ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 9, September 2016

Enhanced CASHMA for Dynamic User Identity and Secure Authentication Over ICT Systems

A. Nabiha Karishma[1], S. Vasundara[2]
[1]M.Tech, Dept of CSE, JNTUA, AP, India.
[2]Professor, Dept of CSE, JNTUA, AP, India.

***Abstract*— In distributed internet environments, the sessions are managed conventionally by applying username and password inorder to access any web application. Sessions are terminated using the logout gimmicks. To an extent the security attacks have been defended using the biometric protocol. In combination to the traditional security framework . This paper predominantly focuses on a new methodology for user identification and for managing sessions that is oppressed in the Context Aware Security for Hierarchical Multilevel Architecture for secure biometric authentication over the internet. CASHMA is capable of working with any kind of web service eg. Banking system. The protocol computes dynamic timeouts on the groundwork of the trust display within the user activity and within the quality and sort of biometric knowledge gained transparently through auditing in background the user's biometric knowledge gained transparently through auditing in background the user's actions.**

Index Terms—**Continuous Authentication, Security, user identity, OTP**

I.INTRODUCTION

The preliminary trait of the modern ICT systems is to bypass secure user authentication. The verification of the user being unique are habitually based on username and a secret password provided only at login session of the application.. The sessions are kept immutable once the user character is verified. The unavoidable issue of the present technological environments is "security" as there is an immense increase in the density and ramification of the cyber attacks.

The proportion of security using single verification point and single biometric attribute is estimated to be insufficient. The 'single shot' authentication indulges user validation, only during login phase i.e. at the start of the web application. Once the client's character has been checked, the framework assets are accessible for a settled timeframe then again until unequivocal logout from the client.

This methodology presume that a solitary check is adequate, and the character of the client is in a steady state throughout the entire session. For an instance, A client has signed into a security-basic administration, and after that the client leaves the computer unattended in the work area intermittently.

This issue is even trickier with regards to cell phones, frequently utilized as a part of open what's more, swarmed situations, where the gadget itself can be lost or coercively stolen while the client session is dynamic, permitting impostors to mimic the client and get to entirely individual information. In such cases, the administrations where the clients are confirmed can be abused effortlessly [2] . An essential arrangement is to utilize short session timeouts and intermittently demand the client to information his/her certifications over also, over, however this is not at all a definitive solution as it degrades the user satisfaction. The use of multi biometrics can improve the performance of the system being built, using finger prints, face recognitions,voice recognitions can vigorously enhance the security [4].

II.RELATED WORK

The paper that helped in this work is Andrea Ceccarelli's user identity verification for secure internet services [1]. The work in his paper focused on how user's identity traits are acquired relatively during the authentication process. The trust inputted to the system by the user during the login phase and how operations can be carried out effectively. The main scenarios employed in user identity are

1. Subsystem trust level m(Sk,t) - the probability that the single subsystem Sk at time t does not authenticate an illegitimate user. This trust level enables the system to check the verified user.

2. User trust level g(u,t) - the trust used by the CASHMA authentication service in the user u at time t. This trust level provides the user with a level of confidence so as to connect to the application.

3. Global trust level (u,t) -the belief that at time t,user u in the system is actually a legitimate user. The operations being done in the system are performed by the legitimate user.

4. Trust threshold gmin - is a lower outset on the global trust level required by a specific web service.

A. Quantitative Security Evaluation of a Multi-Biometric Authentication System:

Biometric validation frameworks check the personality of clients by depending on their unmistakable characteristics, similar to unique mark, face, iris, signature, voice, and so on. Biometrics is ordinarily seen as a solid verification technique; vulnerabilities exist, and security angles ought to be stakingly considered, particularly when it is embraced to guard the access to applications controlling basic frameworks[3]. A quantitative security assessment of the CASHMA multi biometric validation framework is played out, evaluating the security gave by various framework designs against aggressors with various capacities.

The assessment is performed utilizing the ADVISE demonstrating formalism, a formalism for security assessment that broadens assault. It permits to join data on the framework, the assailant, and the measurements which are important to deliver quantitative results. The results gave a valuable knowledge on the security offered to the distinctive framework designs, and to latch on the scenarios in order to cope up with the model security dangers and counter measures in genuine situations.

B. Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform:

Current ICT schemas are described by expanding prerequisites of unwavering quality, security, execution, accessibility, flexibility. A pertinent issue that is to be considered is that the scalability of system is proportional to the number of users using the application. consequently requiring a discreet proportion of assets[5]. Besides, new security issues to be confronted emerge by manifesting applications and information to the Internet, in this manner requiring a heedful investigation of potential dangers and the recognizable proof of more grounded security instruments to be actualized, which may deliver a gloomy impact on framework execution and adaptability properties.

The paper exhibits a model-based assessment of adaptability and security compact of the multi-administration electronic stage, by assessing how the presentation of security components may prompt a debasement of execution properties. The assessment scrutinizes the openness stage, an electronic stage giving distinctive sort of administrations, to various classifications of clients.

The assessment goes for recognizing the bottlenecks of the framework, under various setups, and follow-up the issues of security countermeasures which were distinguished by an intensive danger examination action beforehand did on the objective framework. The demonstrating action has been done utilizing the Stochastic Activity Networks (SANs) formalism, making full utilization of its qualities of measured quality and reusability. The examination model is acknowledged through the creation of an arrangement of predefined format models, which encourages the development of the general framework model, and the assessment of various setup by making them in various ways.

C. Attacks on Biometric Systems: A Case Study in Fingerprints

Disregarding various points of interest of biometrics-based individual validation frameworks over customary security frameworks considering the token or learning, they are defenseless against assaults that can diminish their security significantly. In this paper, the domain of a solo finger impression biometric framework are schemed[6]. An assault framework that uses a slope climbing methodology to blend the objective layouts and assess its achievability with broad trial results led on a huge solo finger impression database. A few measures that can be applied to diminish the likelihood of such assaults and their consequences are likewise displayed. The use of wearable devices for security can also decrease the threats to the application that is transparently logging into the system[10].

III.PROPOSED WORK

The proposed enhancement to continuous authentication protocol provides multiple layers of security and authentication to the cashma system by continuously monitoring the activities of the client log[8]. The CASHMA architecture includes:

1.CASHMA authentication server – which collaborates with the clients and all the operations done in the application are carried out effectively by monitoring the activities of different user groups.

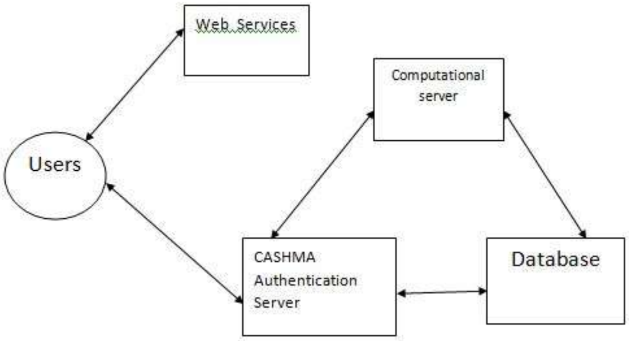
2. Computational servers - the biometric data of the enrolled users is verified by these servers, it gives the optimum results to the authentication server so that it can eventually identify the legitimate users

3. Client - users or consumers who need to access the application so as to perform their desired operations.

4. Database – collection of biometric templates of the enlisted users

5. Web service - system designed for interoperable machine to machine operation over a network.

I



CASHMA Architecture

CASHMA incorporates countermeasures to ensure the biometric information and to ensure client's security of the procured information amid its transmission to the authentication and computational servers and its repositories [9]. The multilayered architecture of the system enforces the surveillance at a high impact. The client data is well safeguarded from the imposter[7]. With the advent of the adaptive session timeouts into the system the user is able to perform the transactions competently.

Let's say if the user has logged into the system and if he is busy at a phone call, keeping the system in idle mode it is a great threat to the usability of the system as any hacker can sense the details of the user and misuses the same. The proposed system overcomes this scenario by dynamically changing the sessions. Say, if the user has previously took 60 seconds in order to perform the transaction then the cashma server updates the session time in its system and handle the logout session if the system is idle for more than 60 seconds. One time password is also generated in order to mantle security. This way security to the system is much to a greater impact.

IV. SYSTEM EVALUATION

The implementation of the enhanced cashma system initiates with the user procuring the registration by entering his credentials to the system. A biometric mechanism is availed as the second layer of security. An email is sent to the registered recipe nt with the details of the passwords i.e. the account and transaction password. Every bit of operation is accommodated with an email to the client.

The user in order to perform operations of his account, logins into the banking application with his account password and the biometric impression, the CASHMA authentication server will check the details if or whether the client is legitimate or illegitimate then grants access to the concerned application. The client is able to modify his passwords and can alter his biometric as per his needs. The client, so as to transfer money, has to add a beneficial pertaining to inter or intra bank accounts. A mail is sent to the beneficial with the details of the same. After The CASHMA authentication server adds the beneficial successfully, the client is alarmed with the mail.

When the client clicks on the transaction tab of the system an OTP is generated and sent to the client. To further proceed through the transaction the user has to enter the OTP sent to the registered mail and can transact the sufficient amount to the beneficial securely. The Cashma system is capable of operating any web service. The user is identified dynamically using the trust levels, the dynamic session timeouts adds usability and quality to the security being provided. Finally the security of the proposed system is inherently increased with increased traceability of the legitimate user.

V.CONCLUSION

Based on the design and verification principles of the enhanced cashma system, this paper has addressed how the user identity is verified throughout the session for securely operating the web service with continuous authentication. Eventually, by using this technique the Cashma authentication server will be able to distinguish the genuine user from the imposter by keeping track of the user log and transparently acquiring the biometric data of the user. The security of the service is immensely increased by keeping multiple layers of security to the web service. The protocol enhances the usability of the system since only the user is able to perform the transactions. Alerts are sent to the mail to alarm the user about the wicked activities from the trespasser. The Cashma authentication system greatly enhances the security compared to the existing system.

REFERENCES

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”, IEEE transactions on dependable and secure computing, vol. 12, no. 3, may/ june 2015.

2.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.

3.L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, “Quantitative Security Evaluation of a Multi-Biometric Authentication System,” Proc. Int’l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.

4. 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.

5.D.M. Nicol, W.H. Sanders, and K.S. Trivedi, “Model-Based Evaluation: From Dependability to Security,” IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Jan.-Mar. 2004.

6.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.

7.M. Afzaal, C. Di Sarno, L. Coppolino, S. D’Antonio, and L. Romano, “A Resilient Architecture for Forensic Storage of Events in Critical Infrastructures,” Proc. Int’l Symp. High-Assurance Systems Eng. (HASE), pp. 48-55, 2012.

8.CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.

9.A.K. Jain, A. Ross, and S. Pankanti, “Biometrics: A Tool for Information Security,” IEEE Trans. Information Forensics and Security, vol. 1, no. 2, pp. 125-143, June 2006.

10. 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.

AUTHORS PROFILE:

A.Nabiha Karishma Parveen received B.Tech degree in Computer Science and Engineering from Intell engineering college,Anantapur affiliated to JNTUA University, Anantapuramu, A.P, India, during 2010 to 2014. Currently pursuing M.Tech in Computer Science(Software Engineering) from JNTUA College of Engineering, Anantapuramu, A.p, India, during 2014 to 2016 batch. Her areas of interest are Secure Computing and Software Testing.

Dr. S. VASUNDRA, presently working as a Professor and Head of the Department CSE, JNTUACEA. She completed her Ph.D from JNTUA University Anantapuramu, M.Tech from JNTUA and B.E from VTU. She is having 17 years of teaching experience and 5 years of research experience. Published 36 papers in various international journals and 21 National and international conferences. Her areas of interest include MANETS, Cloud Computing, Algorithms, Data Structures and Distributed Computing