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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Continuous User Identity Verification Based Secure Internet Services

G. Michael, Sundararajan.M, Arulselvi S

Asst. Professor, Department of Computer Science and Engineering, Bharath University, Chennai, India

Director, Research Center for Computing and Communication, Bharath University, Chennai, India

Co-Director, Research Center for Computing and Communication, Bharath University, Chennai, India

ABSTRACT: We explore the continuous user verification for the secure internet services using biometrics in the session management. We have used the novel biometric modality named "Facial Recognition" for continuous user authentication. Given a camera pointing towards the user, we develop real-time facial recognition algorithm (CMM-Correlation Matrix memories) to automatically extract facial recognition as frames patterns using FPS (frames per second) concept. Unlike the typical continuous biometrics such as keystroke dynamics (KD), Facial recognition provides reliable authentication with a short delay, while avoiding explicit key-logging. For one second 30 frames of user face reaction will be captured and a unique descriptor is extracted based on the shape and position of face, as well as their temporal dynamics in the photo frame sequence. We implement the continuous authentication in online banking for secure services.

KEYWORDS: Continuous authentication, user authentication, biometrics, CMM-Correlation Matrix Memories, FPS-Frames Per Second

I.INTRODUCTION

Secure user authentication is fundamental in most of modern ICT systems. User authentication systems are traditionally based on pairs of username and pass-word and verify the identity of the user only at login phase. No checks are per formed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user.

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 authentication, where username and password are replaced by bio-metric data. However, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially considering their possible application in the financial and banking sectors.

Such observations lead to arguing that a single authentication point and a single biometric data cannot guarantee a sufficient degree of security. In fact, similarly to traditional authentication processes which rely on username and password, biometric user authentication is typically formulated as a "single shot", providing 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 explicit logout from the user. This approach assumes that a single verification (at the beginning of the session) is sufficient, and that the identity of the user is constant during the whole session. For instance, we consider this simple scenario: a user has al-ready logged into a security-critical service, and then the user leaves the PC unattended in the work area for a while. This problem is even trickier in the context of mobile devices, often used in public and crowded environments, where the device itself can be lost or forcibly stolen while the user session is active, allowing impostors to impersonate

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily.

A basic solution is to use very short session timeouts and periodically request the user to input his/her credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users. To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal bio-metric continuous authentication are proposed, turning user verification into a continuous process rather than a onetime 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 credentials to be acquired transparently, i.e. without explicitly notifying the user or requiring his/her interaction, which is essential to guarantee better service usability. We present some examples of transparent acquisition of biometric data. Face can be acquired while the user is located in front of the camera, but not purposely for the acquisition of the biometric data; e.g., the user may be reading a textual SMS or watching a movie on the mobile phone. Voice can be acquired when the user speaks on the phone, or with other people nearby if the microphone always captures background. 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 approach differentiates from traditional authentication processes, where username/password are requested only once at login time or explicitly required at confirmation steps; such traditional authentication approaches impair usability for enhanced security, and offer no solutions against forgery or stealing of passwords.

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., smartphones, Desktop PCs or even biometric kiosks placed at the entrance of secure areas. De-pending on the preferences and requirements of the owner of the web service, the CASHMA authentication ser- vice can complement a traditional authentication service, or can replace it.

The approach we introduced in CASHMA for usable and highly secure user sessions is a continuous sequential (a single biometric modality at once is presented to the system) multi- modal biometric authentication proto-col, which adaptively computes and refreshes session timeouts on the basis of the trust put in the client. Such global trust is evaluated as a numeric value, computed by continuously evaluating the trust both in the user and the (biometric) subsystems used for acquiring biometric data. In the CASHMA context, each subsystem comprises 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 data transmission and management. Trust in the user is determined on the basis of frequency of updates of fresh biometric samples, while trust in each subsystem is computed on the basis of the quality and variety of sensors used for the acquisition of biometric samples, and on the risk of the subsystem to be intruded.

II. CONTINUOUS AUTHENTICATION

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 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 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.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

The work in proposes a multi-modal biometric con-tinuous 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,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 CASHMA assessment, the choice of ADVISE was mainly due to: i) its ability to model detailed adversary profiles, ii) the possibility to combine it with other stochastic formalisms as the Möbius multi-formalism and iii) the ability to define ad-hoc metrics for the system we were targeting.

2.1 Basic Definitions

In this section we introduce the basic definitions that are adopted in this paper. Given n unimodal biometric sub-systems Sk, with k= 1, 2, …, n that are able to decide independently on the authenticity of a user, the False Non-Match Rate, FNMRk, is the proportion of genuine comparisons that result in false non-matches. False non-match is the decision of non-match when comparing biometric samples that are from same biometric source (i.e., genuine comparison).It is the probability that the unimodal system Sk wrongly rejects a legitimate user. Conversely, the False Match Rate, FMRK, is the probability that the unimodal subsystem Sk makes a false match error i.e., it wrongly decides that a non legitimate user is instead a legitimate one (assuming a fault-free and attack-free operation).

Obviously, a false match error in a unimodal sys-tem would lead to authenticate a non legitimate user. To simplify the discussion but without losing the general applicability of the approach, hereafter we consider that each sensor allows acquiring only one biometric trait; e.g., having n sensors means that at most n biometric traits are used in our sequential multimodal biometric system. The subsystem trust level m(Sk, t) is the probability that the unimodal subsystem Sk at time t does not authenticate an impostor (a non-legitimate user) considering both the quality of the sensor (i.e., FMRk) and the risk that the sub-system is intruded.

The user trust level g(u, t) indicates the trust placed by the CASHMA authentication service in the user u at time t, i.e., the probability that the user u is a legitimate user just considering his behavior in terms of device utilization (e.g., time since last keystroke or other action) and the time since last acquisition of biometric data. The global trust level trust(u, t) describes the belief that at time t the user u in the system is actually a legitimate user, considering the combination of all subsystems trust levels m(Sk=1,…n, t) and of the user trust level g(u, t). The trust threshold gmin is a lower threshold on the glob-al trust level required by a specific web service; if the resulting global trust level at time t is smaller than gmin (i.e., g(u,t) < gmin), the user u is not allowed to access to the ser-vice. Otherwise if g(u,t) ≥ gmin the user u is authenticated and is granted access to the service.

III.THE CASHMA ARCHITECTURE

3.1 Overall View of the System

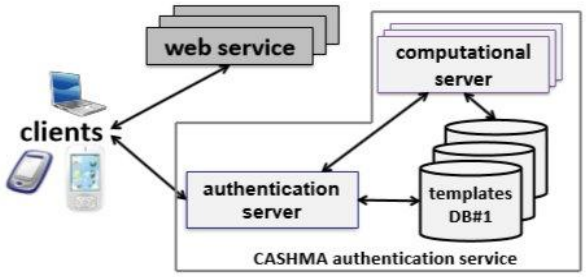
The overall system is composed of the CASHMA authentication service, the clients and the web services (Fig. 1), connected through communication channels. Each communication channel in Fig. 1 implements specific security measures which are not discussed here for brevity.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015



The CASHMA authentication service 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 en-rolled users, and iii) databases of templates that contain the biometric templates of the enrolled users (these are required for user authentication/verification). The web ser-vices are the various services that use the CASHMA authentication service and demand the authentication of en-rolled 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 ser-vice, expressing also their trust threshold. If the web ser-vices adopt the continuous authentication protocol, during the registration process they shall agree with the CASHMA registration office on values for parameters h, k and is used.

Finally, by clients we mean the users' devices (laptop and desktop PCs, smartphones, tablet, etc.) that 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 i) sensors to acquire the raw data, and ii) 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 compare the raw data with the stored biometric templates.

Transmitting raw data has been a design decision applied to the CASHMA system, to reduce to a minimum the dimension, intrusiveness and complexity of the application installed on the client device, although we are aware that the transmission of raw data may be restricted for example due to National legislations.

CASHMA includes countermeasures to protect the biometric data and to guarantee users' privacy, including policies and procedures for proper registration; protection of the acquired data during its transmission to the authentication and computational servers and its storage; robustness improvement of the algorithm for biometric verification. Privacy issues still exist due to the acquisition of data from the surrounding environment as for example voices of people nearby the CASHMA user, but are considered out of scope for this paper.

The continuous authentication protocol explored in this paper is independent from the selected architectural choices and can work with no differences if templates and feature sets are used instead of transmitting raw data, or independently from the set of adopted countermeasures.

3.2 Sample Application Scenario

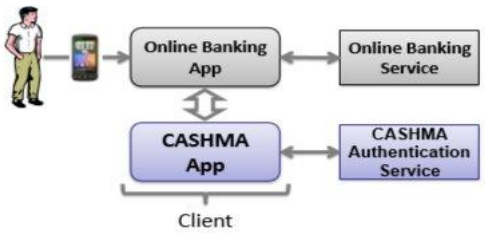
CASHMA can authenticate to web services, ranging from services with strict security requirements as online banking services to services with reduced security requirements as forums or social networks. Additionally, it can grant access to physical secure areas as a restricted zone in an airport, or a military zone (in such cases the authentication system can be supported by biometric kiosk placed at the entrance of the secure area). We explain the usage of the CASHMA authentication service by discussing the sample application scenario in Fig. 2 where a user u wants to log into an Online Banking service using a smartphone.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015



It is required that the user and the web service are en-rolled to the CASHMA authentication service. We assume that the user is using a smartphone where a CASHMA application is installed.

The smartphone contacts the Online Banking service, which replies requesting the client to contact the CASHMA authentication server and get an authentication certificate. Using the CASHMA application, the smartphone sends its unique identifier and biometric data to the authentication server for verification. The authentication server verifies the user identity, and grants the access if: i) it is enrolled in the CASHMA authentication service, ii) it has rights to access the Online Banking ser-vice and, iii) 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 bio-metric 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.

IV.CONCLUSION

We exploited the novel possibility introduced by biometrics to define a protocol for continuous authentication that improves security and usability of user session. The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data acquired transparently through monitoring in background the user's actions.

Some architectural design decisions of CASHMA are here discussed. First, the system exchanges raw data and not the features extracted from them or templates, while crypto-token approaches are not considered; as debated in Section 3.1, this is due to architectural decisions where the client is kept very simple. We remark that our proposed protocol works with no changes using features, templates or raw data. Second, privacy concerns should be ad-dressed considering National legislations. At present, our prototype only performs some checks on face recognition, where only one face (the biggest one rusting from the face detection phase directly on the client device) is considered for identity verification and the others deleted. Third, when data is acquired in an uncontrolled environment, the quality of biometric data could strongly de-pend on the surroundings. While performing a client-side quality analysis of the data acquired would be a reasonable approach to reduce computational burden on the server, and it is compatible with our objective of designing a protocol independent from quality ratings of images (we just consider a sensor trust), this goes against the CASHMA requirement of having a light client.

We discuss on usability of our proposed protocol. In our approach, the client device uses part of its sensors extensively through time, and transmits data on the Inter- net. This introduces problematic of battery consumption, which has not been quantified in this paper: as discussed in Section 7, we developed and exercised a prototype to verify the feasibility of the approach but a complete assessment of the solution through experimental evaluation is not reported. Also, the frequency of

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

the acquisition of biometric data is fundamental for the protocol usage; if biometric data are acquired too much sparingly, the protocol would be basically useless. This mostly depends on the profile of the client and consequently on his usage of the device. Summarizing, battery consumption and user profile may constitute limitations to our approach, which in the worst case may require to narrow the applicability of the solution to specific cases, for example only when accessing specific web sites and for a limited time window, or to grant access to restricted areas, These characterizations has not been investigated in this paper and constitute part of our future work.

It has to be noticed that the functions proposed for the evaluation of the session timeout are selected amongst a very large set of possible alternatives. Although in literature we could not identify comparable functions used in very similar contexts, we acknowledge that different functions may be identified, compared and preferred un-der specific conditions or users requirements; this analysis is left out as goes beyond the scope of the paper, which is the introduction of the continuous authentication approach for Internet services.

REFERENCES

[1] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli,
[2] Sathish Kumar M., Karrunakaran C.M., Vikram M., "Process facilitated enhancement of lipase production from germinated maize oil in Bacillus spp. using various feeding strategies", Australian Journal of Basic and Applied Sciences, ISSN : 1991-8178, 4(10) (2010) pp. 4958-4961.
[3] CASHMA - Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB 2005
[4] Kaliyamurthie K.P., Parameswari D., Udayakumar R., "QOS aware privacy preserving location monitoring in wireless sensor network", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4648-4652.
[5] L. Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Per- formance?," *Proc. AutoID'99*, Summit, NJ, pp. 59–64, 1999.
[6] Sharmila D., Muthusamy P., "Removal of heavy metal from industrial effluent using bio adsorbents (Camellia sinensis)", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) pp.10-13.
[7]S. Ojala, J. Keinanen, J. Skytta, "Wearable authentication device for transparent login in nomadic applications environment," *Proc. 2nd International Conference on Signals, Circuits and Systems (SCS 2008)*, pp. 1-6, 7-9 Nov. 2008 phase directly on the client device)
[8] Udayakumar R., Khanaa V., Saravanan T., Saritha G., "Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 16(12) (2013) pp.1781-1785.
[9] Kalaiselvi V.S., Prabhu K., Ramesh M., Venkatesan V., "The association of serum osteocalcin with the bone mineral density in post menopausal women",Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 7(5) (2013) pp.814-816.
[10] Kulanthaivel L., Srinivasan P., Shanmugam V., Periyasamy B.M., "Therapeutic efficacy of kaempferol against AFB1 induced experimental hepatocarcinogenesis with reference to lipid peroxidation, antioxidants and biotransformation enzymes", Biomedicine and Preventive Nutrition, ISSN : 2210-5239, 2(4) (2012) pp.252-259.
[11] Sangeetha Rajagurusamy, Analysis of Work study in An Automobile Company ,International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753 , pp 5622-5631,Vol. 2, Issue 10, October 2013.
[12] V.G.Vijaya,Analysis of Rigid Flange Couplings ,International Journal of Innovative Research in Science, Engineering and Technology ,ISSN: 2319-8753 , pp 7118-7126,Vol. 2, Issue 12, December 2013.
[13] V.G.Vijaya ,DESIGN OF HUMAN ASSIST SYSTEM FOR COMMUNICATION ,International Journal of P2P Network Trends and Technology(IJPTT),ISSN: 2319-8753 ,pp 3687-3693,Vol. 2, Issue 8, August 2013.
[14] V.G.Vijaya, V.Prabhakaran ,Design of Human Assist System for Communication ,International Journal of Innovative Research in Science, Engineering and Technology ,ISSN: 2249-2651,pp 30-35, Volume1 Issue3 Number1–Nov2011.
[15] V.Krishnasamy, R.Kalpana devi ,Isomorphous Salts with Abnormal Water Of Hydration ,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753 , pp 3500-3509,Vol. 2, Issue 8, August 2013.
[16] Veera Amudhan R ,Tracking People in Indoor Environments ,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753 , pp 15996-16003,Vol. 3, Issue 9, September 2014.