International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 03 , March 2017
www.ijarse.com

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

THREE LEVEL PASSWORD AUTHENTICATION SYSTEM

Swarna Lakshmi M[1], Roobini S[2], Shalie Monicka A[3],
Saraswathi V[4], Ms. N. Radha[5]

[1,2,34] Final year CSE Students, Saranathan College of Engineering,Trichy, (India)

Assistant Professor, Department of CSE, Saranathan College of Engineering,Trichy, (India)

ABSTRACT

Inspite of many efforts taken nowadays security threats existing, so using just single level authentication factors is not sufficient to ensure security. In this paper, an idea is to implement three levels of security for authenticating for true users. The effort is taken to resist shoulder surfing attack through the text based graphical password which constitutes first level of authentication. The unique one-time password (received through registered email id of authentication) forms the second level of authentication. Third level uses a smartcard containing the unique token (this card is given to the user either directly or through post (to the address given by user during registration)). These three levels of password in securing the resources from unauthorized use.

Keywords: HOTP, Graphical Password, Multi- Factor Authentication, Smartcard, RFID, Shoulder Surfing

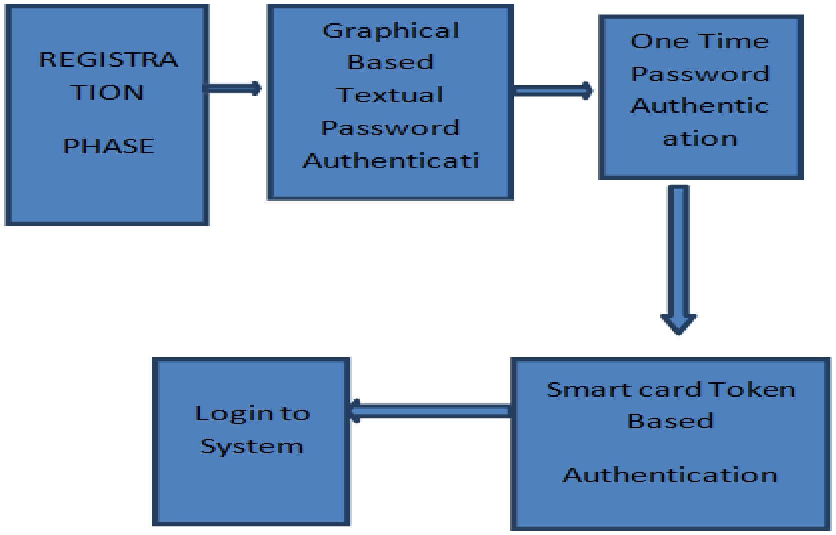
I INTRODUCTION

Today providing security is considered as a major problem in several areas which may include internet banking and in some areas where high level of security to preserved confidentiality of users data. Using static passwords alone makes it easy for the hackers to hack the users account. Especially static password are vulnerable to many security attacks such as shoulder surfing. So this paper uses static password combined with dynamic password(OTP) and smartcard login facility is used as a additional level which provides high security. Multifactor authentication is a system where in two or more different factors are used in conjunction authenticate. Using more than one factor is sometimes called "Strong Authentication". This paper suggest the use of both hardware token (smartcard) and the software token (HOTP which is system generated). These two tokens are used as separate levels of authentication to ensure the security to user profile.

Even though if one token is known to hacker accidently, without knowing the other one users account cannot be accessed by unauthorized person. Software tokens are programs that run on computers and provide a one-time password that it is changed after a short amount of time. In this paper section 2 explains the existing authentication mechanism and the problems with them. The section 3 explains the proposed system and its merits when compared to the existing ones. Multifactor authentication solution equips customers with a cost effective means of providing flexible and strong authentication to very large scale. However, since fraud rate is reduced as compared to that of One- Factor authentication. The goal of computer security to maintain the integrity, availability and privacy of the information entrusted to the system can be obtained by adapting this authentication technique.

II EXISTING SYSTEM

Authentication is an act of confirming the truth of an attribute of a single piece of data claimed true by an entity. There are many password schemes which are existing currently. They can generally categorized into four such as follows:


REGISTRA TION PHASE
Graphical Based Textual Password Authenticati
One Time Password Authentic ation
Smart card Token Based Authentication
Login to System

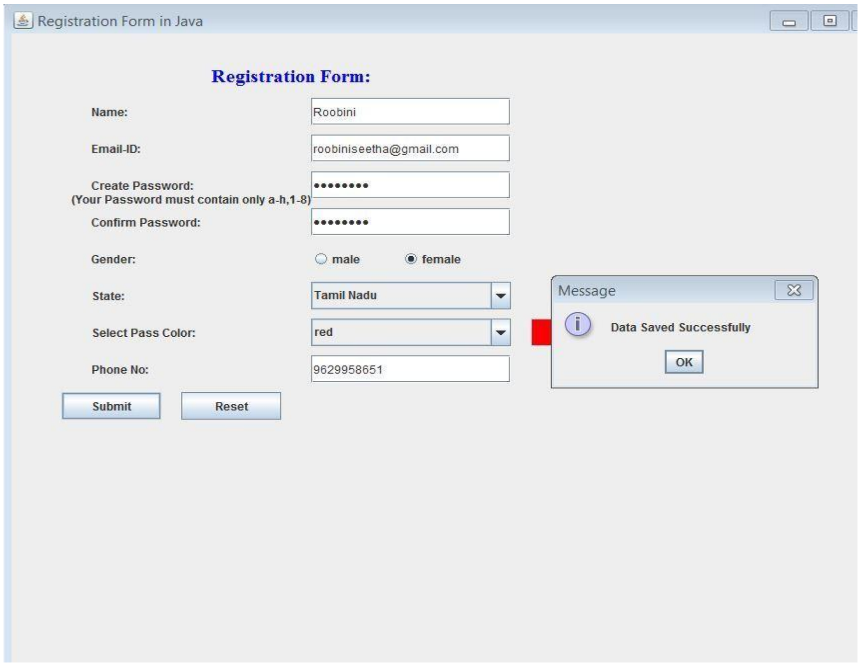
III PROPOSED SYSTEM ARCHITECTURE

1. the knowledge factors: Something the user k `````` nows (a password, personal identification number (pin),security question)
2. The ownership factors: Something the user has(security tokens, hardware token, cell phone holding the software token)
3. The inherence factors: Something the user is(finger print, retinal pattern, DNA sequence, voice)
4. Graphical password (color,images)

Most of the organizations use biometrics as a authentication method. But for capturing, storing users physical features such as fingerprint, iris etc. . many devices are required. These devices are more expensive and requires maintenance charges too. Considering alphanumeric password which is static in nature and they are simple but not much secured. Since many of the users choose the easily guessable password such as their favorites, date of birth.

These kind of passwords can be easily broken by brute force attacks. Eventhough when the user selects an alphanumeric password which is difficult to guess hacker can use shoulder surfing attack to get that password. When hardware tokens alone is used, if the user loses the hardware token accidently and if it reaches the hands of an unauthorized person then the user cannot gain access to his account.

In the Registration phase, the user should provide user's details along with his/her email id, mobile number, address, textual password and choose a pass color for them. The user also has to choose a security question and answer that question. It can be used to recover the password when the forget it. After the registration phase executed successfully, all the details are stored in the database for later verification. Then, the smartcard having a unique PIN number generated for that particular user will be handed over to him by the organization.



Registration Form in Java

Registration Form:

Name:	Roobini
Email-ID:	roobiniseetha@gmail.com
Create Password: (Your Password must contain only a-h,1-8)	•••••••••
Confirm Password:	•••••••••
Gender:	○ male ● female
State:	Tamil Nadu
Select Pass Color:	red 🟥
Phone No:	9629958651

Message

Data Saved Successfully

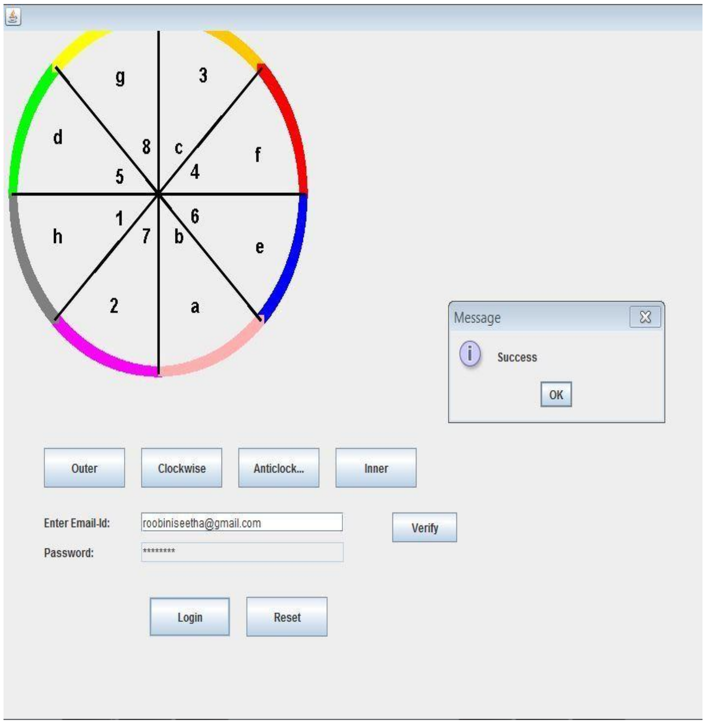
The reason for making the user to choose the pass color is to cross the first level of authentication which is text based graphical password explained as follows:

The textual password chosen by the user should have the length between 8 to 15 and contain characters a-h,1-8 of any length from minimum 8 to maximum 15. The user is allowed to choose one of the eight colors provided by the system as pass color. When the user request to login the system, the system displays the circle composed of eight equally sized sector the colors of the arcs of the eight sectors are different and each sector is identified by the color of its arc.

3.1. A shoulder surfing resistant graphical password scheme:

Initially, sixteen characters (a-h , 1-8) are placed randomly among the sectors as each sector will have two character such that one character is in inner side and other in the outer sector. The user is first prompted to enter the registered email id which act as his username. This username is verified against the one in the database after successful verification the user is allowed to enter the password. In the login screen, the user is provided with four buttons namely clockwise, anti-clockwise, inner orbit, outer orbit. When the user clicks on the clockwise button, the circle is rotated in a clockwise direction such that the color of particular sector moves into its adjacent sector in a clockwise manner. Similar operations take place, when the user clicks on anti-clockwise button but the rotation happen in a anti-clockwise direction.

The user has to rotate circle in such a way that in moves his pass color arc into the sector having his text password character. If the desired character is present on the inner side of the sector, then the user has to click on the inner orbit button. If the character is present on the outer side, then user has to click the outer orbit button. By doing this so, the password character is entered in the text box without directly type through keyboard thus avoiding the shoulder surfing attack. These steps are repeated until the user enters the complete password. After doing so, login button is clicked and the password of the user is verified. If the password matches with the one in the database, then the user has successfully crossed the first level of password.



Message

Success

Enter Email-Id: roobiniseetha@gmail.com

Password: ********

3.1.2. Algorithms Used

There is no static position of characters placed in the sectors. So, for the random printing of the characters when the user login Fisher Yates algorithm is used which does the random shuffling of the characters in the array which gets printed into the sectors. Bersanham algorithm is used for drawing a circle and divided it into eight equally sized sectors .

Algorithm: Bresanham Algorithm

Step 1 − Get the coordinates of the center of the circle and radius, and store them in x, y, and R respectively. Set P=0 and Q=R.

Step 2 − Set decision parameter D = 3 – 2R. Step 3 − Repeat through step-8 while X < Y. Step 4 − Call Draw Circle

(X, Y, P, Q).

Step 5 − Increment the value of P. Step 6 − If D < 0 then D = D + 4x + 6.

Step 7 − Else Set Y = Y + 1, D = D + 4(X-Y) + 10.

Step 8 − Call Draw Circle (X, Y, P, Q).

3.2. OTP Generation Algorithm

The HOTP algorithm is based on an increasing counter value and a static symmetric key known only to the token and the validation service. As the output of the HMAC-SHA-1 calculation is 160 bits, Truncate this value to something that can be easily entered by a user.

HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))

Where:

The Key (K), the Counter (C), and Data values are hashed high-order
byte first.

- Truncate represents the function that converts an HMAC-SHA-1
value into an HOTP value as defined in following sections.

Generating an HOTP Value:

The operations can be described in 3 distinct steps: Step 1: Generate an HMAC-SHA-1 value Let HS = HMAC-SHA-1(K,C) // HS is a 20-byte string

Step 2: Generate a 4-byte string (Dynamic Truncation)

Let Sbits = DT(HS) // DT, defined below,

// returns a 31-bit string

Step 3: Compute an HOTP value
Let Snum = StToNum(Sbits) // Convert S to a number in 0. . . 2^{31}-1
Return D = Snum mod 10^Digit // D is a number in the range 0. . . 10^{Digit}-1

The Truncate function performs Step 2 and Step 3, i.
e. , the dynamic truncation and then the reduction modulo 10^Digit. The purpose of the dynamic offset truncation technique is to extract a 4-byte dynamic binary code from a 160-bit (20-byte) HMAC-SHA-1 result.
DT(String) // String = String[0]. . . String[19]
Let OffsetBits be the low-order 4 bits of String[19] Offset = StToNum(OffsetBits) // 0 <= OffSet <= 15 Let P = String[OffSet]. . . String[OffSet+3]
Return the Last 31 bits of P

Implementations MUST extract a 6-digit code at a minimum and possibly 7 and 8-digit code. Depending on security requirements, Digit = 7 or more SHOULD be considered in order to extract a longer HOTP value.
The following paragraph is an example of using this technique for Digit = 6, i. e. , that a 6-digit HOTP value is calculated from the HMAC value.

Example of HOTP Computation for Digit = 6

The following code example describes the extraction of a dynamic binary code given that hmac_result is a byte array with the HMACSHA- 1 result:

```
int offset = hmac_result[19] & 0xf ;
int bin_code = (hmac_result[offset] & 0x7f) << 24
| (hmac_result[offset+1] & 0xff) << 16
| (hmac_result[offset+2] & 0xff) << 8
| (hmac_result[offset+3] & 0xff) ;
```

Considering the security analysis, the security of the HOTP algorithm by the following formula:
Sec = sv/10^Digit

Where:

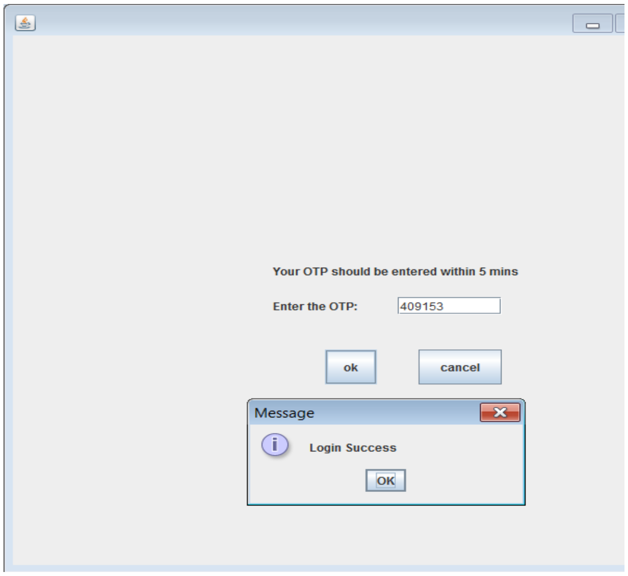
- Sec is the probability of success of the adversary;
- s is the look-ahead synchronization window size;
- v is the number of verification attempts;

- Digit is the number of digits in HOTP values. Obviously, with s, T (the Throttling parameter that would limit the number of attempts by an attacker), and Digit until achieving a certain level of security, still preserving the system usability.

The OTP generated is sent to user's mail id (registered) and the user is allowed to enter the otp sent only within 10 minutes of time interval. If that time interval exceeds ,then the session will get expired and the user has to again start the login process from the first level. Within the time interval if the user enters the correct OTP then he/she will get authenticated to next level.

The algorithm used for generating OTP should be kept secret to ensure that the hacker is not able to deduce the next number in the random sequence.

The user is also required to enter the valid OTP within the certain time constraint. Importing this constraint in time and making the valid for only one login session is essential for improving security. The most important advantage that is addressed by OTP is that, in contrast to static passwords, they are not vulnerable to replay attacks.



Your OTP should be entered within 5 mins

Enter the OTP: 409153

Message

Login Success

3.2.Smart Card Authentication

A **smart card**, **chip card**, or **integrated circuit card** (**ICC**) is any pocket-sized card that has embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene,teraphthalate based polyesters or polycarbonate. Smart cards can provide personal identification,authentication, data storage, and application processing. Smart cards may provide strong security authentication for single signon (SSO) within large organizations. The CCID (Chip Card Interface

Device) is a USB protocol that allows a smartcard to be connected to a Computer, using a standard USB interface. This allows the smartcard to be used as security token forauthentication . Smart-cards can authenticate identity. The magnetic strip contained in the smart card stores RFID tag unique number for particular user. The card reader connected to computer through Serial COM port is used to scan

the card and retrives the data from it and matches it with the one in backend for authenticating particular user.

IV CONCLUSION

This paper describes the importance of multi-factor authentication in overcoming the security threats and this system can be used in high security applications like Internet Banking. The Limitation of this paper is that it may be time consuming for the user to cross multiple levels to login successfully. Keeping this limitation aside and considering the security,high level of security can be achieved through the successive levels of authentication. Several new authentication methods which emerges day-to-day and those which tighten security can be combined to form levels of authentication in future.

V ACKNOWLEDGEMENT

First of all we would especially like to express sincere gratitude to our parents. It gives us great pleasure and satisfaction in presenting the paper on

"Three Level Password Authentication System" Before we get into the depth of the things, we show our sincere gratitude towards respected teachers, guide, colleagues and all who have directly or indirectly helped us in the completion of this paper successfully.

REFERENCES

BOOKS

[1]"Smartcard security and applications" by Mike Hendry published in 1997.

[2]"Cryptography and network security" by William Stallings,6th Edition.

Journal Papers

[1] M. Manjunath, K. Ishthaq Ahamed and Suchithra (2013): Security Implementation of 3- Level Security System Using Image Based Authentication. Web Site: www. ijettcs. org Email:editor@ijettcs. org,editorijettcs@gmail. com Volume 2, Issue 2, March – April 2013.

[2] Manjunath G et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 2277-2280\ Text-Based Shoulder Surfing Resistant Graphical Password Scheme.

[3] S. K. Bandyopadhyay, D. Bhattacharyya, P. Das, "*User Authentication by secured graphical Password Implementation"*, IEICE 2008.