

Evaluation of 3 Level Multifactor Authentication Model based on Click-GPass Graphical Password Scheme

Charanjeet Singh, Tripat Deep Singh

Abstract: *In insecure cloud environment an efficient and robust authentication system can boost security especially when critical data access or financial transactions are to be carried. Usage of single factor authentication (SFA) schemes proves to be inefficient and insufficient in such applications. The security in cloud environment can be boosted by using authentication mechanism that incorporates multiple factors for verifying the user's identity. To meet this need, we propose a multi-level and multifactor authentication scheme called 3 Level Multifactor Authentication (3L-MFA) that incorporates knowledge based factors and Out of Band (OOB) authentication. The scheme uses a novel graphical password based authentication scheme called Click-GPass (Clickable Graphical Password) at its third level of authentication that is not only user friendly but also secure. The proposed study is based on a premise that when multiple levels and multiple factors are incorporated in an authentication scheme it not only becomes difficult to break but also resistant to different forms of attacks. The security analysis of the proposed system was carried out in terms of password guessing, shoulder surfing attacks. Several different factors of usability were also analyzed. Feedback on usability features of scheme was also gathered from user by the mean of questionnaire. The results of empirical study for 3L-MFA and Click-GPass scheme proved that scheme is efficient both in terms of usability and security.*

Index Terms: *Click based graphical password, Multifactor authentication, Out of band, OTP, Security and Usability*

I. INTRODUCTION

Although usage of cloud technology ensures the availability of services and data 24 by 7 but poses various security risks especially for the crucial financial transactions. However, this security can be enhanced by employing a strong and robust authentication mechanism [1]. Authentication process checks the identity of user and acts as one of the first walls of protection against illegitimate users [2]. SFA schemes do not prove to be competent enough to control illegitimate access. It is usually considered that multi-level and multifactor based authentication mechanisms are safer and robust against various forms of attacks and threats.

This paper proposes the design and implementation of secure, user friendly and economical multifactor

authentication mechanism called **3 Level Multi-Factor Authentication model (3L-MFA)** for cloud access. This model has three different levels and uses knowledge based factors at first and third level and OOB authentication at second level of model. The first level is based on knowledge based factor and uses username –password scheme based on double encryption and decryption principle. Second level is based on random One time Password (OTP) and uses OOB authentication .The third level introduces a novice graphical password (GPS) scheme called Click-GPass (**Clickable Graphical Password**) that involves user's interaction with graphical items such as buttons, images and menu items in form of clicks on graphical screen thereby uses knowledge based factor.

Majority of the existing MFA techniques are either possession based using tokens, badges or biometric based using physiological and behavioral characteristics of users that require additional hardware or software to process these characteristics. This, in turn, incurs huge expenditures in terms of setup, maintenance and processing cost [3]. Moreover, usage of biometric based system is considered as invasion in their privacy by some users. Thus, the choice for knowledge based factors in 3L-MFA has been done with intent to minimize the development and processing cost of the system and to propose an economical authentication model.

Several studies suggest that although usage of multiple factors boost security but usability is compromised in such cases [4]. There is a trade-off between the security and usability of MFA techniques but good authentication mechanism should maintain a balance between security and usability [5]. The proposed model based on Click-GPass GPS achieves reasonable level of security as well as usability at the same time.

Thus, deficiency of adequate balance between security and usability and lack of cost effectiveness of existing MFA is the major motivation behind this model that will meet the requirements of desirable security, usability and cost effectiveness. An empirical study carried out for 3L-MFA based on Click-GPass GPS revealed satisfactory results.

Revised Manuscript Received on May 10 ,2019

Charanjeet Singh, Research Scholar, I. K. Gujral Punjab Technical University, Jalandhar, Punjab, India.

Tripat Deep Singh, Assistant Professor, Department of Computer Applications, Guru Nanak Institute of Management and Technology, Model Town, Ludhiana, Punjab, India.



II. RELATED WORK

The various MFA schemes add variety of factors such as hardware or software tokens, QR codes, OTPs, images, retina scan, fingerprints, signature pattern, keystroke dynamics above traditional username-password schemes to create two factor (2FA) or three factor (3FA) authentication schemes. According to [2], adding multiple layer of factors one above the other boosts security of the authentication system.

A. Token based MFA schemes

In a mutual authentication scheme [6] username-password is used for authentication in first phase and a token generated by an application is delivered to the registered mail-id of user in second phase. This protocol counters replay attack and password stolen attack. A two factor authentication technique called SofToken [7] uses username-password as first factor and a pseudo-random number called codeword as a second factor. This random number is generated on client-side by software. To get authenticated user enters this number which is then verified by the server. A strong authentication scheme by Abdul et al [8] uses Dual Factor Authentication Protocol (DFAP) with mobile token to disallow malware. First password verifies the profile of a user and second password allows access to cloud resources. These passwords are sent securely by server using shared secret key and are provided by the user through his mobile phone using mobile token (UMT). The technique is effective against MIM attacks, insider attack and impersonating attacks.

B. Image based MFA schemes

Vemuri et al proposed a 3-level security [9] where text based authentication, image based authentication and OTP to email are used at first, second and third level respectively. Here, introduction of various levels increments security. Even if an intruder is able to cross first two levels, crossing third level requires intruder to have an access to the original user's email id. A 3-level password authentication scheme by Varghese et al [10] uses image ordering, color pixels and the one time password. In this scheme OTP generation is accomplished using SHA-1 and MD5. A unique 3 Level Authentication and Authorization system presented by Meena et al [11] uses a combination of recognition and recall based techniques. First level is based on username-password authentication. At second level user identifies the image that he had set his click points on, during registration phase from a grid of 16 images. At third level an OTP is delivered to user on his registered number that he has to submit to complete authentication. Aldwairi et al [12] proposed a multistage authentication system that consists of three different stages based on two authentication factors. First stage uses possession based factor- devices' serial number where system checks the device serial number to authenticate the user. The second stage uses knowledge based graphical password scheme where user has to highlight at least m right squares from a grid of n independent squares. In the final stage, he has to select s images in a specific order to get authenticated.

C. Biometric based MFA schemes

In a 5 level multi factor and multi-layer authentication scheme Mohammed et al [13] integrated one or more authentication factors such as knowledge based, possession-based or biometric-based at each level. The proposed system consists of two layers with three sub-systems. Layer 1 authenticates using two subsystems: username-password with face recognition system. Layer 2 uses out of band authentication in form of SMS. A two factor authentication called SV-2FA [14] uses SMS and voiceprint challenge response. In this scheme, a user receives one time phone number and an oath via SMS. The user is authenticated by matching the voice print of the oath read by the user after calling on the given one time phone number. The text of oath changes every time, which includes factors such as date. Khan et al [15] presented a two factor authentication scheme based on behavioral biometrics and knowledge based factor. The scheme uses dynamic time warping (DTW) technique to match the handwritten signatures of a user. Although the cost and resource requirements of the proposed system are low and does not depend on user end platform, it has been tested for small group of people only.

D. Cryptography based MFA schemes

A two-factor authentication framework for cloud based on Public Key Infrastructure (PKI) authentication and mobile out-of-band (OOB) authentication by Lee et al [16] uses random one-time authentication code generated using NLM-128. The scheme authorize only registered users with valid certificates. The PKI authentication process is based on usage of public and private keys, digital certificate, digital signature in addition to trusted third party CA security elements. Eldefrawy et al [17] presented an OTP based two factor authentication scheme that uses algorithm with two nested hash functions to provide forward and infinite OTP generation. A seed created using unique parameters of the host and user such as International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), and registration date generates multiple OTPs in parallel. Hussein et al [18] proposed a mechanism in which server generates an OTP by combining the user's various forms of personal information such as PIN, mobile number and IMEI and transmits encoded OTP (using AES) to the user. A two factor authentication scheme using TOTP developed by Kaur et al [19] involves seed exchange, software based token via TLS tunnel that generates OTP. Authentication takes place by verifying OTP generated on server and client side from the seed value.

III. PROPOSED 3L-MFA SCHEME

The proposed 3L-MFA scheme uses textual username-password authentication based on double encryption-decryption principle, random OTP based OOB authentication and novice Click-GPass Graphical Password Scheme at first, second and third level respectively [20].



The first level of scheme uses traditional username-password scheme (figure 1) where password chosen by user is first encrypted using SHA-1 algorithm. The resultant 20 bytes hexadecimal output is further encrypted using AES-128-ECB algorithm using a secret phrase provided by user as a key. The resultant doubly encrypted password and key used for AES-128-ECB encryption are stored in two separate databases.

Once first level credentials have been verified, a random OTP is generated by the server and is delivered to the user on his registered e-mail id. The authentication at this level requires the user to send this OTP back to the server via SMS from his registered mobile number. The server places rigid time constraints to complete this level of authentication. The entire process of fetching the OTP from the registered e-mail id and sending it back to server via SMS from user's registered mobile number has to be completed in a time frame of five minutes. The user is shown a screen that displays the timer that counts backwards and the mobile number to which SMS has to be sent by the user (figure 2). If the process is not completed within the stipulated time the login screen expires and user has to re-start the authentication process from first level again. The successful verification of both random OTP and the user's mobile number takes user to the third level of authentication.

3 Level Multifactor Authentication Scheme

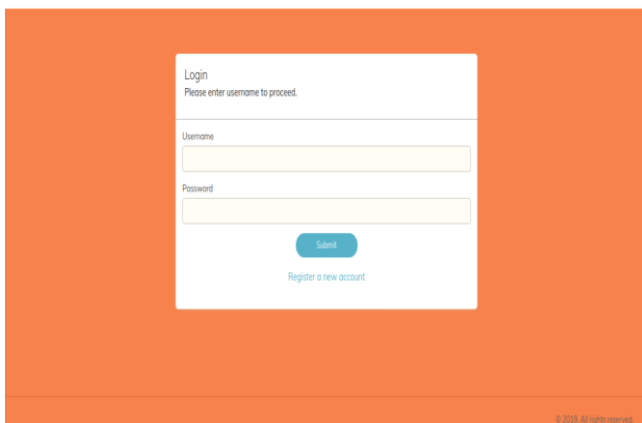


Figure 1. Level 1 of 3L-MFA

3 Level Multifactor Authentication Scheme

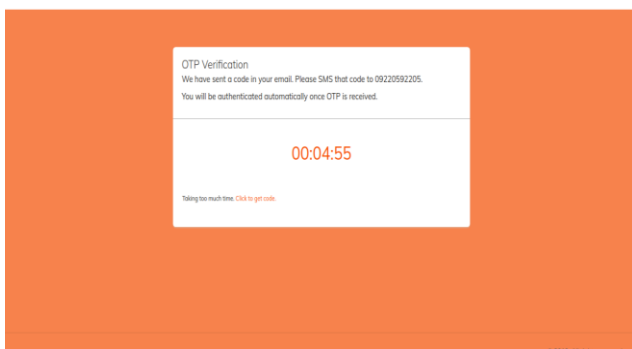


Figure 2. Level 2 of 3L-MFA

At third level, a user is authenticated via a novel graphical password based scheme called Click-GPass (Clickable Graphical Password). This unique scheme is neither recall based nor recognition based where user has to remember either same picture or click point chosen at the registration time rather it requires user to remember three numbers and click various graphical items with that count.

This scheme presents a user with a screen that contains various graphical options like buttons, images and menu items that a user has to click to cross this level. The screen contains a grid of 7 by 6 clickable images in the center, a collection of 24 buttons divided in two sets of 12 buttons each on left and right side of image grid and a menu bar with multiple menu options, each of which further contains 4 sub menu items at the top of screen (figure 3). The images in grid, the caption, color and shape of buttons and the caption of various menu items changes randomly at every login. A user must click on predetermined number of buttons, images and menu options using mouse or touch input in order to get authenticated. The number of images and buttons clicked and number of menu options selected should match with the number chosen by the user at the time of registration. User can click these graphical items in any order or sequence which may include clicking all buttons together followed by all menu items followed by all images. Thus, clicks can be made in any random order with one restriction that user cannot click same instance of particular graphical item twice. The correct combination of these three numbers authenticates a user. If any one number in the combination is incorrect the access is denied. However, clicking same instance of any graphical item more than once is considered as an error and user will not be authenticated even if number of clicks made match the number of registered clicks. This feature has been added to strengthen the Click-GPass scheme.

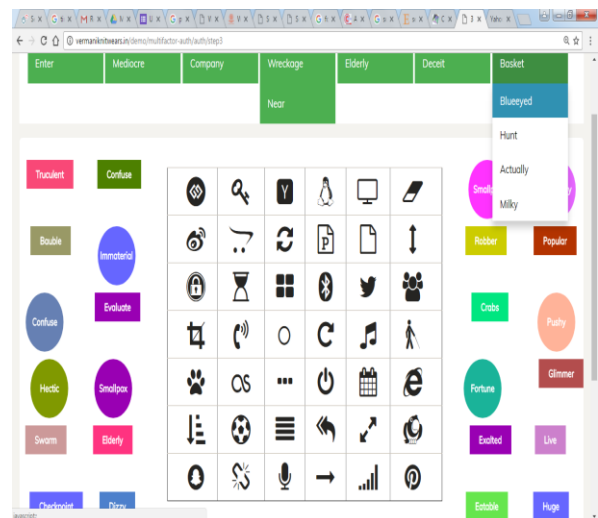


Figure 3. Level 3 of 3L-MFA

A. Phases in 3L-MFA

The 3L-MFA scheme operates in three different phases: registration, authentication and password change phase [20]

Registration Phase

Registration phase requires user to enroll by providing specific details such as username, password, e-mail id, mobile number as shown in figure 4. To elevate the security at first level of authentication, password chosen by user must be eight characters long and must contain at least one uppercase letter, one number and one special character.

Evaluation of 3 Level Multifactor Authentication Model based on Click-GPass Graphical Password Scheme

In addition, a user is asked to provide a phrase that will be used as a key for double encryption process using open SSL AES-128-ECB in the first level of authentication. The plaintext password submitted by user is first encrypted using SHA-1. The 20 bytes hexadecimal output of this encryption is further hashed using AES-128-ECB algorithm using a phrase submitted by user as key for this encryption. User is also prompted to input the number of buttons to be clicked (m), number of images (n) to be clicked and number of menu items (p) to be selected on graphical screen for Click-GPass during the third level of authentication. Figure 4 shows the details of registration form. In order to strengthen the authentication process the total number of clicks chosen must be at least 10. Thus, while registering data for Click-GPass GPS used at level 3, user must satisfy the following condition:

$$m + n + p \geq 10 \text{ where } m, n, p \geq 1 \dots\dots (1)$$

All the details provided are stored in a database with doubly encrypted password and key used for second encryption in separate databases for the verification to be done at the time of authentication.

Authentication Phase

In 3L-MFA, user has to undergo three different levels of authentication one after the other. At level 1, user enters name/email-id as username and textual password. For this, system performs double decryption of password stored in the database using AES-128-ECB and SHA-1 algorithm and then matches it with password submitted by user. If username and password match is valid user is directed to level 2 of authentication. The system then generates a random OTP that is delivered to registered email id of user. At the same time user is shown a screen that displays a mobile number to which user has to SMS this OTP from his registered mobile number. The screen also shows a countdown timer that is set to go off after five minutes. User has to access the OTP from his email id and has to SMS the same to server's number within this time frame. The successful verification of both the received OTP and the mobile number of the user by the server from its database authenticates the user at level 2. If time period expires or OTP and mobile number verification fails, the login process is aborted and user has to start from level 1 again. Thus, level 2 uses two separate channels to send and receive OTP thereby ensuring security using OOB. At the same time, restriction of completing the authentication process in rigid time constraints puts pressure on intruder or hacker which further augments the security of the system.

3 Level Multifactor Authentication Scheme

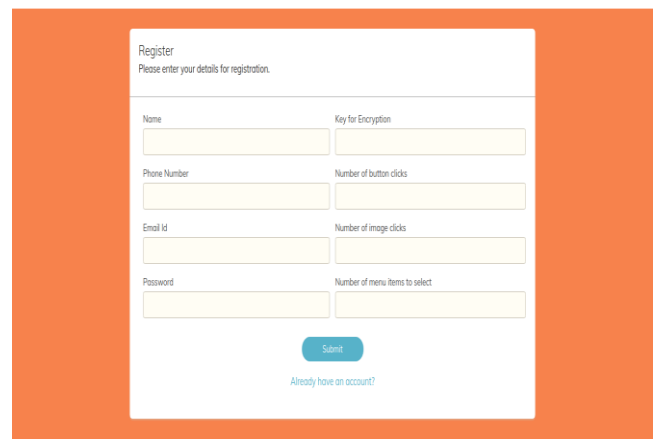


Figure 4. Registration Phase

At level 3, Click-GPass GPS is used where user clicks on specific number of buttons, images and menu items to get authenticated. The count of number of buttons, images and menu items clicked is compared with the count registered by user. It is mandatory that a user has to make correct combination of all three options. A mismatch in any of these three numbers would not let the user to login.

Password Change Phase

Password change facility in 3L-MFA enhances the user friendliness of authentication scheme. To reach this option a user has to go through all three level of authentication. User can change password only after successful login. The selection of password change option provides a user with a screen where a user can update all the information that was given by him at the time of registration. Here, a user can enter changed alphanumeric password, a new key phrase for further encrypting SHA-1 encrypted password, update his email id and mobile number. It also facilitates user to modify password for Click-GPass scheme by changing the number of images, buttons to be clicked and number of menu items to be selected. Figure 5 shows the password change screen of this scheme. In this way password change option enhances the usability of 3L-MFA.

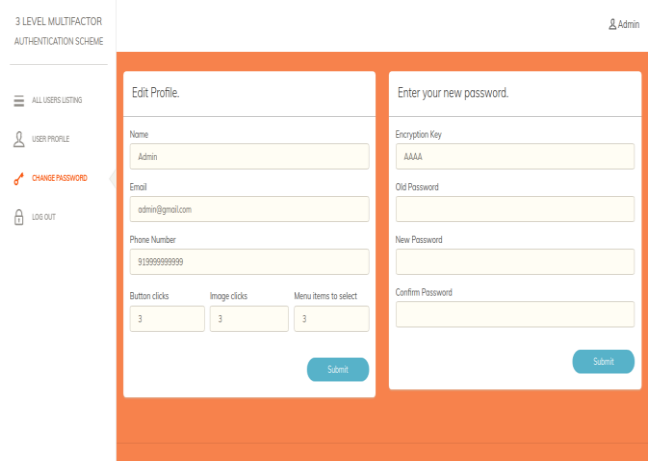


Figure 5. Password Change Phase

B. Working of 3L-MFA

The working of entire authentication scheme is summarized in following steps :

Step1: User registers on the server and provides following information to the server: username, password, mobile number, e-mail id, key phrase, number of images to be clicked, number of buttons to be clicked and number of menu items to be selected.

Step 2: Clicking login option on screen prompts user for username and password.

Step 3: Server verifies the username and password from the database by decrypting the SHA-1 password using the phrase given by the user as a key. This decryption is performed using open SSL and AES-128-EBC.

Step 4: If the username and password match is found in database, server generates a random OTP that is delivered to the registered email id of the user otherwise access is denied. At the same time server shows a screen that starts a countdown timer of 5 minutes.

Step 5: User retrieves the OTP from his mailbox and sends it to the server via a SMS from his registered mobile number.

Step 6: If this OTP is not sent within the time frame of 5 minutes the login time expires and access is denied. Upon receiving OTP from a user, server not only checks the correctness of random code but also ensures that the OTP has been sent through registered mobile number.

Step 7: If both the OTP and mobile number are correct, server displays a graphical screen of Click-GPass that contains a 7 x 6 grid of images, a set of different shaped & colored buttons along with multiple menu items.

Step 8: User has to click on specific number of buttons, images in a grid and select menu items with the same count as was chosen at the time of registration with the condition of not clicking same instance of particular item twice.

Step 9: The correct number of all the three actions viz. button clicks, picture clicks and menu items selected will grant access to the user on the specific resource.

C. Prototype Development

The prototype of 3L-MFA is implemented as a web based application using PHP 5.6, HTML 5.0, CSS 3, Bootstrap Framework, JQuery whereas database development used MySQL 5.7. Separate database were created to record registration data and login data. These tables were user to keep track of registration time, login time at level1, login time in Click-GPass GPS at level 3 and successful login attempts.

IV. USABILITY ANALYSIS OF 3L-MFA AND CLICK-GPASS

A usability study of the proposed scheme was carried out involving 75 participants in a lab environment. All the participants (48 males and 27 females) were tech-savvy college students or faculty members with 91% (68) of them in the age group of 18-25.

A. Methodology of study

Before conducting the study, a training session was carried out where they were demonstrated the working, usage and security measures of 3L-MFA model using video tutorials. The study involved three different sessions: first

after the training, second after one week and third after one month with the view to test the cognitive load and effect of frequency of usage of the scheme.

For each conducted session, the study observed login time for level 1, login time for Click-GPass GPS, login success rate of 3L-MFA (for all three levels of 3L-MFA) for each participant. In addition to the above metrics, first session also recorded registration time taken by each participant for 3L-MFA. During each session, participants were given maximum of three chances to login. The login time was recorded only for successful logins.

Following the first session, a post-test feedback study was carried out where all the participants involved in the experimentation of 3L-MFA were made to fill a questionnaire about the feedback of authentication model. The questionnaire included several interrogations about usability features such as ease of registration in 3L-MFA, ease of login in Click-GPass scheme, screen layout and design of Click-GPass, memory load and ease of use.

B. Results and Interpretations

The study evaluated average registration time (before session 1), login time for level 1, level 3 i.e. Click-GPass scheme and login success rate of all participants during all three session conducted. The average login time with standard deviation for (level 1 & 3) for all three sessions is given in table 1 while table 2 outlines the successful login attempts for all the three conducted session along with login success rate at first attempt.

Registration time

The mean registration time for 3L-MFA is 101 seconds with standard deviation of 49 seconds (see table 1). An important observation made during experimentation was that 44 (59%) participants took less than average time to register. However, 41% participants took more than average time. Majority of participants spent more time in creating their textual password for level 1. This time was consumed due to the compulsion of including at least one uppercase character, one number and one special character in textual password. Even though the participants were instructed to follow this policy of password creation but they were not in the habit of creating password with such restrictions and realized it when error message was flashed. Hence, additional time was spent in retyping textual password during registration process.

Login time

The mean login time taken by all participants for level 1 and Click-GPass (level 3) for three sessions is given in table 1. The mean login time for both schemes (doubly encrypted textual password at level 1 and Click-GPass at level 3) decreased during each successive session. The login time for Click-GPass for 75 participants for all three sessions is shown in figure 6 that shows that login time for session 3 conducted after a month was lowest. Also, the number of participants who were able to login at first attempt for each session also increased.



Evaluation of 3 Level Multifactor Authentication Model based on Click-GPass Graphical Password Scheme

The login success rate increased to 96% from 81% from 1st to 3rd session (table 2). The overall login success rate for all three sessions is 90% (table 3). Here, not only the login time decreased but login success rate also increased during session 3. These observations indicate that Click-GPass scheme not only has low cognitive load but also becomes faster with frequency of use. Also, Renaud [21] suggested that the frequency of use is an important factor to test the cognitive load of any scheme. Thus, the effect of frequency of use of 3L-MFA is that it makes the scheme user friendly and adoptable.

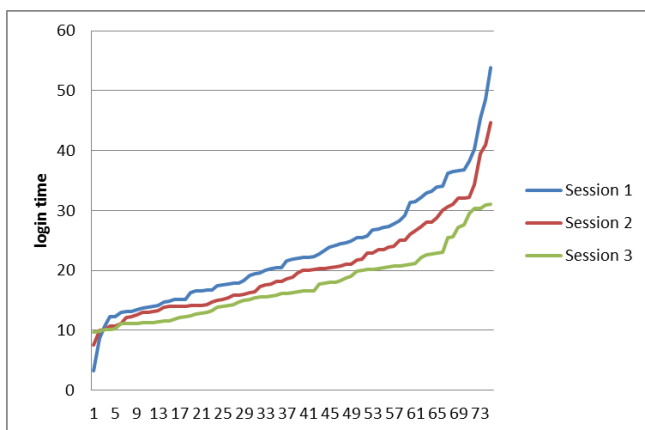


Figure 6. Login time for Click-GPass for three sessions

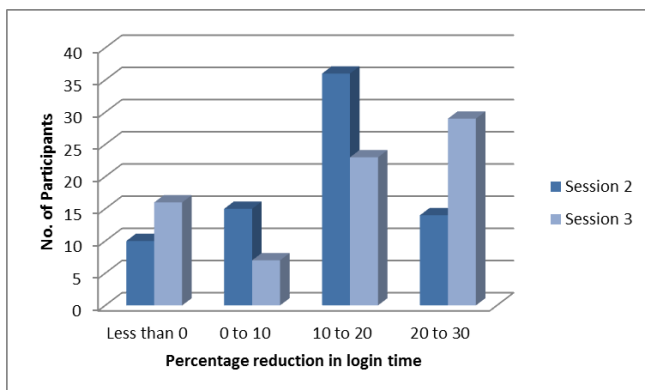


Figure 7. Reduction in login time for Click-GPass during session 2 and 3

When the login times of session 1, 2 and 3 were compared for Click-GPass scheme, it was noticed that there were improvements in login time in successive sessions. Login time was reduced by 10 to 20 percent for 36 (approx. 50%)

participants during session 2. Further, there was 20 to 30 percent reduction in login time for 29 (38%) participants during session 3 (see figure 7).

According to Zangoeei et al [22], the adoption of any authentication scheme is ascertained on the basis of amount of time taken by it to validate the user. Since the textual password based schemes being fastest, the new schemes are usually compared with them to ascertain their efficiency in terms of speed. The proposed Click-GPass scheme used at level 3 of 3L-MFA also passed this test. During all the three sessions, mean login time taken for Click-GPass scheme is less than the doubly encrypted textual password scheme used at level 1 (figure 8). This further establishes the credibility of Click-GPass scheme over textual password schemes.

C. Further analysis of some aspects of 3L-MFA

The criteria chosen by proposed scheme to make level 1 of authentication strong require the participants to keep at least one special character in their password. The password analysis of all 75 participants involved in the study revealed that 65 (87%) participants chose “@” as one of the characters

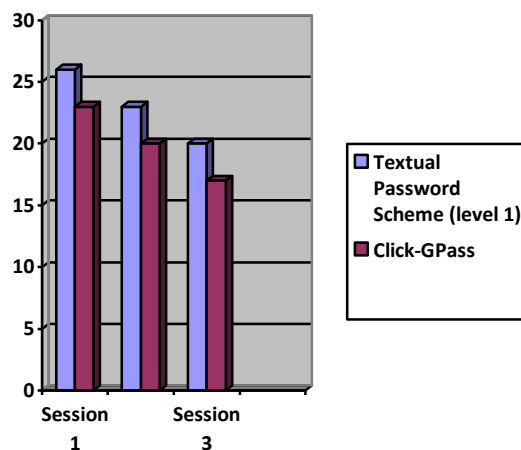


Figure 8. Login time of Click-GPass compared with textual password login

Table1: Registration, login time for level 1 and Click-GPass scheme for three sessions

		SESSION 1	SESSION 2	SESSION 3
Registration Time (in Seconds)	Mean		101.35	
	Standard Dev.		49.40	
Login Time for level 1 (in Seconds)	Mean	26.08	23.86	20.83
	Standard Dev.	12.74	11.23	10.12

Login Time for Click-GPass (level 3) (in Seconds)	Mean	23.08	20.17	17.36
	Standard Dev.	11.15	9.88	8.67

Table 2: Successful login attempts and login success rate during three sessions

	SESSION 1			SESSION 2			SESSION 3		
	Attempt number			Attempt number			Attempt number		
	1 st	2 nd	3 rd	1 st	2 nd	3 rd	1 st	2 nd	3 rd
Successful Logins	61	10	4	69	5	1	72	3	0
Login Success rate (at first attempt)	61/75 (81%)			69/75 (92%)			72/75 (96%)		

in their password. The users prefer this special characters over other characters such as \$, #, &, * etc.

Click-GPass GPS applied at level 3 of proposed scheme made it mandatory for user to keep a minimum of 10 clicks in all in their click based password. All 75 participants chose clicks in the range of 10-20. An interesting observation about this factor is that maximum number 23 (30%) participants kept exactly 10 clicks in their password whereas only one participant kept maximum number of clicks i.e. 20 in his password. Next choice for number of clicks by 19 participants was 15 clicks followed by 12 clicks by 17 participants. The detail of number of clicks chosen as password by the number of users is plotted in figure 9.

In order to study the relationship between the number of clicks chosen by participants and login time taken to perform those clicks, a correlation coefficient(r) was calculated. The r value was 0.075 that indicated that there was no correlation

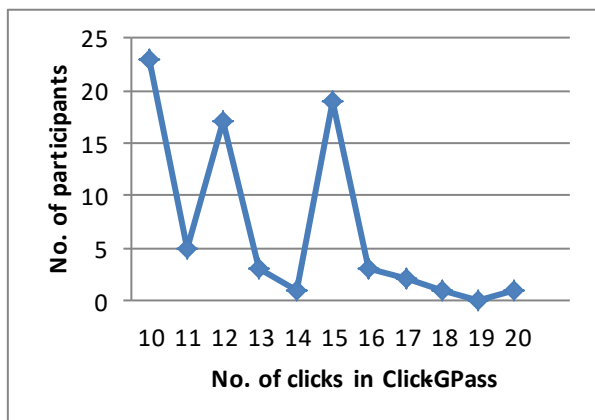


Figure 9. No. of Clicks in Click-GPass chosen by participants

between the number of clicks chosen by participants and the login time taken to perform clicks on graphical items. Figure 10 shows the scatter diagram for the number of clicks versus the time taken. Moreover the average time taken for 10 clicks and 15 clicks was same (23 seconds).

Table 3: Total login attempts and login success rates

	Total login attempts	No. of successful logins at 1 st attempt	Success rate
Session 1	75	61	81%
Session 2	75	69	92%
Session 3	75	72	96%
Total	225	202	90%

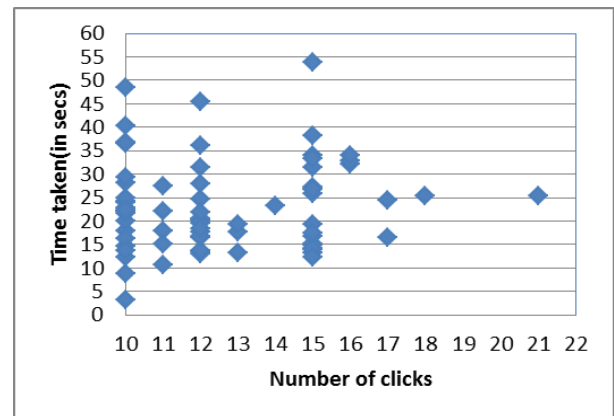


Figure 10. Number of clicks Vs time taken to login

D. Result of user survey

According to Eljetlawi [23], a good graphical password scheme ought to have certain features such as ease of use, ease of creation, ease of learning, ease of memorizing, reliability and screen design & layout. The survey conducted to gather feedback of participants evaluated Click-GPass scheme used in 3L-MFA for these metrics had following results (figure 11):

• *Ease of use*

Respondents were asked to rate the Click-GPass scheme on 5 point scale where 1 indicated very complex and 5 indicated very easy. In all, 57 (76%) participants gave positive feedback on this factor as users just have to click graphical items like buttons, images and menu items with correct count. Users need not to remember certain pictures, buttons etc. or their sequence of selection.

• *Ease of creation*

Click-GPass is neither recognition based nor recall based scheme where user has to either remember set of pictures or recall order of selecting pictures. Registering and creating password for Click-GPass is fairly easy as a user just has to input three numbers for clicking buttons, images and menu items. Thus, registration time is minimal and choosing password is an easy affair. Here, 53 (71%) participants were of the view that Click-GPass has ease of creating password.

• *Ease of memorizing*

The proposed scheme has minimum memory load as user just has to remember three numbers with which they are to click and not the pictures, buttons or their labels itself. In survey, 57 (76%) participants replied “easy” and “very easy” when they were asked about the cognitive load of scheme and how easy is to remember their password.

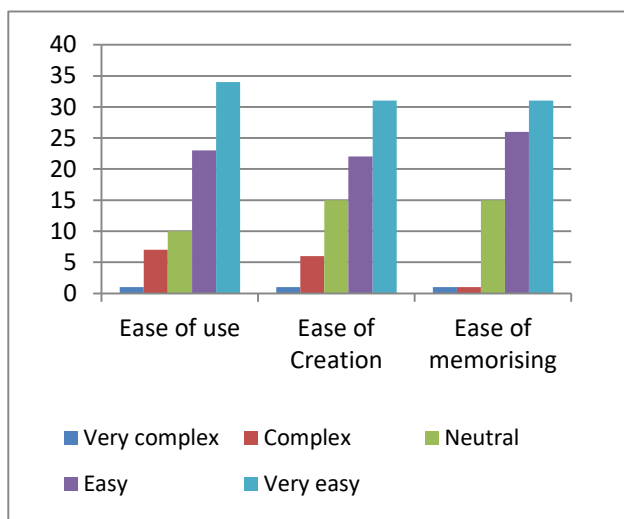


Figure 11. Results of User's Feedback on various usability factors

• *Screen design and layout*

When users were enquired about the design and layout of Click-GPass scheme, 59 (79%) participants gave positive feedback indicating it to be impressive and user friendly.

• *Reliability*

A vast majority (92%) of respondents of study considered 3L-MFA to be secure and unique authentication scheme after using it. This indicates that they have enough confidence in security of the scheme. When they were asked “will you prefer this scheme over other authentication schemes?” major chunk 69% said “yes”. The results of the response are shown in figure 12.

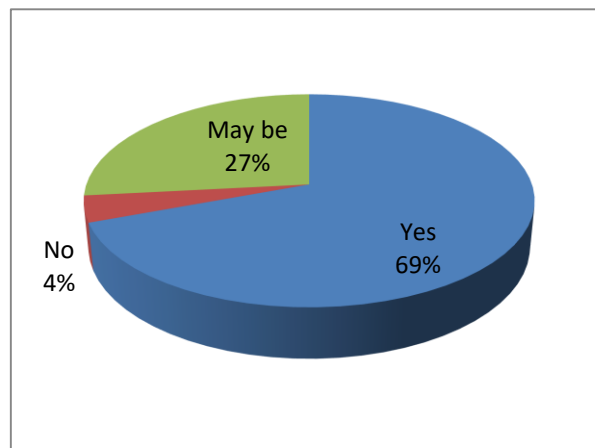


Figure 12. Preference for 3L-MFA

• *Effect of frequency of use*

Participants were also questioned about the effect of frequency of use for the proposed scheme to which 89% believed that frequent use of scheme will make it easy and faster. The empirical study conducted also gave the similar results. It was observed that the login time reduced for 86% participants from session 1 to session 2. It further decreased during session 3 conducted after one month (see figure 6).

V. SECURITY ANALYSIS OF 3L-MFA AND CLICK-GPASS

A. Password space

Password space was determined for level 1 textual password scheme (TPS) and level 3 Click-GPass GPS. The TPS used 26 uppercase, 26 lowercase, 10 numbers and 8 special characters thereby making total of 70 characters. If L denotes the length of password, the password space is:

$$\text{Password Space} = 70^L$$

For example, if a minimum password length of 8 characters is considered, the password space is 9.4×10^9 .

For Click-GPass scheme the various possible click combinations on buttons, images and menu items for total of 10 clicks on all items are 36 as shown in table 4. In order to have reasonable number of combination for Click-GPass scheme minimum condition of 10 clicks was chosen. With

Table 4: Possible combinations of clicks on buttons, images and menu items with total count of 10 clicks

S. No.	No. of clicks on buttons	No. of clicks on images	No. of clicks on menu items
1	1	1	8
2	8	1	1
3	1	8	1
4	1	2	7
5	7	1	2
6	2	7	1
7	7	2	1
8	2	1	7

9	1	7	2
10	1	3	6
11	6	1	3
12	3	6	1
13	1	6	3
14	3	1	6
15	6	3	1
16	1	4	5
17	5	1	4
18	4	5	1
19	1	5	4
20	4	1	5
21	5	4	1
22	2	2	6
23	6	2	2
24	2	6	2
25	2	3	5
26	5	2	3
27	3	5	2
28	2	5	3
29	3	2	5
30	5	3	2
31	2	4	4
32	4	2	4
33	4	4	2
34	3	3	4
35	4	3	3
36	3	4	3

The number of possible click combinations will increase with the increase in the total count of clicks. The relationship between the number of clicks and number of click combination possible is shown in figure 13. With this observation we introduce a new metrics called password space density (PSD) for Click-GPass scheme that will represent number of click combinations possible per click.

$$PSD = \frac{\text{Total no. of click combinations}}{\text{No. of clicks}} \dots(2)$$

Using equation 2, the PSD calculated for various number of clicks is given in table 5. It is ascertained that password space density varies by a factor of 0.5 for various number of clicks. However, the password space can be further increased by including clicks on these items in specific order.

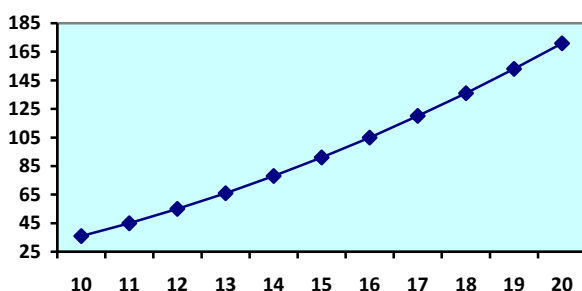


Figure 13. No. of clicks Vs No. of click combinations

Table 5: PSD for various number of clicks

No. of clicks	No. of click combinations	PSD
10	36	3.60
11	45	4.09
12	55	4.58
13	66	5.07
14	78	5.57
15	91	6.06
16	105	6.56
17	120	7.05
18	136	7.55
19	153	8.05
20	171	8.55

B. Shoulder surfing

Shoulder surfing attack is one type of attack that is most likely to affect any GPS. 3L-MFA model was tested for the same where 75 different observers were appointed as shoulder surfers to observe the 75 participants and steal their password during the first login session. The observers were made to stand behind each participant and steal their passwords. The details of passwords captured via shoulder surfing at level 1 and level 3 are given in table 6.

Table 5: Successful shoulder surfing attacks

Level	No. of Passwords captured	Success rate
1 st	0/75	0%
3 rd	5/75	6%

During experimentation it was observed that none of the shoulder surfer was able to capture the textual password. However, only 5 observers were able to successfully steal click based password of Click-GPass scheme at level 3. It was further analyzed that the stolen passwords were majority of those cases where participants performed consecutive clicks on same items one after the other. For example, if a user had chosen 5,5,5 clicks on buttons, images and menu items respectively and clicked on 5 different buttons consecutively followed by 5 images followed by 5 menu items, observers were able to steal this password. Conversely, when participants clicked on various graphical items in random orders i.e. 1 button, 2 images, 3 menu items followed by 2 more buttons, 1 image, 2 menu items and then 3 images and 2 buttons randomly, shoulder surfers were not able to remember the clicks as different items were clicked with different count and different order.

The empirical study conducted for testing shoulder surfing attack revealed that if similar instances of a graphical items are clicked consecutively, password guessing becomes easier. To improve this scheme and reduce shoulder surfing it is required that various graphical items should be clicked in random order. Thus, improving shoulder surfing would require to introduce a pattern or sequence of clicks on these graphical items.

VI. CONCLUSION AND FUTURE SCOPE

3L-MFA model enhances the security for critical data access applications by incorporating three different levels of authentication and multiple knowledge based factors. The proposed scheme also introduces a novice click based GPS called Click-GPass. The results of empirical study conducted with 75 participants showed that Click-GPass scheme maintains a good balance between usability and security. The scheme not only has low memory load but is also easy to learn and use. It has potential to resist shoulder surfing attack to a great extent as only 5 Click-GPass passwords were stolen during the study. The overall security against shoulder surfing is 93%

The future scope of proposed work includes improvement in password space by introducing pattern or sequence of clicks in Click-GPass. It will increase the number of permutations of clicks. To further enhance the security, following improvements can be introduced in Click-GPass scheme:

- Apart from buttons, images and menu items other graphical items such as text boxes, radio buttons, and checkboxes can be introduced. Increase in the number of graphical items will not only increase password space to greater extent but will also enhance security by including several different permutations of clicks.
- Colour and shape attribute of buttons can also be used where count of clicks on buttons can be associated with specific colour and/or shape.
- The limit of minimum 10 clicks can be increased to enhance security as increasing number of clicks will not affect the login time but will increase the password space.

REFERENCES

1. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, 34(1), pp. 1-11, Jan. 2011.
2. Charanjeet Singh, Tripat Deep Singh. "A Systemic Review of Various Multifactor Authentication Schemes", *International Journal of Computer Sciences and Engineering*, 7(2), pp.503-510, 2019.
3. Israa M. Alsaadi, "Physiological Biometric Authentication Systems, Advantages, Disadvantages and Future Development: A Review", *International Journal of Scientific & Technology Research*, 4(12), pp. 285-289, December 2015.
4. N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking" *Computers & Security*, 30(4), 2011.
5. M.D. Hafiz, A.H. Abdullah, N. Ithnin and H.K Mammi, "Towards identifying usability and security features of graphical password in knowledge-based authentication technique", *In: Proceedings of the 2nd IEEE Asia International Conference on Modelling & Simulation*, pp. 96-403, 2008
6. S. K. Nayak, S. Mohapatra, B. Majhi, "An Improved Mutual Authentication Framework for Cloud Computing", *International Journal of Computer Applications*, 52(5), August 2012.
7. J. C. Liou and S. Bhashyam, "A Feasible and Cost Effective Two-Factor Authentication for Online Transactions", *In the Proceedings of the 2nd International Conference on Software Engineering and Data Mining, IEEE*, pp.47-51, June 2010
8. A. M. Abdul, S. Jena, M. Balraju, "Dual Factor Authentication To Procure Cloud Services", *In the Proceedings of the 2016 Fourth International Conference on Parallel Distributed and Grid Computing(PDGC),IEEE*, 2016
9. V. K. Vemuri, S. D. V. Prasad, "A Secure Authentication System by Using Three Level security", *International Journal of Engineering Science and Computing*, ISSN-2321-3361, pp.344-348, 2014.
10. L. Varghese, N. Mathew, S. Saju, V. K. Prasad, "3-Level Password Authentication System", *International Journal of Recent Development in Engineering and Technology*, ISSN 2347 - 6435 (Online) , 2(4), April 2014.
11. M. Meena, H. S. Lamba, D. Taterwal, M. Shaikh, "System For 3 Level Security Verification Using Image Based Authentication & OTP", *IOSR Journal of Engineering (IOSRJEN)* ISSN (e): 2250-3021, ISSN 2278-8719, 13, pp. 46-52, 2018.
12. M. Aldwairi, R. Masri, H. Hassan, M. E. Barachi, "A Novel Multi-Stage Authentication System for Mobile Applications", *International Journal of Computer Science and Information Security*, 14(7), 2016.
13. M. M. Mohammed, M. Elsadig, "A multi-layer of multi factors authentication model for online banking services", *In the Proceedings of the 2013 International Conference on Computing Electrical and Electronics Engineering (ICCEEE)*, pp. 220-224, 26-28 August, 2013.
14. H. Fujii, Y. Tsuruoka, "SV-2FA: Two-Factor User Authentication with SMS and Voiceprint Challenge Response", *In the Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST -2013), IEEE*, pp-283-287, 2013.
15. S. H. Khan, M. A. Akbar, "Multi-Factor Authentication on Cloud", *In the Proceedings of the International Conference on Digital Image Computing: Techniques and Applications*, pp. 1-7, 2015.
16. S. Lee, I. Ong, H. T. Lim, H. J. Lee, "Two factor authentication for cloud computing", *International Journal of KIMICS*, 8, pp. 427-432, 2010
17. M. H. Eldefrawy, M. K. Khan, K. Alghathbar, "OTP-Based Two-Factor Authentication Using Mobile Phones", *In the Proceedings of the 2011 Eighth International Conference on Information Technology: New Generations (ITNG)*, Las Vegas, NV, pp. 327-331, 2011.
18. K. W. Hussein, Dr. N. F. M. Sani, Dr. R. Mahmud, Dr. M. T. Abdullah, "Design and Implementation of Multi Factor Mechanism for Secure Authentication System", *International Journal of Computer Science and Information Security*, 11(7), pp.31-37, July 2013.
19. N. Kaur, M. Devgan, S. Bhushan, "Robust Login Authentication Using Time-Based OTP Through Secure Tunnel", *In the Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 3222-3226, 2016.
20. Charanjeet Singh and Tripat Deep Singh, "A 3-Level Multifactor Authentication Scheme for Cloud Computing", *International Journal of Computer Engineering & Technology (IJCET)*, 10(1), pp.184-195, 2019.
21. K. Renaud, "Quantifying the Quality of Web Authentication Mechanisms: A Usability Perspective". *Journal of Web Engineering*, 3 (2). pp 95-123, 2004.
22. Toomaj Zangoeei, Masood Mansoori, Ian Welch, "A hybrid recognition and recall based approach in graphical passwords", *Proceedings of the 24th Australian Computer-Human Interaction Conference*, Melbourne, Australia, pp.665-673, November 26-30, 2012.
23. A. M. Eljetlawi, "Graphical password: Existing recognition base graphical password usability". *6th International Conference on Networked Computing (INC)*, Gyeongju, Korea (South), 2010.