RESEARCH ARTICLE OPEN ACCESS

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

Neethu T.D [1], Ayana Ajith [2]
PG Scholar [1], Asst.Professor [2]
Department of Computer Science and Engineering
Vidya Academy of Science and technology - Thrissur,
Kerala, India

**ABSTRACT**
Now a day's security of the web based services has become serious concern. Traditional authentication processes rely on username and password, formulated as a "single shot", providing user verification only during login phase .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. The active user allow impostors to impersonate the user and access the personal data and can be misused easily. 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 good solution. 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 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 :—*** Security, Continuous user verification, Biometric Authentication

## I. INTRODUCTION

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 [2]. Biometrics is the science and technology of determining identity based on physiological and behavioural traits. Biometrics includes retinal scans, finger and handprint recognition, and face recognition, handwriting analysis, voice recognition and Keyboard biometrics [1]. Also, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially in the financial and banking sectors.

Biometric user authentication is typically formulated as a "one-shot" process, providing verification of the user when a resource is requested (e.g., logging in to a computer system or accessing an ATM machine). 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 [2].

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 [2]. 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. SECURITY METHODS

Several security methods are available. Which are mainly based on authentication factor. 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).

***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 [1]. They do not provide good compromise detection, and they do not offer much defense against repudiation.

***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 [1]. 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.

***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. Biometrics, the dominant security defense is that they are difficult to copy [1]. However, if a biometric is compromised or a document is lost, they are not as easily replaceable as passwords or tokens.

### *A. Conventional Authentication System*

T he 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].

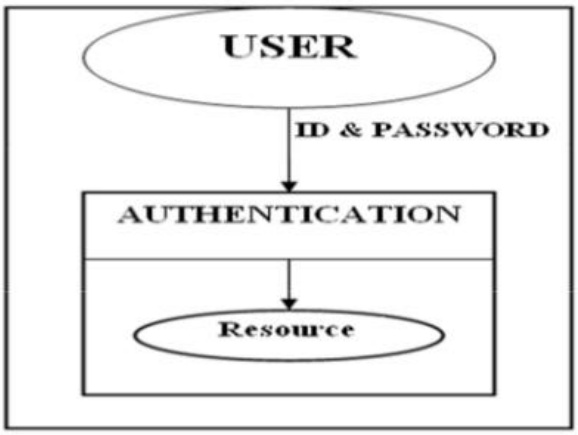


Figure 1 : Conventional Security System.

### *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.

## III. SECURITY THROUGH BIOMETRICS

Biometrics is the science of establishing identity of an individual based on the physical, chemical or behavioural 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.

***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:

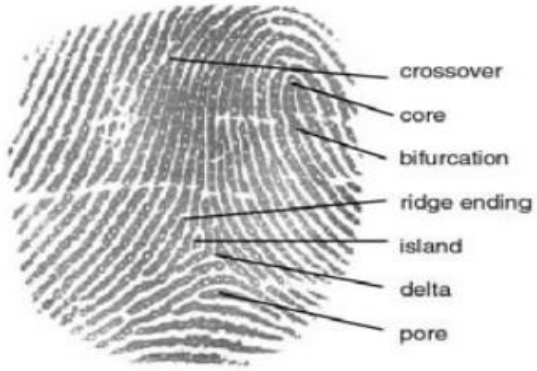


Figure 2: Other Fingerprint Characteristics .

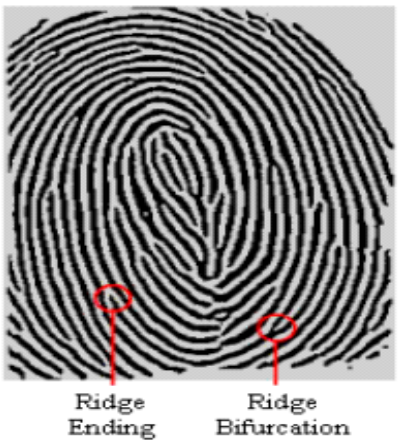


Figure 3 : Minutiae

***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.

## IV.CONTINUOUS USER IDENTITY VERIFICATION THROUGH BIOMETRICS

Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. Session time out may occur during unperformed working sessions or it expires when user is in idle activity period. 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 [2]. 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. User verification and session management that is applied in the CASHMA (Context Aware Security by Hierarchical Multilevel Architectures) system for secure biometric authentication on the Internet. CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services, and it is intended to be used from different client devices e.g., smart phones and Desktop PCs. 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 [2] [7] [8]. Each biometric has its own strengths and weaknesses, and the choice depends on the application.

## V. CONCLUSION

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] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040.

[2] 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.

[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] 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.