Incessant and Transparent User Identity Verification for Secure Internet Services using Continuous Authentication Protocol

N. Venkatesh Naik, G. Srividya
Department of computer Science & Engineering
Sree Visvesvaraya Institute of Technology & Science, Mahabubnagar, Telangana, India.

***Abstract*- Security of the web based services is become serious concern now a days. Secure user authentication is very important and fundamental in most of the systems. In web applications, user authentication is normally based on username and password, come forth biometric solutions allow biometric data during session establishment. But in Unimodal biometric approaches only use a single verification is considered and the identity of the user is permanent during the entire session. A secure protocol is defined for constant authentication through continuous user verification. Biometric techniques suggest solution for secure, trusted and protected authentication. The user's identity has been verified, the system resources are available for fixed period of time and identity of the user is constant during entire session. The proposed system detects misuses of computer resources and prevents malicious activities based on multi-modal biometric continuous authentication. Biometric and user information's are stored in smart phones and web services.**

***Index Terms*- Biometric, Mobile Environments, Web Servers, Identification, Security, authentication.**

I. INTRODUCTION

In this technology era security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks, biometric techniques offer emerging solution for secure and trusted user identity verification, where username and password are replaced by bio-metric traits. Biometrics is the science and technology of determining identity based on physiological and behavioral traits. Biometrics includes retinal scans, finger and handprint recognition, and face recognition, handwriting analysis, voice recognition and Keyboard biometrics. Also, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially in the financial and banking sectors.

Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. Session time out may occur during unperformed working sessions or it expires when user is in idle activity period. Security of web-based application is very important as there is increase in complexity of cyber-attacks. Biometric programs provides more security for authentication process than proving the username and password. Bio-metric user authentication is typically formulated as a "single shot" offering user verification only during login phase when one or more biometric traits may be required. Once the user's identity has been verified, the system resources are available for a fixed period of time or until precise logout from the user. This approach assumes that a single verification is sufficient, and that the identity of the user is constant during the whole session.

For example: consider a user is already logged into the critical service and then and leaves the PC in the work space as a while. This issue is even risky when it is used in mobile phones in public andcrowded areas as the device can be lost while the session is active. The users are authenticated and it can be misused easily. To detect the misuses of the computer resources and prevent that from the unauthorized user replaces an authorized one by providing the solution based on the multimodal biometric continuous authentication turning the user authentication as the continuous process rather than the one time occurrence. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits. Finally, the use of biometric authentication allows qualifications to be acquired transparently, i.e. without explicitly notifying the user or requiring his/her interaction, which is essential to guarantee better service usability. Face can be acquired by using the front camera but not purposely for the acquisition of the biometric data for example the user may be reading a textual SMS or watching a movie on the mobile phone. Key-stroke data can be acquired whenever the user types on the keyboard, for example when writing an SMS, chat-ting, or browsing on the Internet. This paper presents a new approach for user verification and session management that is applied in the CASHMA (Context Aware Security by Hierarchical Multilevel Architectures) system for secure biometric authentication on the Internet. CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services, and it is intended to be used from different client devices e.g., smart phones and Desktop PCs.

CASHMA is used for highly protected, a user session is a continuous successive multi-modal biometric authentication protocol which computes and refreshes session time outs based on the client. In the CASHMA context, each subsystem comprises of all the hardware/software elements necessary to acquire and verify the authenticity of one biometric trait, including sensors, comparison algorithms and all the facilities for information transmission and management.

II. RELATED WORK

2.1 Continuous Authentication:

Continuous Authentication (CA) techniques represent a new generation of security techniques that continuously monitor user behavior and use this as basis to re-authenticate periodically throughout a login session. A problem in continuous authentication is that it aims to tackle the user device (smart phone, laptop, etc.) when it is used, stolen or forcibly taken after the user has already logged into the services. The proposed strategy represents that first the user logs in using a strong authentication procedure, and then a continuous verification process is started based on multi-modal biometric. Similarly, when a multi-modal biometric verification system is presented, it 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.

In CASHMA assessment, the choice of ADVICE was mainly due to:

- Bing able to model detailed adversary profiles,
- The possibility to combine it with other stochastic formalisms as the Mobius multi-formalism, and
- The ability to define ad-hoc metrics for the system we were targeting.

Fig 1 shows the user verification process for registered user. Here user biometric traits are compared with the data in the database and if they are matching the system accept the user otherwise reject the user.

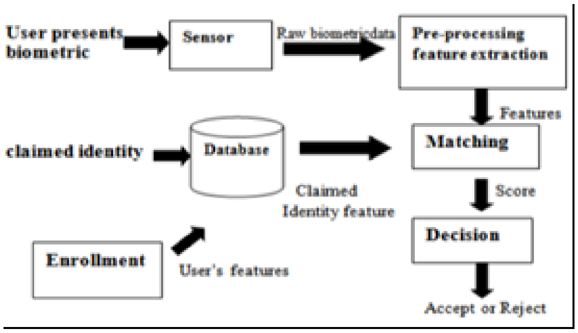

Fig. 1 User verification process

a. Comparing the Fusion Methods:

1) Genuine user using the system:

The biometric findings for 15 minutes. The personal possibilities are not continually high, they occur in a infrequent way. This signifies that anyvalue for the threshold Tsafe will result in significant False Accept and False Reject rates. In continuous verification, a False Accept is a security breach, while a False Reject inconveniences the legitimate user because he must re-authenticate himself. Ideally, Psafe should not fluctuate, but be equal to 1 as long as observations are available. Of the four fusion methods, Holistic Fusion comes closest to this ideal It computes a Psafe value close to 1, except for periods in which there are no observations from both modalities (around 300s and 600s). At such time, Psafe decreases gradually according to the decay function. By comparison, the Psafe computed by Naïve Integration fluctuates wildly because only a single modality is used any at time. Again, this means no Tsafe value will make both FRR and FAR small. As for Modality-first and temporal first Integration, the plots are similar. The Psafe values are not close to 1. Moreover, in the absence of observations, Psafe drops abruptly to zero, resulting in sudden lock outs. From these plots, it is clear that Natural Combination is superior to the other fusion techniques.

2) Imposter taking over the system:

The findings when an imposter requires over the system at some time instant (at around 38s). The probabilities of individual biometrics as well as Psafe for all integration methods drop to near zero after the attack. The goal here is to detect the attack as soon as possible so that damage to the system is minimized. Both Holistic Fusion and Naive Integration detect this situation sooner than the other two methods. However, Psafe for Naive Integration does not remain consistently low; it fluctuates widely. This implies that FAR > 0 for most values of Tsafe. For Modality-first and Temporal-first Integration, the system takes longer to detect the imposter (when Tsafe ¼ 0:5). Choosing a larger value for Tsafe can reduce the time to detection, but at the expense of a higher FRR.

3) Imposter effective in faking one of the biometric (Partial impersonation):

The individual possibilities contradict each other, and outcome in extremely varying plots in both Natural Combination and Naïve Incorporation. This gives us a way to detect partial impersonation: We may just take two thresholds, one high and one low (say, 0.8 and 0.2) and simply count the number of times within a fixed time interval that Psafe jumps between these thresholds. However, comparing we see that Naive Integration cannot distinguish between partial impersonation and the legitimate user. Fluctuating Psafe values seem to be an inherent property of Naive Integration. The plots for Modality-first Integration are relatively flat and arein fact similar to those in (except when there are completely no biometric observations). Again, this means these two methods cannot distinguish partial impersonation from legitimate usage. Only Holistic Fusion provides a way to detect partial impersonation that is different from detecting the real user. We remark that this fluctuating behavior of Holistic Fusion may be intuited from examining.

III. IMPLEMENTATION

The CASHMA authentication service includes:

- An authentication server, which interacts with the users,
- A set of high-performing computational servers that perform comparisons of biometric data for verification of the registered users, and
- Databases of templates that contain the biometric templates of the registered users. Users have to be registered to the CASHMA authentication service, expressing also their trust threshold.

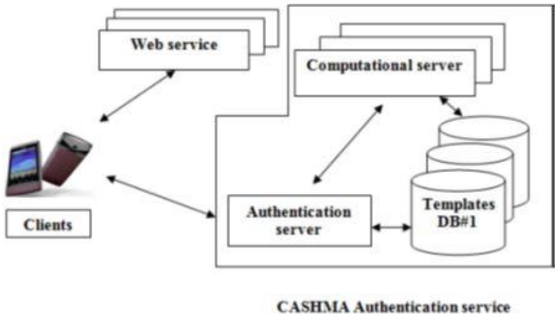

Fig. 2 Overall view of the CASHMA architecture.

The web services are the various services that use the CASHMA authentication service and demand the authentication of registered users to the CASHMA authentication server. These services are potentially any kind of Internet service or application with requirements on user authenticity. By clients we mean the users' devices (laptop and desktop PCs, smartphones, tablet, etc.) that get the biometric data (the raw data) corresponding to the various biometric traits from the users, and sends those data to the CASHMA authentication server as part of the authentication procedure towards the target web service. A client contains

- Sensors to get the raw data, and
- The CASHMA application which transmits the biometric data to the authentication server.

The CASHMA authentication server exploits such data to apply user authentication and successive verification procedures that check the raw data withthe saved biometric templates. Transmitting raw data has been a design decision applied to the CASHMA system, to decrease to a minimum the dimension, intrusiveness and complexity of the application installed on the user device, although we are aware that the transmission of raw data may be restricted, for example, due to National legislations. CASHMA includes counter measures to save the biometric data and to guarantee users' privacy, which including policies and procedures for proper registration; protection of the received data during its transmission to the authentication and computational servers and its storage; robustness improvement of the algorithm for biometric verification.

IV. THE CONTINUOUS AUTHENTICATION PROTOCOL

The continuous authentication protocol allows providing adaptive session timeouts to a web service to set up and maintain a secure session with a client.

4.1 Representation of the Protocol:

The proposed protocol requires a successive multi-modal biometric system consists of n Unimodal biometric sub-systems that are able to decide independently on the credibility of a user. For example, these subsystems can be one subsystem for keystroke recognition and one for face recognition.

The idea behind the execution of the protocol is that the user continuously and transparently gets and transmits evidence of the user identity to maintain access to a web service. The main task of the proposed protocol is to create and then sustain the user session adjusting the session timeout on the foundation of the confidence that the identity of the user in the system is genuine.

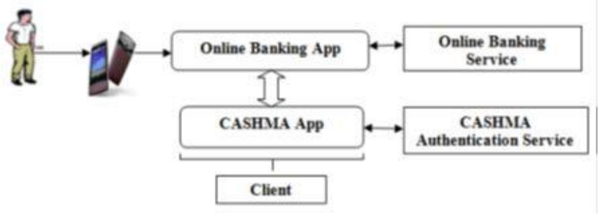

Fig. 3 Example scenario: accessing an online banking service using a smartphone.

The execution of the protocol is composed of two consecutive phases: the initial phase and the maintenance phase. The initial phase aims to authenticate the user into the system and establish the session with the web service. During the maintenance phase, the session timeout is adaptively updated when user identity verification is performedusing fresh raw data provided by the client to the CASHMA authentication server.

The user (the client) contacts the web service for a service request; the web service replies that a valid certificate from the CASHMA authentication service is required for authentication.

4.2Initial phase:

Using the CASHMA application, the client contacts the CASHMA authentication server. The first step consists in acquiring and sending at time t0 the data for the different biometric traits, specifically selected to carry out a powerful verification process (step 1). The application explicitly indicates to the user the biometric traits to be provided and possible retries.

The CASHMA authentication server studies the biometric data received and performs the verification process. Two different possibilities occurs here. If the user identity is not confirmed (the global trust level is below the trust threshold gmin), new or additional biometric data are requested (back to step 1) until the minimum trust threshold gminis reached. Instead if the user identity is successfully verified, the CASHMA authentication server authenticates the user, decides an initial timeout of length T0 for the user session, set the expiration time at T0 + t0, creates the CASHMA certificate and sends it to the client (step 2). The client forwards the CASHMA certificate to the web service (step 3) coupling it with its request.

The web service reads the certificate and authorizes the client to use the requested service (step 4) until time t0 + T0.

4.3 Maintenance Phase:

When some time the user application get fresh (new) raw data (corresponding to one biometric trait), it communicates them to the CASHMA authentication server (step 5). The biometricinformation can be obtained transparently to the user; The CASHMA authentication server receives the biometric data from the user and verifies the identity of the user. If verification is not successful, then the user is marked as not legitimate, and consequently the CASHMA authentication server does not function.

Authentication server applies the algorithm to adaptively estimate a new timeout of duration Ti, the expiration time of the session at time Ti+ ti and then it makes and delivers a new certificate to the client. The user gets a new certificate and forwards it to the web service; the web service reads the certificate and sets the session timeout to expire at time ti+ Ti.

For clarity, steps 1-4 are represented in Fig. 3 for the case of successful user verification only.
Maintenance phase. It is composed of three steps repeated iteratively:
• When at time ti the client application acquires fresh (new) raw data (corresponding to one biometric trait), it communicates them to the CASHMA authentication server (step 5). The biometric data can be acquired transparently to the user; the user may however decide to provide biometric data which are unlikely acquired in a transparent way (e.g., fingerprint). Finally when the session timeout is going to expire, the client may explicitly notify to the user that fresh biometric data are needed.

• The CASHMA authentication server receives the biometric data from the user and verifies the identity of the user. If verification is not successful, the user is marked as not legitimate, and consequently the CASHMA authentication server does not function to refresh the session timeout. This does not imply that the user is cut-off from the current session: if other biometric data are provided before the timeout expires, it is still possible to get a new certificate and refresh the timeout. If verification is successful, the CASHMA authentication server applies the algorithm[1] to adaptively compute a new timeout of length Ti, the expiration time of the session at time Ti + ti and then it creates and sends a new certificate to the client (step 6).
• The customer gets the certification and delivers it to the web service; the web service reads the certificate

4.4 Identification:

Given an input biometric sample, identification decides if the feedback biometric sample is associated with any of a great variety (e.g., millions) of registered identities. Typical identification programs include wellbeing payment, national ID bank cards, border control, voter ID bank cards, driver’s license, criminal investigation, corpse identification, being a parent determination, missing children identification, etc. These identification programs require a huge sustainable throughput with as little human guidance as possible.

4.5 The CASHMA Certificate:

In the following we present the information contained in the body of the CASHMA certificate transmitted to the user by the CASHMA authentication server, necessary to understand details of the protocol. The CASHMA certificate consist of Time stamp and sequence number univocally identify each certificate, and it protect from replay attacks. ID is the user ID, e.g., a number.Decision represents the outcome of the verification procedure carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. Generally, the global trust level and the session timeout are always computed by considering the time instant in which the CASHMA application acquires the biometric data, to avoid potential problems related to unknown delays in communication and computation. Since such delays are not predicable in earlier, simply delivering a relative timeout value to the client is not feasible, so the CASHMA server therefore provides the absolute instant of time at which the session should expire. The CASHMA certificate will be expired when the expiration timeout reach zero.

V. CONCLUSION

This paper provides various existing methods used for continuous authentication using different biometrics. Initial one time login verification is inadequate to address the risk involved in post logged in session.The continuous authentication process improves the user authentication in more secure manner andincrease the usability of user session, where the fingerprint information obtained transparently through monitoring the user’s action .The user is very simple. And the protocol works with no changes using features, templates or raw data. When data is acquired in an uncontrolled environment, the quality of biometric data could strongly depend on the surroundings. While executing a client-side high quality analysis of the information obtained would be a reasonable way of decrease computational burden on the server.

REFERENCES

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

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

[3] L. Hong, A. Jain, and S. Pankanti, "Can Multi-biometrics Improve Performance?," Proc. AutoID'99, Summit, NJ, pp. 59–64, 1999.

[4] BioID "Biometric Authentication as a Service (BaaS)," BioID PressRelease, 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 AuthenticationSystem," Proc. Int'l Conf. Computer Safety, Reliability andSecurity, pp. 209-221, 2012.

[7] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using ContinuousBiometric 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 ContinuousMultimodal 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.

Author's profiles:

N.Venkatesh Naik working as Assoc.Professor & HoD, Department of Computer science and Engineering in Sree Visvesvaraya Institute of Technology & Science, Mahabubnagar, Telangana, India.

Gudipally Srividya pursing M.Tech, Computer Science &Engineering from Sree Visvesvaraya Institute of Technology & Science, Mahabubnagar, Telangana,India.