International Journal of Science Engineering and Advance Technology

Improve the Security and Usability of User Session using Continuous Authentication Protocol

M.V.Vinaya Nagini, CH.Prasada Rao
M. Tech Scholar, Associate Professor,
Dept. of Computer Science & Engineering, Aditya Engineering College,
Surampalem, AP, India, JNTU Kakinada.
vinayanagini31@gmail.com , prasadarao.chatla@aec.edu.in

***Abstract*—**Session organization of distributed web applications is usually depends on textual passwords and biometric verification at the starting of session, but here single authentication is happening. In this the problem is client identity is not verifying during the whole session. To overcome this problem a new approach continuous authentication protocol and the architecture CASHMA (context aware security by hierarchical multilevel architecture) are proposed for user verification. The advantage of the proposed system is to increase usability and security of session with biometric data. Experimental studies have been implemented using java.

Keywords—***Security; web servers; mobile environments; authentication***

I. INTRODUCTION

Web application security is serious issue because there is a lot of increase in cyber attacks. Biometric solutions in [2] offer solution for secure authentication. Here biometric process is replaced in the place of textual passwords. How ever increasing the biometric usage, the misuse also increasing parallel in banking sectors .At the staring of the session, the biometric authentication is not sufficient to provide the high security [7].In addition the time out period of the session may affect the usability of services. Once the client verification process is completed then the system services are available for the client at a certain amount of time or until client logged out. Here there is a problem, if the client using the services by logged into the system and leaves the work place for a certain amount of time, there may be a chance for attacker to hack the resources easily because the session is alive [5]. In [5] continuous authentication, the system verifies whether the client is authorized or not. Here if verification fails then the system will be locked and the client process will be delayed.

II. CONTINUOUS AUTHENTICATION

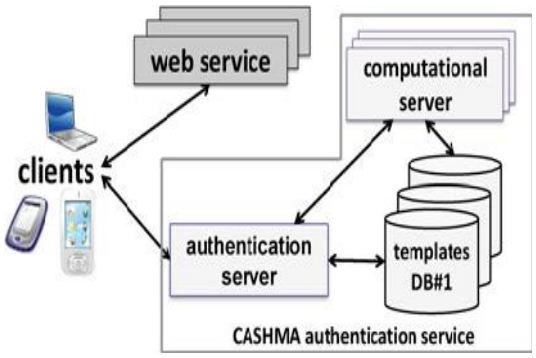
Continuous authentication come into existence because when the client signs into the services using strong authentication process and leaves the work area and then the attacker will hack our services. In [5], the system will continuously verify the client present at the work area. If the failure occurs at the verification time then the process will automatically lock up the services. In [3] wearable devices are present for continuous client authentication .In this client can transparently login through wireless communication.

III. PROPOSED APPROACH

To provide secure biometric verification on the web the CASHMA has been proposed. It provides high security for the services like internet banking and can be applicable for various types of user devices. CASHMA will acquire the biometric data transparently (e.g. key strokes) and logged out the system, if the system is idle for a certain amount of time. By checking the client with biometric data continuously mistreatments can be reduced.

IV. ARCHITECTURE

The architecture of CASHMA is shown below.



This architecture contains three components: Authentication server, Computational server and Database. The Authentication server is used for client interaction, Computational server compares the biometric data with the registered clients and database contains of biometric samples of registered clients. If the client verification has been completed successfully, then the web services can be accessed by the client. When the user verification fails for certain attempts, then the

CASHMA will automatically logged out without the user interference.

In this paper, there are three different trust levels.

Subsystem Trust level: In this level, the unimodal subsystem does not allow the unauthorized user by considering the quality of biometric data.

User trust level: In this level, the CASHMA authentication server verifies the client by considering the device utilization and the time at last acquiring of biometric samples.

Global trust level: At a particular time, the system checks whether the client is authorized or not based on previous two levels.

The *trust threshold* g_{min} is calculated by considering the lower threshold based on global trust level which is required to the specific web service.

If user trust level is greater than or equal to trust threshold (g_{min}), then the client is allowed to use the services.

V. CASHMA CERTIFICATE

This CASHMA certificate is generated by the authentication server and sends to the client when verification completed successfully. This certificate consists of sequence number, time stamp and session time out.

VI. PROPOSED METHDOLOGY

CONTINUOUS Authentication Protocol:

This proposed protocol requires a multi model biometric system to perform the authentication of the client. By using this protocol the client continuously and transparently collects and transmits the user identity to the server for accessing web service. This protocol will create and maintain the user session by adjusting the time out to provide the continuous authentication.

This protocol consists of two phases; initial phase and maintenance phase. In initial phase, the authentication of the client is done and creates the session. In maintenance phase the session time out will be updated and user verification process will be done.

Steps for Initial Phase:

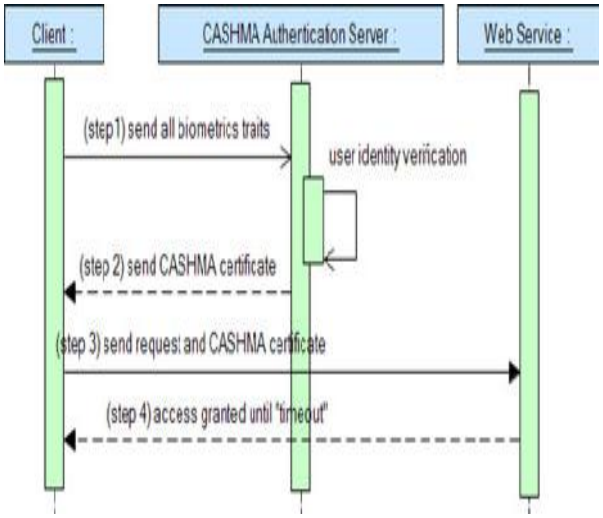
Step1: client sends biometric traits to CASHMA authentication server.

Step2: user verified by authentication server.

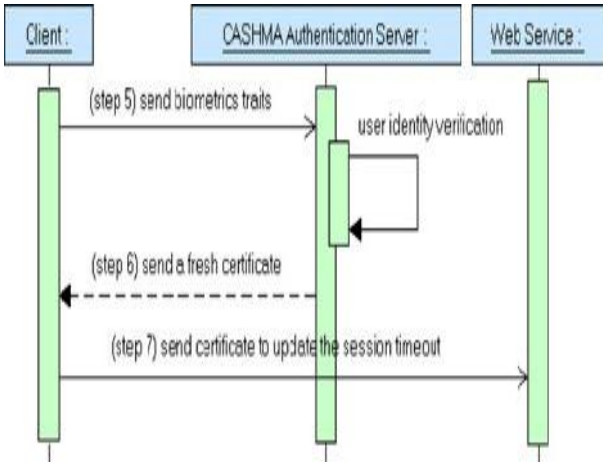
Step3: sending CASHMA certificate to user

Step4: user sending CASHMA certificate request to web service.

Step5: web service gives access to user until timeout.



Steps for Maintenance phase:



Step5: user sends biometric traits to authentication server.

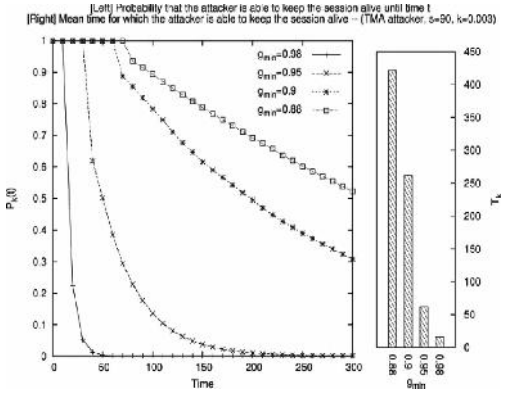
Step6: user verified by authentication server.

Step7: sending new certificate to user by authentication server.

Step8: user sending updated certificate and new time out session to web service.

VII. RESULTS

Technology master individual (TMA) who has the high technological skills, low resources and hide himself from the client.



By increasing the trust threshold $g_{min,}$ the TMA attacks T_k will be reduced. This will happen due to reducing the initial time out of the session and by having the less time, the attacker can't perform the required attack steps.

VIII. CONCLUSION

In this paper the continuous authentication protocol is used to verify the client continuously and transparently using biometric data. Indirectly it is providing the security and usability for the client session. By using CASHMA the TMA attackers will reduce without hacking the resources. The attacker will not be alive for a long time due to continuous authentication.

References

[1] CASHMA-Context Aware Security by Hierarchical MultilevelArchitectures, MIUR FIRB, 2005.

[2] U. Uludag and A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622-633,2004.

[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable AuthenticationDevice for Transparent Login in Nomadic Applications Environment,"Proc. Second Int'l Conf. Signals, Circuits and Systems(SCS '08), pp. 1-6, Nov. 2008.

[4] A.K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Informationm Forensics and Security, vol. 1, no. 2, pp. 125-143, June 2006.

[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "ContinuousVerification Using Multimodal Biometrics," IEEE Trans. PatternAnalysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr.2007.

[6] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina,"Quantitative Security Evaluation of a Multi-Biometric AuthenticationSystem," Proc. Int'l Conf. Computer Safety, Reliability andSecurity, pp. 209-221, 2012.

[7] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using ContinuousBiometric Verification to Protect Interactive Login Sessions,"Proc. 21st Ann. Computer Security Applications Conf. (ACSAC '05),pp. 441-450, 2005.