International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Continuous User Identity Verification Using Biometric Traits for Secure Internet Services

Harshal A. Kute[1], D. N. Rewadkar[2]

[1] Research Scholar, Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

[2] Professor, Head of Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

Abstract: ***Security of the web based services is become serious concern now a days. Secure user authentication is very important and fundamental in most of the systems 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. Emerging biometric solutions provides substituting username and password with biometric data during session establishment, but in such an approach still a single shot verification is less sufficient, and the identity of a user is considered permanent during the entire session. A basic solution is to use very short session timeouts and periodically request the user to input his credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users. 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. Finally, the use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user or requiring his interaction, which is essential to guarantee better service usability.***

Keywords: 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 [1]. 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 [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 already 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 authentication are proposed, that means turning user verification 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.

2. 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.

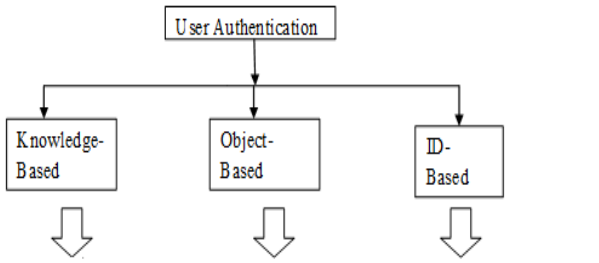
2.2 Object-Based ("what you have"):

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.

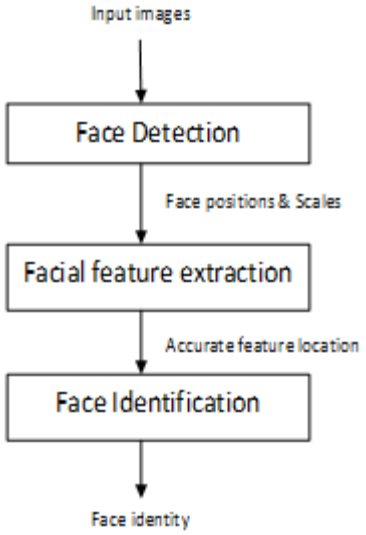
Figure 1: Authenticator Categories

3. Computer 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 the context of several different applications. Some of biometric data is illustrated as follows.

3.1 Face Biometrics

A general face recognition system includes many steps 1. Face detection, 2. Feature extraction, and 3.face recognition. These steps are shown in following figure.



Face detection and recognition includes many complementary parts, each part is a complement to the other. Depending on regular system each part can work individually. Face detection is a computer technology that is based on learning algorithms to allocate human faces in digital images [3].

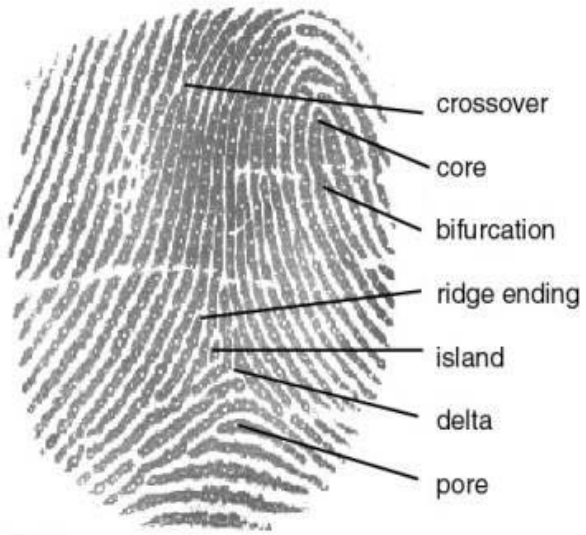
3.2 Keystroke Biometrics

Keystroke biometrics or monitoring keystroke dynamics is considered to be an effortless behavioral 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.

All keystroke dynamics studies involve conducting five main experiment parts in the following order: recruiting participants, requesting a typing task to be done by the Participants, collecting the timing data of keystrokes, obtaining timing features from the raw keystroke data, training the classifier using part of the keystroke data and using the other part for testing the classifier [4].

3.3 Fingerprint Scan Biometrics

Fingerprint identification is one of the most well-known and important biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated due to advancements in computing capabilities. 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.



3.4 Voice Biometrics

A voice biometric is a numerical model of the sound, pattern and rhythm of an individual's voice. A voice biometric or voice print is as unique to an individual as a finger or palm print. Any Authentication application that employs a voice channel during the Authentication session is able to add voice biometric authentication to the process for even higher levels of authentication and security. Voice verification technology uses the different characteristics of a person's voice to discriminate between speakers. Speech recognition allows providing input to an application with voice.

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. In the proposed system only voice will be interaction tool to a user with the system for registration and verification [5]. For the voice recognition part the following steps have to be followed.
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.

After successful log in, the set of questions from database appears on the screen which is read by system itself. And the user will speak out the answer as option A, B, C or D which goes to the database where it matches with the previously stored answer for comparison. Based on the comparison result, the system keeps record of the user's score. For correct matching, at the time of registration, system stores user voice for A, B, C and D. These files are compared for matching the questions answer later [5].

4. Continuous Authentication Using Biometrics (Proposed Work):

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.

5. Challenges

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

5.1 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].

5.2 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.

5.3 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].

5.4 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].

6. 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.

References

[1] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli,, "*Continuous and Transparent 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 for User 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 Based Artificial Neural Networks Algorithms*", The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.1, February 2014.
[4] Arwa Alsultan and Kevin Warwick, "*Keystroke Dynamics Authentication: A Survey of Free-text Methods*", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013.
[5] Dwijen Rudrapal, Smita Das, S. Debbarma, N. kar, N. Debbarma, "*Voice Recognition and Authentication as a Proficient Biometric Tool and its Application in Online Exam for P.H People*", International Journal of Computer Applications, Volume 39– No.12, February 2012.
[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] 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. 48–65, 2004.

[10] 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.
[11] 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.

Author Profile

Harshal A. Kute Research Scholar RMD Sinhgad School of Engineering, University of Pune. He has received B.E. in Information Technology from Information Technology department of Sinhgad College of Engineering from University of Pune, Pune (2013). Currently he is pursuing M.E. in Computer Engineering from RMD Sinhgad School of Engineering, Warje, Pune, University of Pune.

Prof. D. N. Rewadkar Prof. D. N. Rewadkar received M.E.Computer Technology, from S.R.T.M. University, Nanded. (2000). Currently he is working as an Associate Professor & Head the Department of Computer Engineering, in RMD Sinhgad Technical Institutes Campus, Warje, Pune. He was a Member of Board of Study (BOS) committee of S.R.T. Marathwada University, Nanded for Computer Science & Engineering. His area of interest is Traffic Engineering & Mobile Communication. He has 21 years of teaching experience.