BIOMETRIC USER IDENTITY VERIFICATION FOR SECURE INTERNET SERVICE ESTABLISHMENT

[1]SUJITHA.R, [2]SASIKALA.M
[1]Final ME - Computer Science and Engineering
[2]Assistant Professor/CSE
Bharathiyar Institute Of Engineering For Women, Deviyakurichi(Po), Attur(Tk), Salem(Dt)
rsujitha03@gmail.com, sasibtech91@gmail.com

ABSTRACT - ***In distributed internet services the session management is based upon the username and password, explicit logouts and the user session can be kept active if the user uses the system. The user session can be expired based on classic timeouts. The identity of the user remains constant until the entire session. If the user unattended the system or the device can be forcibly stolen then the information can be retrieved by the attacker. Emerging biometric solutions allow the user to provide the username and password with biometric data during session establishment. A secure protocol is defined for protective authentication through continuous user verification. CASHMA (Context Aware Secure by Hierarchical Multilevel Architecture) obtains different biometric traits from the user. The biometric traits can be compared with the already existing templates. The technique of Viola Jones Detection algorithm was adopted to eliminate the background factors and the content based retrieval was adopted to retrieve the information based upon the trust put by the user. The security concern can be improved by obtaining the biometric data transparently acquired from the user. The functional behavior of the protocol is illustrated through Visual studio, while it describes about the type of authentication exercised by the client.***

Index Terms—*CASHMA, Viola Jones detection, Content based retrieval*

I.INTRODUCTION

Network security contains certain set of policies and principles to monitor and eliminate the threats such as unauthorized access, misuse of data, modifications or changes made in data and delay of service attack. Authorization allows the user to access the network. Authentication allows the users to access the network in secure manner. The authentication in traditional system is based on just providing the username and password as identity during login phase. The identity of the user remains constant until the entire working session. In the modern Information and Technology systems secure authentication is necessary. Due to the random improve of cyber attacks, security is needed. Thus the biometric trait can be used since it provides more authentications. The biometric trait such as face and iris recognition can be used for authentication. The biometric trait can be acquired continuously from the user. However face and iris recognition can be assigned for certain sessions. Thus the user has to provide the identity for accessing those sessions. The technique of Viola Jones detection algorithm was adopted to eliminate the background factors. The technique of content based retrieval was used to gather the data based upon the identity of the user. The one factor authentication is providing authentication through username and password. The two factor authentication is defined as providing authentication through username and password using dongle. Providing biometric authentication is a three factor authentication process since it requires username and password along with biometric trait. The biometric trait can be assigned to every session in order to improve the security concerns in banking and financial applications. However the transactions need much privacy.

II.RELATED WORK

Azltinok and Turk suggested an approach, which biometric systems provide access to the user at a specific moment in time, granting or allowing accessing of information to resources for the entire session. The biometric systems does not support for environmental factors. The multimodal system provides more authentications comparing to that of regular biometric verification. The continuous authentication provides more authenticity. The multimodal authentication can be provided through Naïve Bayesian classification. The output is based upon probability function and trust level. The trust level eliminates even the false matches through continuous authentication. Thus the biometric can be used as a tool for information security. A single biometric verification trait is not enough in the modern communication and technology systems. Biometric verification comprises of face, fingerprint, iris, retina and digital signature. The biometric verification does not support for all kind of environmental factors such as dust and poor picture quality. The biometric verification does not support for all types of threats.

Jain proposed the technique of obtaining biometric entity through retina. However retinal verification is quite complicated since the user cannot able to focus at a particular point for a long time. The users have to contact with the device without wearing glasses or lens.

III.SYSTEM MODEL

The CASHMA consist of authentication server, web services and computational services and templates. The timeout of the session depends upon the usability of the internet service and sequential needs of the client. The technique of applying biometrics is adopted in the management of sessions. A secure protocol is defined for secure authentication through continuous and transparent user verification. The protocol depends the biometric entity which is transparently obtained from the user.

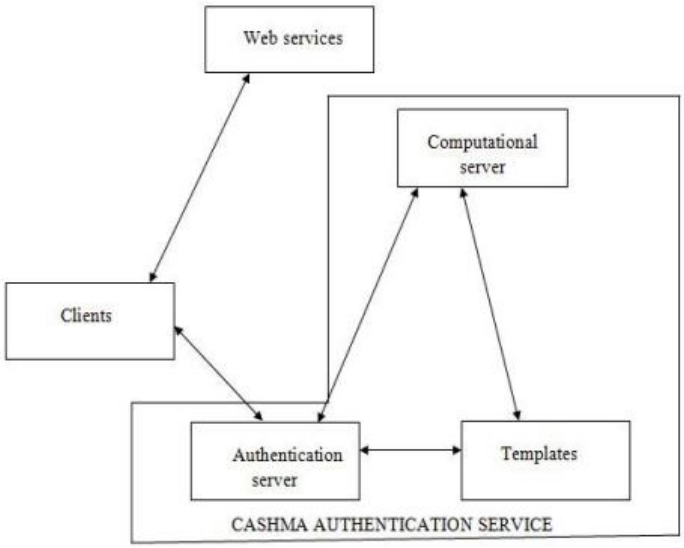

Figure 1. Architecture diagram for providing authentication access using CASHMA service

The Fig.1 explains about the operation of providing authentication access to the client systems by the CASHMA authentication service. The template stores the user's database of keystroke and face. The authentication server issues the CASHMA certificate to the client system for accessing the web services.

IV.OVERVIEW

The session management can be provided through by giving username and password at the login phase. To provide more authentications the system model of CASHMA was adopted. The CASHMA provides its certificate through timestamp, sequence number and identity. The term identity refers to user identity. The timestamp refers the time period of the active session. If the time period completed, then the CASHMA requires the next biometric authentication from the user. The template is a collection of biometric trait since it holds only up to certain limits depend upon the memory allocation for storing the data. The systematic model can be done through visual studio or mat lab simulations.

V. MODEL IMPLEMENTATION

A.CASHMA registration

The CASHMA authentication service contains an authentication server. It interacts with the client systems. The computational server compares the raw biometric data with the already existing templates. Before the user access the web service the user must register into the CASHMA registration phase. The templates are a collection biometric data from the user.

B. Secret authentication

The secret authentication can be provided by obtaining answers for the questions. The web services are the internet and external services that use the CASHMA authentication service. The clients and the web services are linked through the communication channel. The user contacts the web service for a service request. The web service needs the valid certificate from the CASHMA authentication service. The various software systems most often need to transfer data with each other. The Web service is a method of communication that allows the entire software systems to transfer the data over the internet.

C. Viola Jones Detection Algorithm

The integral image is an image representation evaluates rectangular features in constant time. The rectangular features can be marked based upon the attributes. The integral image provides a considerable speed and advantage over more features. The Viola Jones detection algorithm eliminates the background factors such as dust or poor picture quality by considering the user identity as a rectangular area. The Viola Jones detection algorithm eliminates the background features such as dust and poor image quality. The rectangular features mark the attributes of eye and mouth. The Viola Jones detection algorithm is a technique adopted by marking the biometric entity through cross symbols or of rectangular boxes.

D. Iris detection

The iris detection can be acquired by considering only the eye detection algorithm. The eye detection algorithm scans only the eye and allows the user to access the web service. After CASHMA compares the raw data with the existing templates it issues the certificate to the user for accessing the internet services.

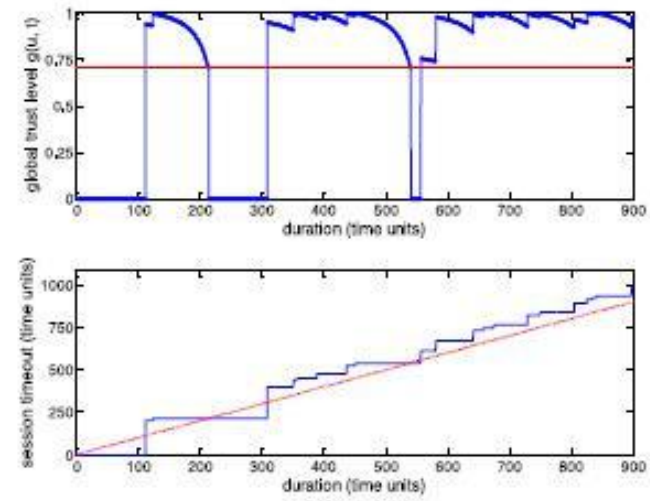

Fig.2 Duration of the session vs session time out and global trust level

VI. CONCLUSION AND FUTURE WORK

The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data acquired transparently through monitoring in background the user's actions. Some architectural design decisions of CASHMA are here discussed. The system exchanges raw data and not the features extracted from templates. The cripto-token approaches are not considerable. This is due to architectural decisions where the client is kept very simple. The proposed protocol works with no changes using features, templates or raw data. The data acquired would be a reasonable approach to reduce computational burden to the server. It is compatible with our objective of designing a protocol independent from quality ratings of images, this goes against the CASHMA requirement of having a light client. The future work is to develop the security and authenticity by

acquiring the biometric entities from the users. The raw biometric traits that are acquired from the users can be compared with the database. The biometric entities that are adopted for enhancement are not sufficient since digital signature is a technique adopted to provide excess authentication.

REFERENCES

[1] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, and Andrea Bondavalli, "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] Azltinok .A and Turk .M, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2014.

[3] BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.

[4] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.

[5] Courtney .T, Gaonkar .S, Keefe .L, Rozier E.W.D, and Sanders W.H, "Mobius 2.3: An Extensible Tool for Dependability, Security, and Performance Evaluation of Large and Complex System Models," Proc. IEEE/IFIP Int'l Conf. Dependable Systems & Networks (DSN '09), pp. 353-358, 2009.

[6] Jain .A, Hong .L, and Pankanti .S, "Can Multibiometrics Improve Performance?" Proc. Workshop on Automatic Identification Advances Technologies (AutoID '99) Summit, pp. 59-64, 2013.

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

[8] LeMay .E, Unkenholz .W, Parks .D, Muehrcke .C, Keefe .K, and Sanders W.H, "Adversary-Driven State-Based System Security Evaluation," Proc. the Sixth Int'l Workshop Security Measurements and Metrics (MetriSec '10), pp. 5:1-5:9, 2009.

[9] Li S.Z and Jain A.K, Encyclopedia of Biometrics. first ed., Springer, 2009.

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

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