IJIRMET

ISSN (Online): 2456-0448

International Journal Of Innovative Research In Management, Engineering And Technology

Vol. 1, Issue 2, March 2016

User Identity Verification For Secure Internet Banking System

[1]Mr.S.Sekar, [2]N.Nihal, [3]S.Prakash, [4]P.R.Prasaanth kumar, [5]V.Suresh

[1] Asst.Professor, Dept of Information Technology, SRM Valliammai Engineering College.

[2] [3] [4] [5]Students, Dept of Information Technology, SRM Valliammai Engineering College.

***Abstract**: Timeouts and session management in internet services were usually based on user name and password. The logout mechanisms of user session expiration were also calculated traditionally. The biometric solutions make a substitute for username and password with biometric data, but it is still not sufficient for user verification. The length of the session timeout will have greater impact on client satisfaction and service quality. This makes user identity immutable. This paper provides promising alternatives by using biometrics in session management. This is accomplished by using a secure protocol for authentication through a unique type of continuous user verification. The protocol calculates adaptive timeout based on the biometric data and its frequency that is transparently acquired from the user*.

Keywords: biometrics, continuous authentication, security, session.

I. INTRODUCTION

In most of the modern ICT system secure user authentication is a fundamental unit. Username and password are the traditionally based authentication service provided till now. Checking identities are not performed during working sessions and are terminated by logouts after an idle activity period of the user.

The cyber attacks have been increasing in a serious concern. This is resolved by the usage of biometric technique that offers solution for secure and trusted identity authentication where the biometric data replaces the username and password. However rapid spreading usage of biometric techniques is growing along with their misuses especially in financial and banking sector. In such a point we come to a conclusion that a safe authentication and a single biometric data cannot provide guarantee for sufficient degree of security.

Biometric usage works similar to the traditional username and password login phase. The system resource is available only for a specific time when the user identity has been verified and authenticated. The logout mechanism starts up after the specified time for the user. For instance, considering a simple scenario: a critical service has been requested by the server who has already logged in and then the user moves away from the PC leaving it unattended in the work area for a while. This problem is more complex in the context of the mobile phones, which are often used in crowded environment where the device itself may be forcibly stolen or lost when the user session is active. This allows intruders to impersonate the user and access his personal data. In these scenarios user data can be misused easily. Primary solution is to use very short session timeout and request the client to input her credential over a periodic time interval.

One of the solutions is to detect the misuses of computers data from an unauthorized user which is based on multi model biometric continuous authentication that terms user verification as a continuous process rather than one time usage.

This paper presents a new approach for user authentication management of session by using Fast Matching and Additive Colour Mixing Algorithm (FMACM) system for secure biometric services on the internet. FMACM is able to securely operate with all clients of web services. Example: Smart Phones and Desktop User.

In the fast growing world, banking is a necessity which in turn consumes a lot of time from the busy schedule of the client. Usage of ATM or paying bill by paper check and mailing them out and check-book management are all considered to be time consuming. Online banking automates many of these processes, saving money and time. The goal for this project is to develop an user friendly secure internet banking application. This application will be build using Java Server Page (JSP) and SQL server as database.

For face detection we use Haar classifier[6] for face detection**.** Jaffre and Joly[7] for localizing body and face**.**

II. EXISTING SYSTEM AND ITS CHALLENGES:

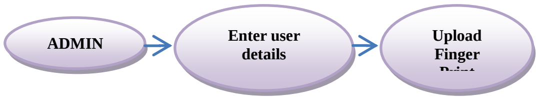
The user session would be open despite of idle activity of the user which may lead to misuse of the user session in public before the traditional logout mechanism could take place. Earlier keystroke data and user talking environment were captured for identifying user presence and ideal activity. But this current system heavily pulls down the service usability and leads to ultimate dissatisfaction of the user.

Novelty

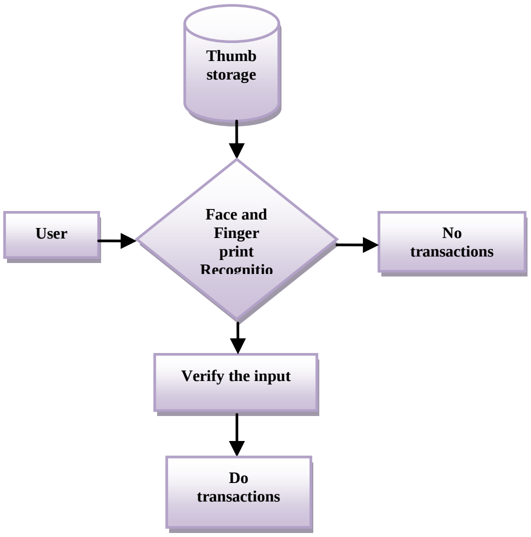
The overall system is grounded to provide highly secure user identity verification and maintain a continuous transparent verification throughout the session. The length of the session has to be computed in such a manner that user session is verified transparently. For user identity verification we provide fingerprint authentication and for continuous authentication we enable webcam to monitor the physical presence of the user. If suspicious motion is detected in the background, a fingerprint authentication is requested inorder to continue the session.

III. DATA FLOW DIAGRAM

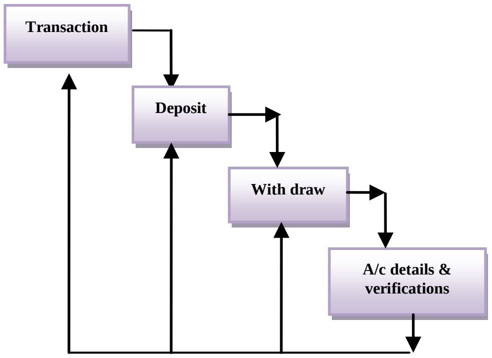
STEP 0:



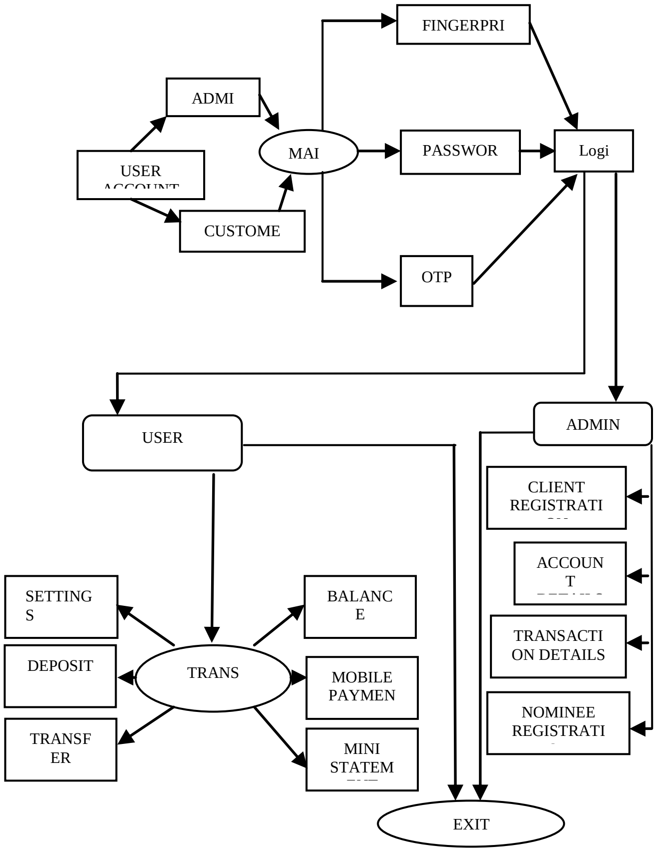
STEP 1:



STEP 2:



IV. SYSTEM FLOW DIAGRAM:



V. CONCLUSION

This user identity verification for secure internet banking system would provide an efficient entry level authentication and continuous verification transparently without affecting the session of the user. Thus traditional logout mechanism could be overcome by performing continuous authentication throughout the session. In future, this system could also be implemented over Smart phones -containing inbuilt fingerprint scanner and camera so that it could be easier and secure for customer to perform banking.

REFERENCE

[1] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini Angelo Marguglio, and Andrea Bondavalli, Member, IEEE -Continuous and Transparent User Identity Verification for Secure Internet Services.
[2] L. Hong, A.Jain, and S.Pankanti, “Can Multibiometrics Improve Performance?” Proc. Workshop on Automatic Identification Advances Technologies (AutoID `99) Summit, pp.59-64-1999.
[3] T. Sim, S.Zhang, R. Janakiraman and S.Kumar, “Continuos Verification Using Multimodal Biometrics, “IEEE Trans. Pattern Analysis and Machine Intelligence, vol.29, no. 4, pp. 687-700, Apr. 2007.
[4] S. Ojala, J.Keinanen, and J. Skytta, “Wearable Authentication Device for Transparent Login in Nomadic Applications Environment,”Proc. Second Int`l Conf. Signals, Circuits and Systems (SCS `08), pp. 1-6, Nov. 2008.
[5] BioID “Biometric Authentication as a Service(Baas),”BioID Press Release, https://www.bioid.com, Mar. 2011.
[6] Gael Jaffre and Philippe Joly, “Costume: A New Feature for Automatic Video Content Indexing,” Proceedings of RIAO2004, pp. 314-325, 2004.
[7] Rainer Lienhart and Jochen Maydt, “An Extended Set of Haar-like Features for Rapid Object Detection,” Proceedings of the 2002 IEEE International Conference on Image Processing, vol.1, pp. 900-903, 2002.