IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Multiple Verification for Continuous Secure User Authentication

Poonam Mahale [1], Mr. Niranjan Bhale [2]

Student, Department of Computer Engineering, MCOERC, Nashik, Maharashtra, India [1]

Head, Department of Information Technology, MCOERC, Nashik, Maharashtra, India [2]

Abstract: In the field of internet services secure internet services is important issue. Traditional distributed internet services are based on session management of username password, logouts and user session expiration based on timeouts. Biometric authentication provides solution to substitute password with biometric information in session creation with single verification. In proposed work, additional level of security can be provided & multiple verification can deployed for authentication. In this paper we present continuous authentication of user by multiple authentication. The user identity is continuously verified by applying different authentication in session management. A secure data flow with privacy preservation for the session management by using biometric systems will be offered. This paper described a technique used to secure raw data along with dummy bit insertion in hash code & for less memory utilization. The use of biometric allows identity to be obtained clearly. The result we have obtained based on real data from this research is satisfactory.

Keywords: Web Security, Authentication, Continuous Authentication, Biometric Authentication, Web Services.

I. INTRODUCTION

The large use of web applications & internet services increases day by day, E-commerce, online banking for transaction processing and email are part of daily practice for many communities. Therefore user authentication is important to create trust between user & internet services, that includes connecting a digital identity with single and accurate person. Previous system is implemented as one time identity proof during first log on process. Again here the legitimacy of user is believed to be same during entire session. Security of internet services & web application is measure issue because of increasing cyber attacks. Authentication method which depends on username & password, biometric authentications are" single shot" offers user verification only in login. One time user identity been verified the system services & resources are made available until user logouts and available for fixed time period. Many of the time user leaves already logged in system unattended for small or longer period in between other person can access same system intentionally for misuse. Solution to this problem is to provide session timeouts but this is not ultimate solution.

Biometric authentication & technique provides [2] solution for trusted and secure authentication, where the password and username is replaced by biometric data. Biometric authentication is a process of determining & identifying the legitimate person's identity based on physiological & behavioural features which include face recognition, fingerprint identification, retinal scans, and voice recognition. Biometric authentication deals with actually identifying person based on their unique physiological or behavioural characteristics instead of their exclusive knowledge (e.g. username/Password) or possession(e.g. smartcard). Traditional biometric solution also provides single authentication it gives authentication only during login phase and the identity of user is stable during entire session and again single authentication cannot provide adequate amount of security [3], [4].we have already discussed this example, consider the situation: a user has login to a security significant web or internet service, and then user/person leaves the system unattended for certain time. In these situation the services can be misused easily [3] [5]. To continuously detect and monitor the adverse misuse of computer resources & internet services from unauthorized entrée, the best solution is provide constant continuous and clear authentication is required instead of one time authentication. This is a guaranteed approach to web services & computer systems than usual one [1]. A major problem that continuous authentication aims to deal with is that user system or devices (mobile, laptop etc.) is used stolen after the user has already logged in. This paper presents a novel approach for continuous multiple verification & session supervision which is applied secure biometric authentication on the internet. It can function securely with different types of web services, with high safety and security requirements like online banking services.

II. LITERATURE SURVEY

The introduction to security issues & its concern is described in previous section. In this literature we have studied earlier research papers related to conventional authentication systems it presents single time authentications of the user. The categorizations of security systems are depend on strength of attack and are classified into strong and weak. The summarizing study of earlier research is as follows:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

1. Primary approach is knowledge based identity for authentication of user involves is password thai is what you know; Password contains single word, PIN (Personal Identification Number), Phrases that can be reserved secret for authentication. But this primary approach Knowledge based identity does not offer good solution it can be searched or guess by an attacker and they do not present security against repudiation [6].
2. Secondary approach is object based identity for authentication of user involves what you have is token; Token means a physical device which provides authentication that can be security tokens, access token, storage devices including passwords such as smart card or bank cards [6]. The main disadvantage of Identity token can be lost or stolen and inconvenience and cost.
3. Last approach is ID based authentication for authentication of user it considers who you are. That is simply biometric such as voice recognition, figure print identification, face recognition and signature or eye scan give stronger defence against attack. Comparing with Knowledge based and object/entity based ID based authentication provides privileged level of security. Four ways are presented to achieve computer security with biometric:

A. Keystroke Biometric
It is a type of behavioural biometric; it's an easy method for authenticating users where the users typing behaviour for validating identity is considered. Keystroke dynamics is simply "how you type not what you type" [7].It uses raw keystroke data to obtain timing features.
B. Voice Biometric
A voice biometric is unique for each and every individual like fingerprint. Voice biometric called numerical modelling consist sound pattern or rhythm of a users voice, sound. Voice biometric uses dissimilar characteristics of individual to distinguish between two speakers. This biometric is an interaction tool to user for verification [8].
C. Face Biometric
Face biometric includes detection and reorganization of human faces from digital image or video source. Facial database is required to distinguish certain feature from image. Face Identification and extraction includes many complementary parts. This type of authentication scheme is normally used in security systems [9], [10].
D. Finger Print Scan Biometric
Fingerprint scan biometric recognition is well known identification due to its easiness of acquisition. Several sources (ten fingers) available for acquisition and because of such uniqueness and uniformity fingerprint recognition are very famous. S. Kumar [4] represented a Multimodal biometric scheme which is developed to discover physical existence of individual sign in a computer. Approach considers that primary user login using strong authentication, and then depends on multimodal biometric continuous verification started. In [11] wristband a wearable authentication device is offered for continuous authentication of user where by wearing device user can login and continuous authentication takes place. In [13] the biometric authentications like face & fingerprint are integrated to improve performance in multimodal biometrics.

III.PROBLEM DEFINITION

Earlier technique consisting fully exposed raw data and information. To overcome negative aspect of previous system & providing further level of security we have developed a novel approach for security enhancement. In current approach raw data is converted into hash code using supervised semantic hashing technique the reliability and integrity of the data can be maintained by dummy packet insertion. System performs continuous verification and it is takes place by providing multiple authentication scenario e.g graphical\text passwords.

IV.SYSTEM DESIGN

System below experimentation is divided into two important parts – framework of CASHMA [12] and web services. In the proposed approach during interactive session client feature will be capture for multimodal biometric textual password as well as graphical password. For continuous and constant authentication different scheme is used which consist multimodal biometric, Graphical password and text based password, CASHMA framework continuously captures data from user. To securely transfer a data CASHMA framework is used, without this secure data transformation is not possible. Fig 1 represents proposed system architecture. Feature extraction module used to extract features by different ways and then extracted features will be combined & used by CASHMA packet to transfer data securely, CASHMA [12] packet is transferred and raw data is extracted from packet along with it features are extracted & compared for authentication. Verification system uses the extracted features and compares it from existing training database for secure user authentication.

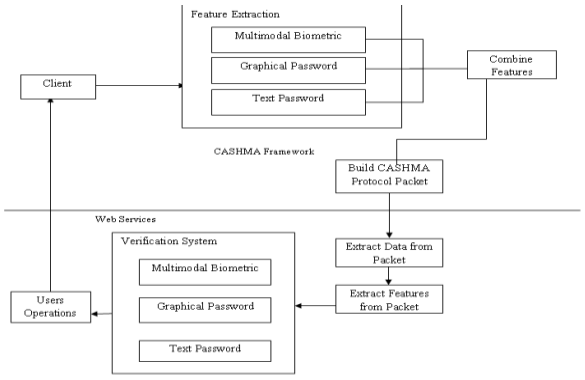

Fig.1. System Architecture

From Multimodal Biometric, Graphical password and Text password verification system performs verification. Success results in authentication & processing of desire operation and failure results in returning to authentication process.This is an step wise working of proposed approach.

DOI 10.17148/IJARCCE.2016.56184

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

V. IMPLEMENTATION DETAILS

The algorithmic details & techniques used in system in experimentation are explained here. The different algorithmic strategies & technique is used. K-Nearest neighbour used for classification, in face recognition for feature extraction we are using PCA principal component analysis algorithm, voila Jones algorithm for face detection.

1. Voila Jones Face Detection

Voila Jones algorithm uses the cascade classifier named for face detection; basically this algorithm works on the cascade data that are stored in the cascade xml file .This classifiers uses these data for the detection purpose.

2. PCA –Principle Component Analysis

After face detection the features of face are extracted using PCA.Advantage of PCA that is extract few number of features as compared to other algorithms and give good accuracy rate compared to others.

3. K-NN Algorithm

At server end the KNN is used for the finding the exact match or if not then most likely one match is identified by using k-NN algorithm.

4. Sensitive Hashing

To convert data into bit representation form Sensitive hashing technique.

5. Privacy preservation

To secure the data transferring between server & client we are using dummy bit insertion the advantage of this technique is at the receiver end we can authenticate the data.

VI. RESULT ANALYSIS

				Trusted level with respect to attack		
Time for face recognition				Trusted level with respect to attack	Result values	Current values
Plain image		Secured image		Trust value	Time	Time
No. of client	Time (ms)	No. of client	Time (ms)	0.94	0	0
1	10	1	10	1	100	50
10	15	10	18	0.9	200	100
25	20	25	22	0.98	400	200

TABLE I

VII. CONCLUSION

In proposed system the user's identity is continuously verified & system has main focus on the data security and integrity. Here a secure data flow with privacy preservation for the session management by using biometric systems will be offered. The data is secure by hashing technique and privacy is preserved using dummy packet insertion. The main benefit is that by continuous user authentication data is transfer securely, easily and fast. This can prevent the hackers and other intruders from accessing the highly secret and confidential.

ACKNOWLEDGMENT

We are satisfied to express our thanks to all who rendered their valuable guidance to us. We would like to convey our appreciation and gratitude to **Prof. Dr. G. K. Kharate**, Principal, M. C. O. E. R. C. Nashik. I am also thankful to **Prof. V. H. Patil**, Head of Computer Department, M. C. O. E. R. C. Nashik.

REFERENCES

[1] Andea ceccarelli, Leonardo Montechhi Francesco Brancati,Paolo Lollini,"Continuous and Transparent User Identity Verification for secure Internet Services",IEEE transaction on dependable & secure computing Vol.12,No.3,May/June 2015

[2] S.Z.Li and A.K.Jain,"Encylopedia f biometrics"First ed.,Springer 2009.

[3] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007

[4] 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

[5] A.Altinok and M.turk,"Temporal Integration for continuous Multimodal Biometrics,"Proc.workshop Multimodal User Authentication,pp.11-12,2003.

[6] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE, Vol. 91, No.12, Dec. 2003, pp. 2019-2040.

[7] Arwa Alsultan and Kevin Warwick, "Keystroke Dynamics Authentication: A Survey of Free-text Methods", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013.

[8] Dwijen Rudrapal, Smita Das, S. Debbarma, N. kar, N. Debbarma, "Voice Recognition and Authentication as a Proficient Biometric Tool and its Application in Online Exam for P.H People", International Journal of Computer Applications, Volume 39– No.12, February 2012.

[9] S.Sudarvizhi, S.Sumathi, "Review on continuous authentication using multi modal biometrics, International Journal of Emerging Technology and Advanced Engineering", Volume 3, Special Issue 1, January,2013.

[10] D. M. Nicol, W. H. Sanders, K. S. Trivedi, "Model-based evaluation: from dependability to security", IEEE Trans. Dependable and Secure Computing, vol. 1 no. 1, pp. 4865, 2004.

[11] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for Transparent Login in Nomadic Applications Environment," Proc.Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 6, Nov. 2008Proc.Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 6, Nov. 2008

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

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

BIOGRAPHY

Poonam Mahale is a M.E student from Computer Engineering Department, MCOERC, Nashik & Savitribai Phule Pune University. Having research interest in Cyber Security, Web Security, Information Retrieval & Data mining etc.