ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Continuous User Identity Verification Using Biometric Traits for Secure Internet Services

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

M.E. Student, Dept. of Computer Engineering, R. M. D. Sinhgad School of Engineering, Pune, India.[1]

HOD, Dept. of Computer Engineering, R. M. D. Sinhgad School of Engineering, Pune, India.[2]

ABSTRACT: 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.

KEYWORDS: Web Security, Authentication, Continuous userverification, biometric authentication.

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. Hence, now day's biometric techniques offer emerging secure and trusted user identity verification. Every biometrics refers that the identification of a person based on his or her physiological or behavioral characteristics. 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]. Also many of the biometric devices are based on the capturing and matching of biometric characteristics in order to produce a properpositive identification. 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].

DOI: 10.15680/IJIRCCE.2015. 0308136

II. LITERATURE REVIEW

System security and their methods always described in terms of weak or strong. If the cost of attack is larger than the potential gain to the attacker then it is called strong systems. Also, if the cost of attack is lesser than the potential gain to the attacker is called weak system. Therefore, factors regarding authentication categorized into following three types:

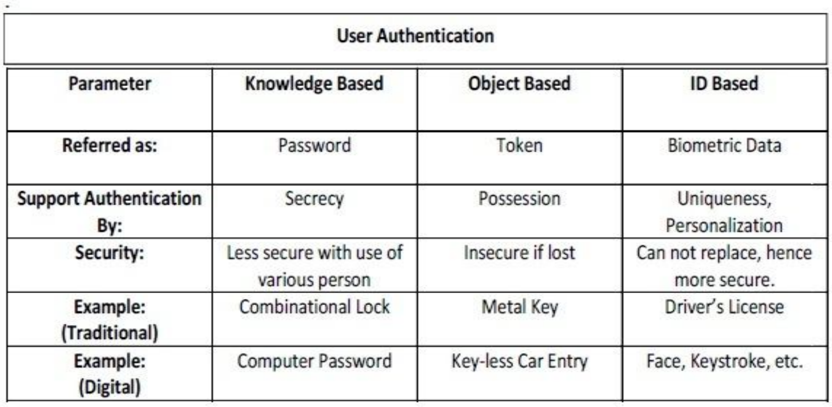
1) What you know i.e. knowledge-based (for example password), this includes secrecy and password. Passwords include single verification words or PINs (personal identification numbers) that are nearly kept private and used for user authentication. But a long, random and changing password is very hard to remember as well as to guess or search. Also, every time the password is being shared for the purpose of authentication, so it becomes less private [2].

2) What you have i.e. object-based (for example token), this approach is token based system such as identity token, security token, access token, or simply token, is a physical device provides authentication mechanism. It can store or generate multiple passwords. Also, it provides compromise detection since its absence is observable. It gives additional protection against denial of service attacks [2]. But, there are two main drawbacks of a token are inconvenience and cost. There are also chances of lost or stolen token.

3) Who you have i.e. ID-based (for example biometric), this approach is addressed by uniqueness to each person. Some examples are a driver’s license, passport etc. all belong in this category. Therefore it uses a biometric data, such as a fingerprint, face, voiceprint, eye scan, signature, and keystroke. The main advantage of a biometric data is that it is less easily stolen than the other authenticators; therefore it provides a stronger defense against repudiation as well as other security attacks [2].

We know that, user authentication is very important for computer and network system security. Currently, knowledge-based methods (for example, passwords) and token-based methods (for example, smart cards) are the most popular approaches. But, these methods have a number of security flaws such as passwords can be easily shared, stolen, and forgotten. Similarly, smart cards can be shared, stolen, duplicated, or lost. However, using biometric traits for authentication is more secure as it is unique to each person and cannot stolen or not able to replace. Table 1 describes the categories of authenticator.

Table 1: Categories of Authenticator



User Authentication

Parameter	Knowledge Based	Object Based	ID Based
Referred as:	Password	Token	Biometric Data
Support Authentication By:	Secrecy	Possession	Uniqueness, Personalization
Security:	Less secure with use of various person	Insecure if lost	Can not replace, hence more secure.
Example: (Traditional)	Combinational Lock	Metal Key	Driver’s License
Example: (Digital)	Computer Password	Key-less Car Entry	Face, Keystroke, etc.

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].

DOI: 10.15680/IJIRCCE.2015. 0308136

B. Introduction of Facial Recognition

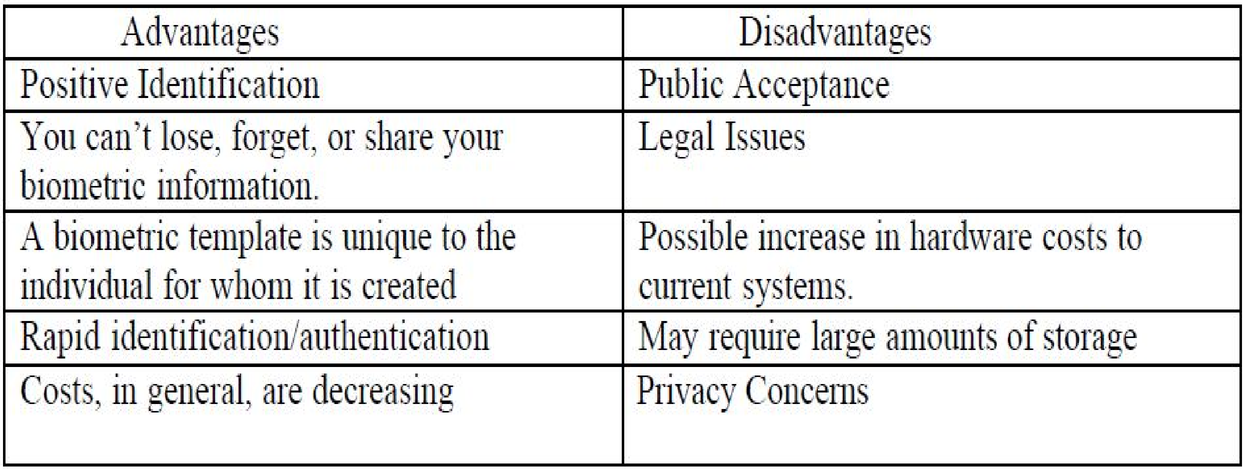
A facial recognition system is a computer application for automatically identifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems [6][7].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

Table 2: Advantage and disadvantage of Biometrics



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

III. Proposed System

A. Problem Statement

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 1 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.

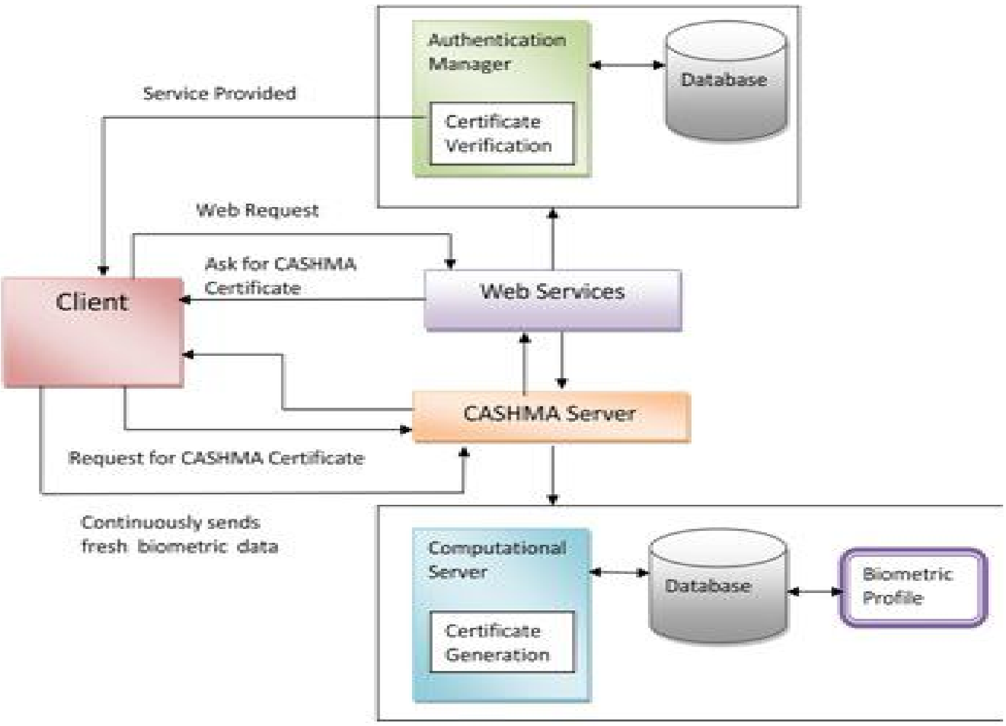


Fig 1. System Architecture

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.

E. Mathematical Model(PCA Algorithm with ANN)

Principal components analysis (PCA) is a method that is used to simplify a dataset. It is also based on an information theory approach that decomposes images into small set of feature images called “Eigen images”. These Eigen images are original training set of human images for principle component analysis. The algorithm of above technique (PCA) is described as follows:

Step 1: Construct the training set.
The initial step is to obtain a set I with S images. Each image is transformed into a vector of size N and placed into the set.

$$I = \{Z_1, Z_2, Z_3, \ldots\ldots\ldots, Z_s\}$$

Step 2: Calculate the mean.

The mean image μ from the set I is $\mu = \frac{1}{N}\sum_{i=1}^{s} Z_i$

Step 3: Calculate the covariance matrix.
The covariance matrix C is calculated in the following manner

$$C = \frac{1}{N} 1/s \sum_{i=1}^{s} (Z_i - \mu)(Z_i - \mu)^T$$

Step 4: Determine the Eigen vectors and Eigen values of the covariance matrix and choose the principal components. Find the eigenvectors of the covariance matrix C has dimension $N^2 \times N^2$ We can solve for N^2 dimensional eigenvectors in this case by first solving the Eigen vectors of n × n matrix.

$$\text{Let } \{(Zi - \mu)_1, (Zi - \mu)_2, \ldots\ldots.., (Zi - \mu)_n\} = A$$

$$(AA^T)V_i = \lambda_i V_i$$
$$A(A^TA)V_i = A(\lambda_i V_i)$$
$$(AA^T)(AV_i) = \lambda_i (AV_i)$$

Where $V_i$and $\lambda_i$are Eigen vectors and Eigen values of the $(n \times n)AA^T$ matrix respectively. The eigenvector of the larger AA^T matrix can be computed by calculating AV_i the eigenvectors are stored in descending order of Eigen values. They are shown in below:

$$U_i = AV_i = \sum_{k=1}^{n} V_k^i A_k$$

Now Eigen images are completed and “training” phase of the algorithm is finished. After the training set has been developed the further step is the classification of new input images.

Step 5: Convert the new image

The new image is converted into its Eigen image components using following computation

$$Wi = U_i^T (Z - \mu)$$

Where W = weight vector, Z= new input image, μ = mean image.

Every value would shows a weight and would be saved on a vector α . The weight vector α^T is given by,

$$\alpha^T = [W_1, W_2, \ldots., W_s]$$

Step 6: Calculate Euclidean Distance

$$\varepsilon_K = |\alpha - \alpha_K|^2$$

The new input image is consider to belong to a class ε_K if is lower than established threshold θ_K, then the human image is considered to be a known image. If the difference is above the given threshold, but lower than a second threshold, the image can be considered as an unknown image. If the input image is above these two thresholds, the image is determined NOT to be a image. If the image is found to be an unknown image, you could decide whether or not you want to add the image to your training set for future recognitions. You would have to repeat steps 1 to 6 to form this new image [10][11].

IV. RESULTS

This section describes result of face recognition accuracy. Figure 2 shows accuracy vs number of eigen faces. Here, we save Eigen faces of persons and then calculate its accuracy. It can be seen that the recognition accuracy (%) of a face recognition system increases with the increase in the number of face models per person. i.e. Recognition accuracy increases with increase in number training dataset (Eigen faces).

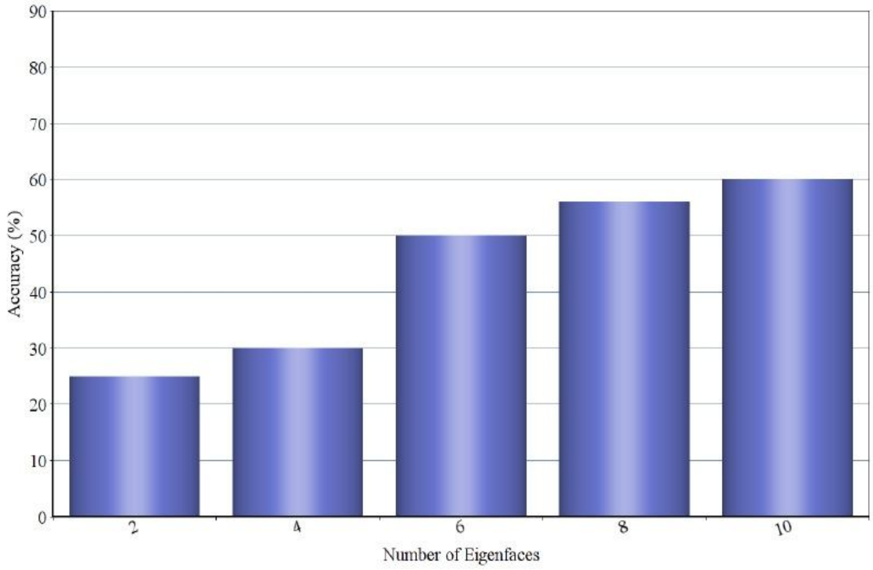


Figure 2: Accuracy vs number of Eigen faces

V. Conclusion and Future Work

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.

VI. Acknowledgment

The authors heartfelt thankful towards the people whose help and support was extremely useful to accomplish this dissertation work on toContinuous User Identity Verification Using Biometric Traits for Secure Internet Services. It is extremely honour to say sincerest regards to P.G. GuideProf.D. N. Rewadkar for his precious inputs, whole co-operation,direction, encouragement, suggestion and comment the during this dissertation work. Also grateful towards H.O.D., Director and the management. TheDissertation is based on research work in "*Continuous and transparent user identity verification for secure internet services*" by Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, AngeloMarguglio, Andrea Bondavalli, IEEE Transactions On Dependable And Secure Computing, December 2013.

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.

BIOGRAPHY

Harshal A. Kute Research Scholar RMD Sinhgad School of Engineering, University of Pune.Received B.E. degree in Information Technology from Information Technology department of Sinhgad College of Engineering from University of Pune, Pune (2013). Currently pursuing M.E. degree 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.