have been used [3-4].

Most of the above mentioned login strategies share a common problem that's they authenticate at user just at the initial login session and then don't re authenticate the owners until the end user logs out. In this particular case virtually anyone can use the system materials if the initial user doesn't effectively logout or perhaps the end user leaves the workstation or perhaps system unattended to take a brief rest without logging out. And so, for resolving this particular issue, the system must continuously monitor and also authenticate the end user after the original login session. To be able to do this objective, we want to develop strong, dependable also as user-friendly techniques for the constant user authentication. It's also appealing that the ensuing strategy is running the great usability by authenticating a user without his proactive cooperation. Continuous Authentication is additionally really important in online examinations in which the user has to be continuously verified throughout the whole session. It may also be used in different real time applications. There's a tremendously need of secure constant verification of user for accessing a protected file or perhaps during the internet banking transactions. However, there exists much number of biometric attributes that are used in numerous programs. Each biometrics is having their personal weaknesses and strengths, and furthermore, the choice is dependent on the application.

Several of the commonly used hard biometrics are Face, Hand geometry, Fingerprint, Iris and Soft biometrics include things like Keystroke, Voice, Colour of the clothes, Facial color etc. A single biometric trait that's unimodal methods are not adequately utilized to authenticate a user constantly because the program sometimes can't observe the bio-metric information accurately. The limits of individual biometrics can be conquered by utilizing multimodal biometrics.

Multimodal biometrics are the mixture of 2 or even more biometric traits for boosting methods security as well as dependability [1-2].
A simple solution is usually to make use of really short session timeouts and regularly ask for the user to type in his/her credentials again & once again. To regular detect misuses of computer energy and stop that an unauthorized user maliciously replenishes an authorized one, treatments based on multi-modal bio-metric constant authentication are actually suggested, turning user verification into a constant process rather than onetime occurrence. To stay away from that an individual biometric trait is actually forged, biometrics authentication may depend on a number of biometrics traits, new method for owners verification as well as session control are actually talked about in this specific paper that's defined and applied in the context of the multi-modal biometric authentication structure CASHMA-(Context Aware Security by Hierarchical Multilevel Architecture). The CASHMA structure realizes a protected biometric authentication service on the web, in that users have to keep in mind just one username and work with their biometric details instead of passwords to authenticate in several web services. CASHMA operate securely with any sort of web service for instance online banking, army zones, and airport zone which in turn need top security services.

## II. RELATED WORK

A significant problem that continuous authentication aims to tackle is the possibility that the user device (smartphone, table, laptop, etc.) is used, stolen or forcibly taken after the user has already logged into a security-critical service, or that the communication channels or the biometric sensors are hacked. In [7] a multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer. The proposed approach assumes that first the user logs in using a strong authentication procedure, then a continuous verification process is started based on multi-modal biometric. Verification failure together with a conservative estimate of the time required to subvert the computer can automatically lock it up. Similarly, in [5] a multi-modal biometric verification system is presented, which continuously verifies the presence of a user working with a computer. If the verification fails, the system reacts by locking the computer and by delaying or freezing the user's processes. The work in [8] proposes a multi-modal biometric continuous authentication solution for local access to high-security systems as ATMs, where the raw data acquired are weighted in the user verification process, based on i) type of the biometric traits and ii) time, since different sensors are able to provide raw data with different timings. Point ii) introduces the need of a temporal integration method which depends on the availability of past observations: based on the assumption that as time passes, the confidence in the acquired (aging) values decreases. The paper applies a degeneracy function that measures the uncertainty of the score computed by the verification function. In [22], despite the focus is not on continuous authentication, an automatic tuning of decision parameters (thresholds) for sequential multi-biometric score fusion is presented: the principle to achieve multimodality is to consider monomodal biometric subsystems sequentially. In [3] a wearable authentication device (a wristband) is presented for a continuous user authentication and transparent login procedure in applications where users are nomadic. By wearing the authentication device, the user can login transparently through a wireless channel, and can transmit the authentication data to computers simply approaching them.

## III. DESIGN METHODOLOGY

The system architecture is consisting of the CASHMA authentication service, the clients and the web services and they are connected through communication channels. Fig. 1 describes the continuous authentication system to a web service. The authentication server, which interacts with the clients, computational servers that perform comparisons of biometric data for verification of the users, and databases of templates contains the biometric templates of the users (that are required for user authentication or verification purpose). The web service demands the authentication of users to the CASHMA authentication server. These services are any kind of Internet service. Finally, by clients we mean the users' devices like (laptops, Desktop PCs, tablets, etc.) which acquire the biometric data corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server towards a target web service.

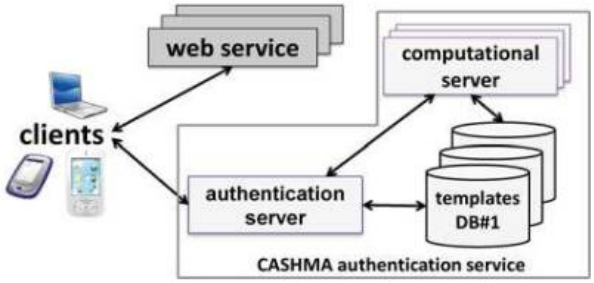


Fig 1. Architecture of CASHMA authentication system

A client contains .i) sensors - acquire the raw data, ii) the CASHMA application - transmits the raw data to the authentication server. The CASHMA authentication server applies user authentication and verification procedures that compare the raw data with the biometric templates stored. The constant authentication protocol enables supplying adaptive session timeouts to a web service to create and keep a secure session with a customer. The timeout is actually taken on the foundation of the trust that the CASHMA authentication device that trust places in the biometric subsystems what about the user.

**Initial phase**

In this phase the user (the client) communicates with the web service for a service request; the web service replies a valid certificate from the CASHMA authentication service is required for authentication. The first step is sending the data for the different biometric traits, specifically selected to perform a strong authentication procedure. The CASHMA authentication server checks the biometric data received and performs an authentication procedure.

There are two different possibilities arises. If the user identity is not verified (step 1:1), new or additional biometric information are requested (back to step 1); this process is repeated until the minimum trust threshold $g_{min}$ is reached. If the user identity is successfully verified (step 1:1), the CASHMA authentication server authenticates the user, computes an initial timeout of length T1 at time instant timestamp1 for the user session. Creates the CASHMA certificate and sends it to the client. - The client forwards the CASHMA certificate to the web service (step 2). The certificate is read by web server and authorizes the client to use the requested service (step 3) until time timestamp.

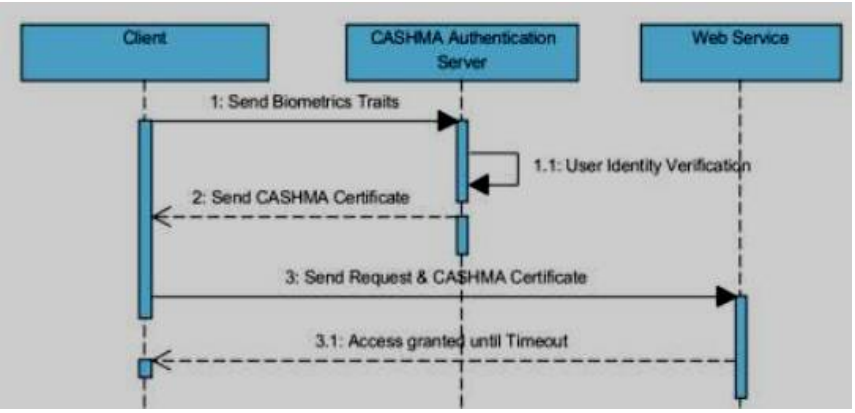


Fig 2. Initial phase of authentication server

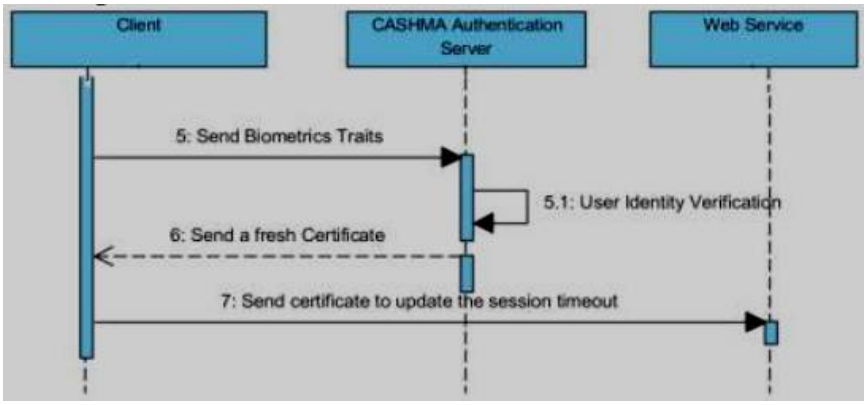


Fig 3. Maintenance phase of authentication server

**Maintenance phase:**

The goal of the maintenance stage is to lessen the risks. It provides the actions repeated iteratively: -

If the client application acquires new raw information which corresponding to a particular biometric trait, it interact them with CASHMA authentication server (step 5). The biometric information may be acquired transparently to the end user. When the session timeout will expire, the client might explicitly indicate to its user that new biometric details are actually needed. - The CASHMA authentication server verifies the identity of the end user. If verification is not profitable (step 5:1) the end user is actually viewed as not appropriate and consequently the CASHMA authentication server doesn't operate to renew the session timeout. This doesn't show that the present session is terminated suddenly if another biometric information are supplied before the timeout expires, though it's feasible to get a brand new certificate and then renew the timeout. If verification is actually effective (step 6) the client gets and forwards certificate to the internet service, which reads the certificate. Sets the consultation timeout to expire at time timestamp+$T_i$(step 7).

## IV. RESULTS AND DISCUSSIONS

The implementation of the CASHMA prototype includes face, voice, iris, fingerprint and online dynamic handwritten signature as biometric traits for biometric kiosks and PCs/laptops, relying on on-board devices when available or pluggable accessories if needed. On smart phones only face and voice recognition are applied: iris recognition was discarded due to the difficulties in acquiring high-quality iris scans using the camera of commercial devices, and handwritten signature recognition is impractical on most of smart phones today available on market (larger displays are required). Finally, fingerprint recognition was discarded1because few Smartphone's include a fingerprint reader. The selected biometric traits (face and voice) suit the need to be acquired transparently for the continuous authentication protocol described.

## V. CONCLUSIONS

We exploit the major possibility introduced by biometrics to define a protocol for continuous authentication which improves security and usability of a user session. The protocol computes adaptive timeouts which is based on the trust put on the activity of user and in the quality as well as the kind of biometric data user is providing. The transparent acquisition of biometric data, realized through monitoring in background the user's actions, allows maintaining the session open without explicit interactions with the user, thus improving usability.

## REFERENCES

[1]. CASHMA-"Context Aware Security by Hierarchical Multilevel Architectures", MIUR FIRB, 2005.
[2]. Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, PaoloLollini, Angelo Marguglio, Andrea Bondavalli,, "Continuous and Transparent user identity verification for secure internet services", IEEE Transactions on Dependable and Secure Computing MAY/JUNE 2015.
[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] 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] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authentication System," Proc. Int'l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.
[7] 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.
[8] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.
[9] C. Roberts, "Biometric Attack Vectors and Defences," Computers & Security, vol. 26, no. 1, pp. 14-25, 2007.
[10] S.Z. Li and A.K. Jain, Encyclopedia of Biometrics. First ed., Springer, 2009.
[11] 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.
[12] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, and W.H. Sanders, "Adversary-Driven State-Based System Security Evaluation," Proc. the Sixth Int'l Workshop Security Measurements and Metrics (MetriSec '10), pp. 5:1-5:9, 2010.
[13] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002.
[14] D.M. Nicol, W.H. Sanders, and K.S. Trivedi, "Model-Based Evaluation: From Dependability to Security," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Jan.-Mar. 2004.
[15] T. Courtney, S. Gaonkar, L. Keefe, E.W.D. Rozier, and W.H. Sanders, "Mobius 2.3: An Extensible Tool for Dependability, € Security, and Performance Evaluation of Large and Complex System Models," Proc. IEEE/IFIP Int'l Conf. Dependable Systems & Networks (DSN '09), pp. 353-358, 2009.
[16] W.H. Sanders and J.F. Meyer, "Stochastic Activity Networks: Formal Definitions and Concepts," Lectures on Formal Methods and Performance Analysis, pp. 315-343, Springer-Verlag, 2002.
[17] T. Casey, "Threat Agent Library Helps Identify Information Security Risks,," White Paper, Intel Corporation, Sept. 2007.
[18] 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.
[19] Adobe Products List, http://www.adobe.com/products, 2014.
[20] T.F. Dapp, "Growing Need for Security in Online Banking: Biometrics Enjoy Remarkable Degree of Acceptance," Banking & Technology Snapshot, DB Research, Feb. 2012.
[21] A.K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security, vol. 1, no. 2, pp. 125-143, June 2006.
[22] 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.