OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

An Enhanced Security System for Web Authentication

Rajnish Kumar[1], Akash Rana[2], Aditya Mukundwar[3]
[1,2,3,](Department of Computer Engineering, Sir Visvesvaraya Institute of Technology, Nashik, India)

Abstract:Web authentication has low security in these days. Todays, For Authentication purpose, Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy tobreak and vulnerable to dictionary or brute force attacks. Also, Textual passwords can be identified by 3rd party software's. Many available graphicalpasswords have a password space that is less than or equal to the textual passwordspace. Smart cards or tokens can be stolen.There are so many biometric authentications have been proposed; however, users tend to resistusing biometrics because of their intrusiveness and the effect on their privacy. Moreover,biometrics cannot be evoked.In this paper, we present and evaluate our contribution,i.e., the OTP and 3-D password. A one-time password (OTP) is a password that isvalid for only one login session or transaction. OTPs avoid a number of shortcomingsthat are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. It means that a potential intruder who manages to record an OTPthat was already used to log into a service or to conduct a transaction will not be able toabuse it, since it will be no longer valid. The 3-D password is a multifactor authenticationscheme. To be authenticated, we present a 3-D virtual environment where the usernavigates and interacts with various objects. The sequence of actions and interactionstoward the objects inside the 3-D environment constructs the user's 3-D password.*

Keywords:OTP, FTP, AES, 3D Virtual Environment.

I. INTRODUCTION

Due to fast technology and evaluation in internet, all type of organization such as business, educational, medical and engineering and even all are having a website. User registers on that website and create an account. They Use textual passwords to login but this textual passwords can be easily hacked by many ways such as using 3rd party software's, by guessing so for Authentication purpose, An OTP password should be required for only one session and this OTP password should come on User's registered Mobile Number or Email Id. This type of security system can enhance the Web Authentication.

In this paper, we present and evaluate our contribution, i.e., the OTPS and 3-D password.A proposed system combines the 3 different password authentication systems.First is Normal and old textual password system, after successfully login to textualpassword system, server will send Password in decrypted form through SMS to valid User. Once the user enter correct password which he had received from server user willsuccessfully pass through OTPS (i.e. One Time Password System) phase, and user will enter to 3D authentication phase.

One-time password systems provide a mechanism for logging on to a networkor service using a unique password which can only be used once, as the name suggests this prevents some forms of identity theft by making sure that a captured username/password pair cannot be used a second time. Typically the user's login name stays the same, and the one-time password changes with each login. One-time passwords area form of so-called strong authentication, providing much better protection to on-linebank accounts, corporate networks and other systems containing sensitive data. The3-D password is a multifactor authentication scheme. To be authenticated, we presenta 3-D virtual environment where the user navigates and interacts with various objects.
The sequence of actions and interactions toward the objects inside the 3-D environmentconstructs the user's 3-D password. The design of the 3-D virtual environment and thetype of objects selected determine the 3-D password key space.The proposed system is multilevel authentication system for Web which is a combinationof three authentication systems and in turn provides more powerful authenticationthan existing authentication system.

II. LITERATURE SURVEY

For any project, Literature Survey is considered as the backbone. Hence it is neededto be well aware of the current technology and systems in market which is similar withthe system to be developed. The dramatic increase of computer usage has given rise to many security concerns.One major security concern is authentication, which is the process of validating who you are to whom you claimed to be. In general, human

authentication techniques canbe classified as knowledge based (what you know), token based (what you have), andbiometrics (what you are). Knowledge-based authentication can be further divided intotwo categories as follows: 1) recall based and 2) recognition based. Recall-based techniquesrequire the user to repeat or reproduce a secret that the user created before.Recognition based techniques require the user to identify and recognize the secret, orpart of it, that the user selected before.

Existing System

These are the following Existing System:

1. **Textual Password System**
2. **Token Based System**
3. **Graphical Based Password System**
4. **Biometric System**

1. Textual Password System

Textual passwords are commonly used. One major drawback of the textualpassword is its two conflicting requirements: the selection of passwords that areeasy to remember and, at the same time, are hard to guess. Even though the fulltextual password space for eight-character passwords consisting of letters andNumbers is almost 2 * 1014 possible passwords; it is easy to crack 25 percentof the passwords by using only a small subset of the full password space. Many authentication systems, particularly in banking, require not only what the userknows but also what the user possesses (token-based systems). However, manyreports have shown that tokens are vulnerable to fraud, loss, or Theft by usingsimple techniques.

2. Token Based System

A token is a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens. Securitytokens are used to prove one's identity electronically (as in the case of a customertrying to access their bank account). The token is used in addition to or in placeof a password to prove that the customer is who they claim to be. The token actslike an electronic key to access something.

3. Graphical Based Password System

Graphical passwords can be divided into two categories as follows:

- Recognition based
- Recall based.

Various graphical password schemes have been proposed .Graphical passwords are based on the idea that users can recall and recognize pictures betterthan words. However, some of the graphical password schemes require a longtime to be performed. Moreover, most of the graphical passwords can be easilyobserved or recorded while the legitimate user is performing the graphical password;thus, it is vulnerable to shoulder surfing attacks. Currently, most graphicalpasswords are still in their research phase and require more enhancements andusability studies to deploy them in the market.

4. Biometric System

Many biometric schemes have been proposed; fingerprints, palm prints, handgeometry, face recognition, voice recognition, iris recognition, and retina recognition are all different biometric schemes. Each biometric recognition scheme hasits advantages and disadvantages based on several factors such as consistency,uniqueness, and acceptability. One of the main drawbacks of applying biometricsis its intrusiveness upon a user's personal characteristic. Moreover, retinabiometric recognition schemes require the user to willingly subject their eyes toa low-intensity infrared light. In addition, most biometric systems require a specialscanning device to authenticate users, which is not applicable for remote andInternet users.

Proposed System

A proposed system is multilevel authentication system in which we combine the 3 different password authentication systems that are textual, OTPS and 3D password authentication system. Following are the proposed system:

1. **OTPS (One Time Password System)**
2. **3D Password System**

1. OTPS (One Time Password System)

One-time password systems provide a mechanism for logging on to a networkor service using a unique password which can only be used once, as the namesuggests. There are two entities in the operation of the OTP one-time passwordsystem. The generator must produce the appropriate one-time password from theuser's secret pass-phrase and from information provided in the challenge fromthe server. The server must send a challenge that includes the appropriate generationparameters to the generator, must verify the one-time password received,must store the last valid one-time password it received, and must store the correspondingone-time password sequence number. The server must also facilitatethe changing of the user's secret pass-phrase in a secure manner.

The OTP system generator passes the user's secret pass-phrase, along with aseed received from the server as part of the challenge, through multiple iterationsof a secure hash function to produce a one-time password. After each successfulauthentication, the number of secure hash function iterations is reduced by one.Thus, a unique sequence of passwords is generated. The server verifies the onetimepassword received from the generator by computing the secure hash functiononce and comparing the result with the previously accepted one-time password.This technique was first suggested by Leslie Lamport.

2.3D Password System

It is the user's choice to select which type of authentication techniques will be part of their 3D password. This is achieved through interacting only withthe objects that acquire information that the user is comfortable in providing andignoring the objects that request information that the user prefers not to provide.
For example, if an item requests an iris scan and the user is not comfortable inproviding such information, the user simply avoids interacting with that item.Moreover, giving the user the freedom of choice as to what type of authenticationschemes will be part of their 3-D password and given the large number ofobjects and items in the environment, the number of possible 3-D passwords willincrease. Thus, it becomes much more difficult for the attacker to guess the user's3-D password.

It is easier to answer multiple-choice questions than essay questions becausethe correct answer may be recognized. To be authenticated in 3D password authenticationstage, we present a 3-D virtual environment where the user navigatesand interacts with various objects. The sequence of actions and interactions towardthe objects inside the 3-D environment constructs the user's 3-D password.
The design of the 3-D virtual environment and the type of objects selected determinethe 3-D password key space.

III. SYSTEM ARCHITECTURE

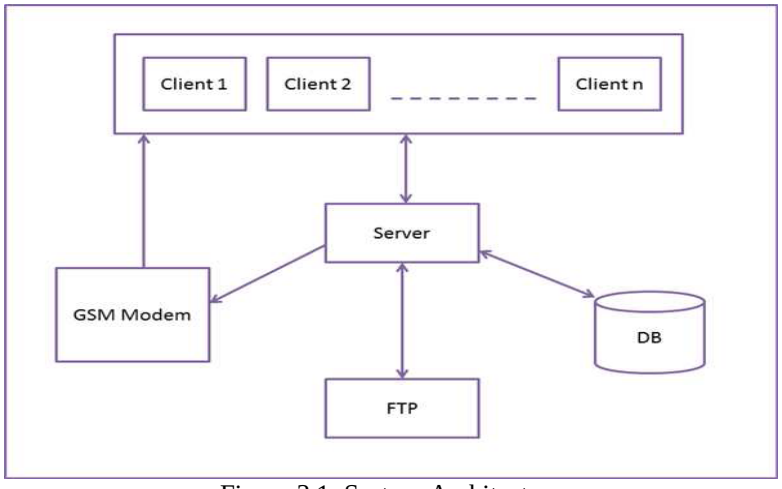

Figure 3.1: System Architecture

There are two modules in the System Architecture:

1. Client Module

When user wants to interact with system or user wants to use the services ofthe system first time, he has to register himself. During registration phase, userneeds to provide his or her basic information including personal mobile numberand at the time of login user needs to provide his valid username which is stringof alphanumeric characters and special symbols in order to get access to the resources.

During login phase user needs to pass successfully through Textual, OTPand 3D password phases. On which user can receive OTP passwords on his/hermobile. Also he has to select one unique username. And at the same time userhas to create 3D password, which user will use at the time of login.

2. Server Module

At the time of login when user login successfully to the textual passwordphase, user will enter into second stage i.e. OTP. In this phase server will generateOTP password which will be stored in encrypted form in database using AESalgorithm and at the same time it will be displayed on user's mobile in decryptedform. And at the time of verification password entered by user will be encryptedfirst and then will be matched with the password stored in database, if it matchesthen server will remove the OTP password from database as it is valid only forone session. Now the last stage is 3D password. In this phase at the time ofregistration 3D chess board virtual environment will be provided to user fromwhich user will select his 3D password which will be stored in encrypted formin database and at the time of login user needs to recall his previously recordedpassword which is encrypted and matched with the stored encrypted passwordand if it matches with the stored password then the user will get access to thesystem. And after that user can perform transaction and can use the serviceswhich particular bank will provide.

IV. MODULES & ALGORITHM

Modules

Proposed system contains different modules such as:

1. Registration module
2. Textual Login module
3. OTP Login module
4. 3D Login module
5. FTP Access module
6. Setting modules
7. Service module

1. Registration Module:

When user wants to access the system first time, then registration moduleis used for registering himself. And it also stores the details of user like name,address, mobile no., email id etc. in database.

2. Textual Login Module:

This module is used for accepting the username from end user and sends it toserver module for validating purpose.

3. OTP Login Module:

This module is used for accepting the OTP password which he/she had receivedon his/her mobile from the system after providing valid username to textuallogin module. And that password is send to server side for matching withpassword stored in the database.

4. 3D Login Module:

After providing valid information in textual as well as OTP login module, in3D login module the 3D chessboard environment will be provided to the end user.In this, user will perform different actions and interactions towards 3D objects which will creates user's 3D password that will be stored in database in encryptedform.

5. FTP Access Module:

Thismodule will be available to the user if and only if user successfully passesthrough login phases. In thismodule FTP services will be provided to the end userwhere user can upload or download to or from server.

6. Setting Module:

Setting module allows user to update contact details, reset 3D password aswell as notification settings according to end users choice.

7. Service Module:

This module is implemented at server side which is used for providing theservices to user. And also maintains the log of requested users. This module willlisten the request from the client side and will provide response accordingly.

Algorithms

1. Proposed System Algorithm

This System contains the combinationof textual, OTP and 3D Password Authentication Techniques. User can use thissystem if and only if he has registered himself. If not then user has to registerhimself before using system first time.

Steps:

1. Registration Process:

In this step, user needs to provide following four types of information.

(a) Users Personal Information:

In this, user will provide his/her personal info like Full Name, Address,State, and City.

(b) Users Contact Details:

In this, user will provide his/her contact no.,mobile no. and emailid.

(c) Credential Details:

At this section, user will provide his/her username and also create3D password from the 3D virtual environment which is provided in theGUI.

(d) Notification Details:

In this final section, user will select notification options such as login notification,update notification, and reset notification according to user'schoice.

2. Login Process:

When user is already registered then for login into system he/she has topass successfully from several stages.

(a) Textual Login:

In this, user will providehis/her valid username, after that server system will verify that username.And if it is valid then system will allow user to enter into nextstage.

(b) OTP Login:

After successfully passed through textual login stage user will getOTP password on his/her mobile and if user enter valid OTP passwordthen he/she will enter into last stage.

(c) 3D Password Login:

Here user has to interact with the 3D chessboard environment andneeds to repeat same movements which he/she had done at the time ofregistration. After doing valid movements user will login successfully.

3. FTP Services:

User login successfully into the system then he/she can access the FTPservices where user can upload or download files.

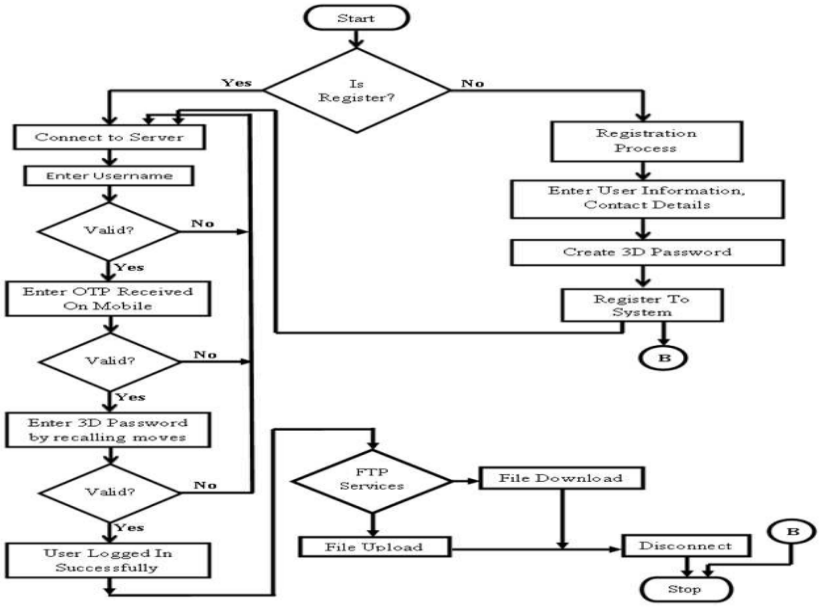

Figure 4.1: System Flow

4. AES Algorithm

In cryptography, the Advanced Encryption Standard (AES) is an encryptionstandard adopted by the U.S. government. The standard comprises three blockciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originallypublished as Rijndael. The Rijndael cipher was developed by two Belgiancryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to theAES selection process. Each AES cipher has a 128-bit block size, with key sizesof 128, 192 and 256 bits, respectively. The AES ciphers have been analysed extensivelyand are now used worldwide, as was the case with its predecessor, theData Encryption Standard (DES).

Steps of AES Algorithm:

1. Key Expansion:

Round keys are derived from the cipher key using Rijndael's key schedule(to expand a short key into a number of separate round keys).

2. Initial Round - AddRoundKey:

Each byte of the state is combined with the round key using bitwiseXOR.

3. Rounds

(a) SubBytes:

SubBytes is used at the encryption site. To substitute a byte, weinterpret the byte as two hexadecimal digits.The SubBytes operationinvolves 16 independent byte-to-byte transformations using lookup table.

(b) ShiftRows:

The ShiftRows step operates on the rows of the state; it cyclicallyshifts the bytes in each row by a certain offset. For AES, the first rowis left unchanged. Each byte of the second row is shifted one to theleft. Similarly, the third and fourth rows are shifted by offsets of twoand three respectively. For blocks of sizes 128 bits and 192 bits, theshifting pattern is the same. Row n is shifted left circular by n-1 bytes.

(c) MixColumns:

In the MixColumns step, the four bytes of each column of the stateare combined using an invertible linear transformation. TheMixColumnsfunction takes four bytes as input and outputs four bytes, where eachinput byte affects all four output bytes. Together with ShiftRows, Mix-Columns provides diffusion in the cipher.

(d) AddRoundKey:

In the AddRoundKey step, the subkey is combined with the state.For each round, a subkey is derived from the main key using Rijndael'skey schedule. The subkey is added by combining each byte of the statewith the corresponding byte of the subkey using bitwise XOR.

4. Final Round (no MixColumns):

(a) SubBytes
(b) ShiftRows
(c) AddRoundKey

V. SCREEN SHOTS

5.1 Server Side Home page

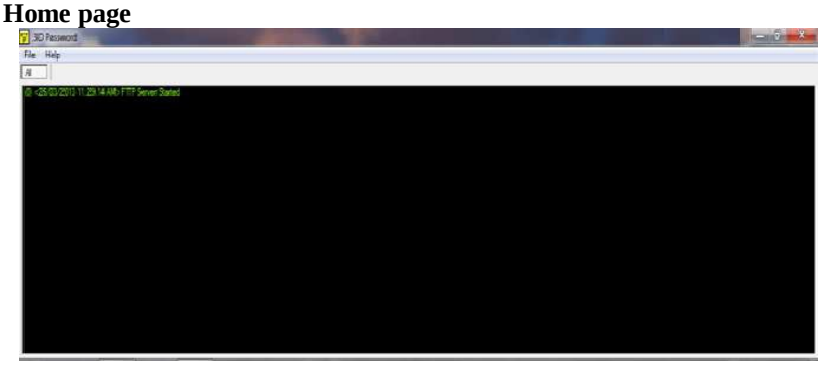

Figure 5.1: Server Side Home Page

5.2 Client Side Main Form

Figure 5.2: Client Side Main Form

5.3 Textual Login Window

Figure 5.3: Textual Login Window

5.4 OTP Login Form

Figure 5.4: OTP Login Form

5.5 3D Login Form

Figure 5.5: 3D Login Form

VI. TECHNICAL SPECIFICATION

Hardware Requirement

1. Processor: Intel Dual Core.
2. Hard Disk: 40 GB. (Client System), 60 GB. (Server System).
3. RAM: 512 MB. (Client System), 2 GB. (Server System).

Software Requirement

1. Database: Oracle 10g
2. Coding language: Java

Advantages

1. Not easy to write down on paper
2. Difficult to crack and Avoid Attacks
3. Large password space

Disadvantages

1. Not feasible for blind people
2. Shoulder surfing attack is possible

Applications

1. Critical server
2. Nuclear and military facilities
3. Air-planes and jetfighters
4. E-Banking& ATMs

VII. CONCLUSION

In Market, there are so many authentication schemes available.Some techniques are based on user's physical characteristics as well as behavioral properties, and some other techniques are based on user's knowledge such as textual and graphical passwords. However, as mentioned before, both authentication schemes are vulnerable to certain attacks. This system is multilevel authentication system for Web because it combines three different authentication system i.e. textual password, one time password and 3D password. So it is difficult to break the system and also provides large password space over alphanumeric password. The proposed system avoids different types of attacks like brute force attack, dictionary attack and well-studied attack. One-time password systems provide a mechanism for logging on to a network or service using a unique password which can only be used once, as the name suggests.

VIII. FUTURE SCOPE

These are the possible future scopes:

1. Enhancing and Improving the User Experience for the 3-D Password
2. Gathering Attackers from different backgrounds to break the system

REFERENCES

[1] Prof. Sonkar S. K., Dr. Ghungrad S. B., "Minimum Space and HugeSecurity in 3D Password Scheme", International Journal of Computer Applications (0975-8887), vol. 29-No. 4,Sept. 2011.

[2] Young Sil Lee, "A study on efficient OTP generation using stream cipher with randomdigit", Advanced Communication Technology(ICACT), 2010The 12th International Conference, vol. 2, pp 1670-1675. Feb. 2010.

[3] Renaud, K. (2009)."On user involvement in production of images used invisual authentication". J.Vis. Lang. Comput. 20(1):1-15.

[4] Haichang, G. L. Xiyang, et al.(2009). "Design And Analysis of Graphical Passwordcheme", Innovative Computing, Information and Control (ICICIC),2009 fourth, International Conference On Graphical Password.

[5] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "Three-Dimensional Password for More Secure Authentication,"IEEE,http://ieeexplore.ieee.org., Last Updated 6 Feb 2008.

[6] Soon Dong Park, JoongChae Na, Young-Hwan Kim, dong KyueKim, "EfficientOTP(One Time Password) Generation using AES based MAC," Journal of Korea MultimediaSociety, vol. 11, No. 6,pp. 845-851, June. 2008.

[7] S.Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon,"Pass Points: Designandlongitudinal evaluation of a graphical password system," Int. J. Human-Comput. Stud. (Special Issue onHCI Research in Privacy andSecurity), vol. 63, no. 1/2, pp. 102127, Jul.005.

[8] S.Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon,"Authentication usinggraphical passwords: Basic results,"in Proc.Human-Comput. Interaction Int. Las Vegas, NV, Jul. 2527, 2005.