International Conference on Recent Trends in Engineering Science and Technology (ICRTEST 2017) ISSN: 2321-8169
Volume: 5 Issue: 1(*Special Issue 21-22 January 2017*) 159 - 163

Advanced Secured Internet Services by Continuous and Transparent User ID Verification

[1]Amit Sontakey, [2]sunil Yadav, [3]Sonali Deshmukh, [4]Pushpa Tandekar
[1,2,3,4] IV[th] year, Dept. of Comp. Sci. & Engg., Shri Sai College of Engg. & Tech., Bhadrawati, Chandrapur

***Abstract*:** Now-a-days 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. 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.

Keywords:- *Web Security, Authentication, Continuous user verification, biometric authentication, credentials*

*****

I. INTRODUCTION

The usage of web based applications and technologies are growing day by day rapidly. There are many world events that have been directed our attention toward safety and security. Therefore security of such web-based applications is becoming important and necessary part of today's technology world. 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. Now days there are many devices based on biometric characteristics that are unique for every person. In the biometric technique, username and password is replaced by biometric data. Biometrics are the science and technology of determining and identifying the legitimate user identity based on physiological and behavioral traits which includes face recognition, retinal scans, fingerprint, voice recognition and keystroke dynamics [3]. The spreading use of biometric security systems increases their misuse, especially in banking and financial sectors. Biometric user authentication is formulated as a single shot verification which provides user verification only during login time. Once the identity of user is verified, the system resources are available to user for fixed period of time and the identity of user is permanent for entire session. Hence, this approach is also susceptible to attack. 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]. To detect the misuse of computer resources and prevent it from unauthorized user, one solution is provided which is called biometric continuous authentication, which turns the user verification into continuous authentication instead of one time authentication. The use of biometric authentication acquires user credentials without explicitly notifying the user to enter data over and over. This provides guarantee of more security to system than traditional one [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. LITERATURE SURVEY

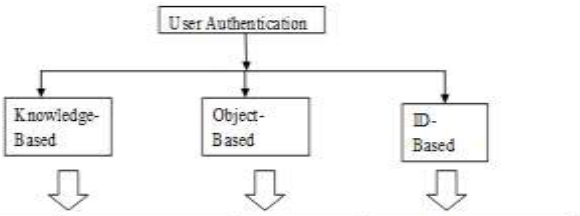
Security systems and methods are often described as strong or weak. A strong system is one in which the cost of attack is greater than the potential gain to the attacker. Conversely, a weak system is one where the cost of attack is less than the potential gain. Authentication factors are grouped into 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

Limitations of Existing System:

a. None of existing approaches supports continuous authentication.

b. 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.

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.

A. 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.

B. 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.

C. 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.

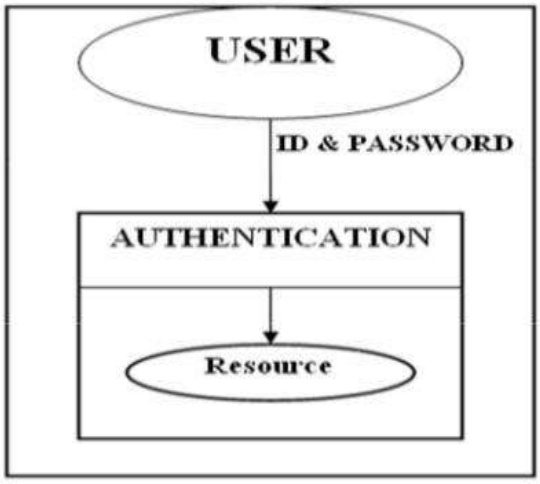


Figure 2 : Conventional Security System.

A. Conventional Authentication System

The conventional authentication system only requests the user to provide the authorized account and password to log into the system once they start to use a computer or a terminal. However, under this authentication frame work, the machine can only recognize the user's

identity from the login information. It lacks the information to know who is using it. The common drawback of the one-time authentication system, which people use in the daily life, is that when the user leaves the seat for a short break [9].

B. Continuous Authentication (CA) System

Most existing computer systems authenticate a user only at the initial log-in session. As a result, it is possible for another user, authorized or unauthorized, to access the system resources, with or without the permission of the signed-on user, until the initial user logs out. This can be a critical security flaw not only for high-security systems (e.g., the intellectual property office of a corporation) but also for low-security access control systems (e.g., personal computers in a general office environment). To deal with this problem, systems need methods for continuous user authentication where the signed-on user is continuously monitored and authenticated. Biometric authentication is useful for continuous authentication. For a continuous user authentication to be user friendly, passive authentication is desirable because the system should not require user active cooperation to authenticate users continuously [11]. In addition, a single biometric trait (unimodal technique) is not sufficient to authenticate a user continuously because the system sometimes cannot observe the biometric information. For example, the system will not be able to capture a user face image if he turns his head away from the monitor. In general, to address the limitations of single biometrics, using multimodal biometrics (combining two or more single biometrics, (e.g., face and finger print) is a good solution.

IV. SECURITY THROUGH BIOMETRICS

Biometrics is the science of establishing identity of an individual based on the physical, chemical or behavioral attributes of the person. The relevance of biometrics in modern society has been reinforced by the need for large scale identity management systems whose functionality relies on the accurate determination of an individual's identity in thecontext of several different applications. Some of biometric data is illustrated as follows.

A .Face Biometrics

A general face recognition system includes many steps 1. Face detection, 2. Feature extraction, and 3.face recognition. Face detection and recognition includes many complementary parts, each part is a complement to the other[10].

B. Keystroke Biometrics

Keystroke biometrics or monitoring keystroke dynamics is considered to be an effortless behavioural based method for authenticating users which employs the person's typing patterns for validating his identity [4]. Keystroke dynamics is "not what you type, but how you type." In this approach, the user types in text, as usual, without any kind of extra work to be done for authentication. Moreover, it only involves the user's own keyboard and no other external hardware.

C. Fingerprint Biometrics

Fingerprint identification is one of the most well- known and publicized biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration .The images below present examples of fingerprint features:

Figure 3: Other Fingerprint Characteristics .

Figure 4 : Minutiae

D. Voice Biometrics

Speech recognition is the process by which a computer identifies spoken words. Basically, it means talking to your computer, and having it correctly recognized what you are saying. Voice or speech recognition is the ability of a machine or program to receive and interpret dictation, or to understand and carry out spoken commands. For the voice recognition part the following steps have to be followed [5].

I) At first, we have to provide the user details as input in the form of voice asked by system.

II) The system will then generate a ".wav" file and the generated file will be saved in the database for future references.

III) At the time of log in by the user, user needs to provide the same information given at the time of registration and the system compares the recorded voice with the one saved

in database. If both match, user logs in successfully, otherwise not.

V. FINGERPRINT DETECTION AND RECOGNITION ALGORITHM

Fingerprints of each person is considered to be unique. Fingerprint detection and recognition is the most accepted biometric recognition method. Fingerprints have been used from long time for identifying persons. A good quality fingerprint contains 30 - 80 minutiae points. Fingerprints consist of a regular texture pattern composed of ridges and valleys[6]. These ridges are characterized by several land mark points, known as minutiae, which are mostly in the form of ridge endings and ridge bifurcations. The minutiae points is be unique to each finger, it is the collection of minutiae points in a fingerprint that is primarily employed for matching two fingerprints. There exists some gap between the ridges, called valleys. In a fingerprint, the dark lines of the image are called the ridges and the white area between the ridges is called valleys.

VI. CONTINUOUS AUTHENTICATION USING BIOMETRICS

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 [1]. Here the system assumes that the identity of the user is constant during the complete session [6]. If the user leaves 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. 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 multimodal 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 [7] [8]. The proposed approach assumes that first the user logs in using a strong authentication procedure; a continuous verification process is started based on multi-modal biometric. After the user performs login to the computer or to the web service, his entire interaction, through keyboard, mouse activities 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 [1] [7] [8]. Each biometric has its own strengths and weaknesses, and the choice depends on the application.

VII. CHALLENGES

Here we organized the fundamental barriers in Biometrics into four main categories: (I) accuracy (II) scale (III) security and (IV) privacy [10] [11].

I. Accuracy: The critical promise of the ideal biometrics is that when a biometric identifier sample is presented to the biometric system, it will offer the correct decision. Unlike password or token-based system, a practical biometric system does not make perfect match decisions and can make two basic types of errors: (I) *False Match:* the biometric system incorrectly declares a successful match between the input pattern and a Non-matching pattern in the database or the pattern associated with an incorrectly claimed identity. (II) *False Non-match:* the biometric system incorrectly declares failure of match between the input pattern and a matching pattern in the database or the pattern associated with the correctly claimed identity (verification) [11].

II. Scale: How does the number of identities in the enrolled database affect the speed and accuracy of the system? In the case of verification systems, the size of the database does not really matter since it essentially involves a 1:1 match, comparing one set of submitted samples to one set of enrollment records [11]. In the case of large scale identification and screening systems containing a total of N identities, sequentially performing N 1:1 match is not effective there is a need for efficiently scaling the system to control throughput and false-match error rates with an increase in the size of the database.

III. Security: The integrity of biometric systems is crucial. While there are a number of ways a perpetrator may attack a biometric system there are two very serious criticisms against biometric technology that have not been addressed satisfactorily: (I) biometrics are not secrets and (II) biometric patterns are not revocable. The first fact implies that the attacker has a ready knowledge of the information in the legitimate biometric identifier and, therefore, could fraudulently inject it into the biometric system to gain access [9] [11]. The second fact implies that when biometric identifiers have been "compromised", the legitimate user has no recourse to revoking the identifiers to switch to another set of uncompromised identifiers. We believe that the knowledge of biometric identifiers does not necessarily imply the ability of the attacker to inject the identifier measurements into the system. The challenge then is to design a secure biometric system that will accept only the legitimate presentation of the biometric identifiers without being fooled by the spoofed measurements injected into the system [11].

IV. Privacy: A reliable biometric system provides an irrefutable proof of identity of the person. The problem of designing information systems whose functionality is

verifiable at their deployed instantiation is very difficult. Perhaps, one needs to devise a system that meticulously records authentication decisions and the people who accessed the logged decisions using a biometric-based access control system. Such a system can automatically generate alarms to the users upon observing a suspicious pattern in the system administrator's access of users logs. One promising research direction may be biometric cryptosystems generation of cryptographic keys based on biometric samples. There are also radical approaches such as total transparency that attempt to solve the privacy issues in a very novel way. While one could stipulate some ingredients of the successful strategy, there are no satisfactory solutions on the horizon for this fundamental privacy problem [11].

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. 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", IEEE Transactions 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] Robert Moskovitch et.al, "Identity Theft, Computers and Behavioral Biometrics", IEEE, 2009.

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

[8] S.Sudarvizhi, S.Sumathi, "Review On Continuous Authentication Using Multimodal Biometrics", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Special Issue 1, January 2013.

[9] Pei-Wei Tsai,Muhammad Khurram Khan, Jeng-Shyang Pan,and Bin-Yih Liao. "Interactive Artificial Bee Colony Supported Passive Continuous Authentication System" IEEE SYSTEMS JOURNAL ,VOL. 8, NO. 2, JUNE 2014

[10] H. Bae and S. Kim, "Real-time face detection and recognition using hybrid information extracted from face space and facial features,"Image Vision Comput.,vol. 23, pp. 11811191, Jul. 2005.

[11] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics,"IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 687700, Apr. 2007.

[12] N. Mendes, A.A. Neto, J. Duraes, M. Vieira, H. Madeira, "*Assessing and Comparing Security of Web Servers*" IEEE International Symposium on Dependable Computing (PRDC), pp. 313-322, 2008.

[13] 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.