IJSES
Volume 9, Issue 10, pp. 1-4, 2025.
International Journal of Scientific Engineering and Science
ISSN (Online): 2456-7361

Smart Android Graphical Password System: Enhancing Security and Usability

Uka Kanayo Kizito[1], Amaefule I. A[2]
[1, 2]Department of Computer Science, Imo State University, Owerri, Imo State Nigeria
Email address: kizzyict@gmail.com, profiyke24@gmail.com

Abstract— *The development and assessment of the Smart Android Graphical Password System, a novel strategy to improve security and usability in Android device authentication, are the primary objectives of this paper. The conventional text-based method is susceptible to assaults and can be difficult to memorize. A possible answer is provided by graphic passwords. Compared to conventional text-based passwords, our system's graphical user interface ensures a more secure and user-friendly approach by allowing users to generate and duplicate passwords by selecting particular spots within a picture. The system's efficacy was validated by testing, which showed improved security and usability. The goal of these enhancements is to produce an authentication system for Android devices that is more reliable, scalable, and extensively used.*

Keywords— *Authentication, Usability, Graphical Password, Android Devices, Security.*

I. Introduction

Due to the ease of access provided by the Internet, people of all types and goals are drawn to it. Some people are motivated to provide knowledge, while others tend to act maliciously. Information security is therefore crucial for any service provider. Actions that establish services that guarantee sufficient protection for information systems utilized by or hosted within an organization are referred to as information security. According to the description, services are administrative or technological techniques applied to the data that has to be safeguarded. Integrity, secrecy, authenticity, and availability are all necessary for protection, and information systems are computer or communication systems that manage the data being safeguarded [1]. As a result, the majority of organizations have password policies that establish guidelines for how passwords should be created and used. These policies usually include minimum length requirements, required categories (such as capital and lowercase letters, numbers, and special characters), and prohibited elements (such as one's own name, date of birth, address, or phone number). National authentication frameworks established by several governments specify the password and other authentication criteria for users accessing government services [2].

A password is a word or string of characters that is used for user authentication in order to verify identification and get permission to access a resource that must be kept private from unauthorized users. Passwords have been around for a very long time. Security would ask anybody approaching or wanting to enter an area to provide a password or watchword, and they would only let people or groups pass if they knew it. Nowadays, users often utilize user names and passwords when logging in to secure computer operating systems, cell phones, cable TV decoders, and automated teller machines (ATMs). For a variety of reasons, including accessing programs, databases, networks, websites, logging into accounts, obtaining e-mail, and even reading the morning newspaper online, the average computer user has passwords. Despite the name, passwords don't have to be real words; in fact, it's a good thing if they're not because they could be more difficult to figure out. Some passwords, which are more appropriately referred to as passphrases, are composed of many words. When the secret information is entirely numerical, like the personal identification number (PIN) frequently used to access ATMs, the words passcode and passkey are occasionally employed. Generally speaking, passwords are brief enough to be quickly input and remembered.

A few of the key security aspects that information security offers to guarantee the dependability of information are confidentiality, availability, data integrity, and authentication. Depending on the kind of organization, each of these has varying levels of importance (for example, the military will place the highest value on confidentiality). The most basic process to guarantee security and grant users access to sensitive online resources over the Internet is authentication, which is connected to identity. The most widely used authentication technique is text-based password authentication, which, in order to prevent unwanted access, needs a valid user ID and password [3]. Although this method is simple and affordable to set up, there are significant security risks associated with using a static password. For instance, people frequently create passwords that are simple to figure out, use the same password across several accounts, write them down, or save them on their computers, leaving them vulnerable to a variety of assaults such as shoulder surfing, dictionary attacks, brute force attacks, and phishing attacks. [4].

The goal of this effort is to provide a platform that will allow users to construct stronger passwords that are simple to remember and use, but challenging for unauthorized people to decipher. This is because consumers' obsession with trivial passwords has turned into an essential foundation for computer hackers and crackers.

II. Literature Review

[5] suggested an authentication system utilizing a variety of methods and strategies. Three authentication methods are included in the suggested system: password setup, registration, and login. After selecting a password, the user selects a picture from a collection that the system displays. The system remembers the pixel coordination when the user picks a piece

of the selected image. The following step involves selecting a number from a rolling list. The user may either enter the numbers they have selected from the rolling list or select random numbers from the rolling list. The user must accurately identify the selected image and the numbers from the rolling list as the system displays images with random numbers next to each image. The user then inputs their text password and username. Entering the CAPTCHA is the final step. The user must successfully complete each of these steps in order to access the application. They have three opportunities to get access to the system; if they don't, their account will be locked for five hours. Following login, a series of pictures will be displayed by the system; the user must identify the proper image and then choose the appropriate area of the image. The user is prompted by the system to choose the right number from a range of rolling numbers. In the final step, the user must properly complete the CAPTCHA challenge and input their username and password. This plan included a variety of methods and strategies, including click-based and choice-based strategies. The click method is used to choose an image from a collection of photos, the choice method is used to choose a series of images, and a recall-based method should be used to determine which image section was chosen during registration when choosing an image again. In this architecture, the password may be set using a variety of graphical password combinations. By utilizing CAPTCHA to verify that the application user is a person and not a robot, which is employed in hacking systems, the system offers increased network security. As a result, it is resistant to malicious software assaults and shoulder surfing attacks. Better security may be achieved by implementing biometric systems. Because the suggested method lacks a clue, the user may forget the image's pixel coordination, make all of their login attempts, and then fail; if this happens, the system would lock the user. As a result, the login procedure is time-consuming and uncomfortable, especially if the region they have chosen is tiny.

[6] suggested a system that makes use of the recognition-based method. The user selects one or more images from the picture pool during registration. The user selects three photos in this system, and each image matrix has a password. The login process involves the user entering their ID and receiving a password on their mobile device. The password is then compared to the password that was stored in the database, and if it matches, the user re-selects the three images that were chosen during registration. A second comparison is made between the generated number of the selected images and the saved password, and if it matches, the user is granted access. The system is more resilient to assaults using graphical passwords. Brute force and dictionary attack: By choosing an arbitrary number of pictures and creating a random number for each one each time, these attacks are reduced. Because the password cannot be obtained via a mouse or keyboard, it also withstands spyware attacks. When using a shoulder surfing assault, the attacker is unable to predict the keyboard and mouse movements. No login attempts are made to stop unwanted logins, and the generated password is set so that the hacker may log in again if they manage to steal it.

[7] suggested a method in which the user clicks on a specific pixel or point in each image in a series of images. The subsequent picture is contingent upon the accuracy of the preceding click point. Three credentials are required for the user to log in: an encrypted password, the user ID, and the suggested graphical password scheme. The account is locked if an intruder makes a specific effort to attack the system. The cued click point approach is employed in this system. The suggested solution offered defense against denial of service attacks and online guessing attacks. Using a bigger number of photos enhance the security but because of employing the cued click point approach, it is hard to recall the picked locations properly.

[8] have out an extensive analysis of the graphical authentication solutions in use today. We have divided these techniques into three primary categories: schemes based on recognition, schemes based on pure recall, and schemes based on cued recall. Compared to text-based passwords, graphical passwords are more secure. We discovered throughout our investigation that graphical passwords are extremely tough to attack using dictionary attacks, brute force assaults, and malware.

The Pass Point system, its security features, and the empirical research and comparison between Pass Point and alphanumeric passwords are all described in [9]. Although there are certain shortcomings, the empirical testing of Pass Points is generally positive.

[10] introduced a novel hybrid graphical password-based system that combines recognition and recall-based methods. This system has numerous benefits over the current ones and could be more user-friendly. Our suggested authentication solution uses graphical password methods as its foundation. Our system has various limits and drawbacks like any other graphical-based password strategies, even though its goal is to lessen the problems with current graphical-based password schemes.

III. Methodology

By removing the predetermined bounds and permitting the use of random pictures, this study expanded on Blonder's concept (Pass Point Method). There are multiple clickable points in the image, which could be any painting or natural scene. Because of this, a user may generate a password by clicking on any location on a picture, rather than just specific pre-dined places. For every selected pixel, a tolerance is computed. The user must click inside the tolerance of their selected pixels in order to be authenticated. The user may be able to rapidly and simply construct a valid password by utilizing this procedure.

Figure 1 of the framework illustrates how a user may register for the system by entering their phone number, email address, and username. After that, they must choose one of the shown pictures. The user must now click on any five locations in the previously selected image. The registration data will thereafter be stored in the database. The username that was registered during the registration phase must be entered by the user during the login process. The user must then confirm that the image they selected during the registration process is the one that appears in the program. The user must next click each

International Journal of Scientific Engineering and Science
Volume 9, Issue 10, pp. 1-4, 2025. ISSN (Online): 2456-7361

of the five points they clicked throughout the registration process. The information will be compared with the database of the system. Whether a user has registered or not, the database server will provide them the results. Lastly, if the user provides accurate information, the user will be authorized.

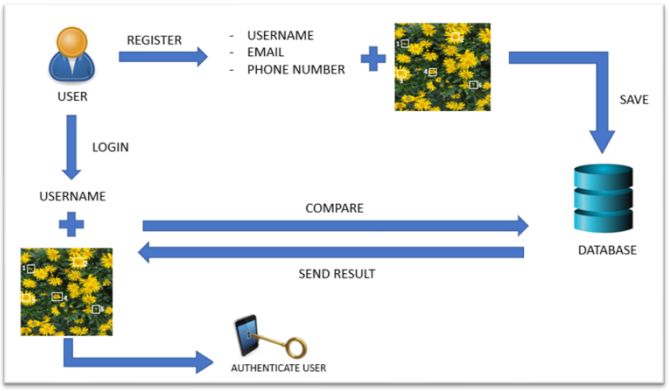

Figure 1: Pass Points Method-Based Smart Android Graphical Password System Framework

The user will provide their name, email address, and phone number during the registration step. The user must next choose an image from a collection of thirty, and then click five spots inside the image. Once the user has fulfilled all the requirements during the registration phase, they will be officially registered.

The user must first provide their previously registered username in order to proceed to the log-in step. The user will next be required to confirm whether or not the photograph is indeed theirs. If so, the user must click the five areas they clicked throughout the registration process. Finally, the user may log into the system after being authenticated. The flowchart for utilizing the Pass Point approach to construct a Smart Android Graphical Password System is displayed in Figure 2.

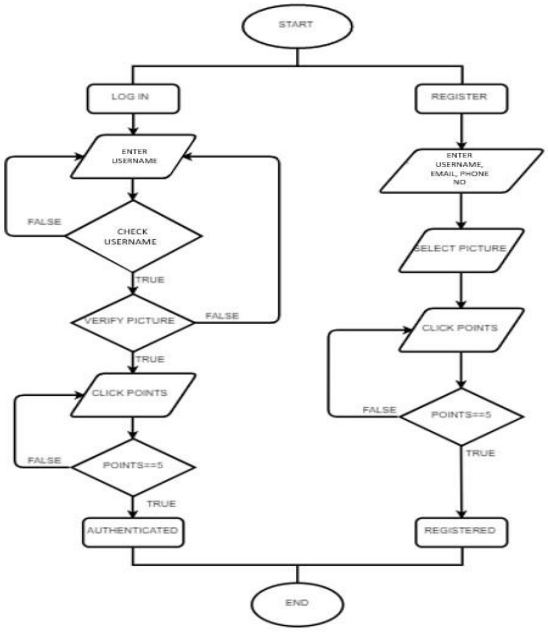

Figure 2: Shows the flowchart for utilizing the Pass Point approach to construct a smart Android graphical password system.

The use case diagram for a smart Android graphical password system that uses the Pass points scheme for new users is displayed in Figure 3. Four use cases—creating a login, creating a password, choosing an image, and saving a password—can be identified by examining the graphic. Furthermore, a new user is the actor in this use case diagram. Anything that interacts with the system is called an actor. The actor may be an internal or external program or a human user. Finding the application boundary, which is depicted in the picture, is another crucial step. Being an external user of the application, the actor user is not part of the system. The use case diagram for graphical password authentication for current users is then displayed in figure 4. The graphic also includes four use cases: authenticate, choose a photo, input a password, and enter a username.

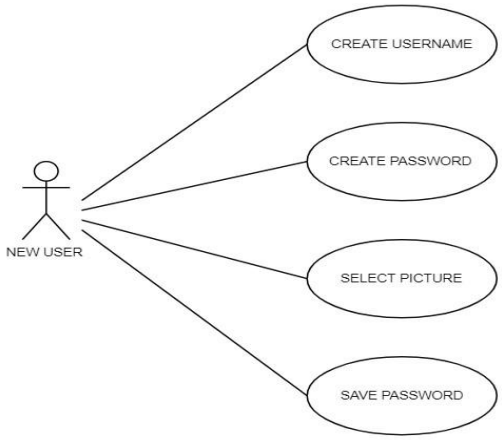

Figure 3: Use case diagram for new user

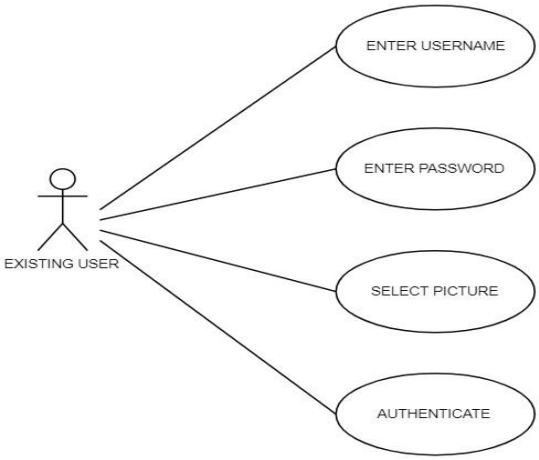

Figure 4: Use case diagram for existing user

The registration procedure sequence diagram is displayed in Figure 5. The user must request the registration page from the server in order to complete the registration process. The registration page will then be returned by the server. After creating a username, the user will be sent to an image selection page. The user must select a single image to use as their password. The user will then get a link to the image they have picked, and they will be able to click five points on it. The user must click the "Confirm" button once all of the clicks have been

completed. All of the user-selected values and data will be sent and saved by the server. The server will reply with a brief popup message informing the user that the data has been submitted if the registration procedure is successful.

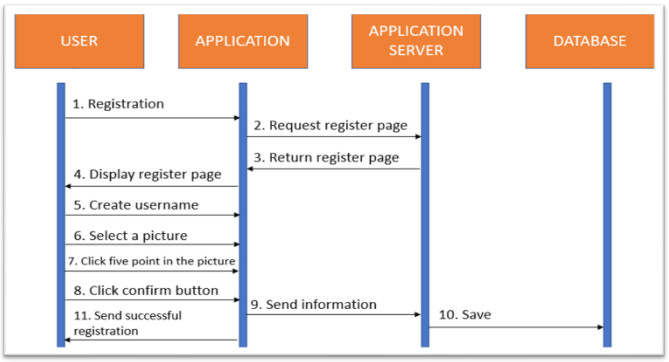

Figure 5: Sequence diagram for registration phase

A sequence diagram of the log-in procedure is displayed in Figure 6. The user must request the log-in page from the server in order to log in. The log-in page will then be returned by the server. The user will then be sent to an image selection screen after entering their username. The user must select a single image to use as their password. The user must then click five points on the previously selected image. The image that the user chooses in the previous picture selection determines the image that the server will return to the user. The user must click the "Confirm" button once all selections have been made. In order to reply to the user, the server will compare the data that is currently in the database with the data that has already been registered. The user will be notified by the popup whether or not the log-in procedure was successful. The user will be directed to the inquiry page if the log-in process is successful; if not, they will be directed to the username entry page, which will allow them to log in again.

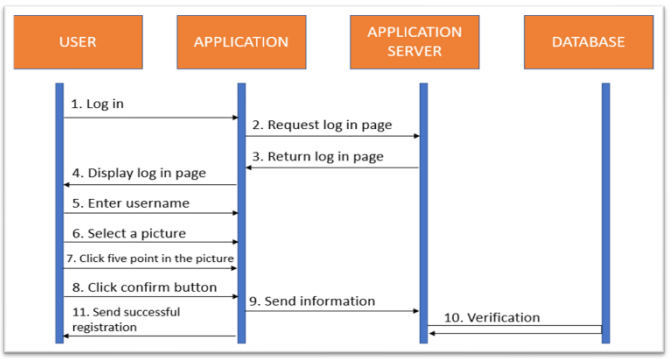

Figure 6: Sequence diagram for login phase

IV. Conclusions

An important development in Android device authentication is the Smart Android Graphical Password system, which provides a safe and convenient substitute for conventional text-based passwords. This solution improves usability and security by utilizing graphical passwords and an easy user interface. Users choose and click on exact points in a selected picture to construct their password during the registration phase. They must precisely duplicate these points at the login phase in order to access the system. By assisting users with the registration and login operations and guaranteeing the precision and dependability of the password scheme, the testing methods validated the system's operation. To guarantee a flawless user experience, every stage—from choosing and authenticating click points to inputting personal information—was carefully tested. The outcomes showed how well the graphical password system worked to improve security without sacrificing usability. In addition to providing a strong substitute for conventional text-based passwords, this system presents a viable substitute method of protecting Android devices by using recognizable visual clues.

References

[1] Timothy J. Shimeall and Jonathan Spring 2014. Introduction to Information Security: A Strategic-Based Approach. @book {shimeall_2014, author= {Shimeall, Timothy and Spring, Jonathan}, title={Introduction to Information Security: A Strategic-Based Approach}, month={{Apr}, year={{2014}, how published={Carnegie Mellon University, Software Engineering Institute's Digital Library}, url={https://www.sei.cmu.edu/library/introduction-to-information-security-a-strategic-based-approach/}

[2] Bander AlFayyadh, Per Thorsheim, Audun Josang, Henning Klevjer 2012. Improving Usability of Password Management with Standardized Password policies. Conference: The Seventh Conference on Network and Information Systems Security (Sécurité des Architectures Réseaux et Systèmes d'Information) (SAR-SSI 2012) At: Cabourg, France

[3] A Menezes, P. Van Oorschot and S. Vanstone, 1997. Handbook of Applied Cryptography, CRC press, Boca Raton, Florida.

[4] Viju Prakash, Alwin Infant and Jeya Shobana 2010: Eliminating Vulnerable Attacks Using One-Time Password and PassText- Analytical Study of Blended Schema. Universal journal of Computer Science and Engineering Technology.

[5] Delphin Raj, K. M., & Victor, N. (2014). A Novel Smart Android Graphical Password Mechanism. *International Journal of Advanced Research in Computer Science and Software Engineering, September 2014*.

[6] Kawale, N., & Patil, S. (2014). A Recognition Based Graphical Password System. *International Journal of Current Engineering and Technology, April 2014*.

[7] Muddam, P., & Raman, D. (2016). Smart Android Graphical Password for Secure Online Services. *International Research Journal of Engineering and Technology, Aug 2016*.

[8] H. Kumar and Farhat Ullah Khan 2013: Graphical password Authentication Schemes: Current Status and key Issues. @in proceedings {Kumar2013 Graphical PA, title= {Graphical Password Authentication Schemes: Current Status and Key Issues}, author= {Harsh Kumar and Farhat Ullah Khan}, year= {2013}, url={https://api.semanticscholar.org/CorpusID:15858104}

[9] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems, p. 26*.

[10] Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang (2011) A Graphical Password Based System for Small Mobile Devices. International journal of Computer Issues, vol 8, issues 5, No 2, September 2011 ISSN (ONLINE) 1694-0814