Secure User Authentication Based on Continuous Multiple Verification

1.Poonam Mahale , *Department of computer Engineering, MCOERC, Nashik*
2.Mr.Niranjan Bhale, *Head, Department of I.T, MCOERC, Nashik*

Abstract—A secure internet service is one of the major issues in the field of internet services. Internet services are based on session management of username password, explicit logouts user session expiration that uses timeouts. Biometric solution allows substitution of password with biometric information in session establishment with single verification. In proposed work, additional level of security can be provided multiple verification can deployed for authentication. The user identity is continuously verified by applying different authentication in session management. Security efficiency of system is exercised by different kinds of attacks. A secure data flow with privacy preservation for the session management by using biometric systems with less memory utilization will be offered. 128-bit Supervised Hashing technique is 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.

Index Terms—Supervise, Web Security, Authentication, Continuous Authentication, Biometric Authentication, Web Services.

1 Introduction

THE use of internet services increasing gradually, the use of internet applications such as e-commerce online banking for transaction processing and email are part of daily practice for many communities. Therefore healthy rich user authentication is essential to maintain trust between user internet services, which indicates connecting a digital identity with single and accurate person. In traditional computer systems, pair of authentications like username and password is used to validate the persons identity at login stage. Identity of user is unverified throughout working session. The web based applications are susceptible to security or threats, which leads to safety security of internet services.

Biometric technique or biometric authentication offers [2] solution for trusted and secure authentication, in which user name and password is replaced by biometric data. Biometric is a technology of determining identifying the legitimate user identity based on physiological behavioral characteristics which involve face recognition, fingerprint, retinal scans, and voice recognition. Biometric authentication deals with actually identifying person rather than of their exclusive knowledge (e.g. username/Password) or possession(e.g. smartcard).Biometric solution also leads to single authentication it provides authentication during login where the identity of user is constant all over session and again single authentication cannot leads to adequate amount of security[3], [4].For example consider this situation: a user has logged into a security significant web or internet service, and then user/person left the system unattended for a while. In these situation the services can be misused easily [3] [5].

To timely detect the undesirable misuse of computer resources internet services from unauthorized access, solution is provide continuous transparent authentication instead of one time verification. This is a promising approach to web services computer systems than traditional one [1].

This paper represents a novel approach for continuous multiple verification session supervision which is applied secure authentication

Organized by PCCOE, In Association with BOS(Comp Engg), SPPU,Pune on the internet. It can be function securely with several types of web services, with high safety security requirements like online banking services.

2 Literature Survey

The introduction to security systems methods are described. Depending on strength of attack security systems are categorized in to strong and weak. The concise study of previous research is as follows:

First approach knowledge based identity is considered what you know is password; Password includes single word, PIN (Personal Identification Number), Phrases that can be kept secret for authentication. Knowledge based identity does not provide good solution it can be searched or guess by an attacker and they do not present defence against repudiation [6].

Second approach object based identity is considered what you have is token; Token includes a physical device which provides authentication it can be security tokens, access token, storage devices including passwords such as smart card or bank cards [6]. The main disadvantage of identity token is inconvenience and cost. Identity token can be lost or stolen.

Third approach ID based authentication it considers who you are. Biometric such as voice recognition, figure print, face, signature or eye scan give stronger defence against attack. Compared to Knowledge based and object/entity based it provides privileged level of security. Four ways available to achieve computer security with biometric:

A. Keystroke Biometric:

It is a behavioural biometric, its an effortless method for authenticating users where the users typing patterns for validating identity. Keystroke dynamics is how you type not what you type [7].Keystroke biometric uses raw keystroke data to obtain timing features.

B. Voice Biometric

Voice biometric called numerical modelling consist pattern or rhythm of a users voice, sound. Voice biometric uses different characteristics of individual to discriminate between speakers. Its an interaction tool to user for authentication [8].

C. Face Biometric

Face biometric consist detecting and recognizing human faces from digital image or video source. Facial database is used to differentiate selected feature from image. Identification and extraction includes many complementary parts. It is normally used in security systems [9], [10].

D. Fingure Print Scan Biometric

Fingerprint recognition is well known identification due to its ease of acquisition. Numerous sources (ten fingers) available for acquisition and due to uniqueness and uniformity fingerprint recognition are very popular.

S. Kumar [4] presented a Multimodal biometric scheme is developed to discover physical existence of individual sign in a computer. Approach considers that primary user login using strong authentication, and then based on multimodal biometric continuous verification started. In [11] wristband a wearable authentication device is offered for continuous authentication of user. Wearing device user can login transparently.

3 Problem Statement

Previous approach consisting fully exposed data. To defeat drawback of previous system providing additional level of security we are introducing a novel approach for security enhancement. In which we converting raw data into hash code using supervised semantic hashing technique the integrity of the data can be maintained by dummy packet insertion along with it continuous verification is takes place by providing multiple authentication scenario e.g graphical / text password.

4 Implementation Details

This section highlights the system architecture,algorithmic details techniques used in system in experimentation.

4.1 System Architecture

System under experimentation is divided into two parts CASHMA framework [12] and web services. In the proposed approach client feature will be capture during interactive session. For continuous authentication different scheme will be used which consist multimodal biometric, Graphical password and text based password, It continuously captures data from user. Fig 1 consist proposed system architecture. Extracted features will be combined will be used by CASHMA packet, CASHMA [12] packet is transferred and raw data is extracted from packet along with it features for authentication will be extracted. Verification system uses the features for comparison from available training database to secure authentication.

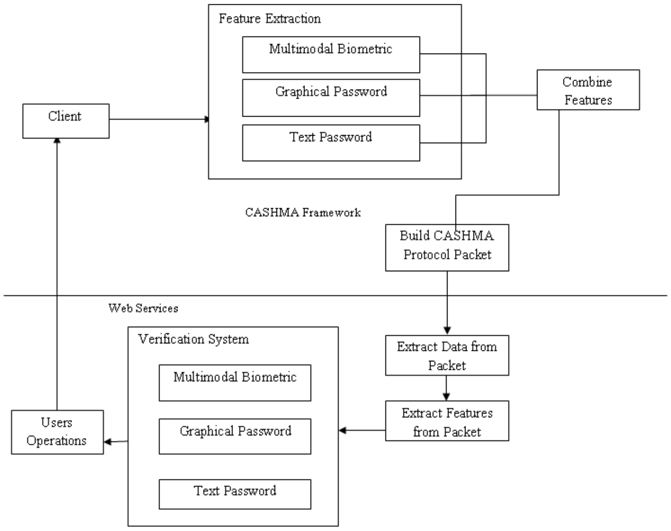


Fig. 1. System Architecture

Verification system verifies from Multimodal Biometric, Graphical password and Text password.Sucessful authentication results in processing of desire operation and failure results in returning to authentication process.This will be an step wise working of proposed approach.

4.2 Algorithms

4.2.1 Viola Jones Face Detection

This algorithm uses the cascade classifier namely adaboost classifier for the detection of the face, basically this algorithm works on the cascade data that are stored in the cascade xml file. The classifiers uses these data for the detection purpose. Subsubsection text here.

Input: Set of training images,

1) In first step of cascade voila Jones recommend constructing of simple prescreening filter including template features.
2) Determine the variation among face based on the template features.
3) Match training set and testing set used for experimentation.
4) Describe concluding result concerning primarily the positive training set and negative training set.

Output: set extracted face images

4.2.2 PCA Algorithm

In face recognition for feature extraction we are using PCA principal component analysis algorithm.After detection the features are extracted using PCA the main advantage of PCA that is extract few number of features as compared to other algorithms and give good accuracy rate compared to others.

Input: Set of face image vector

1) Convert image of training set to image vectors each image is size NxN
2) For each (Image in training set)
   {
   NxN Image
   } Image converted to vector
3) Normalization of face vectors.
   - find the average face vectors "u"
   - Deduct any face vector from every face vector to get normalized face vector.
4) Calculate the Eigenvectors(Eigenvectors represent the variation in the face)
5) Calculating Eigenvectors from reduced covariance matrix.
6) Select p best eigenfaces such that p<=M and can represent complete training set.
7) convert lower dimension p eigenvectors to original face dimensionality.
8) Represent each image a linear combination of all p-eigenvectors

Output: set of feature extracted

4.2.3 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.

Input: training data M and N

1) For all training example, <M, f(m)> to the list of training examples add the example.
2) Categorize (M, N, m) where M: Training data, N: Class labels of M, m unknown sample.
3) For i=1 to x do Calculate Distance d (M_i , m) End for
4) Calculate set P containing indices for k smallest distance d (M_i , m).
5) Return maximum label for(Ni where i∈P)

Output: maximum number of labels L (or instances)

4.2.4 *Sensitive Hashing*

Sensitive hashing is used to convert the data in the bit representation using hashing technique.

4.2.5 *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.

4.3 Mathematical Model

Set theory: Let, U= {C, O, F, G, T, P, A} Where,

C= set of client connected

O= set of operations that are performed by client

F= set of feature extracted from face biometric

G= set of graphical password

T= Set of text password used

P= Protocol build over obtained information

A= is set of authentication process that is carried out

- F_C(o)→C, Where FC is a function that generated operation at every individual client
- F_F(c)→F,Where FF is a function that generates features from face biometric
- F_G(c)→G,Where FG is function for graphical password
- F_T(c)→ T is function for text password
- F_A {F, T, G, O} → FP is a function to generate the set of protocol
- F_A (P)→R

Where, FA is a function that authenticates data in the protocol and performs specified operation. The basic data structure we are using is array and linked list.

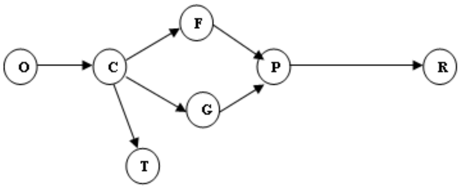


Fig. 2. Dependency Garaph

It takes finite input and gives finite output so we can say our system is NP complete. We are using Object oriented approach for the implementation of our project. Average Time Complexity is **nlogn**

5 Current State of System and Testing

In proposed system user sign in then starts performing an operation simultaneously our proposed approach performs authentication by considering face biometric as well as text based password is used for multiple continuous verification and if it fails during operation results in logout. Testing would be performed on single system check, two client login check and N no. of client check.

The following are the screenshot of how user logs in perform operation with multiple verification scenarios and other represents server end it gives activity performed at time instance.

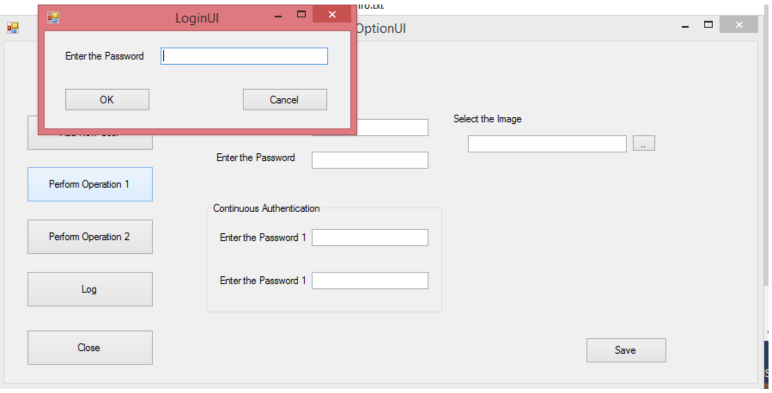
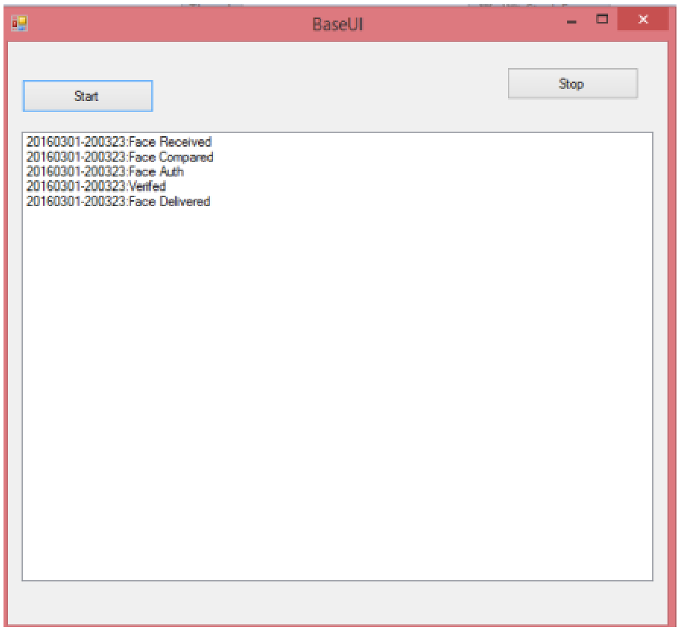


Fig. 3. Operation-UI



```
20160301-200323:Face Received
20160301-200323:Face Compared
20160301-200323:Face Auth
20160301-200323:Verifed
20160301-200323:Face Delivered
```

Fig. 4. Generated value after detection

6 Expected Result

The Existing approach provides a protocol for continuous authentication which improves security usability of session. The proposed system will provide higher security with less time complexity. A secure data flow with privacy preservation for the session management by using biometric systems with less memory utilization will be offered.following table will be our tentative expected result.

				Trusted level with respect to attack		
Time for face recognition				Trusted level with respect to attack	Expected values in the final result	Current values
Input=Plain image		Input=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

7 Conclusion

Our proposed system has main focus on the data security and integrity. The data represents the raw data generated through biometric system and authentication service. The data is secure using the hashing technique and privacy is preserved using dummy packet insertion. The main advantage is that data can transfer secure, easily and fast with continuous user authentication. This can prevent the hackers and other intruders from accessing the highly secret and confidential. So we can say improving the security of the entire system.

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 of biometrics*, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.

[3] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, *Continuous Verification Using Multimodal Biometrics*, First ed.,Springer 2009 .

[4] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, *Using Continuous Biometric Verification to Protect Interactive Login Sessions*, First ed.,Springer 2009Proc. 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 OGorman, *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 Intl Conf. Signals, Circuits and Systems (SCS 08), pp. 6, Nov. 2008Proc.Second Intl Conf. Signals, Circuits and Systems (SCS 08), pp. 6, Nov. 2008.

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

Poonam B. Mahale a M.E student in the Computer Engineering Department, MCOERC, Nashik, Savitribai Phule Pune University, Pune. Her research interests are Web security, Information assurance and security, Cyber security, Information Retrieval etc.

Prof. Mr.Niranjan L. Bhale Head,Department of Information Technology,MCOERC,Nashik.