ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Continuous and Transparent User Identity Verification for Secure Internet Services

Megha A K , Neha T, Sravanthi K V, Sushmithasingha, UmeshM

Bachelor of Engineering, Dept of ISE, SJBIT, Banglore,India

Asst. Professor, Dept of ISE, SJBIT, Banglore, India

ABSTRACT: In distributed internet services, session management is performed based on username and password, session logout and some mechanism of users session expiration using classic timeouts. While establishing session, biometric solutions are used which allows substituting username and password, furthermore the session timeout length may affect on the service usability and also on client satisfaction. Work focuses on alternative provided by using biometric while managing sessions. Verification is conducted to identify a secure protocol for proper authentication. Taking frequency, quality and the kind of biometric data clearly acquired from the user in to consideration, the protocol determines adaptive timeouts. For demonstrating the behavior of the protocol simulation is used and further to determine the kind of attackers and the ability of the protocol model-based quantitative analysis is used.

KEYWORDS: security,web Servers, Mobile Environments, Authentication.

I.INTRODUCTION

Secure client verification may be basic Previously, Client Confirmation frameworks are customarily dependent upon pairs about username Also secret key What's more confirm the personality of the client just at login period. No checks would performed Throughout working sessions, which need aid ended Eventually Tom's perusing a express logout alternately lapse following an unmoving pulley action time of the client.

Security of web-based provisions is a genuine concern, because of those late increment in the recurrence What's more multifaceted nature for cyber-attacks; biometric systems offer rising result to secure What's more trusted authentication, the place username What's more international ID need aid swapped Toward biometric information. However, parallel of the spreading use about biometric systems, those motivator to their abuse will be Additionally growing, particularly acknowledging their time permits provision in the monetary Furthermore saving money parts.

Such perceptions prompt contending that An solitary Confirmation perspective What's more An single biometric information can't surety An addition level for security. To fact, comparatively should conventional verification forms which depend around username Furthermore password, biometric client Confirmation may be regularly figured Similarly as An “single shot”, giving work to client confirmation just Throughout login period The point when one or more biometric qualities might a chance to be required. Once the user’s personality need been verified, the framework assets are accessible to an altered time of time alternately until unequivocal logout from those clients. This approach expects that a absolute confirmation (at the start of the session) is sufficient, Also that the personality of those client will be consistent Throughout those entire session.Will instance, we feel as about this essential scenario: An customer need authoritatively logged under An security-critical service, et cetera the individuals customer abandons the pc attainableness in the worth about exertion go to a few the long haul.

This issue might a chance to be In fact trickier in the association from guaranteeing versatile devices, consistently used openly likewise stuffed environments, those spot those contraption itself could make lost or forcibly stolen same the long haul those customer session might be active, permitting impostors with mirror those customer also get strictly specific majority of the data. To these scenarios, those administrations those spot the customers requirement help

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

checked might settle on abused undoubtedly.An fundamental result is to utilizereally short session timeouts and occasionally solicitation the client on information his/her accreditations through and over, Be that this may be not a conclusive result and vigorously penalizes those administration usability Furthermore Eventually those fulfillment of clients.

II. RELATED WORKS

This paper displays another methodology to client confirmation Also session oversaw economy that is connected in the connection mindful security by hierarchic multilevel architectures (CASHMA) framework to secure biometric confirmation on the web. CASHMA has the ability on work safely with whatever sort of web service, including benefits with secondary security requests Similarly as on the web saving money services, Also it is planned should a chance to be utilized from diverse customer devices, e. G. , smartphones, desktop Pcs or Indeed going biometric kiosks set In those doorway about secure regions.Contingent upon those inclination and prerequisites of the holder of the web service, the CASHMA Confirmation administration supplement an accepted verification service, alternately could displace it.

The approach we acquainted On CASHMA to usable Furthermore profoundly secure client sessions is An nonstop consecutive (a single biometric modality without a moment's delay may be exhibited of the system) multi-modal biometric confirmation protocol, which adaptively computes What's more refreshes session timeouts on the groundwork of the trust place in the customer. Such worldwide trust is assessed Likewise An numeric value, registered Eventually Tom's perusing ceaselessly assessing the trust both in the client and the (biometric) subsystems utilized for securing biometric information. In the CASHMA context, each subsystem comprises every last one of hardware/software components necessary on obtain What's more confirm those genuineness from claiming one biometric trait, including sensors, examination calculations What's more every last one of offices for information transmission What's more administration. Trust in the client may be dictated on the premise for recurrence about updates of new biometric samples, same time trust for every subsystem is registered on the support of the nature What's more mixture of sensors utilized for the procurement for biometric samples, Also on the danger of the subsystem on a chance to be intruded.

III.PROPOSED WORK

The proposed approach assumes that first the user logs in using a strong authentication procedure; a continuous verification process is started based on multi-modal biometric. After the user performs login to the computer or to the web service, his entire interaction, through keyboard, mouse activities are continuously monitored to verify that it remains him. If the verification fails, the system reacts by locking the computer or freezing the user's processes. Continuous authentication is used to detect misuse of computer resources and prevent that an unauthorized user maliciously replaces authorized one. Continuous Authentication is essential in online examinations where the user has to be continuously verified during the entire session. It can be used in many real time applications, when accessing a secure file or during the online banking transactions where there is need of highly secure continuous verification of the user. A number of biometric characteristicsexist and are used in various applications [1] [7] [8]. Each biometric has its own strengths and weaknesses, and the choice depends on the application.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

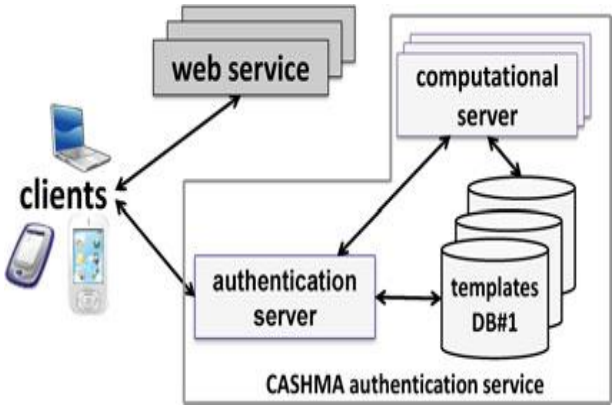

Fig. 1 Architecture of CASHMA service

Continuous Authentication is essential in online examinations where the user has to be continuously verified during the entire session. It can be used in many real time applications, when accessing a secure file or during the online banking transactions where there is need of highly secure continuous verification of the user. A number of biometric characteristics exist and are used in various applications [1] [7] [8]. Each biometric has its own strengths and weaknesses, and the choice depends on the application.

Pseudo-code for image hashing

```
// Initialized with fixed seed
Random generator = new generator(2847)
intnum_iterations = 100

int hash(Image image)
{
//To ensure consistency on each evaluation
generator.reset()
int value = 0
fornum_iteration steps
   {
intnextValue = image.getPixel
(generator.nextInt()%
image.getSize()).getValue()
value = value + nextValue*
generator.nextInt()
   }
return value
}
```

V.RESULTS

Continuous or implicit authentication approaches would provide an additional line of defense, designed as a nonintrusive and passive security countermeasure. Such approaches monitor the user's interaction with the device, and ideally, at every point in time the system estimates if the legitimate user is using the device. Hence, a continuous authentication method can either complement entry-point based authentication methods by monitoring the user after a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

successful login or, if the method satisfies particular accuracy requirements, it could even substitute entry-point based authentication

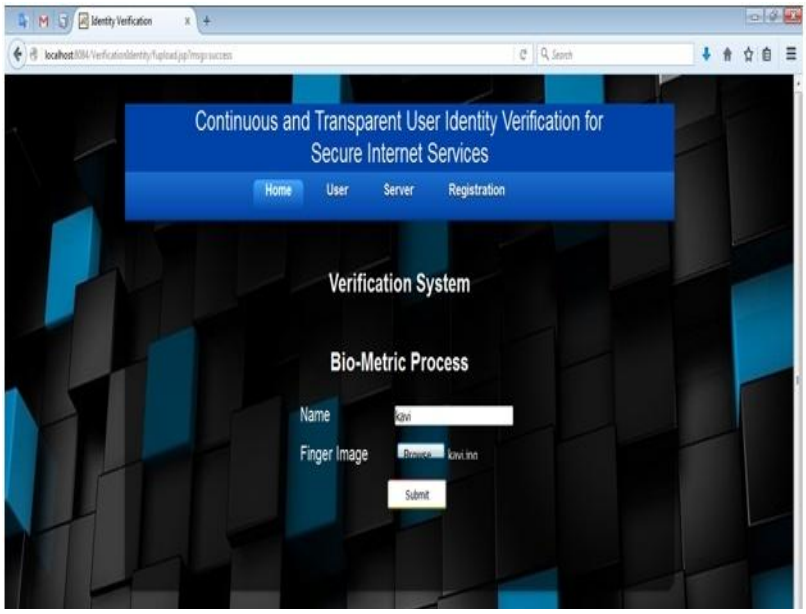

Fig 2shows User authentication with valid credentials

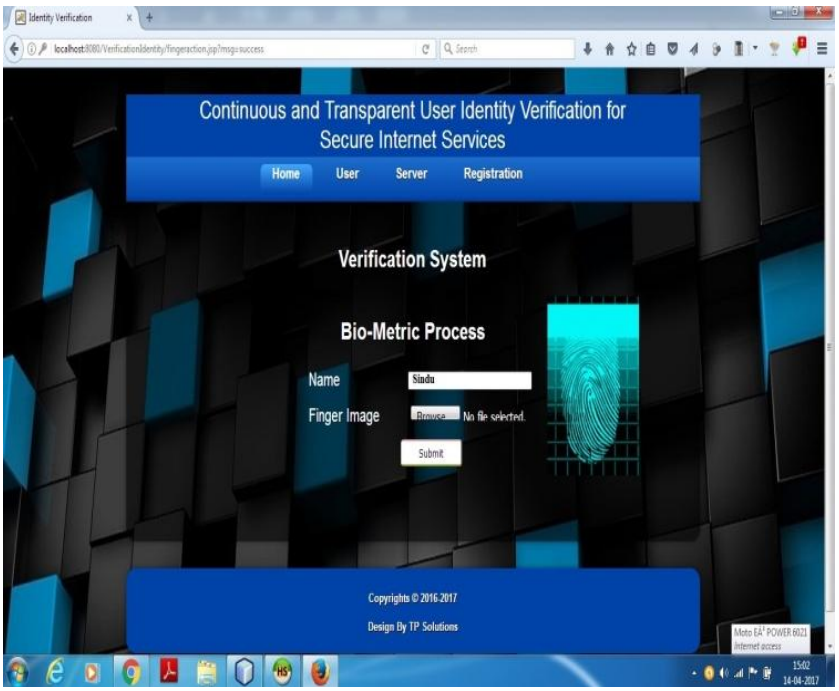

Fig 3shows User login with biometric

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

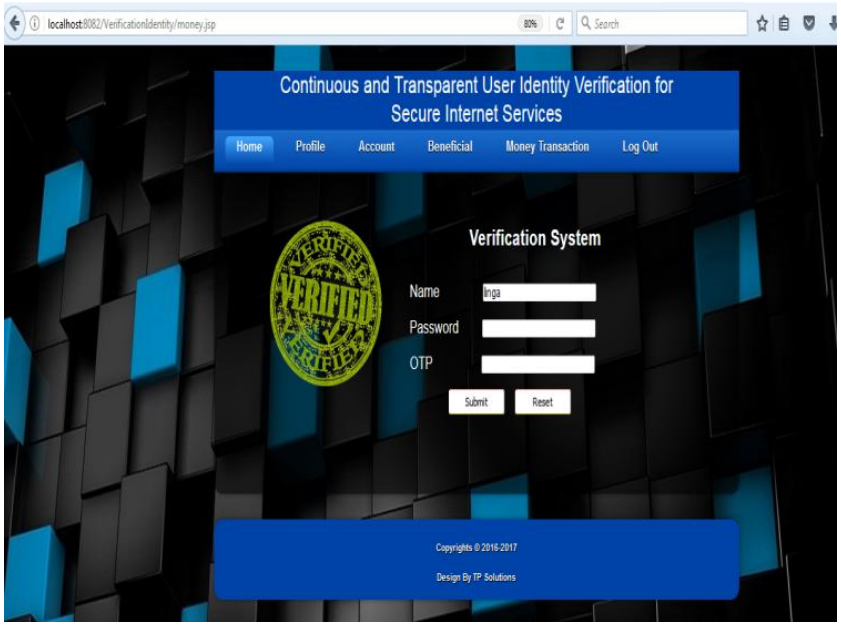

Fig 3 shows Continuous authentication using OTP

VI. CONCLUSION

This paper provides various existing methods used for continuous authentication using different biometrics. Initial one time login verification is inadequate to address the risk involved in post logged in session. Therefore this paper attempts to provide a comprehensive survey of research on the underlying building blocks required to build a continuous biometric authentication system by choosing bio-metric. Continuous authentication verification with multi-modal biometrics improves security and usability of user session.

REFERENCES

1. L. Hong, A. Jain, and S. Pankanti, "Can MultibiometricsImprovePerformance?" Proc. Workshop on Automatic Identification AdvancesTechnologies (AutoID '99) Summit, pp. 59-64, 1999.
2. 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.
3.BioID "Biometric Authentication as a Service (BaaS)," BioIDPressRelease, https://www.bioid.com, Mar. 2011.
4.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.
5. 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.
6. 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.
7. A. Altinok and M. Turk, "Temporal Integration for ContinuousMultimodal Biometrics," Proc. Workshop Multimodal User Authentication,pp. 11-12, 2003.
8. C. Roberts, "Biometric Attack Vectors and Defences," Computers &Security, vol. 26, no. 1, pp. 14-25, 2007.
9. S.Z. Li and A.K. Jain, Encyclopedia of Biometrics. first ed., Springer,2009.
10. 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.
11. E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, andW.H. Sanders, "Adversary-Driven State-Based System SecurityEvaluation," Proc. the Sixth Int'l Workshop Security Measurementsand Metrics (MetriSec '10), pp. 5:1-5:9, 2010.