ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Session Management for Internet Services

D.Sandhya
B.Tech,
Dept of CSE,
MLRIT, Hyderabad.

G.Mounika
B.Tech,
Dept of CSE,
MLRIT, Hyderabad.

Ruksar Fathima
B.Tech,
Dept of CSE,
MLRIT, Hyderabad.

Reshma Sheik
B.Tech,
Dept of CSE,
MLRIT, Hyderabad.

B.Pavani
Assistant Professor,
Dept of CSE,
MLRIT, Hyderabad.

Abstract:

In internet services, the session management is traditionally based on username and password, explicit logouts and user session expiration.Emerging biometric solutions allow substituting username and password with biometric data during session establishment.This paper explores promising alternatives offered by applying biometric (both thumb and photo) in the session management.The protocol determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user. This model-based quantitative analysis is carried outto assess the ability of the protocol to contrast security attacks exercised by different kinds of attackers.

Keywords:
Security, web servers, Session management, Authentication.

I.INTRODUCTION:

Secure authentication is fundamental in most of the modern system. User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at the login phase. No checks are performed during working session, which are terminated by an explicit logout. Due to increase in the frequency of cyber-attacks biometric technique only (thumb) offered solution for secure and trusted authentication where username and password are replaced by thumb biometric data.Such observations lead to arguing that a single authentication point and a single type biometric data cannot guarantee a sufficient degree of security. Biometric user authentication is typically formulated as a “single shot” providing user verification only during login phase. Once the users identity has been verified,the system resources are available for a fixed period of time. To timely detect the misuses of the computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal biometric (both thumb and photo) continuous authentication are proposed.

To avoid that a single type of biometric trait is forged, authentication can rely on multiple biometric traits. A quantitative model-based security analysis of the protocol is performed combing the stochastic activity networks and Adversary View Security Evaluation formalism.

II.RELATED WORK:

Security systems and methods are often described as strong or weak. A strong system is one in which the cost of attack is greater than the potential gain to the attackers. Conversely, a weak system is one where the cost of attack is less than the potential gain. Authentication factors are grouped into three categories: a. what you know (e.g.: password) b. what you have (eg: token) c. Who you are (eg:biometric).Inspite of numerous advantages of biometrics based personal authentication system over traditional security systems based on token or knowledge;they are vulnerable to attacks that can decrease their security considerably. This paper analyses these attacks in the realm of a finger print biometric system [3]. Conventional verification systems, such as those controlling access to secure room, do not usually require the user to re-authenticate him-self for continue access to the protected resource.

This may not be sufficient for high-security environments in which the protected resource needs to be continuously monitored for unauthorized user.In such cases continuous verification is needed. This paper presents theory, architecture; implementation and performance of a multi modal biometrics verification system that continuously verify the presence of a logged-in user. Two modalities can be used – face and finger-print- but our theory can be furtherly extended to include more modalities. This paper shows that continuous verification imposes additional requirements on multi modal fusion when compared to conventional verification system [5]. Current ICT infrastructures are characterized by increasing requirements of reliability, security, performance. A relevant issue is represented by the scalability of the system with respect to the increasing number of users and applications, thus requiring a careful dimensioning of resources.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Furthermore, new security issues to be faced arise from exposing applications and data to the internet, thus requiring an attentive analysis of potential threats and identification of stronger security mechanisms to be implemented, which may produce a negative impact on system performance on scalability properties. This paper presents model based evaluation of scalability and security of multi-service web-based platforms, by evaluating how the introduction of security mechanisms may lead to the degradation of performance properties[2].Biometric authentication systems verify the identity of users by relying on their distinctive traits, like fingerprint, face, iris, signature, voice, etc. Biometrics is commonly perceived as a strong authentication method; in practice several well-known vulnerabilities exist, and security aspects should be carefully considered, especially when it is adopted to secure the access to applications controlling critical systems and infrastructures.

This paper performs a quantitative security evaluation of the CASHMA multi-biometric authentication system, assessing the security provided by different system configurations against attackers with different capabilities. The analysis is performed using the ADVICEmodelling formalism, formalism for security evaluation that extends attack graphs; it allows combining information on the system, the attacker, and the metrics of interest to produce quantitative results [6].Today, security engineering for complex systems is typically done as an ad hoc process. Taking a risk-based security engineering approach replaces today's ad hoc methods with a more rigorous and disciplined approach that uses a multi-criterion decision model. This approach builds on existing techniques for integrating risk analysis with classical systems engineering. A resulting security metric can be compared with cost and performance metrics in making engineering trade-off decisions[4].

III.PROPOSED METHODOLOGY:

This paper presents a new approach for user verification and session management that is applied in the context aware security hierarchical multilevel architectures system for secure biometric authentication on the internet. CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services etc., The approach introduced in this paper is CASHMA [1]for usable and highly secure user sessions is a continuous sequential multi modal biometric authentication protocol, which adaptively com putes and refreshes session timeouts. This paper explores promising alternatives offered by applying biometric (both thumb and photo) in the session management .The protocol determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user. Our continuous authentication approach is grounded on transparent acquisition of biometric data and on adaptive timeout management on the basis of the trust posed in the user and in the different subsystems used for authentication. The user session is open and secure despite possible idle activity of the user, while potential misuses are detected by continuously confirming the presence of the proper user.

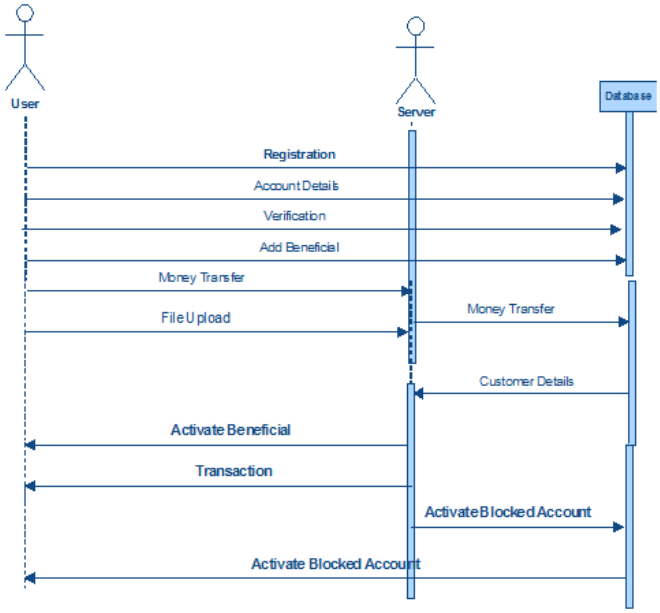


Fig 1: sequence diagram

Step1: Whenever user registers,he/she has to give details of them along with thumb and a photo file.

Step2: when the registration completes,they will get a OTP to their respective mail ID.

Step3: when the user wants to sign-in, he/she has to upload both thumb and photo file which they used at the time of registration time which are going to be scanned.

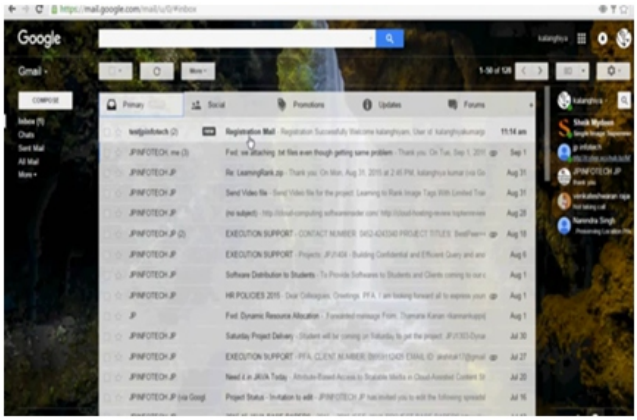
Step4: If user is a genuine user then they are directed to their account, if not they are freezed or asked to re-login.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

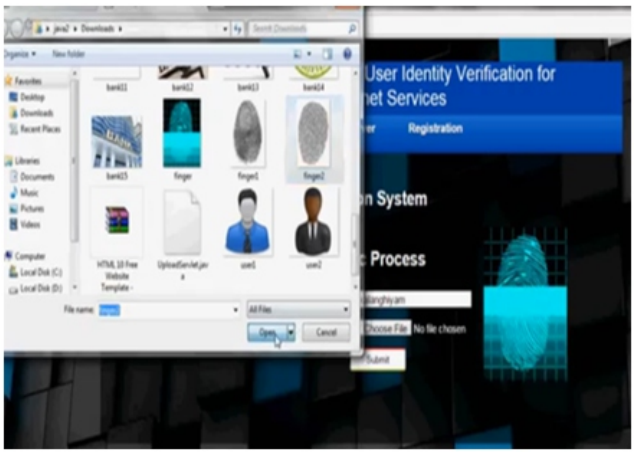
IV.RESULTS:

During registration need to upload both thumb and photo image as shown below

When registered, system generates a password to our mail ID



During the login session,it has to upload the images which are going to scan as shown



V.CONCLUSION:

In this paper exploit the novel possibility introduced by Biometric (include Face) 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 action.In this paper 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. Some architectural design decisions of CASHMA are here discussed. First, the system exchanges raw data and not the features extracted from them or templates, while crypto-token approaches are not considered. This is due to architectural decisions where the client is kept very simple. This paper remarks 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.

REFERENCES:

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

[2] 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 282 IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3, MAY/JUNE 2015.

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

[4] T.F. Dapp, "Growing Need for Security in Online Banking: BiometricsEnjoy Remarkable Degree of Acceptance,," Banking &Technology Snapshot, DB Research, Feb. 2012.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[5] L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, andA. Bondavalli, "Model-based evaluation of scalability and securitytradeoffs: A case study on a multi-service platform," ElectronicNotes in Theoretical Computer Science, vol. 310, pp. 113–133, 2015.

[6] S. Evans and J. Wallner, "Risk-Based Security Engineeringthrough the Eyes of the Adversary," Proc. the IEEE Workshop InformationAssurance, pp. 158-165, June 2005.