

Integration of Sound Signature in 3D Password Authentication System

Mr. Jaywant N. Khedkar¹, Ms. Pragati P. Katakhar², Ms. Shalini V. Pathak³, Mrs. Rohini V. Agawane⁴

Student, Dept. of Computer Engineering, KJCOEMR, Pune, India^{1, 2, 3}

Assistant Professor, Dept. of Computer Engineering, KJCOEMR, Pune, India⁴

Abstract : Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose their nick names, which make textual passwords easy to break. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards can be stolen. Many biometric authentications have been proposed; however, users tend to prevent using biometrics because of their intrusiveness and the effect on their privacy. Therefore, biometrics cannot be revoked. In this paper, we present the 3-D password. The 3-D password is constructed by sequence of the interactions and actions which performed by users. In other words, The 3D Password scheme is a new authentication scheme that combine RECOGNITION + RECALL + TOKENS + BIOMETRIC in one authentication system. The 3D password can combine authentication schemes such as textual passwords, graphical passwords, and different types of biometrics with supportive sound signature. 3D passwords are flexible and they provide unlimited passwords possibility.

Keyword : Authentication, textual passwords, graphical passwords, biometrics passwords, sound signature, multifactor, 3-D password

I. INTRODUCTION

We are provided with many password types such as textual passwords, graphical passwords, biometric scanning, cards (such as an ATM) etc. But there are many weaknesses in current authentication systems. When a person uses textual passwords, he chooses their nick names or favourite thing or place names etc which can be cracked easily. Graphical passwords strength comes from that users can recall and recognize pictures more than words. Token based systems can also be used as way of authentication in banking systems. But cards are loss or theft. Biometric recognition scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic. Most biometric systems require a special scanning device to authenticate users, which is not applicable for Internet users. So, we have introduced 3-D password scheme with sound signature.

Objectives

- The system provides more secure authentication for user.
- 3D password authentication system is more secure system than others.

II. RELATED WORKS

A) Existing System

In existing system, we use Text Password and Graphical Password. But there is some drawbacks likes in Textual Passwords should be easy to remember at the same time easy to crack that password or easy to guess for another users. . Also in Graphical passwords, this passwords came as users can recall and recognize pictures more then words. But most graphical passwords are attacks by attacker can observe or record the valid user graphical password by camera. The main weakness in biometric is that this passwords can not be changed or revoked. Smart cards can be lost or stolen.

B) Proposed System

The proposed system is a multi factor authentication scheme which combines the advantages of more than two authentication schemes. Users can choose whether the 3D password will be combination of textual, graphical and biometrics with supportive sound signature. This choice of selection is necessary because users are different and they have different requirements.

The following features are satisfied in proposed system:

1. The new system provide passwords that are easy to remember and very difficult for another users to guess.
2. The new system provides passwords that are not easy to write down on paper.
3. The new system provides passwords that can be easily revoked or changed.

III. SYSTEM ARCHITECTURE

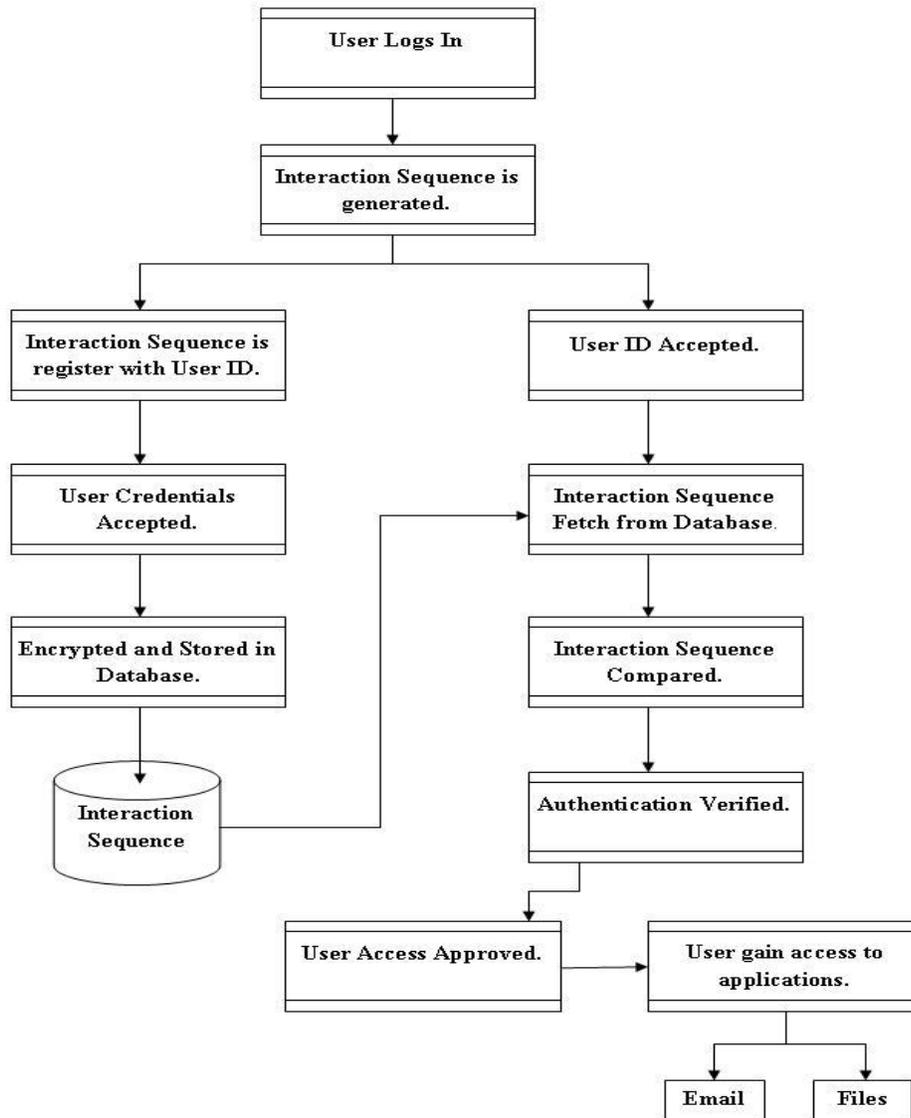


Fig I: System Architecture

A) Working

➤ Registration

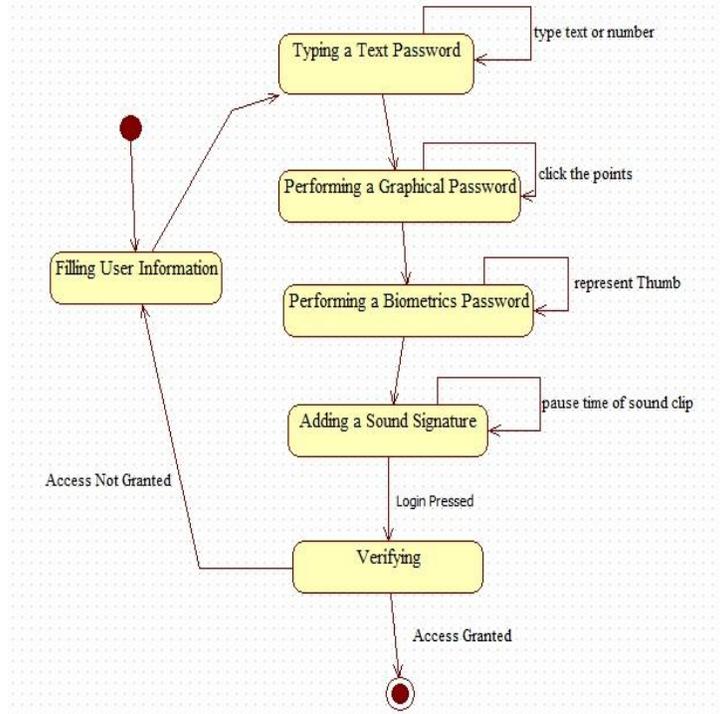
1. When new user register, first enter the all details which give in registration form.
2. Then select any one image from multiple images and also click the minimum 4 points at any sequence.
3. Then represent the Thumb expression of user
4. Then select any one sound clip, play and pause that clip at particular time.
5. This all interactions stored in database in encrypted format.

➤ Authentication

1. Enter username and password.
2. Select proper image and their sequence of click points.
3. Recognize the Thumb expression of that user.
4. Select proper sound clip and their pause time.
5. All interactions fetch from database then compared one by one.

Then access granted to authorized user for access applications.

B) System Flow



FigII:Flow of the System

IV. SYSTEM DESCRIPTION

A) Authentication Schemes :

In this system, we use multiple authentication schemes for give access of data or any system for authorized user and also the security for any system or data. Following schemes are used in this system.

1) Text Authentication

In this scheme, we use simple Username and Password for Authentication. When register the new user, save all detail information of that user and also save Username and Password of that user as per user's choice in System Database. This Password is stored in database in encrypted format using Message Digest 5 Algorithm.

When user log's in, first enter the Username and Password then system check the new Username and Password is same or not. If incorrect then give the error and if it is correct then give permission for next authentication scheme.

- **Algorithm used in this System for Encryption :**

Message Digest 5 (MD5)

1. The MD5 algorithm accepts a message as input and generates a fixed length output which less than the length of input message.
2. The output is called a hash value or message digest.
3. The MD5 algorithm is mostly used for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.”

To compute the message digest of the message five steps are performed as following :

1. Append Padding Bits
2. Append Length
3. Initialize MD Buffer
4. Process Message in 16-Word Blocks
5. Output

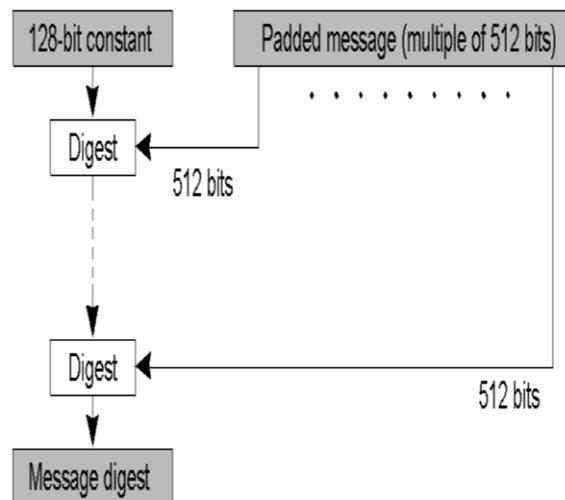


Fig III: Working of MD5

2) Graphical Authentication

In this scheme, we use images for Authentication. When register the new user, first select the one image from given images and then click any four points that is pixel values in sequence which stored in System Database. This click points are also stored in database in encrypted format using Message Digest 5 Algorithm.

When user log's in, first select the proper image and click points in same sequence then system checks that image and click points are same or not. If incorrect then give the error and if it is correct then give permission for next authentication scheme.

3) Bio-Metrics Authentication

In this scheme, we use thumbnail expression of user for Authentication. When register the new user, take the thumbnail expression of user using thumb detection device and stored in image format in System Database.

When user log's in, user give the thumbnail expression using thumb detection device then system checks that image is same or not. If incorrect then give the error and if it is correct then give permission for next authentication scheme.

4) Sound Signature

In this scheme, we use sound clips for Authentication. When register the new user, select one sound clip and play that clip then stored its pause time in System Database.

When user log's in, first select proper sound clip and it's pause time then system checks that sound clip and pause time are same or not. If incorrect then give the error and if it is correct then give permission for access the data or any system.

B) Database Design:

The database which has been created from this system consists USER registration. The detailed information in every table is shown in following table:

TABLE	FUNCTION	FIELD NAME	DATATYPE
USERINFO	PERSONAL INFORMATION OF USER	USERNAME PASSWORD FNAME LNAME AGE MOBNO EMAIL	TEXT TEXT TEXT TEXT TEXT NUMBER TEXT
IMAGEINFO	INFORMATION OF IMAGE CLICK POINTS	USERNAME PIXELS	TEXT TEXT
BIOINFO	SAVE IMAGE OF THUMB OF USER	USERNAME IMAGEPATH	TEXT TEXT
SOUNDINFO	SAVE INFORMATION OF SOUND PAUSE TIME	USERNAME TIME	TEXT TEXT

V. EXPERIMENTAL RESULTS

We have built an experimental 3-D password that contains several schemes. The first type of response is the textual password. The second type of response is requesting graphical passwords. The third type of response is requesting biometrics passwords. The last type of response is requesting sound signature. We asked the users to create their 3-D password and to sign-in using their 3-D password several times.

VI. CONCLUSION

In the existing system, Textual passwords and token-based passwords are the most common used authentication schemes. The main goal of this paper is to have a scheme which has a huge password space and which is a combination of existing, or new, authentication schemes into one scheme. While using 3D password, users have the freedom to select whether the 3D password will be recall, biometrics, recognition, or token based, or a combination of two or moreschemes with sound signature.

Users have the choice to construct their 3D password according to their needs and their preferences .The main application domains of 3D Password are critical resources and systems. Moreover, Airline's system, banking systems and operating system's logins can also make use of 3D passwords to provide more secured authentication.

REFERENCES

[1]. Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, Senior Member, IEEE " Three-Dimensional Password for More Secure Authentication", IEEE transaction on instrumentation and measurement, 0018-9456,2008.

[2]. X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annu. Comput. Security Appl. Conf., pp. 463–472, Dec. 5–9, 2005.

[3]. F. A. Alsulaiman and A. El Saddik, "A novel 3D graphical password schema,"IEEE Journal Virtual Environment, Human-Computer Interfaces,pp.125-128, July 2008.

[4]. I.Jermyn,A.Mayer,F.Monrose,M.K.Reiter,andA.D.Rubin, "The design and analysis of 3D passwords," Special Issue on HCI Research in Privacy and Security,vol. 63,pp.102-127, July2005.

[5] Saurabh Singh and GauravAgarwal "Integration of Sound Signature in Graphical PasswordAuthentication System," International Journal Of Computer Applications (0975 – 8887) Volume 12– No.9, January 2011.

[6] DuhanPooja, Gupta Shilpi ,SangwanSujata, &Gulati Vinita , "Secured authentication: 3D password,"International Journal Of Engineering and Management Sciences , I.J.E.M.S.(242 – 245), VOL.3(2),2012..



BIOGRAPHY



Jaywant Nivrutti Khedkar is student of BE in Computer Science from **KJ College of Engineering and Management Research**, Pisoli, Pune in Pune University. His main areas of interest are image processing and networking.



Pragati Prabhakar Katakhar is student of BE in Computer Science from **KJ College of Engineering and Management Research**, Pisoli, Pune in Pune University. Her main areas of interest are image processing and information retrieval.



Shalini Vinod Pathak is student of BE in Computer Science from **KJ College of Engineering and Management Research**, Pisoli, Pune in Pune University. Her main areas of interest are image processing and networking.



Rohini Vijay Agawane received BE in Information Technology from VPCOE, Baramati, Pune University India in the year 2004 and M.E in Information Technology from SCOE,Pune, Pune University,India,She is working with the Department of Computer in **KJ College of Engineering and Management Research**, Pisoli, Puneas a **Lecturer**,affiliated to the Pune University,India. Her main areas of interest are image processing.