Continuous and Transparent User Identity Verification for Secure Internet Services using Bit-Exchange Algorithms

R.Bargavi[1], Venkat K Vishal[2]

[1] *Student, Computer science department ,Panimalar Engineering college,Tamilnadu India*
[2] *Student, Information technology department,* Meenakshi college of engineering,, *Tamilnadu,India*

ABSTRACT

Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. Emerging biometric solutions allow substituting username and password with biometric data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session. Additionally, the length of the session timeout may impact on the usability of the service and consequent client satisfaction. This paper explores promising alternatives offered by applying biometrics in the management of sessions. A secure protocol is defined 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 functional behavior of the protocol is illustrated through Matlab simulations, while model-based quantitative analysis is carried out to assess the ability of the protocol to contrast security attacks exercised by different kinds of attackers. Finally, the current prototype for PCs and Android smartphones is discussed.security properties is provided, showing its effectiveness and strong.

Keyword : *Security, web servers, mobile environments, authentication, architecture, protocols*

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. 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 time 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 is also susceptible for attack because the identity of the user is constant during the whole session. Suppose, here 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 the user session is active, allowing impostors to impersonate the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution .

2.PROBLEM AND OBJECTIVES

The main objective of this project is to encrypt users sensitive data when users payment processing takes place. This will ensure that the third party pos vendors or merchants cant able to see users personal data like card no ,cvv number etc . this will only be visible to bank admins where they either accept or deny the payments .

3. LITERATURE SURVEY

The introduction to security issues & its concern is described in previous section. In this literature we have studied earlier research papers related to conventional authentication systems it presents single time authentications of the user. The categorizations of security systems are depend on strength of attack and are classified into strong and weak. The summarizing study of earlier research is as follows

1. Primary approach is knowledge based identity for authentication of user involves is password that is what you know; Password contains single word, PIN (Personal Identification Number), Phrases that can be reserved secret for authentication. But this primary approach Knowledge based identity does not offer good solution it can be searched or guess by an attacker and they do not present security against repudiation [6].

2. Secondary approach is object based identity for authentication of user involves what you have is token; Token means a physical device which provides authentication that can be security tokens, access token, storage devices including passwords such as smart card or bank cards . The main disadvantage of Identity token can be lost or stolen and inconvenience and cost.

3.Payment schemes based on mobile devices are expected to supersede traditional electronic payment approaches in the next few years. However, current solutions are limited in that protocols require at least one of the two parties to be on-line, i.e. connected either to a trusted third party or to a shared database. Indeed, in cases where customer and vendor are persistently or intermittently disconnected from the network, any on-line payment is not possible. This paper introduces FORCE, a novel mobile micro payment approach where all involved parties can be fully off-line. Our solution improves over state-of-the-art approaches in terms of payment flexibility and security. In fact, FORCE relies solely on local data to perform the requested operations.Present paper describes FORCE architecture, components and protocols. Further, a thorough analysis of its functional and security properties is provided showing its effectiveness and viability.

4.PROPOSED SYSTEM:

1. This paper presents a new approach for user verification and session management that is applied in the context aware security by hierarchical multilevel architectures (CASHMA) system for secure biometric authentication on the Internet.

2. 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. Depending on the preferences and requirements of the owner of the web service, the CASHMA authentication service can complement a traditional authentication service, or can replace it.

3. Our continuous authentication approach is grounded on transparent acquisition of biometric data and on adaptive timeout management on the basis of the trust posed in the user and in the different subsystems used for authentication. The user session is open and secure despite possible idle activity of the user, while potential misuses are detected by continuously confirming the presence of the proper user.

5.ADVANTAGES OF PROPOSED SYSTEM:

1. Our approach does not require that the reaction to a user verification mismatch is executed by the user device (e.g., the logout procedure), but it is transparently handled by the CASHMA authentication service and the web services, which apply their own reaction procedures.

2. Provides a tradeoff between usability and security.

6.EXISTING SYSTEM:

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.

In existing, a multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer.

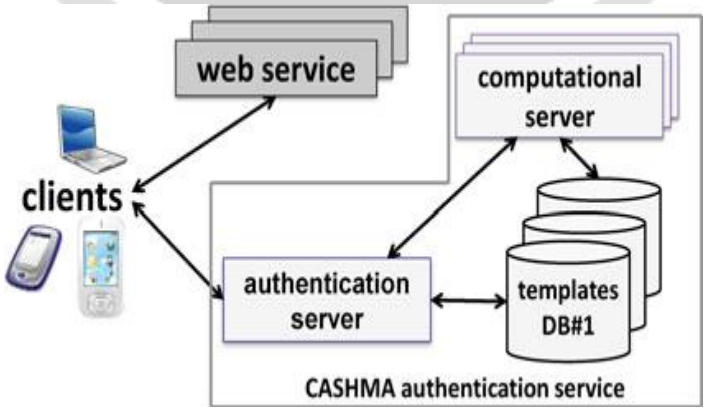
The work in another existing paper, proposes a multi-modal biometric continuous authentication solution for local access to high-security systems as ATMs, where the raw data acquired are weighted in the user verification process, based on i) type of the biometric traits and ii) time, since different 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.

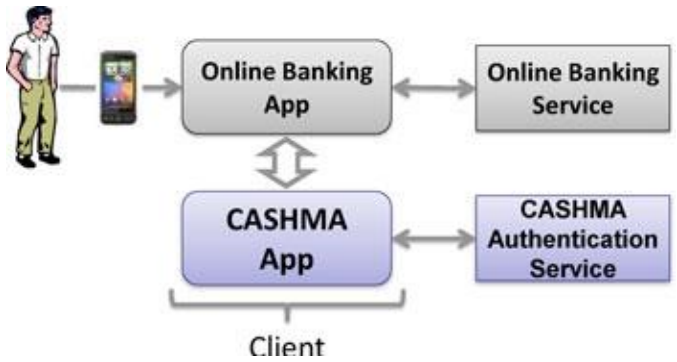
7.DISADVANTAGES OF EXISTING SYSTEM:

None of existing approaches supports continuous authentication.Emerging biometric solutions allow substituting username and password with biometric data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session.

8. SYSTEM DESIGN

The Internet exist (e.g., the BioID BaaS—Biometric Authentication as a Service is presented in 2011 as the first multi-biometric authentication service based on the Single Sign-On), to the authors' knowledge none of such approaches Our continuous authentication approach is grounded on transparent acquisition of biometric data and on adaptive timeout management on the basis of the trust posed in the user and in the different subsystems used for authentication.The user session is open and secure despite possible idle activity of the user, while potential misuses are detected by continuously confirming the presence of the proper user.Our continuous authentication protocol significantly differs from the work we surveyed in the biometric field as it operates in a very different context. In fact, it is integrated in a distributed architecture to realize a secure and usable authentication service, and it supports security-critical webservices accessible over the Internet. We remark that although some very recent initiatives for multi-modal biometric authentication over supports continuous authentication.Another major difference with works is that our approach does not require that the reaction to a user verification mismatch is executed by the user device (e.g.the logout procedure), but it is transparently handled by the CASHMA authentication service and the web services,which apply their own reaction procedures.The length of the session timeout in CASHMA is calculated according to the trust in the users and the biometric subsystems, and tailored on the security requirements of the service. This provides a tradeoff between usability and security. Although there are similarities with the overall objectives of the decay function in [8] and the approach for sequential multi-modal system in [22], the reference systems are significantly differen.. Consequently, different requirements in terms of data availability, frequency, quality,and security threats lead to different solutions





9.Basic Definitions:

In this section we introduce the basic definitions that are adopted in this paper. Given n unimodal biometric subsystems Sk, with k ¼ 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 thedecision of non-match when comparing biometric samples that are from same biometric source (i.e., genuine comparison)[10]. 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 [10], 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 system 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 mðSk; tÞ 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 subsystem 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 trustðu; tÞ 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 mðSk¼1;:::n; tÞ and of the user trust level g(u, t).The trust threshold gmin is a lower threshold on the global trust level required by a specific web service; if the resulting,global trust level at time t is smaller than gmin (i.e.,gðu; tÞ < gmin), the user u is not allowed to access to the service.Otherwise if g(u,t) _ gmin the user u is authenticated and is granted access to the service.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

System	:	Pentium IV 2.4 GHz.
Hard Disk	:	40 GB.
Floppy Drive	:	1.44 Mb.
Monitor	:	15 VGA Colour.
Mouse	:	Logitech.
Ram	:	512 Mb.

SOFTWARE REQUIREMENTS:

Operating system	:	Windows XP/7.
Coding Language	:	JAVA/J2EE
IDE	:	Netbeans 7.4
Database	:	MYSQL

IMPLEMENTATION DETAILS :

The algorithmic details & techniques used in system in experimentation are explained here. The different algorithmic strategies & technique is used.

Bit Exchanging Method:

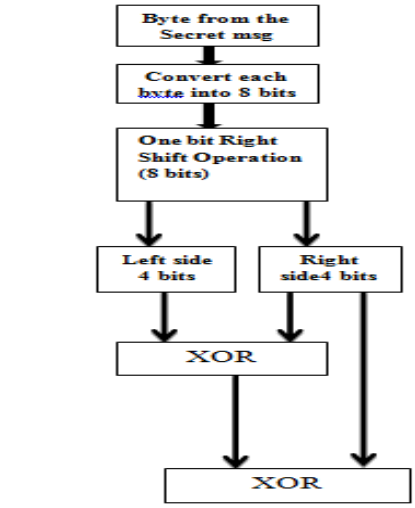
Encryption taken on the secret message file using simple bit shifting and XOR operation.

The bit exchange method is introduced for encrypting any file.

STEPS:-

1. Read one by one byte from the secret data and convert each byte to 8 bits. Then apply one bit right shift operation.

2. Divide the 8 bits into to blocks and then perform XOR operation with 4 bits on the left and 4 bits on the right side.



3. The same thing repeated for all bytes in the file

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 cripto-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 addressed 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 depend 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 Internet.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 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 websites and for a limited time window, or to grant access to restricted areas (see also the examples in Section 3.2). This characterization 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 under 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] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.

[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] 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.

BIOGRAPHY:

R.Bargavi is a B.E student from Computer Engineering Department, Panimalar Engineering college at Chennai Having interest in Cyber Security and cloud computing ,Database Management Systems .The Member of computer society of India.

Id:ravibharkavi@gmail.com

Venkat k vishal is a B.E student from B.tech information technology department ,Meenakshi college of engineering at Chennai having interest in networking and Cyber security, Artificial intelligence.

Id: Venkatkvishal@gmail.com