International Journal of Computer Sciences
July'2016 Issue
ISSN Number: 4142 3453

An Enhanced Security Method through Continous and Transparent Identity Verification for Secure Internet Services

B. Thanuja[1], Dr. A. Subramanyam[2]

[1]M.Tech.,PG Scholar, Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa

[2]Professor, Dept of CSE,Dean of Engineering,Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa

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 User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user. Nowadays, it becomes serious concern to provide more security to web services. So, secure user authentication is the fundamental task in security systems. Traditionally, most of the systems are based on pairs of username and password which verifies the identity of user only at login phase. Once the user is identified with username and password, no checks are performed further during working sessions. But emerging biometric solutions substitutes the username and password with biometric data of user. In such approach still single shot verification is less efficient because the identity of user is permanent during whole session. Hence, a basic solution is to use very short period of timeouts for each session and periodically request the user to input his credentials over and over. But this is not a proper solution because it heavily affects the service usability and ultimately the satisfaction of users. This paper explores the system for continuous authentication of user using his credentials such as biometric traits. The use of continuous biometric authentication system acquires credentials without explicitly notifying the user or requiring user interaction that is, transparently which is necessary to guarantee better performance and service usability

Index Terms- Web Security, Authentication, Continuous user verification, biometric authentication

1. 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.

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 [1]. 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

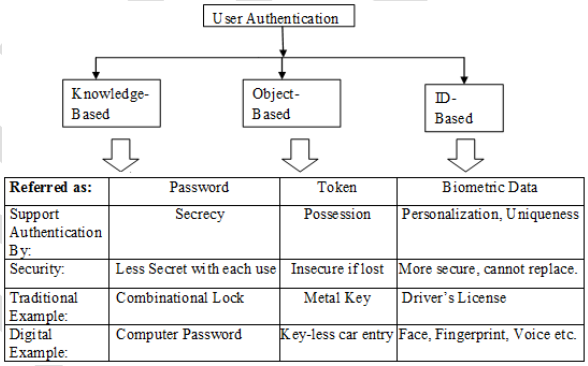
the user leaves the PC unattended in the work area for a while the user session is active, allowing impostors to impersonate the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution [1].

So, to timely identify misuses of computer resources and prevent that, solutions based on bio-metric continuous into a continuous process rather than a onetime authentication. Biometrics authentication can depend on multiple biometrics traits [1]. Finally, the use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user to enter data over and over, which provides guarantee of more security of system than traditional one.

II. RELATED WORK

Security systems and methods are often described as strong or weak. A strong system is one in which the cost of attack is greater than the potential gain to the attacker. Conversely, a weak system is one where the cost of attack is less than the potential gain. Authentication factors are grouped into these three categories: 1) what you know (e.g., password), 2) what you have (e.g., token), and 3) who you are (e.g., biometric). 2.1 Knowledge-Based ("what you know"): These are characterized by secrecy and includes password. The term password includes single words, phrases, and PINs (personal identification numbers) that are closely kept secrets used for authentication. But there are various vulnerabilities of password-based authentication schemes. The basic drawback of passwords is that memorable password can often be guessed or searched by an attacker and a long, random, changing password is difficult to remember. Also, each time it is shared for authentication, so it becomes less secret [2]. They do not provide good compromise detection, and they do not offer much defense against repudiation. 2.2 Object-Based ("what you have"):

They are characterized by physical possession or token. An identity token, security token, access token, or simply token, is a physical device provides authentication. This can be a secure storage device containing passwords, such as a bankcard, smart card [2]. A token can provide three advantages when combined with a password. One is that it can store or generate multiple passwords. Second advantage is that it provides compromise detection since its absence is observable. Third advantage is that it provides added protection against denial of service attacks. The two main disadvantages of a token are inconvenience and cost. There are also chances of lost or stolen token. But, there is a distinct advantage of a physical object used as an authenticator; if lost, the owner sees evidence of this and can act accordingly [2]. 2.3 ID-Based ("who you are"): They are characterized by uniqueness to one person. A driver's license, passport, etc., all belong in this category. So does a biometric, such as a fingerprint, face, voiceprint, eye scan, or signature. One advantage of a biometric is that it is less easily stolen than the other authenticators, so it provides a stronger defense against repudiation. For both ID documents and biometrics, the dominant security defense is that they are difficult to copy [2]. However, if a biometric is compromised or a document is lost, they are not as easily replaceable as passwords or tokens.



Referred as:	Password	Token	Biometric Data
Support Authentication By:	Secrecy	Possession	Personalization, Uniqueness
Security:	Less Secret with each use	Insecure if lost	More secure, cannot replace.
Traditional Example:	Combinational Lock	Metal Key	Driver's License
Digital Example:	Computer Password	Key-less car entry	Face, Fingerprint, Voice etc.

Figure 1: Authenticator Categories

A. Overview of Biometric

Biometrics is the term usually related with the usage of unique physiological characteristics as well as different features to identify an individual. However, biometrics after some time has a much wider relevance as computer interface becomes more real. A number of biometric data have been developed and are used to authenticate the person's legitimate identity [4]. The main idea is to make use of the special characteristics of a person to identify or to recognize him or her by using special characteristics such as face, fingerprint etc.[5].

B. Introduction of Facial Recognition

A facial recognition system is a computer application for automatically identifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems [6][7]. Facial recognition is a type of biometric software application which is used to identify a specific person in a digital image by analysing and comparing

patterns. The face recognition systems are widely used for security purposes but are increasingly being used in a variety of other applications. Facial face identification analyses facial attributes such as overall face structure, which includes the distance between the eyes, nose, mouth, and jaw edges.

C. Advantages and Disadvantages of Biometric Techniques

There are no biometric solutions will be total secure, but when compared to a user name and a password, biometrics may offer a higher level of security [8] [9]. Biometrics generally holds a set of advantages and disadvantages, as the table 2 below summarizes.

Advantages	Disadvantages
Positive Identification	Public Acceptance
You can't lose, forget, or share your biometric information.	Legal Issues
A biometric template is unique to the individual for whom it is created	Possible increase in hardware costs to current systems.
Rapid identification/authentication	May require large amounts of storage
Costs, in general, are decreasing	Privacy Concerns

Table 1: Advantage and disadvantage of Biometrics

Session management in distributed Internet services is traditionally based on username and password, and explicit logouts and timeouts that expire due to idle activity of the user. Biometric solutions allow substituting username and password with biometric data; e.g., a user may submit its fingerprint instead of the pair username-password. However a single verification step is still deemed sufficient and the identity of a user is considered immutable during the entire session. Additionally, the static length of the session timeout may impact on the usability of the service and consequent client satisfaction. 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

III.PROPOSED SYSTEM

The internet is a place that serves anyone connected to it. Its benefits come with the various drawbacks such as incomplete security and trust. Also, the existing authentication system has a number of security flaws. Hence, to detect and prevent from unauthorized access, it provides a solution which is based on biometric data of user and continuous authentication is proposed. Proposed system provides a new method for continuous user authentication that continuously collects biometric information. It turns user verification into continuous process rather than a onetime occurrence. Hence, proposed system provides an implementation of an efficient authentication system for secure internet services that provides continuous and transparent user identity verification using biometric traits.

B. Purpose

To study a system that will help to provide more security to web applications with the help of various biometric traits. The system will continuously authenticate user while ongoing session to provide a more security.

C. Objective

The objective of the system is to provide more security by authenticating user while using web services as well as to build a continuous and transparent user authentication system which gives better performance. As well as it provides mechanism to verify legitimate user identity continuously. Also the system helps to avoid fraudulent use of internet services by using biometric data.

D. System Architecture

The figure 2 illustrates idea about system architecture. Session management is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using timeouts. Hence, user authentication is typically formulated as a one-shot process. Once the user's identity has been verified, the system resources are available for a fixed period of time until the user logs out or exits the session. Here the system assumes that the identity of the user is constant during the complete session. For instance, we consider this simple scenario: a user has already logged into a security-critical service, and then the user leaves the PC unattended in the work area for a while, then also system continues to provide access to the resources that should be protected. This may be appropriate for low-security environments but can lead to session hijacking in which an attacker targets a post-authenticated session. Hence, Continuous authentication requires

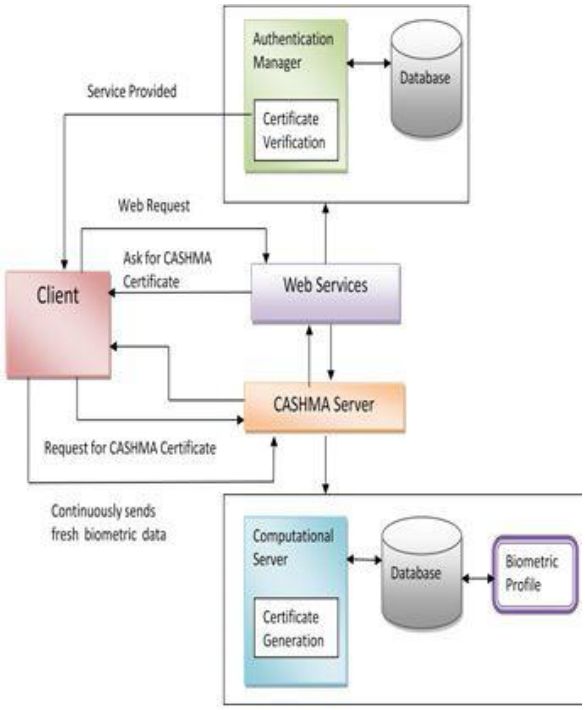


Fig 2. System Architecture

Continuous authentication system continuously checks the physical presence of legitimate user. There is again difference between Re-authentication and continuous authentication. Re-authentication is the traditional way to identify users and cannot identify that the user in an ongoing process. But use of biometric systems in a continuous authentication process is used to verify that the user is now a reality. Continuous biometrics improves the situation by making user authentication an ongoing process. Continuous authentication is proposed, because it turns user verification into a continuous process rather than a onetime occurrence 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; a continuous verification process is started based on biometrics. After the user performs login to the computer or to the web service, his entire interaction, through biometrics are continuously monitored to verify that it remains him. If the verification fails, the system reacts by locking the computer or freezing the user's processes.

Continuous authentication is used to detect misuse of computer resources and prevent that an unauthorized user maliciously replaces authorized one. Continuous Authentication is essential in online examinations where the user has to be continuously verified during the entire session. It can be used in many real time applications, when accessing a secure file or during the online banking transactions where there is need of highly secure continuous verification of the user. A number of biometric characteristics exist and are used in various applications. Each biometric has its own strengths and weaknesses, and the choice depends on the application.

IV. SECURITY EVALUATION

A complete analysis of the CASHMA system was carried out during the CASHMA project [2], complementing traditional security analysis techniques with techniques for quantitative security evaluation. Qualitative security analysis, having the objective to identify threats to CASHMA and select countermeasures, was guided by general and accepted schemas of biometric attacks and attack points as [10], [11], [12]. A quantitative security analysis of the whole CASHMA system was also performed [7]. As this paper focuses on the continuous authentication protocol rather than the CASHMA architecture, we briefly summarize the main threats to the system identified within the project (Section4.1), while the rest of this section (Section 4.2) focuses on the quantitative security assessment of the continuous authentication protocol.

A. Threats to the CASHMA System

Security threats to the CASHMA system have been analyzed both for the enrollment procedure (i.e., initial registration of a user within the system), and the authentication procedure itself. We report here only on authentication. The biometric system has been considered as de-composed in functions from [11]. For authentication, we considered collection of biometric traits, transmission of (raw) data, features extraction, matching function, template search and repository management, transmission of the matching score, decision function, communication of the recognition result (accept/reject decision). Several relevant threats exist for each function identified [10], [11], [12]. For brevity, we do not consider threats generic of ICT systems and not specific for biometrics (e.g., attacks aimed to Deny of Service, eavesdropping, man-in-the-middle, etc.). We thus mention the following. For the collection of biometric traits, we identified sensor spoofing and untrusted device, reuse of residuals to create fake biometric data, impersonation, mimicry and presentation of poor images (for face recognition). For the transmission of (raw) data, we selected fake digital bio-metric, where an attacker submits false digital biometric data.

For the features extraction, we considered insertion of imposter data, component replacement, override of feature extraction (the attacker is able to interfere with the extraction of the feature set), and exploitation of vulnerabilities of the extraction algorithm. For the

matching function, attacks we considered are insertion of imposter data, component replacement, guessing, and manipulation of match scores. For template search and repository management, all attacks considered are generic for repositories and not specific to biometric systems. For the trans-mission of the matching score, we considered manipulation of match score. For the decision function, we considered hill climbing (the attacker has access of the matching score, and iteratively submits modified data in an attempt to raise the resulting matching score), system parameter override/modification (the attacker has the possibility to change key parameters as system tolerances in feature matching), component replacement, decision manipulation. For the communication of recognition result, we considered only attacks typical of Internet communications. Countermeasures were selected appropriately for each function on the basis of the threats identified.

B. Quantitative Security Evaluation

Scenario and Measures of Interest: For the quantitative security evaluation of the proposed protocol we consider a mobile scenario, where a registered user uses the CASHMA service through a client in-stalled on a mobile device like a laptop, a smart phone or a similar device. The user may therefore lose the device, or equivalently leave it unattended for a time long enough for attackers to compromise it and obtain authentication. Moreover, the user may lose the control of the device (e.g. he/she may be forced to hand over it) while a session has already been established, thus reducing the effort needed by the attacker. In the considered scenario the system works with three biometric traits: voice, face, and finger-print. A security analysis on the first authentication per-formed to acquire the first certificate and open a secure session has been provided in [7].

V.RESULTS

Multiple users are created at a centralized location for the data owners and data users. We can see that either of the users can access the system once they login. The exchange of communication between data owners and data users is strictly through E-mail system which enables the system to be secured. Since the contents are encrypted and kept in the cloud, public viewing of these files is impossible. The files or contents can be viewed only after the consent of the data owners, after getting the secret key.

VI.CONCLUSION AND FUTURE

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. Therefore this paper attempts to provide a comprehensive survey of research on the underlying building blocks required to build a continuous biometric authentication system by choosing bio-metric. Continuous authentication verification with multi-modal biometrics improves security and usability of user session. This Authentication System provides a novel approach of continuously validating the identity of a user in real time through the use of biometrics traits. This system shows efficient use of biometrics to identify the legitimate user. Also, it continuously verifies the physical identity of legitimate user through their biometric data. This authentication is able to achieve a good balance between security and usability with continuous and transparent user verification. Hence, continuous authentication verification with biometrics improves security and usability of user session. In future research user satisfaction, security level, cost and maintenance, I think this is the important and main challenges. The next step would be to put more attention to the check level of security, also to do more testing in order to get more accurate results in research area.

.

REFERENCES

[1] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, PaoloLollini, Angelo Marguglio, Andrea Bondavalli,, "Continuous andtransparent user identity verification for secure internet services", IEEETransactions On Dependable And Secure Computing, December 2013.

[2] Lawrence O Gorman, "Comparing passwords, tokens, and biometrics foruser authentication", Proceedings of the IEEE, Vol. 91, No. 12, Dec.2003, pp. 2019-2040.

[3] Omaima N. A. AL-Allaf, "Review of face detection systems basedartificial neural networks algorithms", The International Journal ofMultimedia Its Applications (IJMA) Vol.6, No.1, February 2014.

[4] Robert Moskovitch et.al, "Identity theft, computers and behavioral biometrics", IEEE, 2009.

[5] A. Altinok and M. Turk, "Temporal integration for continuous multimodal biometrics, Multimodal User Authentication", pp. 11-12, 2003.

[6] S.Sudarvizhi, S.Sumathi, "Review on continuous authentication using multi modal biometrics, International Journal of Emerging Technology and Advanced Engineering", Volume 3, Special Issue 1, January 2013.
[7] D. M. Nicol, W. H. Sanders, K. S. Trivedi, "Model-based evaluation: from dependability to security", IEEE Trans. Dependable and Secure Computing, vol. 1 no. 1, pp. 4865, 2004.
[8] N. Mendes, A.A. Neto, J. Duraes, M. Vieira, H. Madeira, "Assessing and comparing security of web servers", IEEE International Symposiumon Dependable Computing (PRDC), pp. 313-322, 2008.
[9] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, "Biometrics: a grand challenge, Proceedings of International Conference
on Pattern Recognition", Cambridge, UK, Aug.2004.
[10] Sneha K. Patel, Dr. D. C. Joshi, "Mathematical Model Based Total Security System with Qualitative and Quantitative Data of Human", IntJr. of Mathematics Sciences Applications, Vol.3, No.1, January-June2013.
[11] Cassandra M. Carrillo, "Continuous Biometric Authentication ForAuthorized Aircraft Personnel: A ProposedDesign," Naval Postgraduate SchoolMonterey, CaliforniaThesis, June 2003.
[12] Harshal A. Kute, Prof. D. N. Rewadkar "Continuous User Identity Verification Using Biometric Traits for Secure Internet Services" Proc. CPGCON, March 2015.