A Survey Paper on

Continuous Authentication by Multimodal Biometric

Nikita M. Agashe
Department of computer Science and Engineering
G.H. Raisoni College of Engineering,Nagpur, India

Prof. Sonali Nimbhorkar
Department of computer Science and Engineering
G.H. Raisoni College of Engineering, Nagpur,

Abstract- Recent wireless network systems authenticates the users only at the initial login session, and no verifications are performed during working sessions that are terminated by explicit logout or expire after idle activity period of users. Security of the web based applications is very important as there is increase in complexity of cyber attacks. Thus to ensure the authenticity of users during their entire active login period, a continuous verification is required. This paper considers continuous biometric authentication as an approach to eliminate this problem and also explores the promising alternatives which are offered by applying biometrics in the management of sessions to improve security and usability of users session.

Index terms - Verification, cyber attack, authentication, biometrics

1. INTRODUCTION

USER authentication is extremely very important for the computers and network system security. Recently , knowledge based methods (e.g., passwords) and token-based methods (e.g., smart cards) are the most popular approaches. However, these methods are having a number of security flaws. For example, passwords can be shared, stolen, and forgotten easily [1, 2].Similarly, the smart cards can be shared, stolen, duplicated, or may lost. To overcome these issues, a number of login authentication methods like textual, graphical passwords and biometric authentication have been utilized [3-4].

All of the above login methods share a common issue that is they authenticate at user only at the initial login session and do not re authenticate the users until the user logs out. In this case anyone can access the system resources if the initial user does not properly logout or the user leaves the workstation or system unattended to take a short break without logging out. So, for resolving this problem, the system must continuously monitor as well as authenticate the user after the initial login session. In order to accomplish this objective, we need to develop robust, reliable as well as user-friendly methods for the continuous user authentication. It is also desirable that the resulting system is having the good usability by authenticating a user without his active cooperation. Continuous Authentication is also very essential in online examinations where the user has to be continuously verified throughout the entire session. It can also be used in various real time applications. There is a highly need of secure continuous verification of user for accessing a

ISSN: 2278 – 1323

secure file or during the online banking transactions. There exist various number of biometric characteristics which are used in various applications. Each biometrics are having their own strengths and weaknesses, and also the choice depends on the application.

Some of the widely used hard biometrics are Face, Hand geometry, Fingerprint, Iris and Soft biometrics include Keystroke, Voice, Colour of the clothing, Facial color etc. A single biometric trait that is unimodal techniques are not sufficiently used to authenticate a user continuously because the system sometimes cannot observe the bio-metric information properly. The limitations of single biometrics can be overcome by using multimodal biometrics. Multimodal biometrics are the combination of two or more biometric traits for increasing systems security and reliability [1-2].

Multimodal has several advantages over unimodal. Combining the results obtained by different biometric traits by an effective fusion scheme can significantly improve the overall accuracy of the biometric system. Multimodal system increases the number of individuals that can enroll. It provides resistance against spoofing. Allows credentials to be acquired transparently i.e. without explicitly notifying the user to enter data again and again, which provides guarantee of more security of system than traditional one.

In continuous verification many situations can be observed like, a particular modality is missing or noisy observed samples etc [4]. For example, keystroke dynamics based detection is not available when user is reading, verification of face fails during user's non-frontal pose in front of the computer or by poor surrounding light. To overcome these problem a verification process by using multiple biometric traits are designed which brings in the possibility of different level of fusion and fusion strategies which are suitable for a continuous verification system.

1.1 Level of Fusion

In multimodal biometric systems information fusion are classified into two main categories: pre-classification fusion and post classification fusion. In the pre classification fusion information can be combined prior to applying any matching algorithm, and in the post classification fusion information can be combined after the application of the matching algorithm[6].

Pre classification fusion can be done in two levels that is in sensor level and feature level. Post classification fusion can be classified into four categories which is based on the level of fusion: classifier selection level, decision level, rank level and matching score level [6].

Table 1. State-of-Art Error rates associated with different Biometric systems [6]

Modality	Test Lable	FNMR	FMR
Fingerprint	FpVTE 2003	0.1 %	1 %
Fingerprint	FVC 2004	2 %	2 %
Face	FRVT 2002	10 %	1 %
Voice	NIST 2004	5-10 %	2-5 %
Iris	IRIRT 2005	0.99 %	0.94 %

Fusion at the decision level is consider as very rigid because of the availability of limited information and it is done by logical AND, OR majority voting rule. Fusion at the match score level is generally preferred because it is relatively very easy to access and combine the scores represented by the different modalities [7].

ISSN: 2278 – 1323

2. Literature Survey

Security systems and methods are described as strong or weak. A strong system is one in which the cost of attack is very greater than the potential gain to the attacker. Whereas, a weak system is one in which 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

These are characterized by the secrecy and also includes password. Password includes single words, phrases, and PINs (personal identification numbers) that are closely kept secrets used for authentication. But there are much vulnerability of password-based authentication schemes.

Memorable password can be guessed or searched by an attacker. Long and random, changing password is difficult to remember. They do not provide good compromise detection, and defense against repudiation.

2.2 Objects-Based

These are characterized by the physical possession or token. An identity token, security token, access token, or simply token are physical devices which provides authentication. This can be secure storage device having passwords like bankcard, smart card [2]. It stores or generate multiple passwords and provides compromise detection since its absence is observable. Also 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 [2].

2.3 ID-Based

These are characterized by uniqueness to one person like driver's license, passport, etc. Biometric are not easily stolen than other authenticators and provides a stronger defense against repudiation. [2]. However, if the biometric is compromised or a document is lost than they are not easily replaceable as passwords or tokens.

Method	Inatances	Properties
What you know	ID,Password, PINs,etc	Can be shared and forgotten
What you have	Cards,Keys, Badges, etc	Can be shared and duplicated
What you are	Fingerprint, Face, Iris,ETC	Not possible to shareand repudiate

Table 2: Existing User Authentication Methodology[2]

Some research studies have been reported on continuous authentication. Many of them use multimodal biometrics, but none of them can identify the user in the absence of biometric observation.

Sclera recognition method which can be achieve comparable accuracy (EER = 1.34% and 3.83%) with two iris recognition methods by using visible light acquired images (EER = 2.38% and 3.72%). In particular, iris patterns in dark eyes are very hard to extract under visible light illumination. Therefore, these results show that the sclera recognition have some advantages over iris recognition in the visible wavelengths [10].

They defined fingerprint which is most important biometric technology as it is more distinct, persistence and ease of acquisition. Fingerprint recognition is a process of determining whether two sets of fingerprint

ISSN: 2278 – 1323

ridge detail are from the same person [4]. There are many approaches used in different ways for fingerprint recognition. These types of approaches are categorized as minutiae or texture based recognition [8].

They characterizes the three basic criteria for continuous authentication by using hard biometric traits: 1) different reliability of the various modalities must be accounted for; 2) older biometric observations must be discounted to reflect their increasing uncertainty about continued presence of the legitimate users 3) the users authentication certainty is needs to be established at any point of time even when there is no observation of any of the biometric traits is available [4].

They defined Soft biometric trait's characteristics which provide information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate between any two individuals. These traits include gender, ethnicity, eye color, skin, hair, height, weight, and SMT (scars, marks, and tattoos) [13].

In this the keystroke biometric technique is proposed for continuous authentication. When compared to proposed method that is based on single biometric i.e. unimodal technique, so in the absence of keystroke data, the system is unable to authenticate the user [1].

Here presented Continuous authentication techniques using face, voice, and fingerprint. They claimed that continuous biometric authentication system are able to provide a meaningful estimate for authentication certainty at any given time, even in the absence of any of the biometric data.

They also presented a new temporal integration technique which satisfied this requirement. Each and every match score is modeled as a Gaussian random variable and the authentication uncertainty increases over time [11].

Continuous authentication technique presented by using face and fingerprint biometrics and used a mouse with an already built in fingerprint sensor, that made fingerprint authentication as a passive method for authentication [7][10].

This technique also had the same limitations as [11];when there is no biometric observations are available, authentication certainty must go down rapidly with the time in order to protect security, irrespective of whether user is in front of the console or not.

On comparison with the proposed method uses the same fingerprint biometric mouse for verification since the sclera is more accurate biometric than face.

Continuous authentication technique is proposed by using the face and fingerprint biometrics. Their system checks the identity of the users only on the basis of face recognition. If the authentication certainty of face recognition falls below a threshold value, then a new fingerprint acquisition is required [12][13].

In this continuous authentication method is proposed by using face and behavioral biometrics. Face trajectory and its pose used as behavioral features.

Behavioural features are not consistent throughout session and if it is soft biometric then are very less reliable when compared to proposed method where hard biometrics are used.

ISSN: 2278 – 1323

Biometrics	Advantages	Disadvantages
Fingerprint recognition	**Widely accepted and easy to use** **Good accuracy**	**Require additional hardware** **High quality image is not easy to obtain**
Face recognition	**Widely accepted and easy to use** **Non intrusive and good quality**	**Require additional hardware like camera** **Doesn't work well in poor lightening**
Iris/retina recognition	**Non intrusive** **High accuracy**	**Require additional hardware and high cost**
Hand recognition	**Easy to use** **Less intrusive**	**Require additional hardware like scanner** **Medium accuracy affected by hand injury**
Palm vein recognition	**High accuracy** **Commonly accepted**	**Require additional hardware like scanner** **Expensive to implement**
Voice recognition	**Widely accepted and easy to use** **Remote authenticate**	**Relatively low accuracy** **Does not work well under poor condition**
Signature recognition	**Widely accepted** **Non intrusive**	**Relatively low accuracy** **Require consistent writing trails**
Gait recognition	**Continuous authenticate** **Can work without user intervention**	**Low accuracy** **Performance is easily affected by terrain, injury, etc**
Behavior profiling	**Continuous authentication**	**Does not work well if users perform inconsistently**
Keystroke dynamics	**Continuous authentication**	**Does not work well if users perform inconsistently** **Accuracy is inconsistent**
Touch dynamics	**Continuous authentication** **Does not need additional hardware**	**Does not work well if users perform inconsistently** **Accuracy is inconsistent**

Table 2. Summary of Advantages and disadvantages of each biometric techniques [16]

4 . Challenges

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

4.1 Accuracy

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

4.2 Scale

How the number of identities in the enrolled database will affect the speed and accuracy of the system? In verification systems, size of the database does not really matters a lot since it is

ISSN: 2278 – 1323

essentially involves 1:1 match that is by comparing one set of submitted samples to another set of enrollment records [11]. In 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.

4.3 Security

The integrity of biometric systems are very crucial. There are many ways that a perpetrator may attack a biometric system. Basically there are two 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 states that the attacker has a ready knowledge of the information in the legitimate biometric identifier. Hence, could fraudulently inject it in the biometric system for gaining access [9] [11]. The second fact shows that when biometric identifiers have "compromised", the legitimate user don't have any recourse to revoking the identifiers to switch to another set of uncompromised identifiers. The challenge is to design such a secure biometric system that accept only legitimate presentation of the biometric identifiers without getting fooled by the spoofed measurements that injected into the system [11].

4.4 Privacy

A reliable biometric system provides an irrefutable proof of identity of the person. Problem of designing the information systems is very difficult whose functionality is verifiable at their deployed. So, there is a need to devise a system that will meticulously records the authentication decisions and the people who accessed the logged decisions by using a biometric based access control system. Such system can generate alarms to the users automatically by observing a suspicious pattern in the system administrator's access of users logs. There are also radical approaches like total transparency that attempt to solve privacy issues in a very novel way. While one could stipulate some ingredients of this successful strategy, there are no satisfactory solutions on the horizon for this fundamental privacy problem [15].

5. CONCLUSION

It is very realistic that initial one time login verification is inadequate to address the risk that are involved in post logged in session. Therefore this paper attempts to provide such a comprehensive survey of research on the underlying building blocks required to build a continuous biometric authentication system. The very first challenge is the choice of biometric. The challenge of unavailability of observation of one or more modalities at a particular time is addressed in the section on fusion of modalities. Also viewed various existing methods used for continuous authentication using multi modal biometrics. Continuous authentication is an emerging technique that reduce the error rates and to improve the accuracy and speed of the systems.

6. References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to bio-metric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1,pp. 4–20, Jan. 2014.

[2] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security", IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp.125–143, Jun. 2013.

[3] X. Suo, Y. Zhu, and G. Owen, "Graphical passwords: A survey", in Proc. Annu. Computer Security Applications, 2012, pp. 463–472

ISSN: 2278 – 1323

[4] Zhi Zhou, Student Member, IEEE, Eliza Yingzi Du, Senior Mem-ber, IEEE, N. Luke Thomas, and Edward J. Delp, Fellow, IEEE,"A New Human Identification Method: Sclera Recognition", IEEE transactions on systems, man, and cybernetics part a: systems and humans, vol. 42, no. 3, may 2012

[5] Sandeep Kumar,Terence Sim,Rajkumar Janakiraman and Shen Zhang,"Using Continuous Biometric Verification to Protect Inter-active Login Sessions", School of Computing,National University of singapore.

[6] Anil Jain,Kathik Nandakumar and Arun Ross,"score Normalisation in multimodal biometric systems",Pattern Recognition 38(2005)2270 2285.

[7] S. Zhang, R. Janakiraman, T. Sim and S. Kumar, "Continuous Verification Using Multimodal Biometrics", Proc.Second Int'l Conf. Biometrics, pp. 562-570, 2010.

[8] A. K. Jain, S. Prabhakar, and S. Chen, "Combining multiple Matchers for a High SecurityFingerprint Verification System", Pat-tern Recognition Letters, 20(11-13), 1371-1379,1999.

[9] A. K. Jain, S. C. Dass, and K. Nandakumar, "Soft biometric traits for personal recognition systems",LNCS, vol. 3072, pp. 731–738, 2004.

[10] 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. 687–700, Apr. 2011.

[11] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics",Proc. Workshop on Multimodal User Authentication, pp. 131-137, 2013.

[12] Antonia Azzini, Stefania Marrara, Roberto Sassi and Fabio Scotti, "A fuzzy approach to multimodal biometric continuous authentication", Fuzzy Optimal Decision Making, vol. 7, pp. 243-256, 2010.

[13] Antonia Azzini and Stefania Marrara, "Impostor Users Discovery Using a Multimodal Biometric Continuous Authentication" Fuzzy System,Lecture Notes In Artificial Intelligence, vol. 5178, Proceedings of the 12th International Conference on Knowledge-Based Intelligent Information and Engineering Systems, Part II, Section II,pp. 371-378, 2009.

[14] Hang-Bong Kang and Myung-Ho Ju, "Multi-modal Feature Integration for Secure Authentication", International Conference on Intelligent Computing, pp.1191-1200, 2012.

[15] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Andrea Bondavalli,, "Continuous and Transparent User Identity Verification for Secure Internet Services", IEEE Transactions On Dependable And Secure Computing, December 2013.

ISSN: 2278 – 1323