International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I5P223

Volume 69 Issue 5, 166-176, May 2021
© 2021 Seventh Sense Research Group®

Hybrid Graphical User Authentication Scheme Using Grid Code

Salim Istyaq[1], Afrah Nazir[2], Mohammad Sarosh Umar[3]

[1]*University Polytechnic, Aligarh Muslim University, Aligarh, India.*

[2,3]*Computer Engineering, Aligarh Muslim University, Aligarh, India.*

[1] saleemishtiyak@gmail.com, [2] afrahnazir@zhcet.ac.in, [3] saroshumar@zhcet.ac.in

Abstract *— Security is an essential part of any organization, due to the fact that it protects our resources such as confidential data and information from third-party access point. Numerous algorithms and models are developed for a search of better protection. But they have limited protection shields or they have some bugs, which allows a hacker to access the principle framework. Consequently, numerous security systems are implemented utilizing various methodologies of which one is graphical based security. Here, we propose a security system based on text as well as graphical password that works on the generation of Unique Grid Code (UGC) for each selected image by the user for their password. Our system's most significant security highlight is that it assigns a unique code for each selection, composed of coordinated selected image, which will also vary from one image to another.*

Keywords — *OTP, UGC, Matrix Authentication, Passface, Shoulder Surfing, HGC*

I. INTRODUCTION

The present system is catering to many problems regarding security. The primary issue is either the system is very stringent or the system is very lenient. It is possible for a person to hack into someone's computer for resources and information. Therefore, to protect these valuable resources, many theories and algorithms have been developed, with their new approaches to overcome these loopholes, such as authentication systems including textual password system, biometric-based system, and token-based system (ATM, Credit card). But any one of them is not entirely secure.

In textual passwords, generally users set their stringof passkey related to their initials such as: Name, Address, DOB etc. This weakness can become a huge advantage for the hacker to misuse user's account. In biometric based systems, the setup cost of the device is very costly, so it is difficult to be used by every person. On the other hand, token-based authentication system, like ATM cards, credit cards, VIP cards etc. suffer from attacks and hacking such as cloning of chips inside the ATM, illegal accessing of One Time Password (OTP) [18]. According to the report [24] there are various ways in which the attackers can easily clone the magnetic chip fixed inside the card at the time of point of sale (POS) [25]. The POS are the biggest source of stolen payment cards for cyber criminals. Although it has made the headlines since past few years, the POS threat was growing after 2005 and caused a lot of losses in the US from 2013 to 2014. A major issue in this authentication system is illegal accessing. Anyone can take advantage if someone leaves their card somewhere by mistake or by stealing the card from the person. The graphical authentication [9][16] approach is based on the principle of recall and recognizing ability of human behavior [17]. The approach is powerful as compare to alphanumeric passwords. The number of password depends on the selection on the graph. It is slightly low cost and easy to use everywhere rather than biometric device, so in order to use graphical authentication [16] technique in the best way; we proposed a system that is based on this approach and strengthen this authentication [18] scheme by proposing the hybrid GUA scheme on a single system.

The paper is organized in the following sections. Section 2 sets the related work or background for user authentication. Section 3 deals with the proposed scheme. Section 4 deals with result and analysis. Finally, Section 5 deals with conclusion and future work.

II. RELATED WORK

Recognition Techniques

In this (Cognometric) approach, a set of images is given to the user to select some images from it, in order to authenticate the system. The images shown can be of any type whether a scenery or logo etc. Some of the techniques based on this approach are as follows:

Dhamija *et al*. implemented a technique that is based on hash visualization. In this technique user has to select an image from multiple images. To authenticate, they would have to identify the preselected image. However, a limitation of this system is that it is prone to hacking by illegal user because server stores the address of the selected image in plain text. The process takes a lot of time to authenticate [21].

Xie *et al.* [15] used the blockchain to enhance protection and privacy on the Internet of Vehicles (IoV) and on 5G-VANET transportation systems [22]. Attempts have been made to combine IoT with blockchain technology. All these activities contribute to the growth and sophistication of the usage of blockchain in the Internet of Things [7][8][9][10].

Akula and Devisettys algorithm proposed a technique that is similar with Dhamija and Perrig [21] but a point of dissimilarity in their technique is that system is more secure, take less memory and time in order to login. Hash function SHA-1 is used in this giving (20 byte) output.

Weinshell *et al.* proposed and studied a method in which user is given training to recognize (100-200) images from a set of 20000 pictures [29]. There studies include picture recognition, object recognition and pseudo word recognition.

Sobardo *et al*. made a system in which the user has to select a preselected object and click between the set of images in the convex hull formed. In order to make the system more complex they add 1000 objects which make the interface too overwhelming [12].

Triangle scheme [5] is made only to overcome the problem due to shoulder surfing [7]. It was created by a group that also made many schemes earlier in 2002. The working of this system is that there are N set of objects which could be 100 to 1000 on the display. The k objects represent the user password; the user have to remember the subset of k objects. At login, the system will place the position of N objects. The user is required to select three of his passwords and click inside the triangle made by those objects.

Movable frame scheme [5] is based on triangle scheme with the same assumption and ideas by the creator of triangle scheme. In this authentication system [13] the user is asked to move three objects from the k objects in order to make the password.

Passface [21] is easily stated that human brain can easily recognize the face better than anything. For recognition, a user is required to select four different faces among the image set [29]. At the time of login, the user is required to select those faces one by one at the registration time in order to login.

Jansen proposed a scheme in which there are 30 images corresponding to its numerical value. This numerical value is chosen in a sequence in order to login. But due to limitations of only 30 images the password is very short [28].

Memory Based Techniques

Memory based techniques are divided into two sub categories i.e.

1. Pure memory-based technique
2. Cued memory-based technique

This method is also known as Drawnmetric system. In this method the users have to draw something that is the same in registration phase.

1-Pure recall-based technique: In this authentication, there is no hint or clue provided. Many systems are based on this approach:

DRAW A SECRET (DAS) technique **-** In this, the user registration is done by drawing a sketch on 2D grid at the registration time and at login time, the user is required to draw the same sketch in the same sequence in order to authenticate [11].

Syukri *et al*. proposed a system in which the user has to enter the signature on a 2D grid which is done by mouse or stylus. To authenticate, the user has to redraw his/her signature. It uses the signature drawn by the mouse which is difficult for some users [1].

2-Cued recall-based system: It is also termed as iconmetric system. In this system, authentication is done by providing some hint, so that it is easy for the user to recall. Passlogix scheme [6] is basically based on repeating sequence. In their proposed VGO scheme, the user is asked to select the background of the scheme such as Dining hall; kitchen etc. and the user can change the position of any item present in the current scene. The password column is small which is the major limitation of this Hybrid Scheme [30]. These are the schemes that are made up of combination of 1 or 2 techniques for e.g. combining textual based scheme with graphical password [2] [25] schemes.

III. PROPOSED SCHEME

Our Hybrid Grid Code (HGC) system is a GUA system and uses two approaches that come under this technique. These approaches are as follows:

1. Passface
2. Cued click points

Both approaches are already discussed in the related section. Our aim is to create a more secure system which is easy to use by any user. We strengthen the concept of traditional GUA schemes, which use single algorithm. This is done by making hybrid composed of two approaches. Both the approaches have their own advantages over the entire system. The approaches are linked together in such a way that both are dependent on each other to take decision in order to minimize any chances of attack.

For this paper, we find a newer approach for authentication [20] from the Unique Grid Code (UGC). The concept of UGC is discussed in detail later in this paper.

The frame of the proposed system is designed in such a manner that it is easy to understand the working of different techniques used in the system. This is shown step by step. For understanding purpose, we divide the system in two phases- Registration and Login.

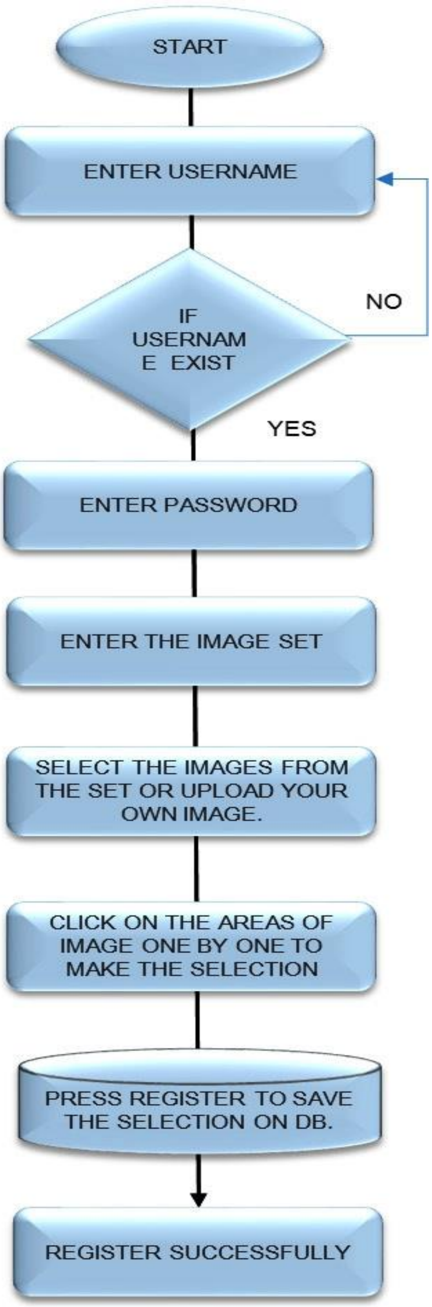

START
ENTER USERNAME
IF USERNAM E EXIST
NO
YES
ENTER PASSWORD
ENTER THE IMAGE SET
SELECT THE IMAGES FROM THE SET OR UPLOAD YOUR OWN IMAGE.
CLICK ON THE AREAS OF IMAGE ONE BY ONE TO MAKE THE SELECTION
PRESS REGISTER TO SAVE THE SELECTION ON DB.
REGISTER SUCCESSFULLY

Fig. 1: Registration process

Registration

This is the first interface of our system in which the user has to register in the security modules of the system. It has a specified column for gathering user's initial credentials. The full working of registration phase is explored in detail in this section. The main frame of the registration phase of this authentication system design is shown in Fig.1

A portion of alphanumeric authentication system is present which registers every single user with unique username, password along with an option of choosing a matrix of images e.g. (3x3), (4x4) etc. but not more than (10x10), e.g. if a user chooses 3x3 as an option, it means there are 3 rows and 3 columns that are composed of images. The system will automatically set the sizes of the images that will be displayed further, at the time of login process by doing image normalization, scaling for displaying in selected region.

The portion of GUA is present in the proposed system and is divided into two phases of GUI.

I. Phase 1 contains Passface approach.
II. Phase 2 contain Cued click point approach.

In the 1st phase of GUA, the user is asked to choose either 1 image from a randomly generated set of images or upload their own. But before this, it should be chosen appropriately, either random image or upload image option.

Suppose a user chooses to upload an image, the green mark will be displayed on their choice. On the other hand, if he/she chooses a random image then the process will continue in the same manner. Depending upon the complexity that the user wants, he/she has a freedom to choose more than 1 image up to a maximum of 5 images; every image is passed through both the GUA phases. The 2nd phase of GUA is registering clicks on the selected image which is registered at the pass face section. Here, in this process of registering clicks the images are divided into 30x30. That means 30 horizontal grids and 30 vertical grids and the resolution of image are fixed i.e. 180x180 pixels.

Now, generation of UGC takes place in order to approach the next level of authentication in the GUA technique. The concept of UGC is that each single click that is registered on the image in 2nd phase is giving two coordinates i.e. vertical coordinate and horizontal coordinate. Both the coordinates in the system are termed as User Vertical Coordinate (UVC) and User Horizontal Coordinate (UHC) respectively.

Some values are fixed in our system which is stated below:

Here the size of the image is fixed i.e. 180x180 pixels:

Length of Image =180 (LOI)

Breadth of Image =180 (BOI)

And

All vertical grids =30 (AVG)

All horizontal grids =30 (AHG)

These fixed values along with UVC and UHC of each click is converted in the corresponding row and column through this algorithm. The visual representation of variables in the algorithm is shown in Figure 2.

Each combination of Row and column is further changed into the unique grid code (UGC) through this algorithm.

$$Row = (int)\frac{User\ vertical\ cordinate}{Breadth\ of\ image} \text{X}\ All\ Vertical\ grids$$

$$Column = (int)\frac{User\ horizontal\ cordinate}{Length\ of\ image} \text{X}\ All\ horizontal\ grids$$

Unique Grid Code
= (Maximum column x All rows) + All columns

For example:

$$Row = (int)\frac{90}{180} \text{X}\ 30$$

$$=15$$

$$Column = (int)\frac{75}{180} \text{X}\ 30$$

$$= 12$$

Unique Grid Code = (30 X 15)+12

= 462

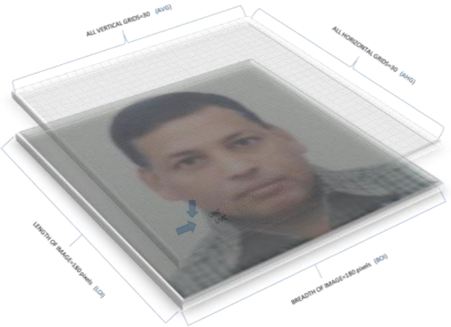
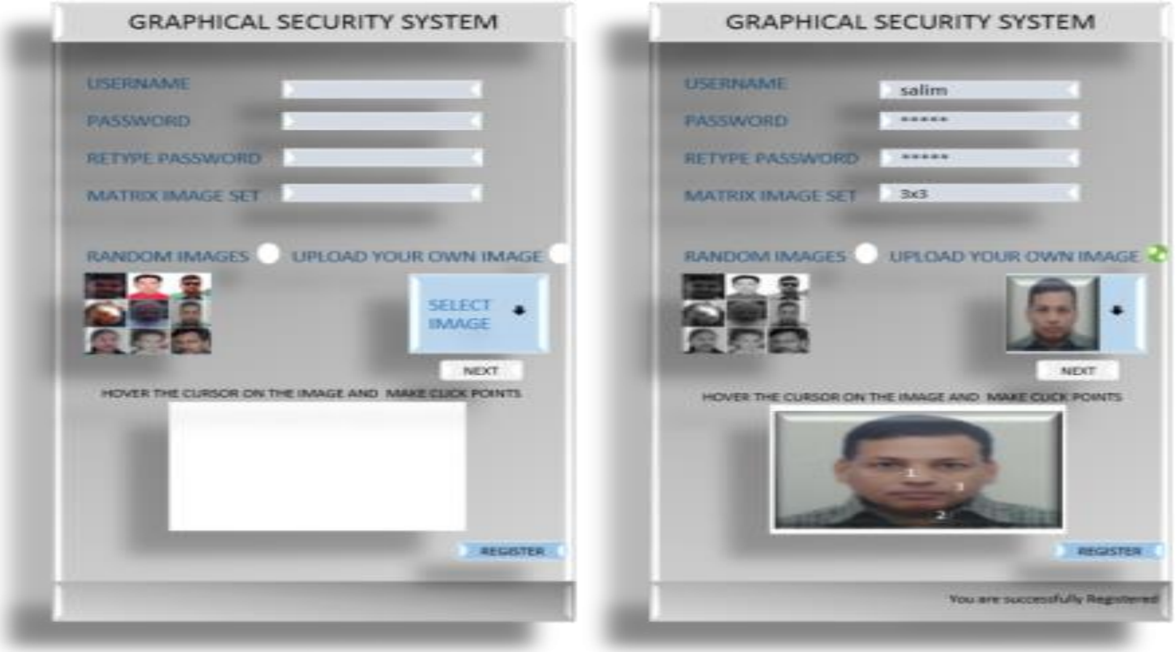

ALL VERTICAL GRIDS=30 (AVG)
ALL HORIZONTAL GRIDS=30 (AHG)
UHC
UVC
LENGTH OF IMAGE=180 pixels (LOI)
BREADTH OF IMAGE=180 pixels (BOI)

Fig. 2(a): Representation of fixed quantity over the image in the system


GRAPHICAL SECURITY SYSTEM

USERNAME
PASSWORD
RETYPE PASSWORD
MATRIX IMAGE SET

RANDOM IMAGES ○ UPLOAD YOUR OWN IMAGE ○

SELECT IMAGE

NEXT

HOVER THE CURSOR ON THE IMAGE AND MAKE CLICK POINTS

REGISTER

GRAPHICAL SECURITY SYSTEM

USERNAME salim
PASSWORD *****
RETYPE PASSWORD *****
MATRIX IMAGE SET 3x3

RANDOM IMAGES ○ UPLOAD YOUR OWN IMAGE ●

NEXT

HOVER THE CURSOR ON THE IMAGE AND MAKE CLICK POINTS

REGISTER

You are successfully Registered

Fig. 2(b): Interface of Registration Phase

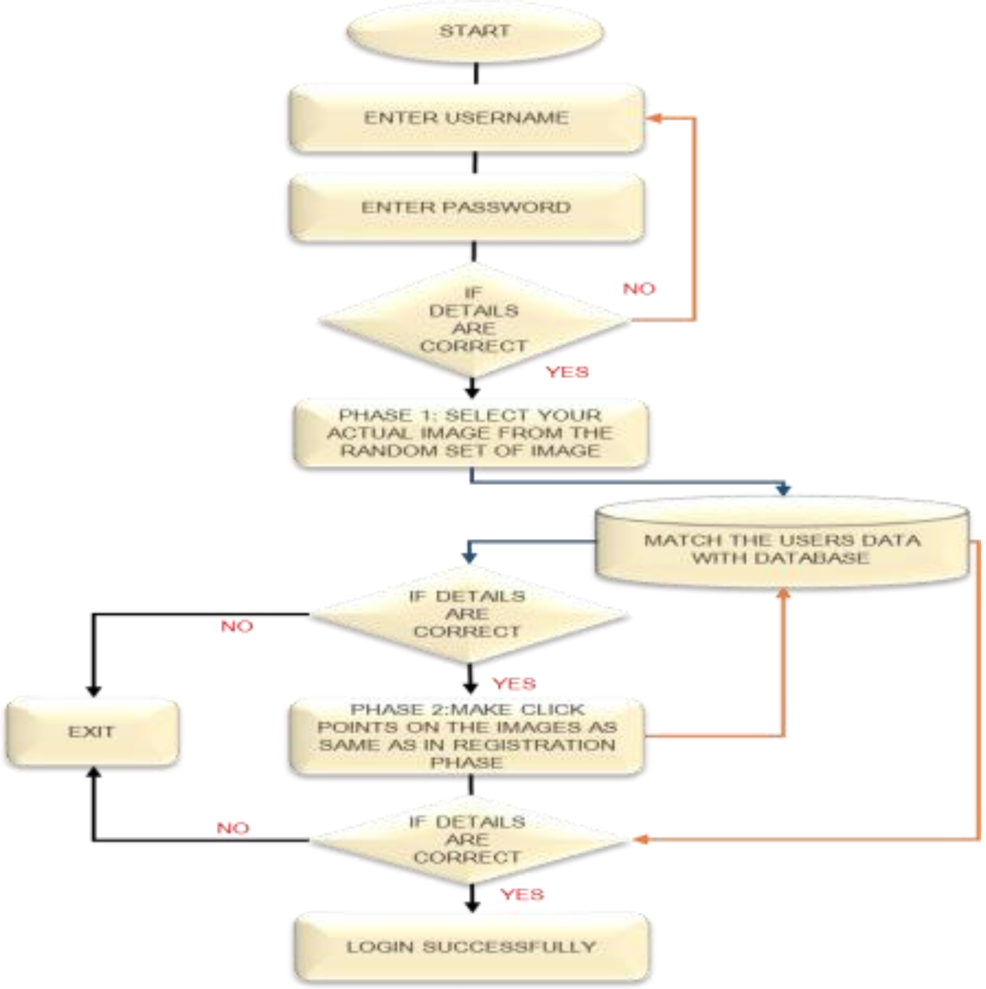

START
ENTER USERNAME
ENTER PASSWORD
IF DETAILS ARE CORRECT
NO
YES
PHASE 1: SELECT YOUR ACTUAL IMAGE FROM THE RANDOM SET OF IMAGE
MATCH THE USERS DATA WITH DATABASE
IF DETAILS ARE CORRECT
NO
YES
EXIT
PHASE 2:MAKE CLICK POINTS ON THE IMAGES AS SAME AS IN REGISTRATION PHASE
IF DETAILS ARE CORRECT
NO
YES
LOGIN SUCCESSFULLY

Fig. 3(a): Flowchart of Login Phase

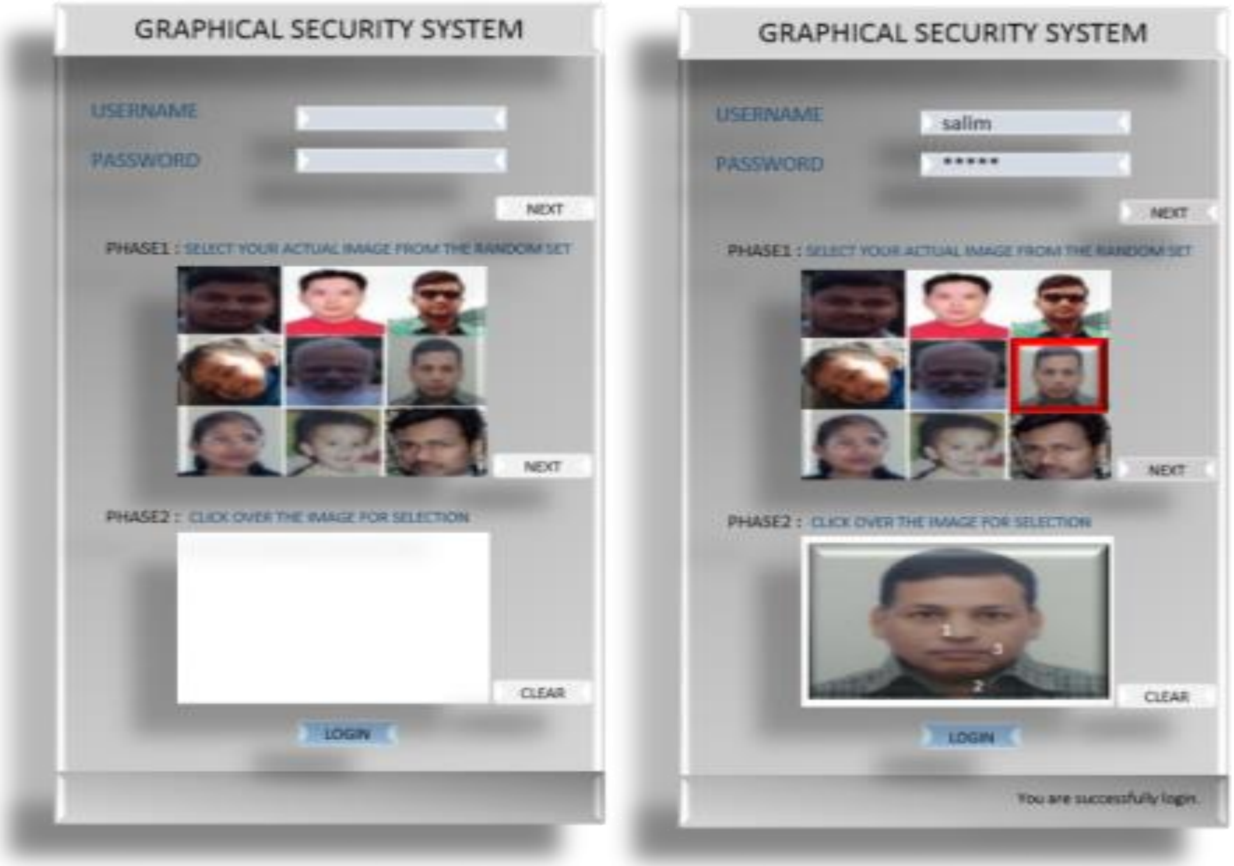
Now, the generated UGC is stored in the database, and the system will continue the same process for further next click to register, as many as, user wants. It is easy for the system to match between a single set of values, which is the reason to produce UGC.

At the time of login, both the generated UGC, one at registration time and another at login time are compared. Tolerance level is also considered as an important factor and concluded in terms of 'int' in the system. The proposed system gives freedom to the user to increase the security level at any GUA phase whether they enhance the security in phase 1 by increasing number of images or increasing number of clicks in phase 2 under some limitation in the system.

Fig. 2(b) shows the basic interface of registration phase and small demonstration of registering the user. Here, a user registers their username as "salim" with password "12345" along with matrix image set i.e. 3x3. Now, the system gives a choice whether to choose a unique image from a set of random images or upload their own image. This image will be displayed among many images at the time of login, from which he/she has to choose the right image. After this, the image is available for registering clicks and a Unique Grid Code is generated, corresponding to each click he marks on image. Fig. 1 shows flowchart of Registration Phase.

Login Phase

The interface of login phase of the system consists of Username and Password columns. The user is asked to give correct details in those columns. After matching the user's information from database, the system proceeds. Next column is displayed with random image set from which user is required to select the


GRAPHICAL SECURITY SYSTEM
USERNAME
PASSWORD
NEXT
PHASE1 : SELECT YOUR ACTUAL IMAGE FROM THE RANDOM SET
NEXT
PHASE2 : CLICK OVER THE IMAGE FOR SELECTION
CLEAR
LOGIN
GRAPHICAL SECURITY SYSTEM
NEXT
PHASE1 : SELECT YOUR ACTUAL IMAGE FROM THE RANDOM SET
NEXT
PHASE2 : CLICK OVER THE IMAGE FOR SELECTION
1
3
2
CLEAR
LOGIN

USERNAME salim

PASSWORD *****

You are successfully login.

Fig. 3(b): Interface of Login Phase

correct face image. The sequence of images are in a random order. This is to minimize the chances of attack from shoulder surfers. If the user is correct in choosing the right image, the system proceeds with the image further for noting clicks on it. On the basis of their clicks on the image, the login UGC is formed with each click information. Then both Registration UGC and Login UGC are processed for match at the same time. If the match is successful, the user will be forwarded to choose the next image (if any) or successfully login (if he hadn’t chosen more than one image).

Here in Fig.3(b) the login form is displayed. For demonstration purpose, information is filled in Fig. 3(b). In this authentication process, the user select a single image from the random set and registers three clicks on the image. After successful authentication the system prompts "login successful" at the bottom left corner of the interface. Figure 4 shows flowchart of Registration Phase.

The generated Unique Grid Code can also be converted into Row and Columns further from the algorithm below:

$$Row = \frac{\mathrm{UGC}}{\mathrm{AHG}}$$

$$Column = \mathrm{UGC\%AVG}$$

$$Row = \frac{462}{30}$$

$$=15$$

$$Column = (462\%30)$$
$$=12$$

The algorithm is implemented using Java programming language. For illustration purpose some values are taken in particular number rather than a particular image. Here, the username and password are taken as the combination of numbers.

The users are shown as a random set of 3x3 matrixes of images. Its required to select one image (in this program the user only selects 1 image and register 1 click point).

Based on the selection performed in 1st phase of GUA, the user has to register their clicks on that image.

At the time of login, user has to give their basic information same as in the registration phase. If the given information is correct then the user further proceeds to the next phase of the GUA module. At the end, if all the information including login UGC is matched successfully then the program will authenticate the user. During the Registration time and Login time, Unique Grid Code is hidden from the user and the matching is done at the back end.

IV. RESULT AND ANALYSIS

In our proposed system, we displayed the working of a hybrid GUA based authentication system. It is easy to operate, and considers all parameters of security. We deeply analyze our system on many conditions regarding password combinations, chances of attacks, ease of access for the user and check if the system is resistant to attacks under any circumstances. Our system is a hybrid approach GUA system. The biggest advantage is that all the security modules are dependent on each other for processing further decision in making successful authentication. Even if a hacker is successful in cracking one of the security modules, still it is impossible to crack the whole system. There are no warning messages corresponding to the illegal access or wrong selection, the system will directly exit the user. This step shows how the system tackles the situation and shows its resistance against dictionary attack, brute force attack etc.

In the 2nd phase of registering clicks, by a single click of mouse, no reflex response will show in the background. If the user is found wrong in attempting to login more than three times, then their account will be disabled for 24 hours. The system also maintains records of users.

Experimental Analysis of Our GUA Based System Compared to Other Systems

Here in this paper, we will conduct two surveys one for calculating the average of all registration times and login times of various users along with rate of failure between our proposed system and a text-based system for analyzing the ratings.

In the first survey, 20 participants who were studying in Diploma in Engineering, Aligarh Muslim University, are asked to choose between our proposed system and alphanumeric system. They have to perform registration and login on their own. After concluding the report, we calculate the average registration time and average login time of each user based on their security model and plots the graph between their sets of values. The results display that the average registration phase and login phase timings of all users with text password was 12.67 sec and 16.08 sec respectively. The average of registration and login times of users of our GUA based implementation was 8.1 sec and 6.79 sec respectively. On comparison, we understand that the time required in registering and login with GUA based password is much lesser than required for text-based password. The users can hence do faster registration and authentication with graphical password-based implementation as compared with textual password implementation. Failure rate was found on the basis of number of attempts required for every successful authentication. Failure rate for our GUI based implementation was 1.6 while failure rate for textual password implementation was 2.46. It therefore infers, any user needs less attempts for having a successful login in our graphical password system in comparison with a text based one.

$$\textit{Average Registration time} = \frac{\text{Sum of time for all users to register}}{\text{Total registered users}}$$

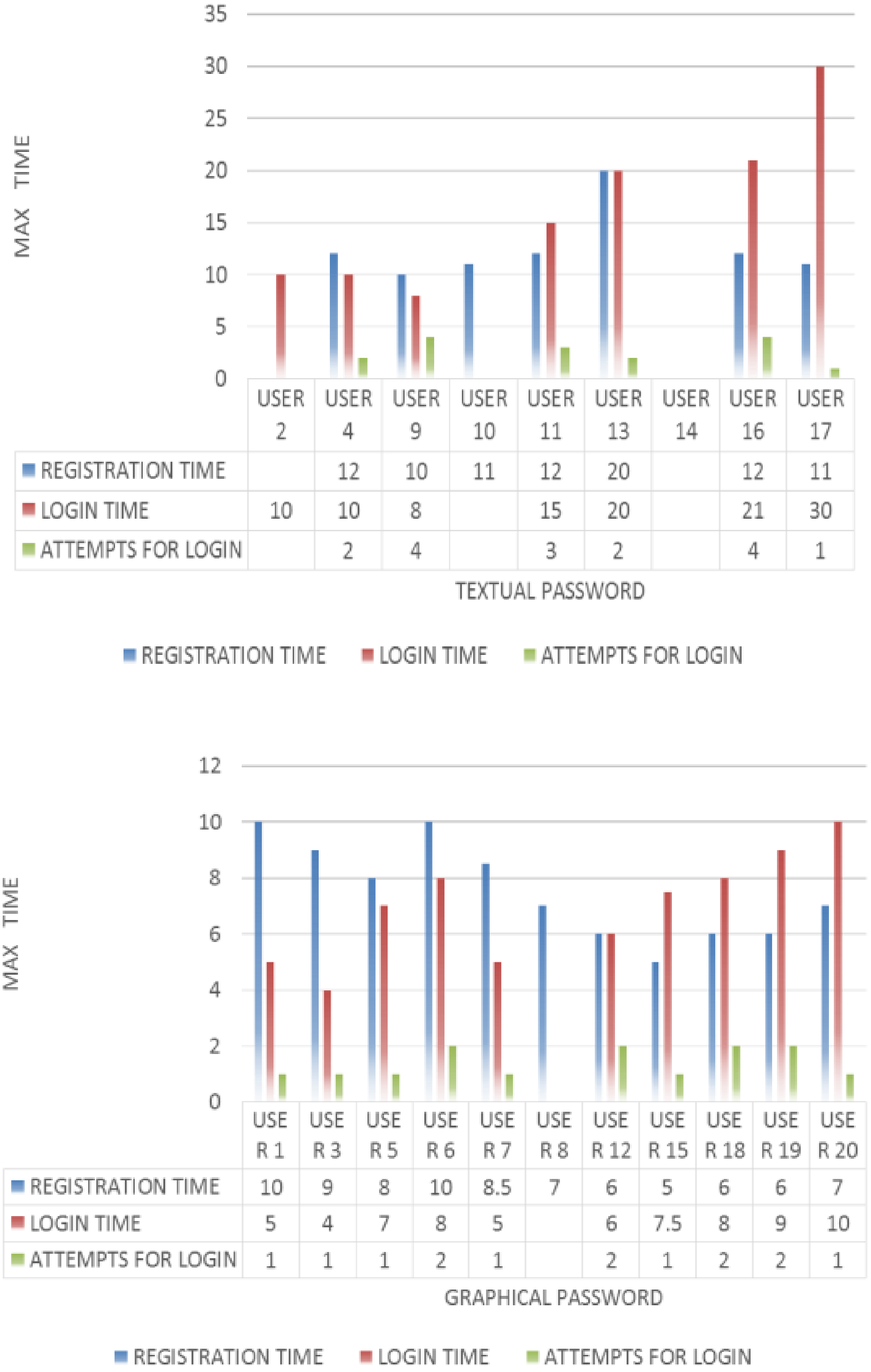
$$\textit{Average Login time} = \frac{\text{Total time required by all logged in users}}{\text{Total number of logged in users}}$$

$$\textit{Rate of Failure} = \frac{\text{Total attempts}}{\text{Number of successful login}}$$

Theoretical Analysis of our GUA based System compared to others explored and Mentioned in Section II

Passfaces: A user has a higher tendency to select an image similar to his/her own image. If such a facial image is chosen, then possibility of attacks increases manifold. This is the primary disadvantage of that system.

Our system doesn't store anything related to user’s personal information, hence chances of knowing user’s information and using it for attacks is reduced greatly.



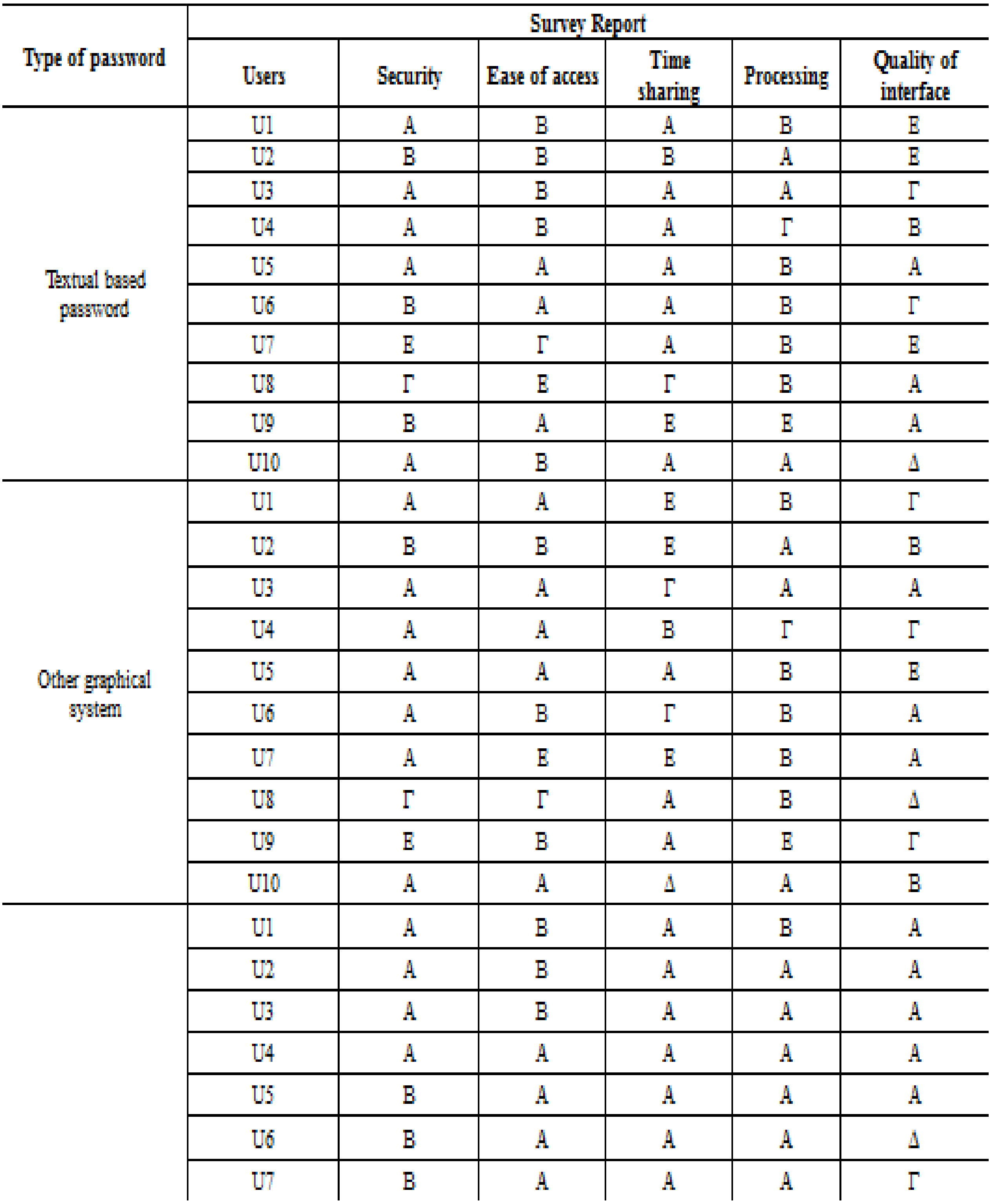
	USER 2	USER 4	USER 9	USER 10	USER 11	USER 13	USER 14	USER 16	USER 17
🟦 REGISTRATION TIME		12	10	11	12	20		12	11
🟥 LOGIN TIME	10	10	8		15	20		21	30
🟩 ATTEMPTS FOR LOGIN		2	4		3	2		4	1

	USE R 1	USE R 3	USE R 5	USE R 6	USE R 7	USE R 8	USE R 12	USE R 15	USE R 18	USE R 19	USE R 20
🟦 REGISTRATION TIME	10	9	8	10	8.5	7	6	5	6	6	7
🟥 LOGIN TIME	5	4	7	8	5		6	7.5	8	9	10
🟩 ATTEMPTS FOR LOGIN	1	1	1	2	1		2	1	2	2	1

Fig. 4: Experimental Chart

TABLE 1: SURVEY REPORT

`



Type of password	Survey Report					
	Users	Security	Ease of access	Time sharing	Processing	Quality of interface
Textual based password	U1	A	B	A	B	E
	U2	B	B	B	A	E
	U3	A	B	A	A	Γ
	U4	A	B	A	Γ	B
	U5	A	A	A	B	A
	U6	B	A	A	B	Γ
	U7	E	Γ	A	B	E
	U8	Γ	E	Γ	B	A
	U9	B	A	E	E	A
	U10	A	B	A	A	Δ
Other graphical system	U1	A	A	E	B	Γ
	U2	B	B	E	A	B
	U3	A	A	Γ	A	A
	U4	A	A	B	Γ	Γ
	U5	A	A	A	B	E
	U6	A	B	Γ	B	A
	U7	A	E	E	B	A
	U8	Γ	Γ	A	B	Δ
	U9	E	B	A	E	Γ
	U10	A	A	Δ	A	B
	U1	A	B	A	B	A
	U2	A	B	A	A	A
	U3	A	B	A	A	A
	U4	A	A	A	A	A
	U5	B	A	A	A	A
	U6	B	A	A	A	Δ
	U7	B	A	A	A	Γ

Syukri: The most essential thing in her approach is the use of touch sensitive device. Such devices are not yet commonplace. Obtaining and getting familiar to the usage of such devises can be a challenge for most users. Without this, user would not be able to match their signature within the login time range required. Our system is not dependent on using any special devices hence there is no such challenge.

Blonder: For this, a predefined location is set where the user is required to select the approximate region. For this type of approximation, it is essential to define a tolerance level of error. If the tolerance level is too high, there is a higher chance of successful authentication by a hacker. If it is set too low, it would not be user friendly and would take more time for a user to authenticate oneself. In our system, the user has to select from a matrix. Hence there is no such problem of false successful authentication or lack of user friendliness for higher security.

Comparison on the Basis of Ratings

We conduct a second survey with 10 participants from computer science background, who were studying in diploma in computer engineering in Aligarh Muslim University, Aligarh, India. The users are required to work on the system and mark some rating like alpha for best and delta for fair, on different types of graphical system, text based system and our proposed system as shown in Table 1. The result achieved is amazing that most of the participants liked our system and the ratings were very high.

Password Combinations & Limitations

We limit the selection of users chosen image from the random set in phase 1 of GUA with not more than 10x10 matrix image set (100 images). Users can select up to 5 images maximum in their overall security account and on each image they have to register their click on them, which is not more than 10 clicks on single image. Therefore, possible passwords formed from the outcomes are:

$$ {}^{100}C_5 \times 10^5 = 7{,}528{,}752{,}000{,}000 $$

Though the scheme is secure enough from different types of attacks, still some improvements could be made to enhance it:

The robustness of this scheme can be improved by making it hybrid & combining with other authentication approaches like biometric etc.

V. CONCLUSION

We are supporting the view of creating digital India campaign [27], it is only possible if our security system is robust to avoid any attacks. In order to make them successful, we have to introduce new authentication technique day by day to come parallel with latest technology. Our proposed system is designed by taking care of such possibilities in mind and makes authentication better with the advancement of security. We are inspired from the study [2] which focuses on the transformation of people through education. For future endeavors, we will make hybrid security modules from concatenating two or more authentication techniques such as combining GUA with Biometric system, Token based system etc. Our aim is to provide the best protection to the upcoming technologies to survive in the virtual world against illegal acts and make authentication safe and reliable for the users.

VI. REFERENCES

[1] F. Syukri, E. Okamoto, and M. Mambo, A user identification system using signature written with mouse, in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1438(1998) 403–414, doi: 10.1007/bfb0053751.

[2] C. P. Katsini, C. Fidas, M. Belk, G. Samaras and N. Avouris, A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication, International Journal of Human–Computer Interaction, 2019, doi:10.1080/10447318.2019.1574057.

[3] D. Weinshall and S. Kirkpatrick, Passwords you'll never forget, but can't recall, 2004, doi: 10.1145/985921.986074.

[4] E. K. Wang, C. M. Chen, D. Zhao, W. H. Ip and K. L. Yung, A dynamic trust model in internet of things, Soft Computing, 24(8)(2020) 5773-5782.

[5] F. Towhidi and M. Masrom, A Survey on Recognition Based Graphical User Authentication Algorithms, Dec. 2009, [Online] Available: http://arxiv.org/abs/0912.0942.

[6] Fujitsu integrates PalmSecure with Passlogix v-GO SSO, Biometric Technol. Today, 2010(9)(2010)2, doi: 10.1016/s0969-4765(10)70176-4.

[7] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, A new graphical password scheme resistant to shoulder-surfing, in Proceedings - 2010 International Conference on Cyberworlds, CW 2010, 2010, 194–199, doi: 10.1109/CW.2010.34.

[8] H. Xiong, Y. Wu, C. Jin, and S. Kumari, Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIOT, IEEE Internet of Things Journal, 2020.

[9] H. Zhao and X. Li, S3PAS:A Scalable shoulder-surfing resistant textual-graphical password authentication scheme, 2007, doi: 10.1109/AINAW.2007.317.

[10] H. Zhu, X. Wang, C. M. Chen, and S. Kumari, Two novel semi-quantum-reflection protocols applied in connected vehicle systems

with blockchain, Computers & Electrical Engineering, 86(2020) 106714.

[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, The design and analysis of graphical passwords, 1999.

[12] J. C. Sobardo, L.Birget, "Graphical Passwords, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, 4(2002).

[13] J. Goldberg, J. Hagman, and V. Sazawal, Doodling our way to better authentication, in Conference on Human Factors in Computing Systems - Proceedings, (2002)868–869, doi: 10.1145/506621.506639.

[14] J. H. Hsiao, R.Tso, C. M. Chen, and M. E. Wu, Decentralized e-voting systems based on the blockchain technology, in Advances in Computer Science and Ubiquitous Computing, pp. 305-309, Springer, Berlin, Germany, 2017.

[15] L. Xie, Y. Ding, H. Yang and X. Wang, Blockchain based secure and trustworthy internet of things in SDN-enabled 5g-VANETs, IEEE Access, 7(2019) 56 656-56 666.

[16] M. S. Umar and M. Q. Rafiq, A graphical interface for user authentication on mobile phones, 2011.

[17] M. S. Umar and M. Q. Rafiq, Select-to-Spawn: A novel recognition-based graphical user authentication scheme, 2012, doi: 10.1109/ISPCC.2012.6224382.

[18] M. S. Umar and Salim Istyaq, Encoding Passwords using QR Image for Authentication, IEEE Xplore Digit. Libr., 2016.

[19] M. Sulzmann and K. Z. M. Lu, "A type-safe embedding of XDuce into ML," 2019, doi: 10.1016/j.entcs.2005.11.047.

[20] P. Golle and D. Wagner, Cryptanalysis of a cognitive authentication scheme, in Proceedings - IEEE Symposium on Security and Privacy, (2017) 66–70, doi: 10.1109/SP.2017.13.

[21] R. Dhamija and A. Perrig, Déjà Vu: A user study using images for authentication, 2000.

[22] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, 5G for vehicular communications, IEEE Communications Magazine, 56(1)(2018) 111-117.

[23] S. Istyaq, SALIM-WASET, World Acad. Sci. Eng. Technol., 10(2016), [Online] Available: https://www.researchgate.net/publication/309179512_Hybrid_Authentication_System_Using_QR_Code_with_OTP.

[24] Symnatec, 2014 INternet Security Threat report, Symantec Corp. Internet Secur. Threat Rep., 2013.

[25] S. Man, D. Hong, and M. Matthews, A shoulder-surfing resistant graphical password scheme - WIW, in Proceedings of the International Conference on Security and Management, 1(2003) 105–111.

[26] S. Xiaoyuan, Z. Ying, and G. S. Owen, Graphical passwords: A survey, in Proceedings - Annual Computer Security Applications Conference, ACSAC, 2005, (2005) 463–472, doi: 10.1109/CSAC.2005.27.

[27] V. Mahindrakar, DIGITAL INDIA: 'A Program to Transform India into a Digitally Empowered Society and Knowledge Economy, Int. J. Adv. Eng. Res. Technol., 5(9)(2017) 705–708,[Online]. Available: www.ijaert.org.

[28] W. A. Jansen, Authenticating Users on Handheld Devices, Proc. Can. Inf. Technol. Secur. Symp., 2003.

[29] W. Jansen, Authenticating Mobile Device User through Image Selection, 2004.

[30] Z. Zheng, X. Liu, L. Yin, and Z. Liu, A hybrid password authentication scheme based on shape and text, J. Comput., 5(5)(2010) 765–772, doi: 10.4304/jcp.5.5.765-772.