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 10, October 2017

Survey on Continuous Eye on Authorized User

Prof.Trupti Suryawanshi[1] , Dnyaneshwar Chavan[2] , Pratik Borate[3], Suraj Yadav[4]

Dept. of Computer Engg, Keystone School of Engg, Savitribai Phule University, Pune, India

ABSTRACT : User authentication systems aretraditionally based on pairs of username and password andverify the identity of the user only at login phase. No checksare performed during working sessions, which are terminatedby an explicit logout or expire after an idle activityperiod of the user.Emerging biometric OTP generation, question and answers solutions allow substituting username and password with data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session. Additionally in this system we are going to implement the session authentication with various approach like biometric, OTP(one time password) generation, question and answers with specified time limiting. A secure protocol is defined for perpetual authentication through continuous user verification. The protocol determines adaptive time outs based on the quality, frequency and type of biometric, OTP generation, question. And answers data transparently acquired from the user.

KEYWORDS: Continuous user authentication; CASHMA verification certificate ;various authenticationdata like biometric, OTP generation, question. And answers data

I. INTRODUCTION

User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user.

Security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks; biometric, OTP and questions & Answers techniques offer emerging solution for secure and trusted authentication, where user-name and password are replaced by one of this biometric, OTP and questions &answers data. However, parallel to the spreading usage of biometric , OTP and questions &answers data systems, the incentive in their misuse is also growing, especially considering their possible application in the DBA authentication, financial and banking sectors etc, Such observations lead to arguing that a continuous authentication point and a single biometric, OTP and questions & answers data can guarantee a degree of security .

II. SAMPLE APPLICATION SCENARIO

CASHMA can authenticate to web services, ranging from services with strict security requirements as online banking services to services with reduced security requirements as forums or social networks. Additionally, it can grant access to physical secure areas as a restricted zone in an airport, or a military zone (in such cases the authentication system can be supported by biometric kiosk placed at the entrance of the secure area). We explain the usage of the CASHMA

III. PROPOSED ALGORITHM

A. Design Considerations:

- Client login page
- Authentication server stores authentication data.
- Server sends the authentication request to client.

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 10, October 2017

- Client sends the authentication data and sever compares the this data with database template and generates CASHMA certificate
- Servers sends the CASHMA certificate client after verifying it.
- After getting the certificate client may have access permissions to web services until timestamp ends

.

B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is toidentifies theauthorized user by verifying the user with variousauthentication data like biometric, otp and answers & questionwhich is generated by the authentication server and sends to client in a random variations to give high degree of security. The proposed algorithm is consists of step.

Step:Generating random authentication data
The authentication server(ASr)will generates a random verification modes
eq. i=biometrics,otp,q&a's

1.ASr=bio ……iteration i=1
ifASr= =bio
access granted
else
DENY

2.ASr=OTP ……iteration i=2
ifASr= =OTP
access granted
else
DENY

3.ASr=Q&A ……iteration i=3
ifASr= =Q&A's
access granted
else
DENY

This process will runs according to time i iteration after i=1 finishes it generates another verification phase.
eq.

ASrα i^n
ASr = =correct data
Access granted
Else
Deny

where$i^n$is timestamp of client system and n is generating number of iteration factor.

IV. PSEUDO CODE

1.start
2.registration
3.login:
-OTP
-Bio_metriics
-Q&A's
4.Valid certificate from CASHMA Authentication Service .
- Analyse
-comapre successfully
5.login -Time session start till end of timestamp
6.create CASHMA certificate amd send to client

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 10, October 2017

7.web services reads the certificate to assume it authorized user
8.session time going to expire the client may explicitly notify

V. PROPOSEDSYSTEM ARCHITECTURES

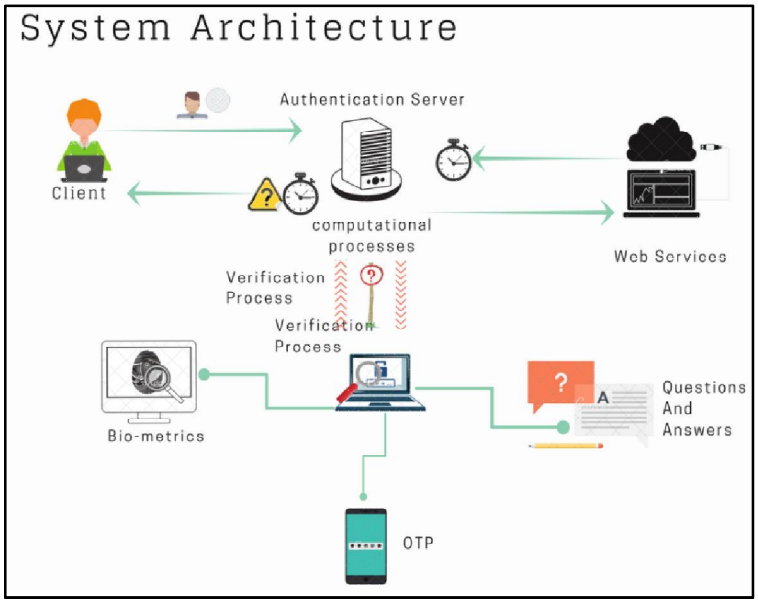

Fig 1.Basic Architecture of Proposed system

A significant problem that continuous authentication aims to tackle is the possibility that the user device (smartphone, table, laptop, etc.) is used, stolen or forcibly taken after the user has already logged into a security-critical service, or that the communication channels or the biometric sensors are hacked.In 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 authentica-tion procedure, then a continuous verification process is started based on multi-modal biometric. Verification failure together with a conservative estimate of the time required to subvert the computer can automatically lock it up.

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 10, October 2017

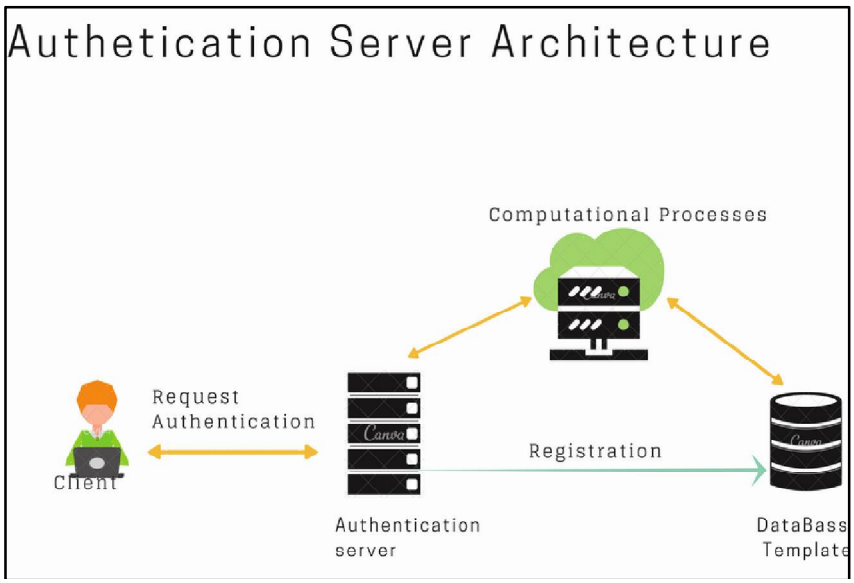

Fig2.BasicArchitecture of Authentication Server with CASHMA

The approach we introduced in CASHMA for usable and highly secure user sessions is a continuous sequential (a single biometric modality at once is presented to the system) multi-modal biometric authentication protocol, which adaptively computes and refreshes session timeouts on the basis of the trust put in the client. Such global trust is evaluated as a numeric value, computed by continuously evaluating the trust both in the user and the (biometric) subsystems used for acquiring biometric data. In the CASHMA context, each subsystem comprises all the hardware/software elements necessary to acquire and verify the authenticity of one bio-metric trait, including sensors, comparison algorithms and all the facilities for data transmission and management. Trust in the user is determined on the basis of frequency of updates of fresh biometric samples, while trust in each sub-system is computed on the basis of the quality and variety of sensors used for the acquisition of biometric samples, and on the risk of the subsystem to be intruded.

The context aware security by hierarchical multilevel architectures (CASHMA) 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, and it is intended to be used from different client devices, e.g., smartphones, Desktop PCs or even biometric kiosks placed at the entrance of secure areas. Depending on the preferences and requirements of the owner of the web service, the CASHMA authentication service can complement a traditional authentication service, or can replace it.

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.

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 10, October 2017

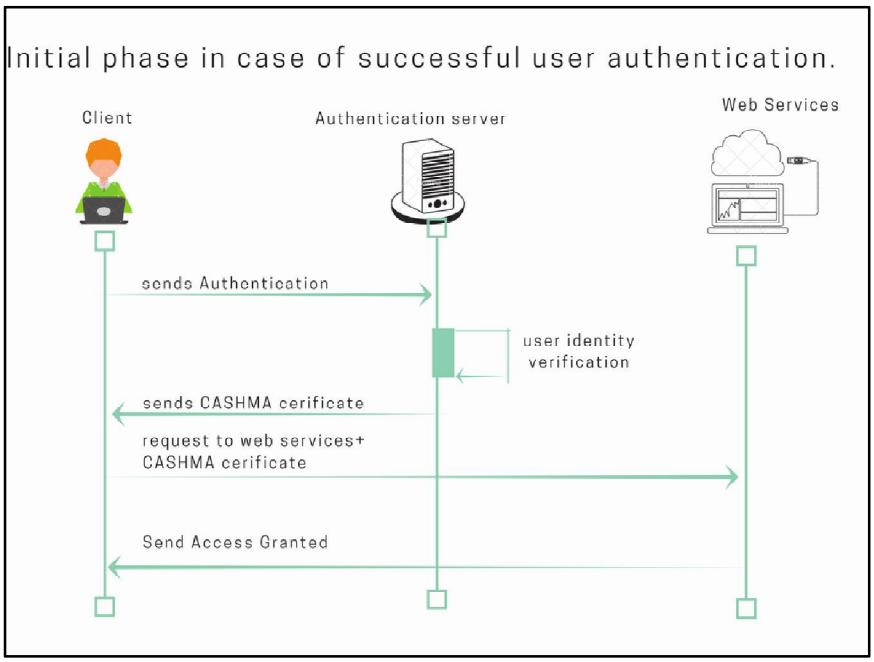

Fig 2.Basic Architecture of Authentication Server with CASHMA

In the above we present the information contained in the body of the CASHMA certificate transmitted to the client by the CASHMA authentication server, necessary to under-stand details of the protocol. Time stamp and sequence number univocally identify each certificate, and protect from replay attacks. ID is the user ID, e.g., a number. Decision represents the outcome of the verification proce-dure carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. In fact, the global trust level and the session timeout are always computed considering the time instant in which the CASHMA application acquires the bio-metric data, to avoid potential problems related to unknown delays in communication and computation. Since such delays are not predicable, simply delivering a relative time-out value to the client is not feasible: the CASHMA server

The CASHMA authentication server analyzes the biometric data received and performs an authenti-cation procedure. Two different possibilities arise here. If the user identity is not verified (the global trust level is below the trust threshold g_{min}), ew or additional biometric data are requested (back to step 1) until the minimum trust threshold g_{min} is reached. Instead if the user identity is success-fully verified, the CASHMA authentication server authenticates the user, computes an initial timeout of length T_0 for the user session, set the expiration time at $T_0 þ t_0$, creates the CASHMA certificate and sends it to the client (step 2).The client forwards the CASHMA certificate to the web service (step 3) coupling it with its request.The web service reads the certificate and authorizes the client to use the requested service (step 4) until time $t_0 þ T_0$.
For clarity, steps 1-4 are represented in Fig. 3 for the case of successful user verification only.

VI. CONCLUSION

We exploit that 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 OTP , question and answers data transparently acquired through monitoring in background the user's actions.

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 10, October 2017

REFERENCES

[1]. CASHMA-"Context Aware Security by Hierarchical Multilevel Architectures", MIUR FIRB, 2005.
[2]. Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, PaoloLollini, Angelo Marguglio, Andrea Bondavalli,, "Continuous and
[3]. Transparent user identity verification for secure internet services", IEEE Transactions on Dependable and Secure Computing MAY/JUNE 2015.
[4]. L .Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?" Proc. Workshop on Automatic Identification Advances Technologies (Auto ID '99) Summit, pp. 59-64, 1999.
[5]. [4] 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.
[6]. S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions" Proc. 21st Ann. Computer Security Applications Conf. (ACSAC '05), pp.441-450, 2005.
[7]. 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.

BIOGRAPHY

Name : Prof.Trupti Suryawanshi, Qualification: M.Tech Computer Engineering, **Experience :** 3 Years Teaching She has completed his bachelor's degree from Shivaji University, Kolhapur in 2011, with Distinction and master's degree from BharatiVidyapeeth , Pune in the year 2016. She is having total 03 years of professional teaching experience. She has worked with SCSCOE fromBhor. She has presented and published 2 International Papers in the reputed journals. She is expertise in field of Computer Graphics, Software Engineering ,High Performance Computing.

Mr.DnyaneshwarSatishChavan, pursing in the Keystone School of engineering ,pune. He have received the Diploma from the Department of computer Science and Engineering ,Jaywantraosawant polytechnic ,pune,India in 2015 . His research interests include Database(My0Sql,No-Sql),programming languages (i.e. c,c++,java,python,Android),Data Mining,compilers and algorithms.

Mr.Suraj Sanjay Yadav , pursing in the Keystone School of engineering ,pune. He have received the Diploma from the Department of computer Science and Engineering ,Jaywantraosawantploytechnic,pune,India in 2015 . His research interests include Database(Sql,No-Sql), programming languages (i.e. c,c++,java,python),testing(manual and automation),Security and privacy,DataMining,compilers and algorithms.

Mr.Pratik Dilip Borate pursing in the Keystone School of engineering ,pune. He have received the Diploma from the Department of computer Science and Engineering ,Jaywantraosawantploytechnic,pune,India in 2015 . His research interests include Database, programming languages (i.e. c,c++,python),testing(manual and automation)and algorithms.