SECURE ACCESS TO INTERNET SERVICES AND SESSION MANAGEMENT THROUGH PCA SYSTEM

Jenisha .J , Kasthuri .N , Krishnaveni .M

Department of computer science and engineering, DMI college of engineering Anna University ,

Chennai, India.

ABSTRACT

Basically online services provides security based on username, password and authentications using distributed biometric data during session establishment ,but the session timeout leads to the home page after the authentication. This project eliminates distributed biometrics and overcomes the problem that the user faces during the session timeouts by using single biometric data like face recognisation which reduces the complexity . And the session timeouts leads to the direct page in which the session expired. This process may be useful during important online services like online payments, reservation of Tickets , authentication etc

KEYWORDS:

CASHMA (Context Aware Security by Hierarchical Multilevel Architectures), **PCA**(Principle Component Analysis).

INTRODUCTION:

Secure Computing is the determining factor in the classification of an enclave of servers/computers . A Network with the different security domain is kept separate from other networks. A secure computing is considered to be an application or collection of applications that all trust a common security token for authentication, authorization or session management. Example: All the web application that trust a session cookie issued by a web access management product

ARCHITECTURE

The proposed architecture consists of the session management is done by giving user name and password along with the biometric authentication protocol i.e, by continuous authentication with protocol and time limitation. Here, the CASHMA system is used to evaluate the process of face estimation and face detection with a template database in the server and provide the authentication by issuing the CASHMA certificate. The server will provide web services to the client along with the timeout in the session.

The overall system is composed of the CASHMA authentication service. The clients and the web services connected through communicational channel. The CASHMA authentications services includes: i) An authentication server, which interact with the clients, ii) A set of high-performing computational servers that perform comparisons of biometric data for verifications of the enrolled users, and iii) Databases of templates that contain the biometric templates of the enrolled users(these are required for user authentication/ verification). The web services are the various services that use the CASHMA authentication service and demand the authentications of enrolled user to the CASHMA authentication server. Finally by clients we mean the users' devices(laptop and desktop PCs, smart phones, tablets etc.) that acquire the biometric data (the raw data) corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server as part of the authentication procedure towards the target web service. A client contains i)sensors to acquire the raw data, and ii) The CASHMA applications which transmit the biometric data to the authentication server. The CASHMA authentication server apply user authentication and successive verification procedure

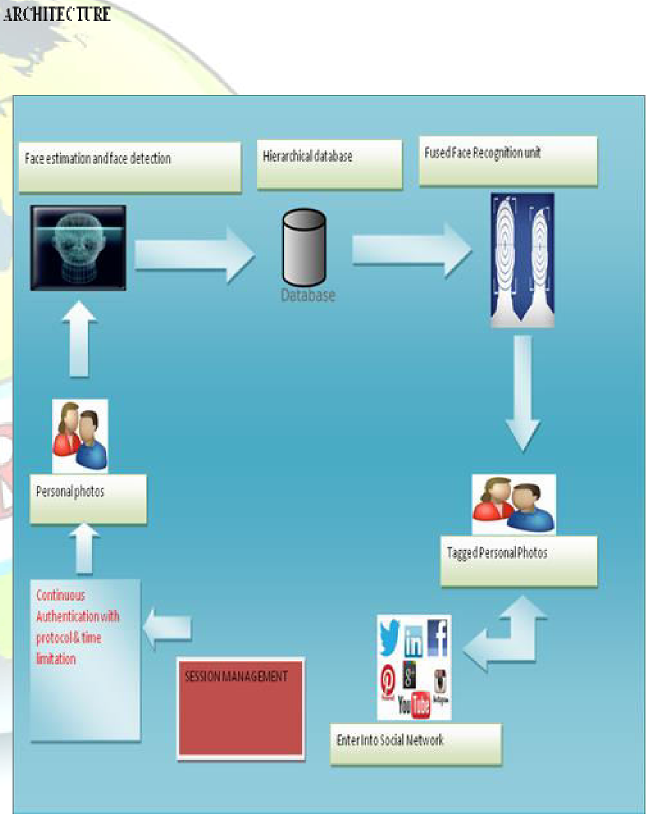

ARCHITECTURE
Face estimation and face detection
Hierarchical database
Fused Face Recognition unit
Database
Personal photos
Tagged Personal Photos
Continuous Authentication with protocol & time limitation
SESSION MANAGEMENT
Enter Into Social Network

Figure1: session Management &Authentication

LITERATURE SURVEY

1. E.LeMay, W.Unkenholz, D.Parks, C.Muehrcke, K.Keefe and

W.H.Sanders,**”ADVER“ARY- DRIVEN STATE BASED SYSTEM SECURITY EVALUATION”**,Proc.the sixth Int’l Workshop Security Measurements and Metrics(MetriSec’10),pp.5:1-5:9,2010

CASHMA multibiometric authentication : percieved as strong authentication but Several well known vulnerablities exist and The Biometrics are security aspect should be considered for each session timeouts

2.A.Altinok and M.Turk, **“TEMPORAL INTEGRATION FOR CONTINUOUS MULTIMODAL BIOMETRIC“”,** Proc.WorkshopMultimodelUser Authentication,pp.11-12,2003.

In design c25.5-to- accessible PDF workflow at a glance.Producing a pdf form indesign that’s machine readable and optimised for screen reader.Updates and revisions are faster and easier but Multistep tasks in earlier version of indesign

3. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, **“AUTOMATED GENERATION AND ANALYSIS OF ATTACK GRAPH“”,**Proc.IEEE Symp.Security And Privacy,pp.273-284,2002.

Banking and technology snapshot Authentication on basis of individual physical trait such as veins and face recognition and finger print but no warrenty or representation in made as to the correctness,completeness and accuracy of the information.

4. S. Kumar, T. Sim, R. Janakiraman, and S. Zhang,**”USING CONTINUOUS“ BIOMETRICS VERIFICATION TO PROTECT INTERACTION LOGIN “E““ION“”**,Proc.21st Ann Computer Security ApplicationConf(ACSAC’05),

pp.441-450,2005.

Sequential Probablity Ratio Test Saves time,cost and performance used in computerized testing variance, correlation and parameters of linear modules (regression modules)must be tested.

5. L. Montecchi P. Lollini A. Bondavalli and E. La Mattina,**”QUANTITATIVE “ECURITY EVALUATION OF A MULTI-BIOMETRICS AUTHENTICATION “Y“TEM”**,Proc.Int’l Conf Computer Safety,Reliability and Security,pp.209-221,2012.

Novel solution-it uses finger print, hand scans, Retina scan and voice authentication, facial scan etc. but image are not accurate when token facing acquisition camera.

SYSTEM MODULE:

Continuous Authentication

A multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer. The proposed approach assumes that first the user logs in using a strong authentication procedure, and then a continuous verification process is started based on multi-modal biometric.

required to subvert the computer can automatically lock it up. Similarly, in a multi-modal biometric verification system is presented, which continuously verifies the presence of a user working with a computer. If the verification fails, the system reacts by locking the computer and by delaying or freezing the user's processes .The continuous authentication protocol allows providing adaptive session timeouts to a web service to set up and maintain a secure session with a client. The timeout is adapted on the basis of the trust that the CASHMA authentication system puts in the biometric subsystems and in the user.

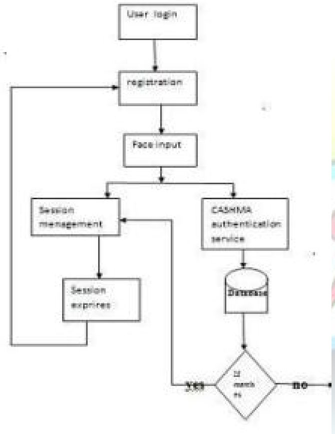


Figure 2: Continuous Authentication

Quantitative Security Evaluation

Security assessment relied for several years on qualitative analyses only. Leaving aside experimental evaluation and data analysis model-based quantitative security assessment is still far from being an established technique despite being an active research area. Specific formalisms for security evaluation have been introduced in literature, enabling to some extent the quantification of security. Attack trees are closely related to fault trees: they consider a security breach as a system failure, and describe sets of events that can lead to system failure in a combinatorial way they however do not consider the notion of time

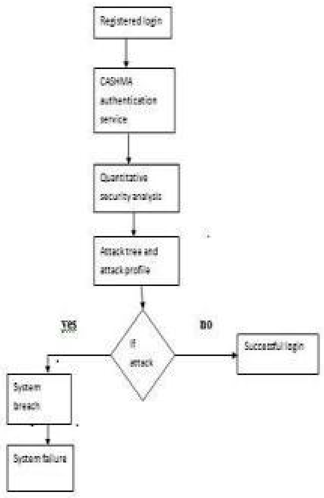

Registered login
CASHMA authentication service
Quantitative security analysis
Attack tree and attack profile
yes
no
If attack
Successful login
System breach
System failure

Figure 3: Quantative Security Evalution

The CASHMA Architecture

The overall system is composed of the CASHMA authentication service, the clients and the web services, connected through communication channels. Each communication channel in implements specific security measures The CASHMA authentication service includes: i) an authentication server, which interacts with the clients, ii) a set of high-performing computational servers that perform comparisons of biometric data for verification of the enrolled users, and iii) databases of templates that contain the biometric templates of the enrolled users (these are required for user authentication/verification). The web services are the various services that use the CASHMA authentication service and demand the authentication of enrolled users to the CASHMA authentication server. These services are potentially any kind of Internet service or application with requirements on user authenticity. They have to be registered to the CASHMA authentication service, expressing also their trust threshold.

Finally, by clients we mean the users' devices (laptop and desktop PCs, smart phones, tablet, etc.) that acquire the biometric data (the raw data) corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server as part of the authentication procedure towards the target web service. A client contains i) sensors to acquire the raw data, and ii) the CASHMA application which transmits the biometric data to the authentication server. The CASHMA authentication server exploits such data to apply user authentication and successive verification procedures that compare the raw data with the stored biometric templates.

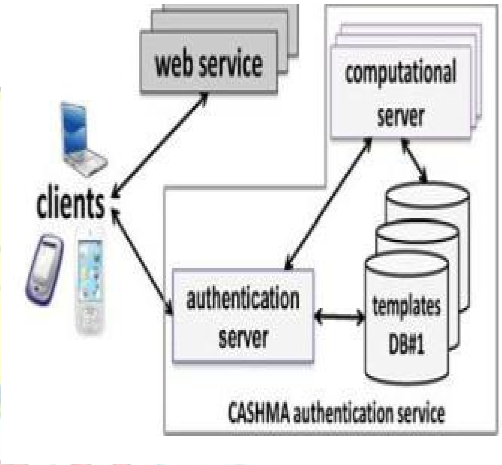


Figure 4:CASHMA Architecture

Trust Levels and Timeout Computation

The algorithm to evaluate the expiration time of the session executes iteratively on the CASHMA authentication server. It computes a new timeout and consequently the expiration time each time the CASHMA authentication server receives fresh biometric data from a user. Let us assume that the initial phase occurs at time t0 when biometric data is acquired and transmitted by the CASHMA application of the user u, and that during the maintenance phase at time ti > t0 for any i ¼ 1; :::;m new biometric data is acquired by the CASHMA application of the user u (we assume these data are transmitted to the CASHMA authentication server and lead to successful verification

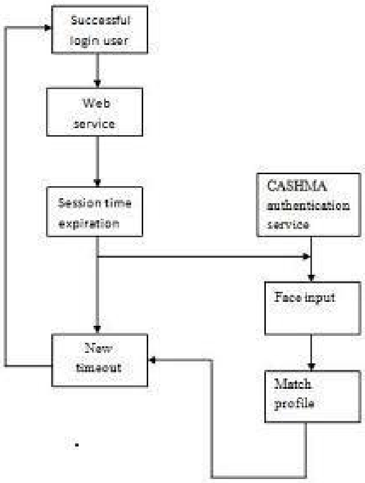


Figure 5:Timeout Computation

EXPERIMENTAL RESULT

The experimental results starts with the registration.

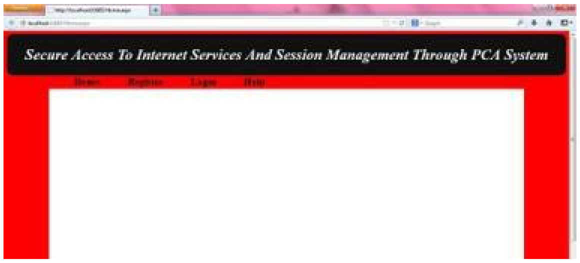

Secure Access To Internet Services And Session Management Through PCA System
Home
Register
Login
Help

Figure 6:Home Page

The home page which includes Registration and login.If the user is newuser means they have to registered first,if it is old user means login by using user name and password.

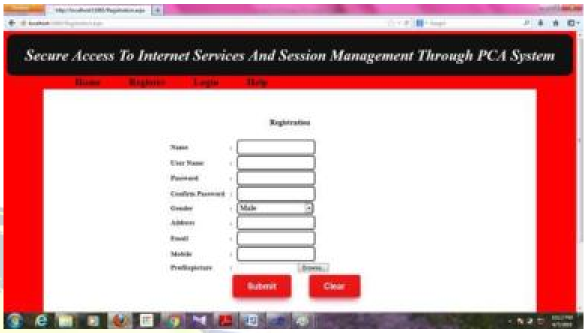
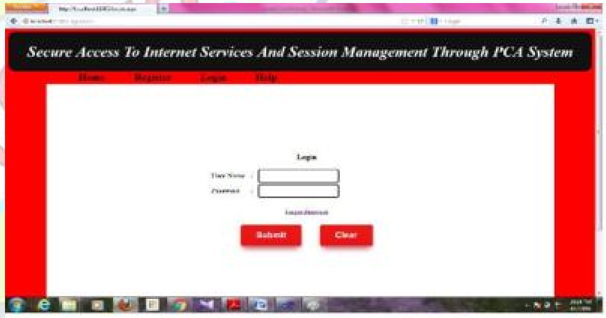
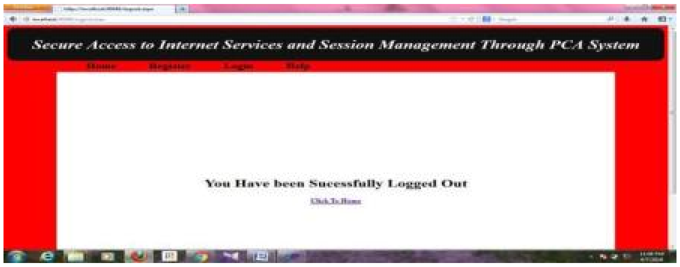


Figure 7: User's Registrstion Page


Secure Access To Internet Services And Session Management Through PCA System
Home
Register
Login
Help
Login
User Name
Password
Submit
Clear

After login the user can share images, vedios & messagesetc,if incase timeouts it will be



Secure Access to Internet Services and Session Management Through PCA System

You Have been Sucessfully Logged Out

Figure 7:Session logout Page

CONCLUSION:

We exploited the novel possibility introduced by biometrics to define a protocol for continuous authentication that improves security and usability of user session. 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. We remark that our proposed protocol works with no changes using features, templates or raw data. Second, privacy concerns should be addressed considering National legislations.

At present, our prototype only performs some checks on face recognition, where only one face (the biggest one rusting from the face detection phase directly on the client device) is considered for identity verification and the others deleted. Third, when data is acquired in an uncontrolled environment, the quality of biometric data could strongly depend on the surroundings. While performing a client-side quality analysis of the data acquired would be a reasonable approach to reduce computational burden on the server, and it is compatible with our objective of designing a protocol independent from quality ratings of images.

It has to be noticed that the functions proposed for the evaluation of the session timeout are selected amongst a very large set of possible alternatives. Although in literature we could not identify comparable functions used in very similar contexts, we acknowledge that different functions may be identified, compared and preferred under specific conditions or users requirements; this analysis is left out as goes beyond the scope of the paper, which is the introduction of the continuous authentication approach for Internet services

REFERENCES:

[1]E.LeMay, W.Unkenholz, D.Parks, C.Muehrcke, K.Keefe and W.H.Sanders,”**ADVER“ARY- DRIVEN STATE BASED SYSTEM SECURITY EVALUATION”**,Proc.the sixth Int'l Workshop

Security Measurements and Metrics(MetriSec'10),pp.5:1-5:9,2010.

[2]A.Altinok and M.Turk, **"TEMPORAL INTEGRATION FOR CONTINUOUS MULTIMODAL BIOMETRIC""**, Proc. WorkshopMultimodelUser Authentication,pp.11-12,2003.

[3]O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, **"AUTOMATED GENERATION AND ANALYSIS OF ATTACK GRAPH"",**Proc.IEEE Symp.Security And Privacy,pp.273-284,2002.

[4]S. Kumar, T. Sim, R. Janakiraman, and S. Zhang,**"U"ING CONTINUOU" BIOMETRIC" VERIFICATION TO PROTECT INTERACTION LOGIN "E""ION""**,Proc.21st Ann Computer Security ApplicationConf(ACSAC'05),pp.441-450,2005.

[5]L. Montecchi P. Lollini A. Bondavalli and
E. La Mattina,**"QUANTITATIVE "ECURITY EVALUATION OF A MULTI-BIOMETRICS AUTHENTICATION SYSTEM"**,Proc.Int'l Conf Computer Safety,Reliability and Security,pp.209-221,2012.