iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52681

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Graphical Password Authentication: Image Grid Based Digital Lock for Mobile Apps

D Loganathan[1], Umme Kulsum[2], Shakthi S [3], Sania M[4], Arbaz Ahamed[5]
Computer Science Department, Visveswaraya Technological University

Abstract: ***Over the past few decades, research on authentication methods has advanced significantly. While the initial focus was on using standardised password selection and management approaches to secure textual passwords, this was made possible by learning about the flaws in the existing systems based on the attacks performed on the same systems' vulnerabilities. With the rise of biometric-based authentication, the next stage in the study and development of improved solutions has begun. Although initially rather entertaining, this authentication method is very insecure. Once a person's biometrics have been stolen or replicated, new biometrics cannot be made. Compared to a person's one-step biometric authentication, biometrics in the multifactor authentication of an enterprise are less vulnerable. The development of graphical passwords is the result of all these issues with authentication systems. While multifactor graphical passwords impede smartphone users' usability and speedier processing-computational flexibility, overly simplistic graphical passwords are prone to shoulder surfing. Users of Android devices need an authentication system that is easy to use, quick, secure, and that gains faster access to the device. A study was done evaluating the usability, predictability, resistance to various attacks, and other characteristics of various graphical passwords. Grid-based graphical passwords outperformed their rivals among the different types of graphical passwords that were taken into consideration. The majority of graphical password implementations in the past have been on personal computers (PCs), while smartphone usage is far more prevalent than on PCs. We propose to develop an Android application with grid-based image-based graphical password authentication that will be secure and help a lot of users protect the secondary identities that they carry about in the form of smartphones. After evaluating which factors must remain in the system, the application was divided into five modules. Each module was first built using flowcharts, and later, the Java programming language was used to build the app in Android Studio.***

Keywords: Graphical password authentication, Android application, Authentication, Grid based graphical passwords, Usability.

I. INTRODUCTION

A computer security system's weakest link is frequently regarded as human factors. Authentication, security operations, and creating safe systems are the three main areas where human computer interaction is crucial, according to Patrick et al. Here we focus on the authentication problem Password is the string of the characters used to verify the identity of a user during the authentication process. Password provide the first line of defense against unauthorized access to personal information in computer and Smartphones

In today's digital age, the authenticity of security has become a major concern. With rise in the need for applications that can authenticate images and ensure their veracity. An image authentication application is a tool designed to verify the authenticity and integrity of an image. These applications use various methods, such as digital signatures, watermarking, to ensure that the image has not been tampered with in any way. They also provide users with the ability to detect any changes made to the image since it was created, ensuring that any alterations made to the image are immediately apparent.

Graphical password authentication is a type of authentication system that uses images or graphical elements as a means of verifying a user's identity. Instead of entering a traditional alphanumeric password, users are asked to select a set of images, draw a pattern, or use other graphical elements to prove their identity.

The graphical password authentication system typically consists of a series of images or graphical elements that are presented to the user. The user is then asked to select one or more of these elements, or to draw a pattern using them. The system records these choices or patterns and stores them as the user's password.

When the user wants to log in, the system presents a series of images or graphical elements again. The user then selects the previously chosen elements or draws the pattern they previously created. If the selected elements or pattern match the ones previously recorded, the user is granted access.

The advantage of graphical passwords is that they can be easier to remember than traditional alphanumeric passwords. They can also be more secure in some cases, as they are harder to guess or brute force. However, they can also be vulnerable to some types of attacks, such as shoulder surfing or smudge attacks, where an attacker can observe the user's pattern or selected elements.

The strong password is what protects us from the cyber criminals . Relying on a weak password combination of the letters and numbers you select to secure your device, by contrast makes it easy for the cyber criminals to gain access to your account , steal your identity and even take your money. As a result, system resources are not used up on securing every component of the environment which is particularly crucial given the inherent limitations of mobile devices.

II. LITERATURE REVIEW

In recent years, graphical password authentication has received increasing attention from both academia and industry, and numerous studies and designs have been proposed in this area. In this section, we will provide a comprehensive literature survey of graphical password authentication, according to the, current state of research, and potential future directions.

Nida et al, the graphical password authentication system was created using picture division algorithm in this system the user selects a desired picture and the image undergo divisions according to the grids given by the users , then the user's needs to select the grids and during login stage the girds in the image will be shuffled. According to the study conducted among different user it was stated that this system is complex as the images or the grids gets shuffled [1].

Alexander et al, the graphical password scheme involves two steps. In the first step, an image is generated using a computer algorithm. The algorithm maps a set of alphabet symbols onto the image in a random sequence and assigns a common colour to each symbol. The symbols are rotated, zoomed and overlapped randomly. The resulting image looks like a Captcha image with symbols arranged in a sine wave format [3]. In the second step, a grid with green background and white circles is displayed on the screen. The user draws a pattern by connecting the circles into one set. The circles are labelled with numbers in a specific order. The pattern can be drawn in eight different directions. The image and the grid are combined to form the password scheme. The user has to follow the image pattern and then draw the corresponding pattern on the grid. The scheme is more secure than traditional passwords as it is difficult for hackers to guess or crack the image and the pattern.

This may have usability issues which results in difficulty to the user to draw and connect patterns [2]. Gi-Chul Yang et al, In Pass Positions, the user selects a sequence of points on the screen, and the system records the positions of these points relative to each other. However, the position of the first point is not recorded. This helps create a password that is based on the relative positions of the chosen points.

The disadvantage of Pass Positions is that it may be more difficult for some users to remember the relative positions of the chosen points, especially if they are not familiar with the system. It also requires a larger amount of memory to store the relative position information for each password [4].

S. Rajarajan et al , the user first need to enter the PIN then we would be asked to upload an image the image uploaded by him should be the photo taken by him as it will be more secure than taking the picture from online. The uploaded image will undergo grid and user needs to select the click points which will act like password this method uses bcrypt (12 rounds) hash algorithm. Hash value generated will be equivalent to the password and it will store at the server if the attacker's try to attack the server, they will only find hash value and not the actual password [5][6].

This method prevents shoulder surfing as it involves headphones which provides a secret code to the users before clicking the points on the image registered by user. which is to be moved horizontally or vertically towards the click point. The user will be authenticated only if he has his mobile phone with picture and remember the click points [7].

Harshini et al, it is a recognition-based technique where a user must first register the images as password there are three options to setup the image by image with grids, randomized images and blurred images user can setup the password from the selected category which will have 9 cells which is to be selected and saved. The major drawback is that it has smaller grid which limits the resolution of the image [11].

Yuhua Yin et al, With the help of pass image we can generate a strong password. It consists of 3 components namely password generation, password Management, parameter synchronization. In the first phase the user provides specific image by taking photo, uploading or scanning it. Which will later undergo hashing the next step requires the URL and master password. Hence this will generate a strong password by undergoing Argon2 secret and Base85 encoding the length of the password can be set by the users. password Management can regenerate password and manage the metadata without storing them.

Synchronization involves regeneration of password based on metadata within the QR code which is used in configuring the image. During synchronization of the QR code image it will pass the hash value of the image The major issues is of Usability and vulnerability [5].

Muhammad et al, the proposed system consists of graphical matrix of the form 7×11 matrix grid composed of three components that is Login pointer , Password verified and feature evaluation. During registration the user needs to give username to register two alphabets that are call process alphabets which will have mathematical operators such as addition and subtraction is provided as per the user's selection after this the user needs to set two numbers called process code. Hence it will generate a pair of row and column which can be used by the users to draw a pattern. This type of system results in time consuming process as it has series of steps to be followed and the dataset is trained using ml algorithms [7].

Nikita et al, the proposed system for creating user passwords involves selecting symbols in the form of numbers, shapes, and colours. During the registration phase, users are prompted to choose a specific sequence of symbols that will be used as their password. In the event that the desired image is not available in the selection, there is an option to refresh. If someone tries to view the password from an angle, they will only see that an image has been selected, but they will not be able to determine which symbols within the image are part of the password. This makes it difficult for potential intruders to gain access to the account. The selection of the symbols available to the user's will be limited[8].

In conclusion, our literature survey has highlighted the various types of graphical password authentication systems that have been proposed in recent years. Despite the growing popularity of graphical passwords, there are still some concerns regarding their security and usability. Many studies have shown that users often struggle to create memorable, secure graphical passwords, which can lead to a higher risk of password guessing attacks. Additionally, some systems have been found to be vulnerable to shoulder-surfing attacks or other forms of visual hacking. Overall, while graphical passwords offer some unique advantages over traditional text-based and other password authentication systems, there is still much work to be done to improve their security and usability.

III.PROPOSED SYSTEM

Keeping in mind the limitations of existing system. A new system was proposed that had improved usability, lesser steps during registration and better recall using images provided both by the users and the system images.

The proposed system has five modules namely registration module, login module, app selection module, change password module, forgot password module

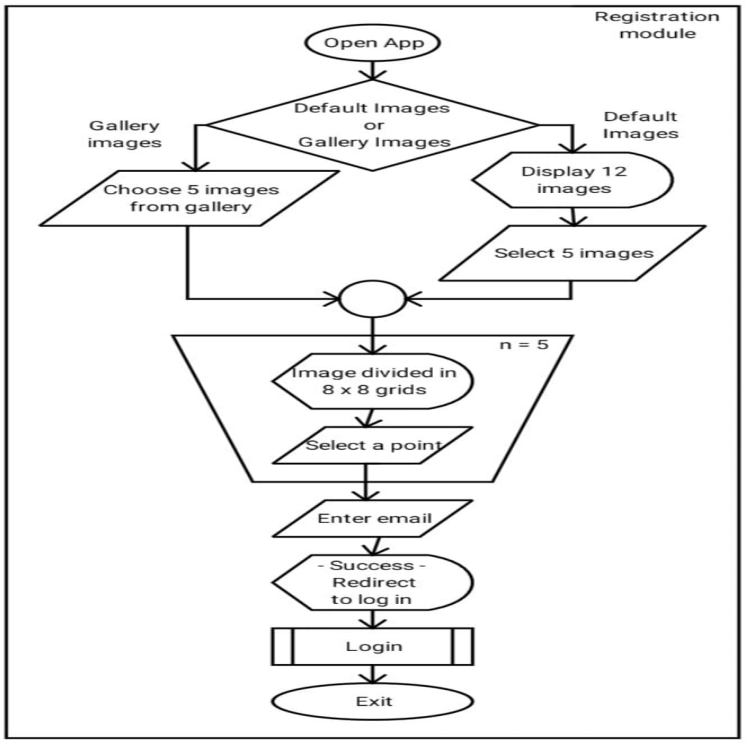


Fig. 1 Registration module

In the registration module is the very first module that was built. Once the user opens the app, they are met with the choice to select default or gallery images as it increases security but during the first few tries to be familiar with the app or in case desired images from gallery are not available one may use the default images.

While the user of the app needs to select five images when they are choosing images from the gallery. The users are provided with a choice of twelve default images. Once that is done the five selected images from default or gallery images will be segmented in 8 x 8 grids and the same will be presented to the user to choose a point. This step is repeated five times. After the user is done selecting the points the app will ask the user to provide an email address in case, they forget their password. This is completion of the registration module. The user will then be directed to the login or may exit the app. Fig. 1 represents the registration module.

The login module will display the images selected during registration. The user will select the point that was earlier selected as the password. If the selected points match the registered points, the next image will be displayed. If not, the images not present in the password will be displayed for selection of points to confuse the intruders and ensure safety.

If the login is a success, then the authentication process is complete or the user will have to re-enter the image password. In cases where the genuine users are unable to recall the password which is reported to be a rare case; forgot password feature can be used. This will be further discussed in detail in the upcoming sections. The processes involved in login module are represented in Fig. 2.

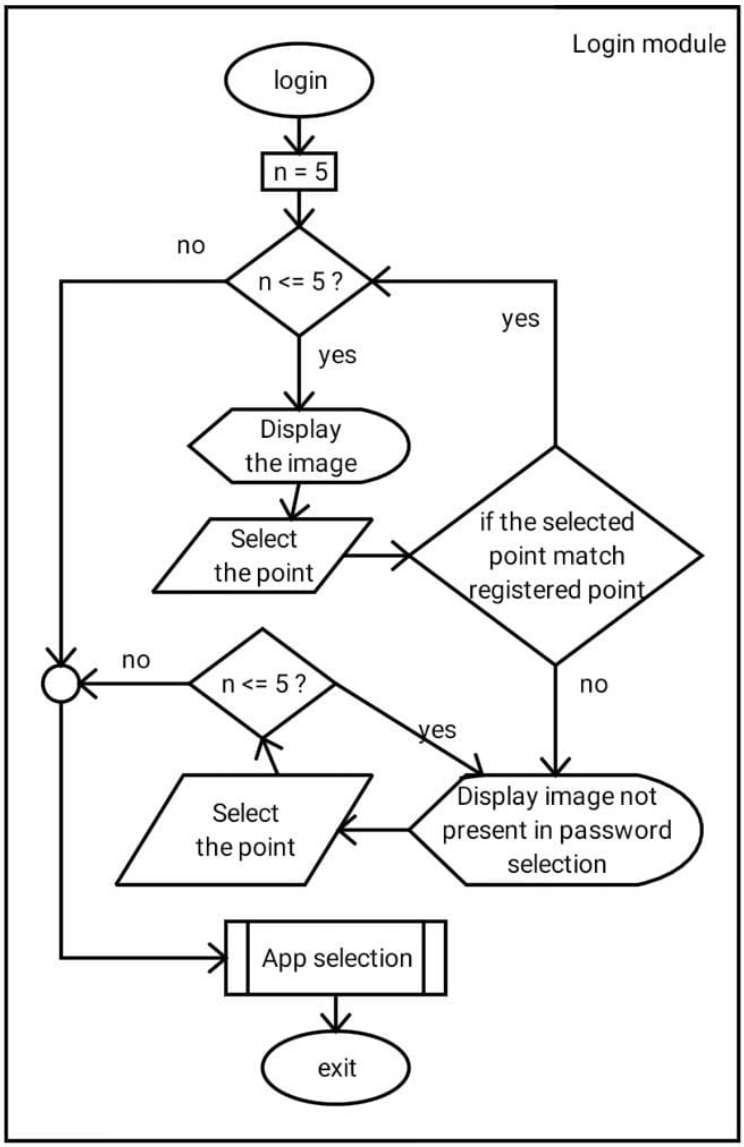


Fig. 2 Login Module

The process of selecting apps to be protected by the graphical password authentication is shown in the Fig. 3. Once you have gained access to the graphical password authentication app-lock, you can select which apps you want to protect using this authentication system. Once the user is done selecting the apps to be locked, the user will be asked if they want to stay in the app or exit the application.

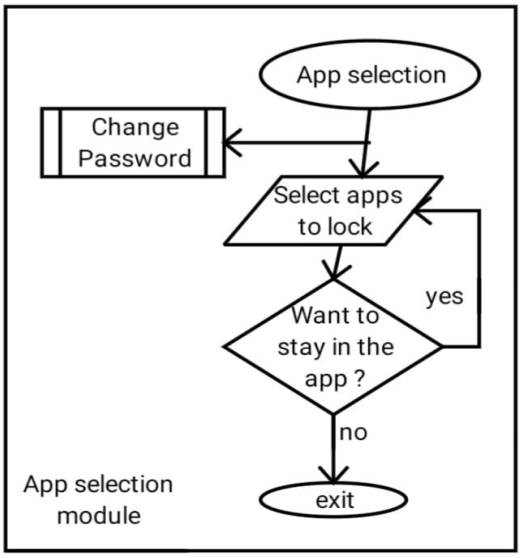


Fig. 3 App selection module

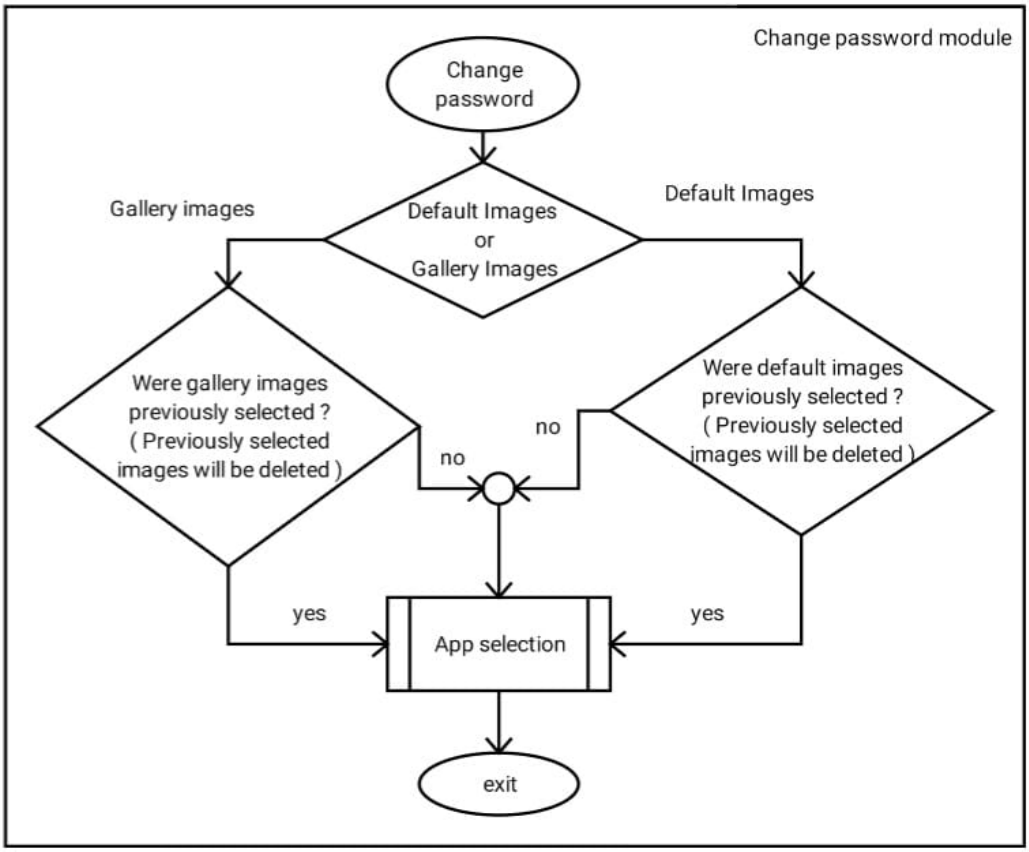


Fig. 4 Change password module

One other feature that is present inside the graphical password authentication system is the change password feature. Similar to the way in which images were selected, the change password module will ask the user if they want the new password to be from default images or gallery images. Once that is done the system will ask the user confirmation, if they choose a different category to select the password from. The completion of change password will again lead to the app selection module processes as shown in Fig. 4. As mentioned earlier the user is free to exit the app in between any process.

It is very rare that the user might forget the password that is in the form an image and even the specific point in that image. Nevertheless, for such events one can utilize the forgot password feature. A shown in Fig. 5, when the user clicks on forgot password, the system will prompt the user to switch internet connectivity. In cases when the internet connection is already available, the password is sent to the email address provided during registration.

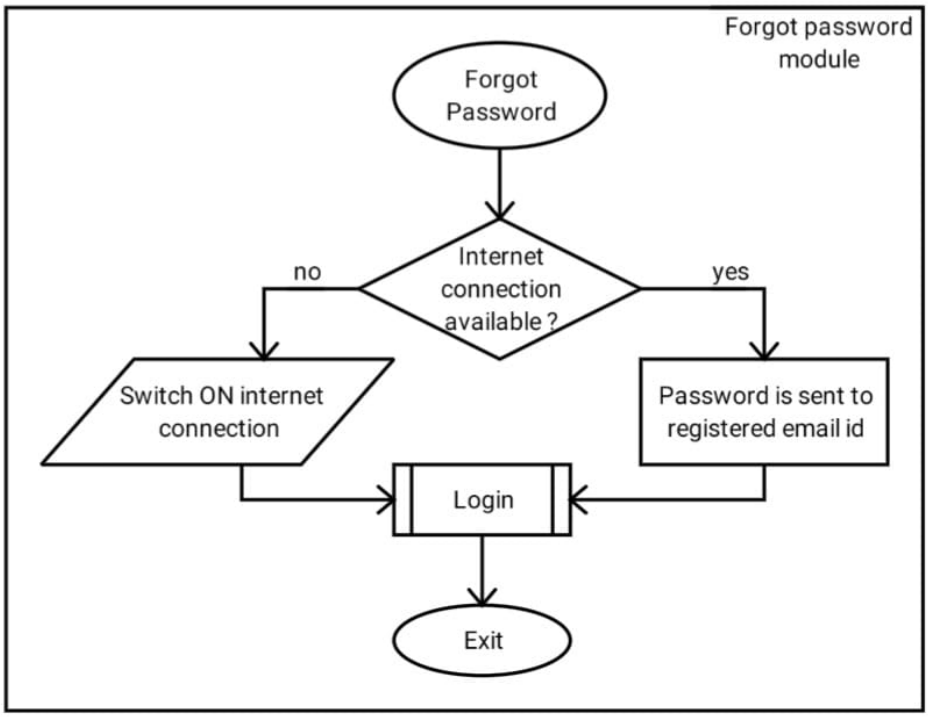


Fig. 5 Forgot password module

IV. RESULT

In our proposed system, we have used the concept of image grid Based graphical password which overcomes the limitation of the existing system . We have two phases : registration phase and login phase.

A. Registration Phase

We have two options during the registration phase: either use the default photographs provided by the programme as the password or select images from the gallery without using an internet-based image as shown in the Fig. 6.00

In the default image section user must select any five from the 12 photos from the present images to use as their password as shown in the Fig. 7.

If we choose the Gallery images as the password then we must select 5 photographs from the gallery as shown in the Fig. 8 if we choose the option for gallery images since internet-based images might be compromised. In eye-tracking research, the Cued Click Point (CCP) algorithm is a method used to pinpoint the exact second a participant fixes their gaze on a particular target on a computer screen. The subject is shown a sequence of visual stimuli as part of this algorithm, and an eye tracker is used to monitor their eye movements. The method analyses the time of the mouse click to determine the precise instant when the fixation happened. The participant is asked to click the mouse button when they have focused on the target.

The creation of an application that employs eye tracking to control the movement of a pointer on the screen serves as an illustration of how the CCP algorithm may be implemented in Android Studio. An eye tracker would be used by the app to monitor the user's eye movements while it displayed a succession of visual stimuli, such as text or images.

The algorithm would utilize the timing of the mouse click to pinpoint the precise instant the user fixed on the button when they were directed to click the mouse button after focusing on a particular target, such as a button on the screen. The cued click point method is used to divide the chosen photos into grids, which are then divided into 8X8 grids. The chosen grid is then set as the password, and the procedure is repeated for the other five chosen images.

Fig. 6 Registration page.

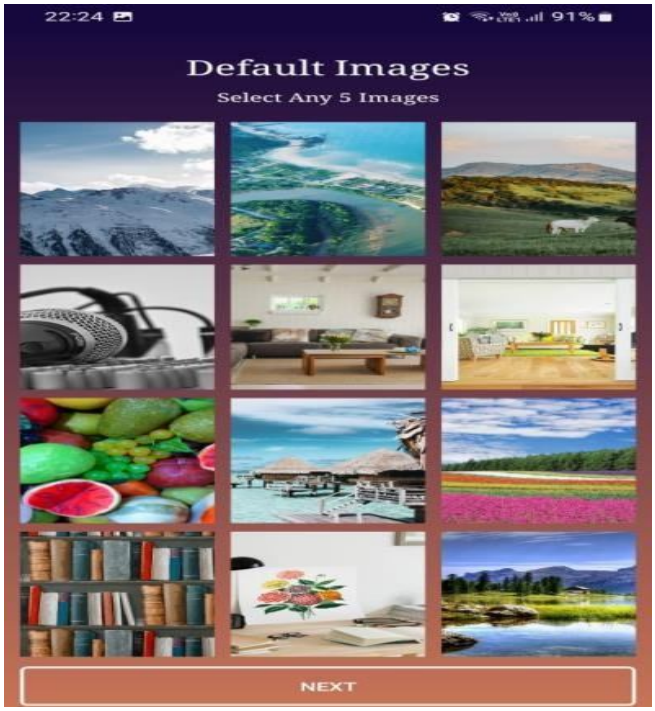


Fig. 7 Default Section Images

When you select the particular grids as the password a red dot will appear in order to ensure the grid you have choose and then click the submit .After the registration process you will be redirected to the login process .And also you have to provide the email in case if you forget the password or if you want to change the password. Application also allows us to give the permission to the data access and this app also consumes the less data and overcomes the disadvantages of the large data consumption due to the usage of the graphical advantages and it is user friendly without much confusion to operate the application.

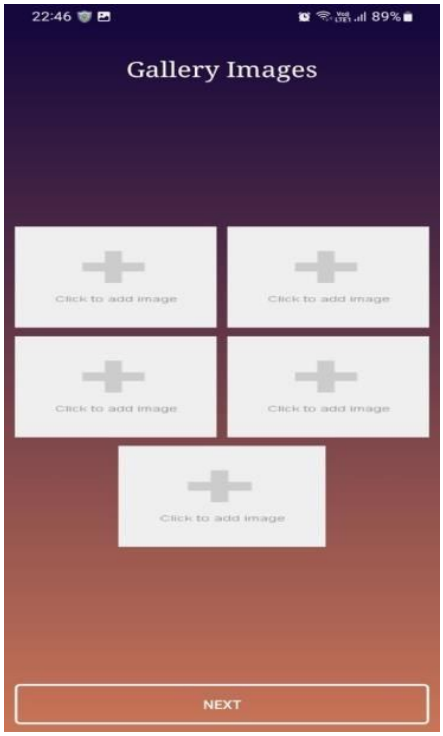


Fig. 8 Gallery Section Images

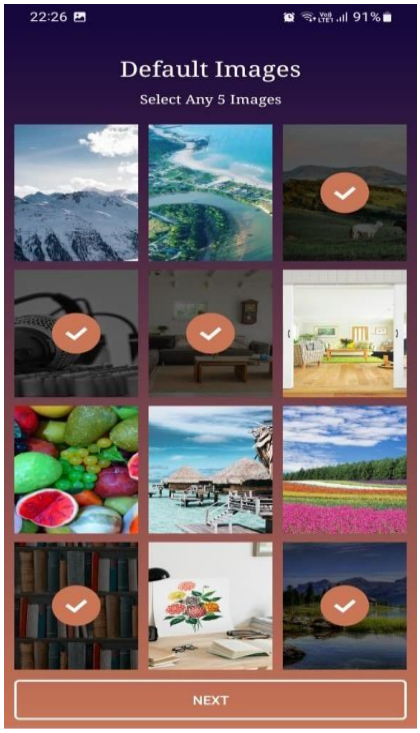


Fig. 9 Selecting the images

Fig. 10 Selected Image Divided into Grids

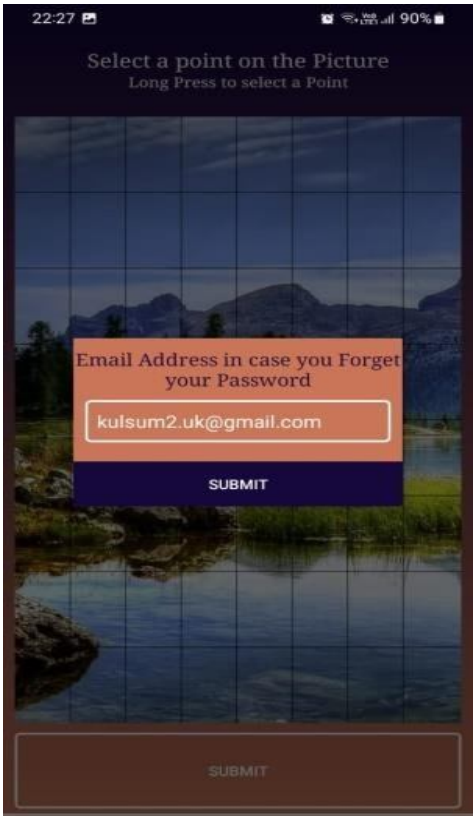


Fig. 11 Providing Email

Fig. 12 Successful Registration

B. Login Phase

The five photos we chose during registration will be presented during the login procedure without any grids. The user must choose the same grids in the image that was chosen as the password during registration for the application to launch. When image is displayed the user has to remember the point where he tapped for more than a second and after the successful login, we have the options to lock the other system applications and the installed applications so when we try to open the particular locked application there again the graphical password will be visible providing it to be easily accessible and preventing the shoulder surfing attack and dictionary attacks.

Fig. 13 Login process.

After the successful Login process, we have that choices to lock the installed or the system application which is shown in the Fig.14.

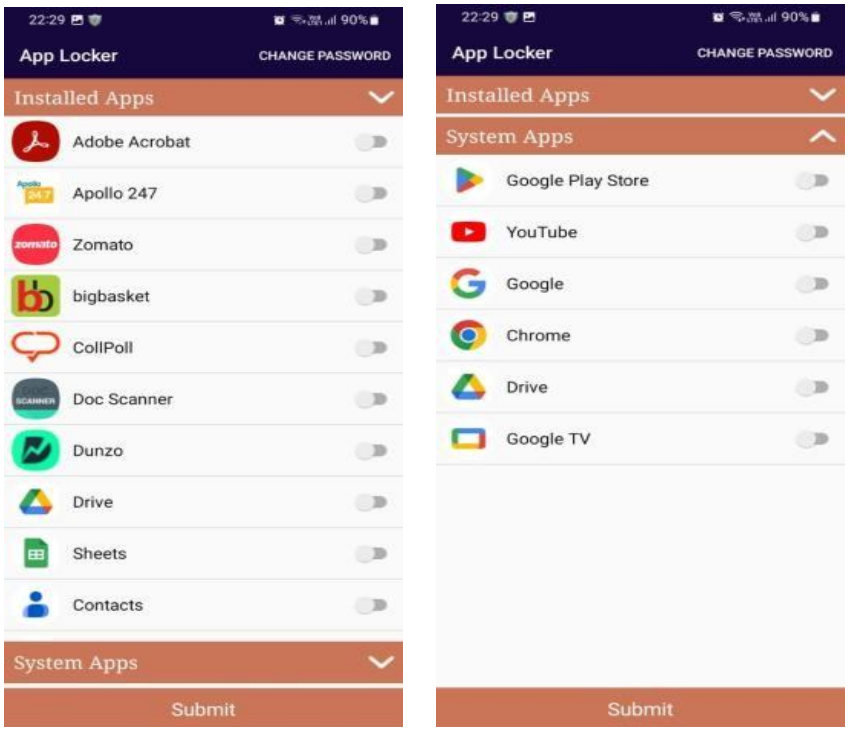


Fig. 14 Installed and System Applications.

If we want to change the password then we have to give change password option as given in the Fig. 15 in the change password options, we have options to choose either the default images or the gallery image and the process continues the same .

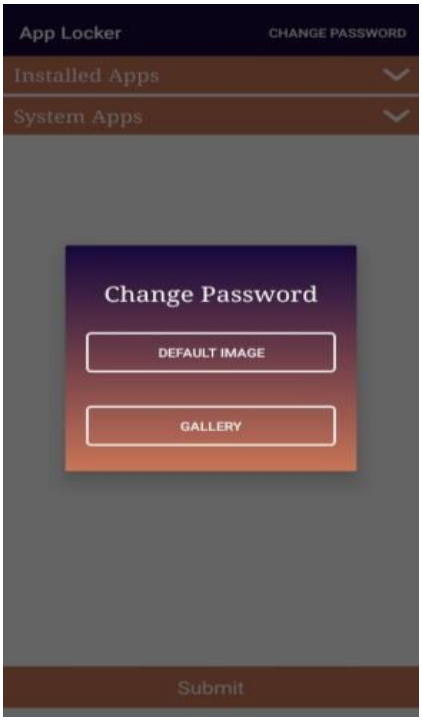


Fig. 15 Change Password

As shown in the below Fig. 16 you will be again redirected to the login process again in the changing of the password.

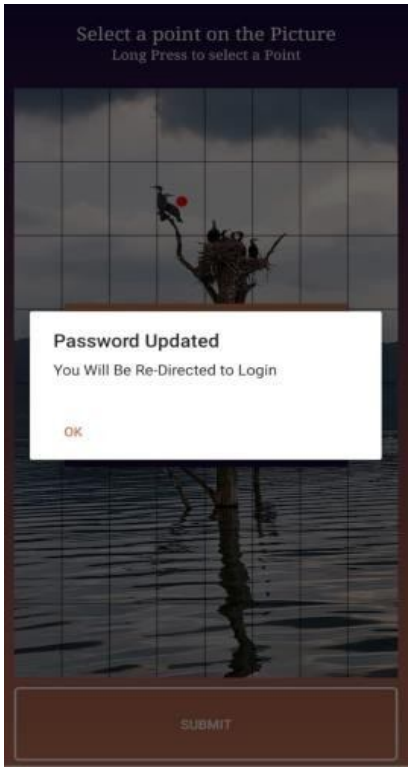


Fig. 16 Password Changed Successfully.

During the change of the password our previous password will be deleted whether it is from the gallery or the default image the new password which we set again, will be the password for the rest of all the application which we have locked using the app lock application

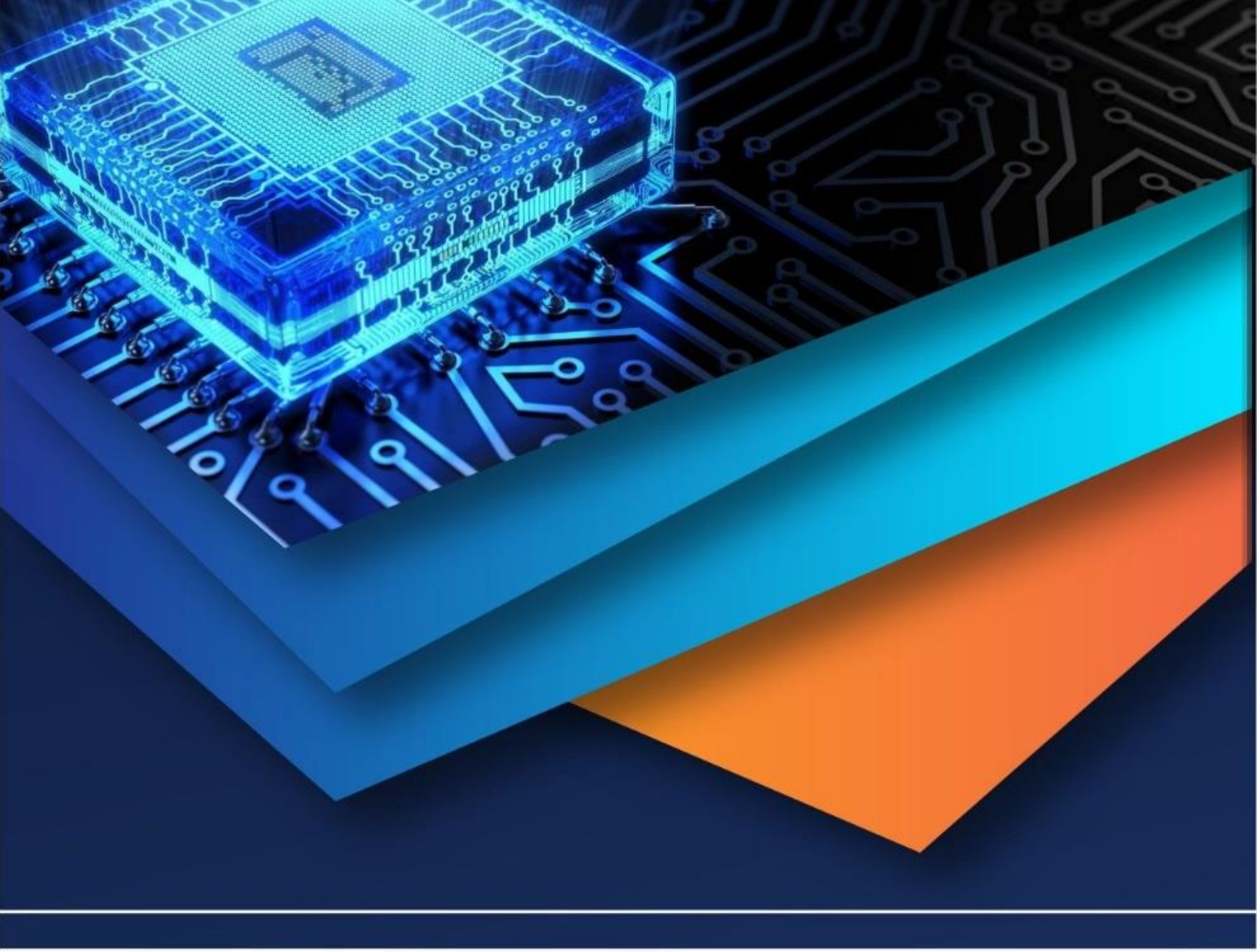
V. CONCLUSIONS

Graphical password authentication systems are been widely used, since it provides great security and usability while compared to other authentication methods. The image grid and cued click points algorithm is a graphical password authentication method that we used in our Digital Mobile App lock system. It involve grid images where the user selects the specific images and selects a click point that will be set as a password. The cued click point algorithm helps in enhancing security of the user's data on the mobile applications, since it will be difficult for attackers to guess the user's password by selecting the images randomly. In addition cued click point also provides usability which makes the process of using the authentication system easier and memorable. In conclusion, image and click-point grid algorithms are promising approaches for graphical password authentication systems on mobile application. Its effectiveness in enhancing security and usability makes it a viable alternative to traditional password and other authentication systems. Overall, the digital app lock provides a promising solution by combining security and usability in mobile devices which results in securing the sensitive user's data.

REFERENCES

[1] N. Asmat and H. S. A. Qasim, "Conundrum-Pass: A New Graphical Password Approach," 2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE), Islamabad, Pakistan, 2019, pp. 282-287, doi: 10.1109/C- CODE.2019.8680989.
[2] A. Khan and A. G. Chefranov, "A Captcha-Based Graphical Password with Strong Password Space and Usability Study," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 2020, pp. 1-6, doi: 10.1109/ICECCE49384.2020.9179265.
[3] M. Kaushik, A. Rawat, V. Sisaudia and L. Parashar, "A Novel Graphical Password Scheme to Avoid Shoulder-Surfing Attacks in Android Devices," 2022 2nd International Conference on Intelligent Technologies (CONIT), 2022, pp. 1-6, doi: 10.1109/CONIT55038.2022.9848122.
[4] G. -C. Yang, "PassPositions: A secure and user-friendly graphical password scheme," 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta Bali, Indonesia, 2017, pp. 1-5, doi: 10.1109/CAIPT.2017.8320723.
[5] Y. Yin, J. Jang-Jaccard and N. Baghaei, "PassImg: A Secure Password Generation and Management Scheme without Storing," 2022 IEEE 25th International Conference on Computer Supported

[6] Cooperative Work in Design (CSCWD), 2022, pp. 341-346, doi: 10.1109/CSCWD54268.2022.9776045.
[7] B. N. V. V. P. Chimakurthi and K. B. PRAKASH, "Image and Video-based Graphical Password Authentication," 2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), 2022, pp. 01-08, doi: 10.1109/ICEEICT53079.2022.9768604.
[8] S. Rajarajan and P. Priyadarsini, "SelfiePass: A Shoulder Surfing Resistant Graphical Password Scheme," 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), 2021, pp. 563-567, doi: 10.1109/RTEICT52294.2021.9573972
[9] N. Zujevs, "Authentication by Graphical Passwords Method 'Hope'," 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE), London, UK, 2019, pp. 94- 99, doi: 10.1109/iCCECE46942.2019.8941758.
[10] A. HameedShnain, H. M. A. Ghanimi, W. A. Mohammed, M. I. Sabri and S. H. Shaheed, "An Effective Graphical Password Authentication Method in Health Care Sectors," 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), 2021, pp. 38-41, doi: 10.1109/IICETA51758.2021.9717888.
[11] Manju Mohanan.M; Dr.Loganathan.D; Nisha.M, 2019, "C App - A Mobile App for Crime Report", International Journal of Computer Science and Network, Vol 8, Issue 3, pp- 294-299
[12] Kannu Priya, Dr. R. Kesavamoorthy, Dr. Raja M, Dr. S. P.Anandaraj, Dr. D. Loganathan, Dr. Thanga Mariappan L, September 2022, "Multimodal Biometrics Authentication Using Thermal Hand Vein and Hand Dorsa" Neuro Quantology , Volume 20, Issue 9 , Pp 3423-3432.
[13] M. Harshini, P. L. Sai, S. Chennamma, Thanuja, A. G. Reddy and H.
[14] S. Kim, "Easy-Auth: Graphical Password Authentication using a Randomization Method," 2021 IEEE Latin-American Conference on Communications (LATINCOM), 2021, pp. 1-6, doi: 10.1109/LATINCOM53176.2021.9647825.
[15] N. Anbalagan, R. A. Abbas Helmi, M. A. Hameed Ashour and A. Jamal, "Trusted Application Using Biometrics for Android Environment," 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), 2020, pp. 7-12, doi: 10.1109/CSPA48992.2020.9068715.
[16] L. Wang, W. Meng and W. Li, "Towards DTW-based Unlock Scheme using Handwritten Graphics on Smartphones," 2021 17th International Conference on Mobility, Sensing and Networking (MSN), 2021, pp. 486-493, doi: 10.1109/MSN53354.2021.00078.
[17] Z. I. Khan and V. K. Shandilya, "Enhanced Recognition Based Image Authentication Scheme to Save System Time & Memory," 2020 IEEE Bombay Section Signature Conference (IBSSC), 2020, pp. 84-90, doi: 10.1109/IBSSC51096.2020.9332183.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY