ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

A Survey on "Improving Security of Internet Services Using Continuous User Identity Verification"

Shafiya Taranum[1], Shabana Sultana [2]

P.G. Student, Department of Computer science and Engineering, NIE College,Mysore ,Karnataka, India[1]

Associate Professor, Department of Computer Science and Engineering, NIE College,Mysore, Karnataka, India[2]

ABSTRACT*:* Web services or internet services has become a popular way of communication and online transactions nowadays. These services are widely distributed and used by people all over the world. Security of internet services is a serious concern. So, secure user authentication and verification is the fundamental task in security systems. To achieve the security, better user authentication mechanisms are important in such systems. A traditional security system verifies the logged in user using the username and password at the time of user login only. Once the user has been successfully authenticated and verified with the username and password, then he/she is able to access the service and no further checks are done during the working sessions in which users are working. Emerging biometric solutions allows substituting biometric data instead of username and password during the login time or session establishment. But still a single verification is not sufficient, and the identity of a user is considered immutable or permanent during the entire session. Hence, a basic solution is to request the user periodically to input his/her credentials often and have very short period of timeouts for each session. This proposed system is defined for authentication through continuous/ regular user identification and verification. The biometric authentication in this work will allow users to acquire the credentials clearly. Clear user identity verification is essential for service usability and better performance.

KEYWORDS: Internet services, Security, Continuous user verification, Multimodal biometric authentication.

I. INTRODUCTION

Security of internet/web applications is a very serious concern, due to the increase in the frequency of cyber-attacks. Biometric techniques provide solution where username along with the password are replaced with the biometric data. However, the misuse of biometric data is continuously increasing, especially considering their possible application in the internet services. Such observations lead to conclusion that a single user verification point and a single biometric data cannot guarantee a sufficient degree of security. In fact, similarly to the conventional authentication processes which uses a pair of username and password, biometric user authentication is a "single shot", which provides user verification during login phase only where one or more biometric traits are required. Once the user has been verified as authorized user, the resources of system are available for a fixed period of time or resources are available until the user logout explicitly. This method assumes that single user verification at the beginning of the session is sufficient, and that the identity of the user is permanent or constant during the whole session.

For instance, consider a scenario where a user has been already logged into a web service, and then user leaves the system/any device unattended in the work area for a while. This problem is trickier in the context of mobile phones, which is often used in public places, where the device itself can be lost or stolen while the session of user is active, allowing impostors to access the personal data. In such cases, the services can be misused easily .Hence, A solution is to provide a very short session timeouts and ask the user periodically to input his/her credentials often [1].Solutions based on multi-modal biometric continuous authentication are proposed to timely detect misuses of system resources and prevent that an unauthorized user doesn't replaces an authorized one, where the user verification is a continuous process. Multiple biometrics traits are used for biometric authentication to avoid that a single biometric trait is forged.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

II. RELATED WORK

In this section, we have studied about the previous concepts related to the traditional authentication systems. These concepts focus only on the single shot authentication of the user. The system security methods are described as a strong or weak depending on the intensity of the attack. The factors regarding authentication are categorized into following 3 types,

- Knowledge-based (example password): What you know -It includes secrecy and password.
- Object-based (example token): What you have - It includes access token, security token ,identity token , or simply token,which is a physical device that provides authentication mechanism.[3]
- ID-based (example biometric): Who you have -It is addressed by uniqueness to each person. The biometric data cannot be stolen easily [5][6].

User authentication is very important for network system security. Currently, the most popular approaches such as knowledge-based methods and token-based methods [3] are used. But, these can be easilystolen,shared and forgotten. In a similar way smart cards can be, stolen, duplicated,shared or lost. However, biometric data cannot be stolen or able to replace. The biometric traits used for authentication are unique to each person and are more secure than other methods.

Overview of Biometric

Biometrics is the term which is unique ,measurable characteristic of human being which can be used to automatically recognize an individual and verify his/her identity. There are number of biometric data that are used to authenticate the person's legitimate identity.[5]. A person can be identified or recognized using the special characteristics such as face, fingerprint, voice etc.

- Face Biometrics:

Face biometrics includes detection and recognition of human faces from a digital image or a video frame from a video source [7][8].

A facial database is used to do this & selected facial features from the image are compared with database. Face Detection and recognition includes many complementary parts, each part is complement to one another.

- Keystroke Biometrics :

It is considered to be an effortless behavioural based method for authenticating users. It uses the person’s typing patterns for verifying his identity and it does not check what you type, but checks how you type.[4]

- Finger Print Scan Biometrics:

It is one of the most popular and important biometrics. They have been used for identification of people everywhere because of their uniqueness.

- Voice Biometrics:

It is the numerical modelling which consists of pattern, soundand rhythm of an individual’s voice. Voice is unique to an individual like a finger or palm print. This technology uses the different characteristics of a person's voice to differentiate between speakers. It is an interaction tool to a user with the system for registration and verification[9].

III. PROPOSED SYSTEM

The proposed work presents a new approach for verification of user and managing a session which allows secure multi modal biometric authentication while using internet applications. Continuous authentication is the process of authenticating the user identity through the complete working session of the logged in user. A multi-modal biometric verification system detects the physical presence of the logged in user to the system. The Proposed multimodal biometric authentication approach first lets the user to log in first using a strong authentication procedure and then based on multimodal biometrics a continuous verification process is started using various biometric data. On the failure of verification the computer automatically locks up. Hence, the proposed system provides an implementation of an

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

efficient authentication system for secure Internet services that provides continuous user identity verification using biometric traits.

The proposed approach uses "Context Aware Security by Hierarchical Multilevel Architectures (CASHMA[10]) Authentication System" .[1].As per the webService owner's requirement, the CASHMA authentication service can replace the traditional authentication service and can operate securely with any kind of internet service. It can also operate with the services having high security Needs such as online banking services. It can be accessible from different client devices, like Smartphone's, Desktop PCs etc. kept at the entrance of secure areas.

In the proposed approach, multimodal biometric authentication is done by fingerprint verification, face recognition and checking OTP. The physical presence of user is checked continuously by using multimodal biometric authentication.

Face Detection and Recognition is done using EmguCV.EmguCV is a cross platform ,Net wrapper to the OpenCV image processing library .It Allows OpenCV functions to be called from .NET compatible languages such as, VC++, C#, VB etc. The Viola-Jones algorithm is used for face detection because it is the easiest face detection method which is supported by

EmguCV and has proven to return great results. A face detector called Cascade Classifier/Detector that has been trained on thousands and thousands of human faces (face detection is a subject under machine learning) using this algorithm.

Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. It is one of many forms of biometrics used to identify an individual and verify their identity. Optical sensors are mainly used in fingerprint acquisition system. The sensors are of highly acceptable accuracy and high efficiency. To extract a minutia or uniquefeatures of fingerprint, To extract a minutia a three step approach is used such as, I) pre-processing stage II) minutia extraction stage III) post-processing stage.

A one-time password (OTP) is a password which is valid only for one transaction or one login session on the digital device or on a computer system. A number of shortcomings that are associated with static or traditional password-based authentication can be avoided by using OTP .The most important advantage that of OTPs is that, they are not vulnerable to replay attacks, in contrast to static passwords. OTP is based on the algorithm HMAC SHA. The HMAC SHA is generally used to perform authentication by challenge response. This algorithm is not an encryption algorithm but it is a hashing algorithm which transforms a set of bytes to another set of bytes. It is not reversible algorithm which means that you cannot use the result to go back to the source. .

IV. CONCLUSION AND FUTURE WORK

The proposed multimodal biometric Authentication System provides a novel approach of continuously verifying the identity of a user in real time through the use of biometrics traits. This proposed system shows efficient use of biometrics to identify the legitimate use and it continuously verifies the physical identity of the logged in user through their biometric data. This authentication is able to achieve a good balance between usability and security with continuous and clear user verification.

Hence, multimodal continuous biometric authentication verification improves usability and security of user session. In future research user satisfaction, security level, cost and maintenance is the important and main challenges. In the next step more attention to be paid to check level of security, also to do more testing in order to get more accurate results in research area.

V.ACKNOWLEDGMENT

The authors heartfelt thankful towards the people whose help and support was extremely useful to accomplish this dissertation work on to improving security of internet services using continuous user identity verification. It is extremely honour to say sincerest regards to P.G. GuideProf.Shabana Sultana for her precious inputs, whole cooperation, direction, encouragement, suggestion and comment the during this dissertation work. TheDissertation is based on research work in "Continuous and transparent useridentity verification for secure internet services" by Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, and Andrea Bondavalli, Member, IEEE,May/June 2015.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

REFERENCES

1. Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, PaoloLollini, Angelo Marguglio, Andrea Bondavalli,, "Continuous and transparent user identity verification for secure internet services", IEEETransactions On Dependable And Secure Computing,May/July 2015.
2. 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.
3. Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040.
4. ArwaAlsultan 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. 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.
6. Anil K. Jain, SharathPankanti, SalilPrabhakar, Lin Hong, Arun Ross, James L. Wayman, "Biometrics: a grand challenge, Proceedings of International Conference on Pattern Recognition", Cambridge, UK, Aug.2004
7. 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.
8. 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.
9. DwijenRudrapal, 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.
10. CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.
11. S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," Proc.21st Ann. Computer Security Applications Conf. (ACSAC '05), pp. 441-450, 2005.
12. T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.
13. A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.