International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

# Secure Remote User Authentication using Pass Script & PassText

**Raj Mohammed Mohd, C.Shoba Bindu, D. Vasumathi**

***Abstract*: Authenticating users to secure systems is a crucial task for security experts to solve a password problem, where user should able to memorize a password or secret and password should be hard to guess and crack by adversaries. In general, Most of the secure systems were designed with text passwords along with additional factors such as tokens like smart card, mobile device. Text passwords are not resistant to dictionary, brute-force and guessing attacks. This paper proposes a novel graphical password method, which solves the password problem and secure against all password vulnerabilities. Theoretically, graphical passwords are easy to memorize and recall them easily for long term and resistant to dictionary and brute-force search attacks.***

***Keywords* : Authentication, Password, PassScript, Graphical Password, Security and Usability.***

## I. INTRODUCTION

Most of the enterprises use authentication methods to secure their system and access to corporate resources in remote fashion. These enterprises adopt user authentication solutions to secure their sensitive banking and e-commerce web applications [1]. These websites are storing or allowing access to sensitive personal information, based on user authentication process, which is an important aspects to secure from unauthorized access and identity theft. There are some obvious examples such as online banking and various commercial sites which store the details of payment card associated with a user account [2]. Even though, most of the online accounts are protected with help of username and password which lead to inappropriate use of the traditional mechanism. In spite of this, the agencies are still using the one factor authentication, as it is primary controlled task. but, it is not sufficient for high-risk sensitive transactions over the network which involves access to customer resources, hijack or transfer the funds to third parties. cards and USB tokens.

Manuscript published on November 30, 2019.
* Correspondence Author
**Raj Mohammed Mohd.***, Research Scholar (JNTUH Hyderabad), CSE Department, GITAM Deemed to be University, Hyderabad, India.
**C.Shoba Bindu**, Professor, CSE Department, JNTUA College of Engineering, Anantapuramu, India.
**D.Vasumathi**, Professor, CSE Department, JNTUH College of Engineering, Hyderabad, India.



There are some alternatives such as OTPs, PKI, biometrics and smart cards. Users are familiar and easy to use smart cards extensively in the applications such as remote host login, access control of restricted vaults, activation of security devices, online banking and many more[7]. As the evolution of technology 80% of the population using the mobiles for their daily transactions over the internet, there is

necessity to keep mobile token as factor. However, all these methods are proposed and designed to protect the secure systems without consideration the impact on individual users. These systems are implemented without users in mind results in high workload for the users to memorize their Passwords [11]. In order to resolve the problem of recalling the passwords, researchers have been proposed the cognition based user authentication methods with alternatives. One of among them is graphical password, which is a set of images or image regions are chosen as password. These graphical passwords can be further categorized into three ways. One-recognition -based graphical password, a set of images are selected or recalled from portfolio of images; second-recall-based graphical password, draw a secret or pattern or doodle on grid to form a graphical password by recalling. Third-cued recall based graphical password, recognize and recall (select) a portion of an image region on a single image to form a graphical password [5]. In all these schemes, user no needs to remember the password but, recall or recognize the image or pictures in a sequence. Graphical password concept is proposed based on the motivation of the fact that users can recall pictures rather than textual passwords and it is very difficult to guess the pictures [2]. There are two schemes, Pass faces [4] and vidoop[12] deployed on websites for authenticating the users. But, these methods maintain a password/ verification table at the server along with the image database. From the motive of recognition and recalling the pictures, we have proposed method with passscript, which uses the telugu language script letters as pictures display on grid. The user needs to select the letters in a sequence to form a graphical password [14]. This paper proposes remote user authentication method using mobile device and OTP as two factors along with pair of username and graphical password (Passscript) used for websites and make use of a secure protocol[15] that does not require verification table at the server. The proposed scheme is resistant to ID theft, insider attack, guessing attack, phishing attack, replay attack, Stolen-verifier attack, Shoulder surfing attack and Server spoofing attack. The rest of paper organized in sections as follows. Section 2 review the concept of the remote user authentication methods.

Section 3 discuses the remote user authentication protocol. Section 4 analyzes the security of the proposed scheme, Section 5 analyzes the efficiency of the proposed scheme and finally concluded in Section 6.

## II. EXISTING REMOTE USER AUTHENTICATION METHODS USING GRAPHICAL PASSWORDS

In this section, we review the existing two methods with their login and registration phases. One-Wei-chi-ku et al. Scheme and the second is Misbah et. al Scheme. The notations used throughout paper are represented in Table 1.

**Table I:. Notations Used In This Paper**

| | |
|---|---|
| Ui, | The *i*th User |
| S | The Server S |
| AS | Authentication Server |
| GPwi | The password of User i |
| Ni,Ni+1, Nj Nj+1, Nk ,rs,rc | nonce generated by client and server |
| Ex , Dx | Encryption & Decryption of 'x' respectively |
| SK | Session Key |
| $\oplus$ | The Ex-OR Operator |
| $\|\|$ | Concatenation |
| x | Master Secret key of S |
| yi | Server's secret key stored in each registered user's mobile device |
| TIDi | Token identifier for mobile mapping of IDi |

### A. Wei-Chi-Ku et. al Scheme

Wei-chi-ku et. al scheme reviewed in this section and it consists of registration and login phases.

**I. Registration Phase**

In this phase, Ui initially registers or re-registers to *S*.

Step1. *U*=>*S*: reg_request.

Step2. *S* sets *T* to the value of his current timestamp. If it is initial registration then sets *N* to 1.if not, S sets $N = N + 1$.

Step 3. *S* =>*U* : *T*, *N*.

Step 4. *User 'U'* enters his graphical password by drawing a secret on $G \times G$ grid to generate the corresponding code *GP*, and then computes the verifier

$$V = h^2(S \| GP \| N \| T).$$

Step 5. *U*=>*S*: *V*.

Step 6. *S* computes the storage key

$k_U^{(T)} = h(ID \| h(x \| T))$, and then computes the sealed verifier $sv^{(N)} = h^2(S \| GP \| N \| T) \oplus k_U^{(T)}$

Next, *S* stores $sv^{(N)}$, *T*, and *N* in his password file.

***II. Login Phase***

User will login to Server 'S' using protocol with following steps. Now, assume that $N = n$ and $T = t$.

Step 1. *U*=>*S*: *ID, rc*. // *rc* is a random nonce generated by *U*. //

Step 2. *S* obtain *t* from his password file and computes $k_A^{(t)} = h(ID \| h(x \| t))$, and then uses the computed $kU(t)$ to derive the verifier $h^2(S \| GPW \| n \| t)$ from the stored sealed verifier $sv^{(n)}$ $(= h^2(S \| GPW \| n \| t) \oplus k_U^{(t)})$. Next, *S* computes $h(h^2(S \| GPW \| n \| t) \oplus rc)$.

Step 3. *S*=>U: *n*, *rs*, $h(h^2(S \| GPW \| n \| t) \oplus rc)$, *t*.

// *rs* is a random nonce generated by *S*. //

Step 4. *U* enters his graphical password by drawing a secret on $G \times G$ grid to generate the corresponding code *GP*. Next, *U* computes $V = h2(S \| GP \| n \| t)$ and $h(V \oplus rc)$.

If the computed $h(V \oplus rc)$ equals the received $h(h2(S \| GP \| n \| t) \oplus rc)$, *U* authenticates *S*.

Otherwise, *U* terminates this session. Then, *U* computes

$d1 = h^2(S \| GP \| n \| t) \oplus h(S \| GP \| n \| t)$

$d2 = h(S \| GP \| n \| t) \oplus h^2(S \| GP \| n + 1 \| t)$

$d3 = h(h^2(S \| GP \| n + 1 \| t) \| rs)$

Step 5. *U*=>*S*: *d*1, *d*2, *d*3.

Step 6. *S* uses previously derived verifier to compute

$u1 = d1 \oplus h2(S \| GP \| n \| t)$

$u2 = d2 \oplus u1$

If $h(u1)$ equals the retrieved $h^2(S \| GP \| n \| t)$ and $h(u2 \| rs) = d3$ holds, *S* authenticates *U*.

Otherwise, *S* rejects *U* *and* terminates session. Then, *S* computes $sv^{(n+1)} = u2 \oplus k_U^{(t)}$ $(= h^2(S \| GPW \| n + 1 \| t) \oplus k_U^{(t)})$, replaces $sv^{(n)}$ with $sv^{(n+1)}$, and sets $N = n + 1$ for *U*.

This scheme is designed with help of time-stamps to avoid the replay and MITM attacks. But, Time stamp based protocols suffers from time synchronization problem. This scheme also maintain password file at the server.

This scheme designed with pure recall-based graphical password mechanism where user draw a secret (DAS) on the grid and password will be the sequence of stroke points on the grid. This scheme is also vulnerable to shoulder-surfing attack.

### B. Misbah et.al scheme

This section reviews the misbah et.al scheme and it consists of registration, login verification and key exchange phases.

**I. Registration Phase**

The registration phase is executed by two parties Ui and S in secure environment and communication channel. The registration phase consist of following steps.

Step 1: Ui =>S:ID, reg_request.

Step 2: if received ID is available, S sends images to the client. The client displays three 3x3 image grids one after the other.

Step 3: Ui selects a graphical password by selecting 3 images from 3x3 grids (at least one from each) and send h(PWi) to S.

Step 4: After receiving h(PWi), S computes Qi, Gi, Vi and Hi one after the other:

Qi = h(IDi||yi); Gi = h(x $\oplus$ h(IDi)); Vi = h(PWi||IDi) $\oplus$ Qi; Hi = h(Qi). where yi = IP-address followed by current time.

Step 5: S personalizes the user along with a smart card that contains {h(.), yi, Vi, Gi, Hi}.

**B. Login Phase**

User will login to the server using a smart card and IDi and password with following steps.

Step 1: Ui insert smart card into the card reader and enters his identity IDi

Step 2: Smart card computes Hi* = h(IDi||yi) and checks whether h(Hi*) equals Hi; if it holds then, smart card generates a nonce Ni and computes Ri = h(IDi) $\oplus$ Ni.

Step 3: Ui=>S: Ri, Ni.

Step 4: After receiving Ri, Ni, S computes h(IDi) =Ri $\oplus$ Ni; and checks the validity of h(IDi), if valid, S generates a nonce Nj, and sends the user profile images and Nj to Ui as Eh(Ni+1) (Images, Nj)

Step 5: After receiving Eh(Ni+1) (Images, Nj), the smart card first checks the freshness of nonce to resist phishing attack by computing Dh(Ni+1) (Images, Nj) and displays the received set of images on 3x3 grids as challenge to Ui.

Step 6: Ui enters his password by selecting images from portfolio.

Step 7: The smart card computes Vi' = h(Pwi||IDi)⊕ Vi and checks whether h(Vi') equals Hi. If it holds, it proceeds to compute Ci = h(Gi ⊕ (Nj+1)) ⊕ Nk,
Step 9: Ui =>S: Ci.

**Verification and Key agreement Phases**: These phases are between Ui and S by generating a secret session key and its exchange can be done in following steps:
Step 1: Gi'=h(x ⊕ h(IDi)); Nk = Ci ⊕ h( Gi' ⊕ (Nj+1)) Ci' = h(Bi' ⊕ (Nj+1)) ⊕ Nk and checks for comparing Ci equals to Ci', If it holds, S accepts the login request and both client and server compute session key
SK = h((Nk+1)⊕ (Nj+1) ⊕ Gi).
If Ci is not equal to Ci' then S rejects the login request.
Client and server communication is done in encrypted manner with the session key SK.
This scheme uses smart cards for storing the password related information in a message digest form with Vi,Gi,Hi and yi.
It uses a knowledge based graphical password along with text password (I, p) for three grids which are displayed in 3x3 grid. spyware and observational attacks) of text password. But, it reduces the guessing probability of password.

## III. PROPOSED PASSSCRIPT METHOD

In this section, we discuss the concept of the proposed two factor authentication scheme using smart cards for web site users. The main idea is to allow the user to choose regional telugu text password in the form of images (passscript letters). The user need to select the sequence of script letters from the 10x10 grid consisting telugu passscript letters to form a graphical password.
In our previous paper[ ], we have used 8x8 grid with only vowels and consonants. But, In this paper, We have included conjunctive consonants to make a 10x10 grid. The set of vowels, consonants and conjunctive consonants are displayed on the grid with different colours make easy accessible to user at the time login. We propose to use only low resolution images to ensure fast access.
We have also experimented with telugu keyboard to make password by clicking on a letter as shown in the figure 1.
But, we find difficulty to obtain conjunctive consonants to make a word or sentence in telugu language.
There are no Unicodes are available for the conjunctive consonants. In order to construct a conjunctive consonant, we are supposed to use tri-gram (a combination of three uni code values). It makes the user difficult to enter or type the correct password in ****** pattern.

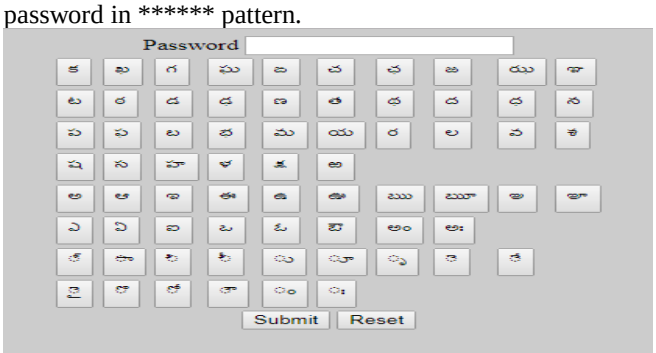


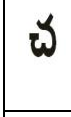

**Fig 1: Telugu virtual keyboard to make password by clicking on the letters to make a password.**

There is a problem of Unicodes in building the telugu virtual keyboard for an application. There may be a chance of having a dictionary for telugu words or sentences in the near future with existing Unicode values to obtain or guess the passwords from dictionary. So, In order to avoid this problem, we have recommended and proposed method with telugu script letters in the form of images and display in a grid. The proposed graphical password scheme works as follows: First, If user register with server by sending a registration request and enters an user ID. After validating received request, the server sends multiple low resolution images of regional script letters to the client or user and displayed in 10x10 grid as shown in the figure 2. It shows an examplelogin interface with set of passscript letters in the form of images in a 10x10 grid. Since images are used as passwords, our scheme provides a very large password space.
The user selects □□□□ as password by selecting alphabets అ+ మ+ శ from the 10x10 grid based on their position with respect to their row and column from a hand hidden keypad ( pressing the keys 6 times to enter the position). If the user want to do the same thing with telugu keyboard, then user supposed to click on letters 5 times to obtain that word. But, it is susceptible to shoulder-surfing attack.
The user wants to use నవలas password then he has to select న+వ+లalphabets one after the other from the 10x10 grid with their position displayed on the grid. The position of the alphabets will change time to time.


**Fig 2: Registration and Login Interface in 10x10 grid, where user enter the position of the alphabet to make a passscript**

The same set of images is repeated at client side until the password is generated. These images can change their positions randomly on the grid when next button is clicked and generate a string after modifying the text file and generated hash of modified text file. This can be done for all the script letters in graphical passscript password.
The password is created by concatenating all the hashes in a sequence when user clicks on the Done button. The user name and password will be send to the server in the form of hash. The proposed scheme facilitate telugu virtual keyboard with hand hidden keypad to enter the row and column of the script letter to generate a password. The password will be the hash value of set of the script letter images.

**Table-II. Sample Password Generation from Text file Using Image indices**

| Image | Image hash(SHA-256) | index | Image size | Text file | Hash of Text file after modification (SHA-256) |
|---|---|---|---|---|---|
|  | 260AD9AD2D13DA35EC7DB7278FA44900A7A11FDC064EA3AC171D79E7E9CF8E63 | 63 | 2.10 KB | Sample.txt 1.24KB | 6EF07DFB09C5D42D4478E31F145AE6DF9C711564BFAC4335ACCE0CEEF707721D ( T1) |
|  | 1433BA39FE70170DE6F9639C5620F68633303D4E205EA73A7C0CD48AD8C3F629 | 29 | 1.83KB | 1.24KB | 063A452A9E6106CB39C7C2363F9AC5ECCDE8F792B1FFEE90DF31091A36423581 ( T2) |
|  | 4E44F2C245193C00AA01587B236A196C7CB81C8A901D08D6A56E6F26DA42ED53 | 53 | 3.01KB | 1.16KB | B802E24B1CD9A1279E1387CF68178DD3FC06BCBE9615951E4E98CD93202109E1 ( T3) |
| **Hash of Hash of all Text file modifications in a sequence GPW= H(T1\|\|T2\|\|T3)** | | | | | 9D88EDCC2B5A7459F84017F20F37B1E4EC9A5C1FC7B6C01E555566B9F3DC3B7E |
| Image | Image hash(SHA-256) | index | Image size | Text file | Hash of Text file after modification (SHA-256) |

The sample pseudo code for the strong password generation algorithm is given below:

```
function Password Gen(Text file, index of Hashed Image )
{
 Index:=indexof Hash Image
 String := Load the text file content
 Switch(index)
{
    case 0: Replace 1st letter of each word with x
        replacefirstx(String);
        break;
    case 1:Replace 3rd letter of each word with $
        replacethirddol(String);
            break;
    case 2: Reverse all odd words in the text file
            reverseoddwords(String);
        break;
    case 3: Reverse all even words in the text file
         reverseevenwords(String);
         break;
              ..... .....
    case 98: Convert all odd words to uppercase
convertoddtoupper(String);
          break;
    case 99: Append after 3rd letter in word with next letter
              appendnext(String);
              break;
    default: Something went wrong with index value
}
}
```

There are 100 modifications can be available in the algorithm and these modifications can be done with help image hash index values. The input text file is changed or used by the users may be different even if both the users use same passscript letters as their password. So, the generated password is not available in the dictionary.

The proposed scheme resistant to dictionary (telugu dictionary),brute-force attack ( uses text file to make long password), spyware attack (key loggers didn't obtain any information about the password from row and column numbers which are random in nature), shoulder-surfing attack (observer didn't obtain the image and its position on the grid even though they are 100 passscript letters which are static in nature).

This scheme generates a password which is different for same set of passscript letters with different text file. User need to remember set of passscript letters and text file (a string, phrase which is used at the time of enrolment).

The scheme resistant to brute-force search and dictionary attacks with message digests. There is a possibility to obtain password-message digest pair to obtain the password which is very difficult, because, user uses text file with modifications done with help of password generation algorithm.

## IV. PROPOSED REMOTE USER AUTHENTICATION PROTOCOL

The proposed protocol has three phases such as registration phase, login and password change phases. It consists of simple hash functions for effective and efficient computations with less cost. This method use random nounce to counter the replay or MITM attacks and also overcome the weakness of time concurrency.

### A. Registration Phase

The registration is done by the user with help of a mobile token (replacing smart card) as shown in the figure 2.

Step 1: Ui=>AS: registration_request

After receiving the registration request from the user, AS submits user's mail ID to mail server(MS) and generates OTP and Mail server verifies it and AS obtain the user's profile data from the mail server(MS)

Step 2: AS =>Ui: registration link, Images;

Step 3: Ui =>AS: h(PWi).

Where $h(PWi)= h[F(Text, h(I_1))|| F(Text, h(I_2))|| F(Text, h(I_3))]$

Image indices ($I_1$, $I_2$and $I_3$) are used to modify the text file contents and generate a strong password using SPGA algorithm.

Step 4: AS computes *a*, *Ni* as follows:

$a= h$(mail ID)

$Ni= h(PWi)\oplus h(x\oplus TIDi)$

Where x is server' s master secret key, TIDi is a mobile token identifier.

Step 5: AS =>Ui : MT (*Ni*, *h*(), a, TIDi, $x_i$ )

Where $x_i$ is server' s secret key shared with each MT which is identified by TIDi and mapping of IDi.

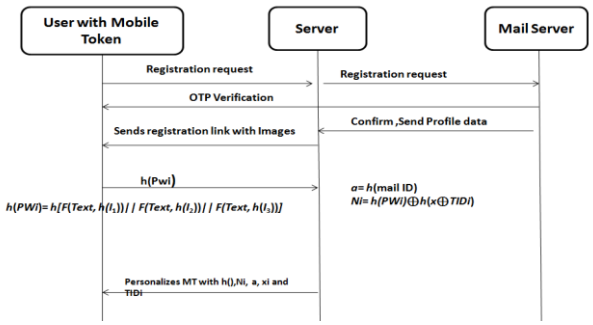



**Fig. 3.Registration protocol**

**B. Login**

User will login to his account with a mobile or web application to access the services from the server.

Step 1: Ui =>S,AS: login_request(ID);
Step 2: AS=>Ui: Images(Passscript Letters).
Step 3: Ui => AS: h(PWi)

Ui uses a MT and compute strong password from SPGA algorithm as follows.

$h(PWi)= h[F(Text, h(I_1))|| F(Text, h(I_2))|| F(Text, h(I_3))]$

Step 4: Ui (MT)=>AS:E

MT verify whether $h'(PWi) == h(PWi)$. If it holds, MT proceeds to compute $Bi = h'(PWi)$, $Bi= h(PWi)\oplus Ni$; $Ci= h(Bi\oplus r)$ and $E = Eyi(Ci, a)$

where $E$ is encryption of message using yi.

Step 5: AS receive E value and computes Dyi $(Ci, a)$ using yi, where D is decryption. It retrieves TIDi using ' a' and also computes

$Bi=h(x\oplus TIDi)$; $Ci=h(Bi\oplus r)$

Step 6: AS verify whether if $Ci = = Ci$ or not. If it holds then AS sends authentication success and forwarded to S in order to access the resources.

The authentication protocol is shown in fig 3.

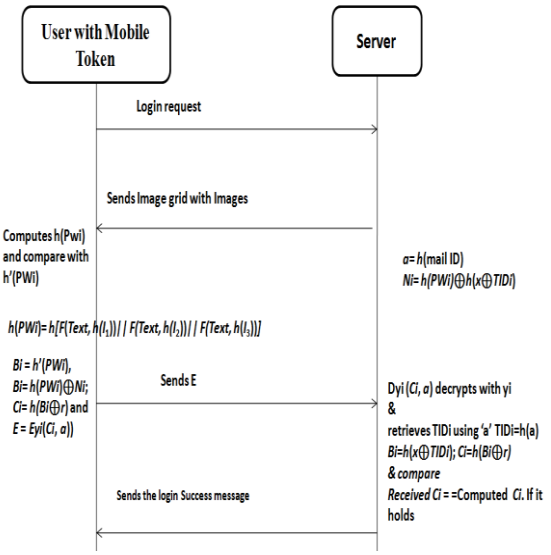



**Fig. 4.Authentication protocol**

**C. Password Change and Recovery Phases**

User has flexibility to change his password and also recover his password even when the mobile token (MT) lost.

**I. Password Change** *:* User has to login to S inorder to change his password in following steps.

Step 1: Ui => AS: change_pwd_request.
Step 2: AS=>Ui: images, *Eyi* $(h(PW))$
Step 3: Ui uses MT and compute h(PWi) by select new graphical password with help of text file and generate strong password.
Step 4: Now, MT computes $N_{in} = h(\text{h(PWi)}\oplus x)$ and update *Ni* with new *Nin*, $h(PWi)$.
Step 5: MT=>AS: Pwd_change_message;

**II. Password Recovery:** User Ui may forgot his password and it will be recovered by following steps:

Step 1: Ui =>AS: mail Id or ID.
Step 2: AS =>MS: IDi;
Step 3: MS verify Ui with help of OTP
Step 4: MS=>AS,ACK (on success).
AS=>Ui: password-reset-link
Step 5:User has to re-register with new passscript letters and text file as similar to registration phase. The user Ui lost his MT or deletes the application in the mobile he has to get a new MT from server and re-register with new graphical password and text file.

**You can use color figures as per the requirement but fonts should be in black.** Authors can use any number of color diagram, chart, picture, screenshots, and any snap which is required for the research of the title. Misbah et.al scheme uses a random nonce to resist the replay attack when transmitting a login messages.

*Insider Attack*: This attack is done by the person, who has access to system and obtain the user's password related information and reveal the user's sensitive secret information to others.

The proposed scheme doesn't store user's password information anywhere in the system.

None of the parameters required in protocol do not provide password information even after computation. To counter this attack, all the user credentials are stored in the database as message digest which is irreversible.

Even if he obtains the password generation algorithm and images chosen by the user he wouldn't obtain password because, the text file is not shared to the server. So, there is no possibility to get an insider attack.

## V. ANALYSIS

The proposed scheme is secure against attacks such as replay, insider, stolen-verifier attack, server-spoofing (Phishing), fraudulent-copying token, DoS attacks.

*Replay Attack*: This is an interception attack on confidentiality of the secure system. Adversary plays with messages transmitted over the network by observing and modifying the contents. It is also called as MITM attack. The proposed method is secure against replay attack because, message Eyi (Ci, a) is encrypted and both client and server checks for freshness or nonce to discard the modified messages.

Existing (Wei-chi-ku et.al and Misbah et.al) both schemes are secure against to replay attacks. Wei-chu-ki et.al scheme use the time stamp for every message to avoid the replay attacks. But, it may leads to time concurrency problem.

The wei-chi-ku et.al scheme may be vulnerable to insider attack because it uses a password file to store sealed verifier, storage key ,T,N.

*Stolen-Verifier Attack*: This attack is on the database server and steals password verifier table and obtain the password using offline guessing attack. The proposed scheme doesn't maintain a verifier table at server. So, the proposed scheme is resistant to stolen-verifier attack.

The wei-chu-ki scheme may be vulnerable to stolen verifier attack, because, it maintains a password table consists of storage key, sealed verifier etc.

Misbah et.al scheme is also resistant to stolen-verifier attack, because, it doesn't maintain any verifier table at the server.

*Server Spoofing Attack*: This attack is done by an adversary, who acts or pretends as legitimate server or website and steals the user's sensitive information as genuine server.

The proposed scheme resistant this attack, it is very difficult to create image grid along with user selected images as similar to images during enrollment. if an adversary succeeded in getting the images then it is difficult
to get password generation algorithm which makes a strong password from text file. Hence, the attack is not possible.
In wei-chu-ki et.al scheme, They have used grid to draw the secret and it is possible to display plain grid to the user and make a fake webpage and trap the user easily. So, wei-chu-ki et.al scheme is not resistant to server-spoofing attak.
Misbah et.al scheme uses a portfolio images along with text password related to image, it is quasi-resistant to server-spoofing attack.
*Denial of Service Attack*: This is an attack on availability service. The system doesn't allow the valid user even when he enters his valid credentials to prove his identity. The user's credentials are modified and updated in the database by an attacker and deny the service to valid user.
In the proposed scheme, since there is no secret information stored on the server, the denial of service attack will not work. DoS attack is not possible in both the existing Misbah et.al and Wei-chu-ki et.al schemes.
*Fraudulently copying the Token:*
Most of the protocols are using the tokens and store the data related to user in it. The token may be either smart card, PDA or MT etc.The proposed scheme uses MT as token and stores parameters *Ni*, *h*(*I*), *h*(*Pwi*), a, yi,

The attacker can neither retrieve the user' s secret *Pwi* nor the server' s master secret ' x' from the available parameters as the *Pwi*, x are stored as digest even though the attacker copy the data from MT or smart card.
Wei-chu-ki scheme is not vulnerable to fraudulently copying token attack where as Misbah et.al scheme is resistant to this attack.
The proposed scheme is secure against password vulnerabilities such as brute-force search, dictionary, guessing and observation attacks (spyware, shoulder-surfing).
*Secure against brute force search attack*: The attacker obtain the password by trial and error method with all possible number of attempts. The proposed method uses PassText Password, entire text file treated as password after making modification with help of image indices using SPGA algorithm.
Misbah et. al scheme uses both image and text password to make strong password. It quasi resistant to brute-force-search attack.
Theoritically, Wei-chu-ki scheme uses a recall based graphical password , which is resistant to brute-force attack.
*Secure against dictionary attack*: There is no dictionary for what kind of changes done by the system (SPGA Algorithm) in a user chosen document. SPGA algorithm is not disclosed and even if it is disclosed it is difficult to obtain both text file and set of passscript letters chosen by the user. So, it is difficult to carry out dictionary attack compared to traditional text passwords.
Both Misbah et.al and Wei-chu-ki schemes are resistant to dictionary attacks, because, all the graphical passwords doesn't have dictionary information to crack the password.

*Secure against guessing attack*: The attacker may guess the password either offline or online with user specific guessing the passwords. Most of graphical password schemes are vulnerable to guessing attack. But, proposed method is resistant to guessing attack because, It is very more difficult to know what modifications have been done to the base document by user with help of images. So, it is secure against guessing attack.
If adversary guess the all the images correctly then only they can login to the system and they didn't obtain the information about the password as well as text file chosen by the user.
*Secure against Shoulder-surfing attack*.
This is observation attack on graphical passwords done by an adversary who observe the login process and obtain password information. It is also done by external camera recording of login process. The proposed scheme is quasi-resistant to shoulder-surfing attack, adversary must know the row and coloumn as well as images shown on a grid.
Wei-chu-ki et. al scheme is not resistant to shoulder-surfing because, recall based graphical methods are more vulnerable to this attack.
Misbah et. al scheme is quasi-resistant to shoulder-surfing because, adversary supposed to enter the image label from keyboard for a specified image.
*Secure against Spyware attack*:
This is an internal observation attack done by malwares such as keyloggers or mouse-listeners.
The proposed method is resistant to spyware because it requires both keylogger and screen captures to obtain the password.
Misbah et. al scheme quasi-resistant to spyware because it requires only keyloggers[7] for specific image to obtain the password.
Wei-chu-ki et. al scheme is not resistant to spyware attack because, it requires only mouse-listeners to obtain the graphical password.

**Table-III: Comparisons of Security Properties with related works**

| S.No | Security Properties | Wie-ch-ku et.al | Misbah et.al | Ours |
|---|---|---|---|---|
| 1 | Insider Attack | No | No | No |
| 2 | Replay Attack | No | No | No |
| 3 | Stolen verifier attack | Yes | No | No |
| 4 | Reconnaissance attack | Yes | No | No |
| 5 | ID Theft/ Mobile token lost | Yes | No | No |
| 6 | Denial of Service Attack | No | No | No |
| 7 | shoulder surfing attack | Yes | No | No |
| 8 | Spyware Attack | Yes | May be | No |
| 9 | Brute-force attack | Yes | Yes | No |
| 10 | Guessing attack | Yes | May be | No |
| 11 | Dictionary attack | Yes | May be | No |
| 12 | Server spoofing attack | Yes | No | No |
| 13 | Mutual Authentication | Yes | Yes | Yes |
| 14 | Time Synchronization Problem | Yes | No | No |

| | | | | |
|---|---|---|---|---|
| 15 | Password table /verifiable table maintained | Yes | No | No |
| 16 | Copying the token(Smart card/Mobile) | Yes | Yes | No |
| 17 | Password recovery (if something goes wrong with Mobile Token/Smart card) | No | No | Yes |

## VI EFFICIENCY ANALYSIS OF PROPOSED PROTOCOL

In this section, The efficiency of proposed scheme is analyzed and compared with existing Wei-chi-ku et. al schme and Misbah et.al scheme in terms of the computational cost and the communication cost.

**Table –IV. Efficiency analysis of Proposed Method**

| | | Wei-chi-ku et.al Scheme | | Misbah et.al scheme | | Proposed Scheme | |
|---|---|---|---|---|---|---|---|
| | | C | S | C | S | C | S |
| Registration | E1 | 2 $T_h$ | $T_h$ | $T_h$ | 3*$T_h$ | 4$T_h$ | 3$T_h$ |
| | E2 | $T_h$ | $T_x$ | $T_c$ | 2*$T_x$ | 0$T_x$ | 2$T_x$ |
| | E3 | -- | -- | 384 bits | 256 bits | | |
| | E4 | -- | -- | 256 bits | 540k bits | | |
| | E5 | | | 2ms | | 1ms | |
| Login | E1 | 3$T_h$ | 6$T_h$ | 6$T_h$ | 5$T_h$ | 4$T_h$ | 2$T_h$ |
| | E2 | 2$T_x$ | 3$T_x$ | 9$T_x$ | 8$T_x$ | 2$T_x$ | 2$T_x$ |
| | E3 | -- | -- | 384 bits | -- | | |
| | E4 | -- | -- | 384 bits | 128 bits | | |
| | E5 | | | 2ms | | 1 ms | |

E1: Time required for hash computations ($T_h$)
E2: Time required for XOR operations (Tx)
E3: Memory needed;
E4: Communication cost of authentication
E5: Time required rendering the images
The proposed scheme takes less time to render the images because, the passscript letter icons

## VI. CONCLUSION

With the increase in websites storing and allowing to user sensitive information, the need for a secure & user friendly website authentication mechanisms through mobiles is day by day increasing. In this paper, we proposed a secure and user friendly authentication mechanism using mobile token for website users.

The proposed protocol has several unique features such as user has flexibility choose images(passscript letters) as passwords and text file that can be easily recognized and selected at the time of login. In future work, the usability of the proposed scheme will be compared with other existing graphical password methods.

## REFERENCES

1. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42,pp. 41-46, 1999.
2. R. N. Shepard, "Recognition memory for words, sentences, and pictures", Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.
3. G. E. Blonder, "Graphical passwords," in LucentTechnologies, Inc., Murray Hill, NJ, U. S. Patent 5559961, Ed. United States, 1996.
4. Passfaces. [Online] Passfaces Coporation. http://www.passfaces.com. Last accessed 31st May 2008
5. Suo, X., Zhu, Y., & Owen, G. (2005). Graphical Passwords: A Survey. In Proc. ACSAC'05.
6. Wei-Chi Ku1 and Maw-Jinn Tsaur "A Remote User Authentication Scheme Using Strong Graphical Passwords" Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05) 0-7695-2421-4/05 $20.00 © 2005.
7. Two-Factor Authentication – A total cost of ownership;Verisign – White paper; http://www.verisign.com/static/029263.pdf last accessed 31st May 2008.
8. Steven Funnel, A comparison of Website User Authentication Mechanisms, Computer Fraud & Security, Volume 2007, Issue 9, September 2007, Pages 5-9.
9. Authentication in an internet banking environment, http://www.ffiec.gov/pdf/authentication_guidance.pdf, Last accessed 31st May 2008
10. Nesic Dragoljub, Stronger Security, Card Technology Today, Volume 19, Issue 1, January 2007, Pages 9-10
11. Sasse, M.A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Flechais, I. and Kearney, P. 2007. Human Vulnerabilities in Security Systems. White Paper, Human Factors Working Group, Cyber Security Knowledge Transfer Network.
12. Vidoop; [Online] https://myvidoop.com/ ; Last accessed 31st May 2008.
13. Misbahuddin , P. Premchand, A. Govardhan "A User Friendly Password Authenticated Key Agreement for Multi Server Environment" International Conference on Advances in Computing, Communication and Control (ICAC3'09.
14. Wei-Chi Ku and Maw-Jinn Tsaur "A Remote User Authentication Scheme Using Strong Graphical Passwords" Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05) 0-7695-2421-4/05.
15. Raj Mohammed , Shoba Bindu C, P Chandra Sekhar, B Satya Narayana "Remote user authentication using cognition based graphical passwords" i-manager's Journal on Software Engineering,Vol 3,No.1,July-Sep 2008.
16. [16] Raj Mohammed , Shoba Bindu C, Vasumathi D "An Improved cognition based authentication scheme using PassScript" International Journal of Advanced Research in Computer Science,Vol 2,No.4,July-Aug 2011.
17. Raj Mohammed , Shoba Bindu C, Vasumathi D "Secure user authentication with graphical passwords and PassText" Springer Proceedings of the First International Conference on Computational Intelligence and Informatics,Advances in Intelligent Systems and Computing 507,DOI 10.1007/978-981-10-2471-9_5.