ISSN No:-2456-2165

Evaluation of the Effectiveness of PIN Code Authentication on Android Smart Devices

Abubakar Bello[1]
Department of Public Admin
Kebbi State Polytechnic Dakin-gari,
Dakin-gari, 862106, Nigeria

Anas Shehu[2], Shamsu Sani[3]
Department of Computer Science
Kebbi State Polytechnic Dakin-gari,
Dakin-gari, 862106, Nigeria

Zauwali Sabitu Paki[4]
Department of Computer Science
Yusuf Maitama Sule University,
Kano 800001, Nigeria

Abstract:- The authentication system on Android devices aims to ensure that only the rightful owners of the devices get access to them. This work tested the usability of increasing the size of PIN from the conventional 4 digits to 5 digits using a specially designed Android app. We experimented with the scheme with 104 volunteers. Although only 2.88% of the respondents did not authenticate successfully after the allowable 3 retries, 41.45% of the users succeeded only after the third attempt. The average authentication time was 9 seconds.

I. INTRODUCTION

Authentication ensures that only the right owners of smart devices have access to them. It is a line of defense against impersonation [1]. Nowadays, users must authenticate themselves before allowing access to computing devices [2]. It tries to block all possible attempts by imposters to gain access to unauthorized devices. The PIN system on Android devices is a numeric display with which a user inserts the required passcode by discrete touches on the device's screen [3]. The ability of an authentication system to resist attacks lies in the difficulty of its break by attackers. This work focuses on the usability and security of Android authentication mechanisms. The authentication strategy aims to provide access to the smartphone's content to the authorized user. It ensures that only the right user accesses the device. That is security. Normally, security specialists measure the quality of a given security scheme by how difficult it is for an attacker to break it without any prior knowledge of the scheme.

However, usability entails the ease or difficulty with which the user uses the authentication (in our case). It includes all aspects of a product like software, such as the menus, the dialogs, the displays, etc.

To achieve that, we will develop an Android app that simulates this authentication mechanism. we will fine-tune some parameters related to this authentication mechanism to determine the best thread-off [4]. The app will be used to experiment with real smartphone users to get real authentication data. The authentication data that the app will collect will help determine the scheme's ease or otherwise with the new PIN sizes and consequential acceptability.

Other common authentication mechanisms besides the PIN system are used to secure the content of smartphones. Examples are fingerprint biometrics, facial recognition, and passwords. Implicit authentication (IA) [5] that uses behavioral biometrics to authenticate users of a smartphone is receiving attention in the research community in recent times. This mechanism allows the user to be authenticated by using his behavior such as how the user picks his phone. This can be used to create a two-factor authentication for better security.

II. LITERATURE REVIEW

The classical textual password is employed for authentication reasons in a variety of applications[6]. Substantial improvements have been achieved in user authentication systems on Android devices in recent times. A context-based authentication method has been proposed to securely authenticate users with minimal or no user intervention [7]. Context-based authentication utilizes a combination of sensor data to verify the authenticity of the authentication request. Shin and Woo [6] researched the password using the tensor decomposition method and discovered that the length of a password constitutes a factor in its strength.

Nyang, et al. [8] proposed a PIN entry method that could be resistant to observation attacks. The proposed method requires a user to use visual and touch interactions with multi-touch screen. The idea to block observing/recording attacker. In a similar effort, Binbeshr, et al. [9] conducted a study on the PIN entry methods used by users. The authors found that majority of the methods are susceptible to shoulder surfing and observation attacks. A strategy that thwarts attacks success is need by possibly making the appearance of the number pad random so that there is not direct and fixed mapping between the numbers and the screen location.

ISSN No:-2456-2165

III. MATERIAL AND METHOD

This research was conducted with the help of a specially-developed Android app that simulates the PIN system on Android devices. Figure 1 illustrates the components of the app.

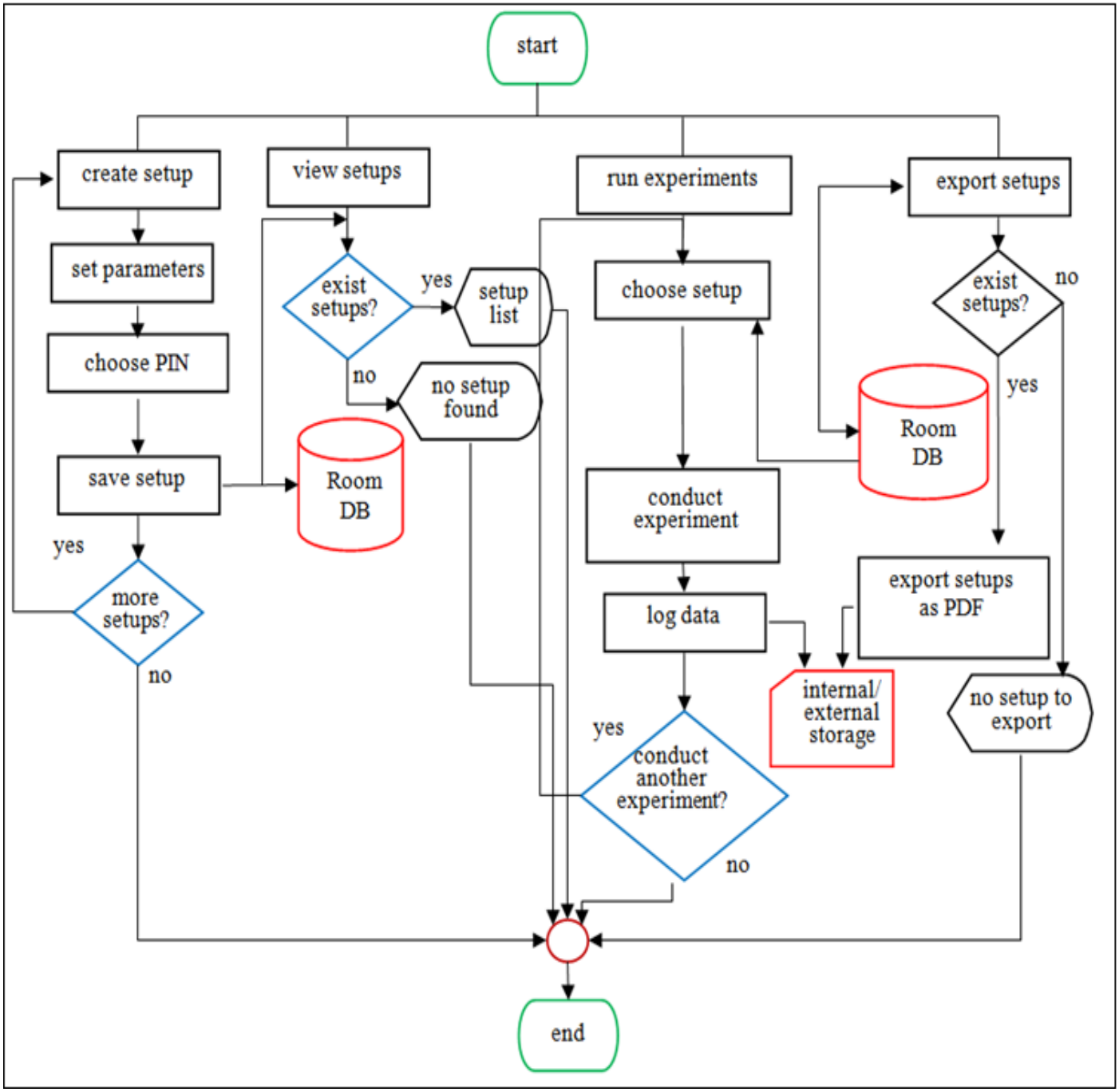

Fig 1 Schematic Diagram of the PIN Authentication Simulation Android app

The app records the user activities during an experiment and stores them on the phone's memory as a comma-separated values (CSV) file. The information it records comprises the duration of an experiment, success status, number of retries (if any). We retrieved the CSV file for analysis at the end of our experiments.

ISSN No:-2456-2165

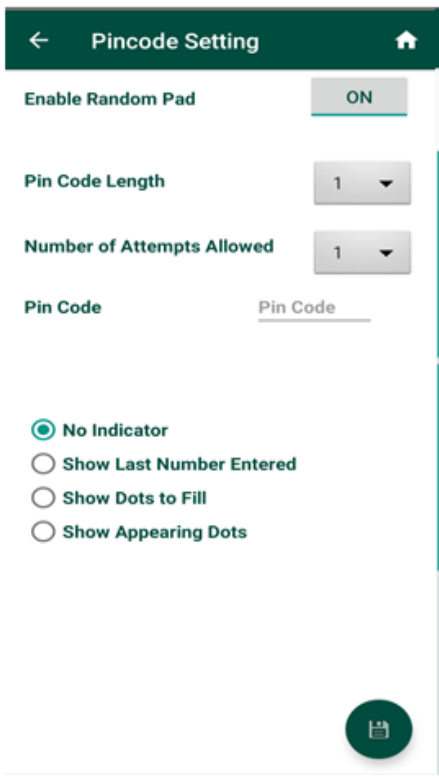

Fig 2 Create Setup

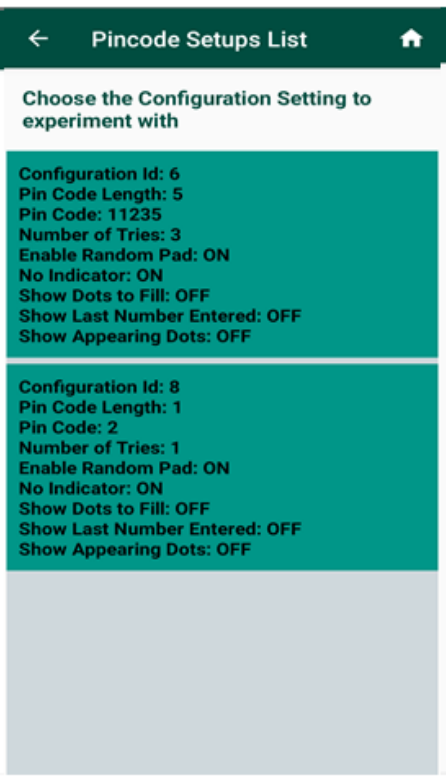

Fig 3 View Setup

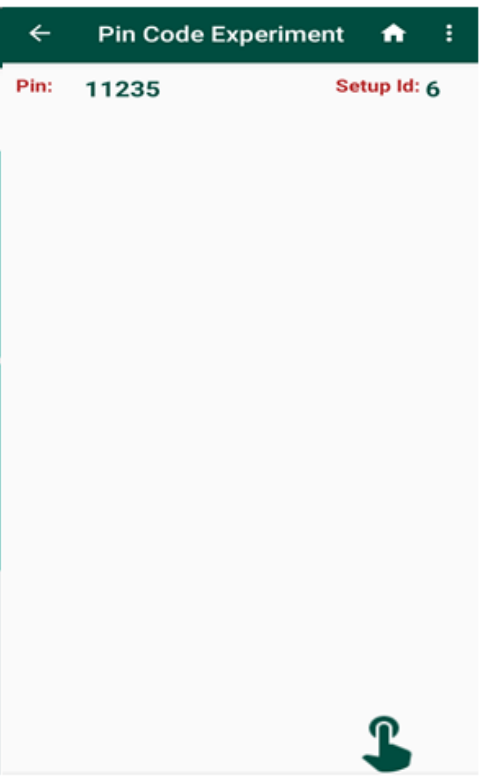

Fig 4 Run Experiment

The app has several screens as shown above that let the user (experimenter) carry out different tasks.

➢ *Create Setup/ Set Parameters*

The fig2 above lets the person experimenting create as many setups as s/he needs with varying parameters. These parameters include the size of the PIN, the number of allowable attempts in the event of an error, and how the PIN pad displays to the user (rearrangement of the pad, random appearance of dots, e.t.c). A critical feature is the how the number pad is oriented. The app is designed in such a way that pad reshuffles the numbers on each authentication time. This can greatly help in thwarting the success of shoulder surfing and observation attackers. The app also lets an experimenter select the digits that would make up a PIN. After setting the parameters and choosing the PIN numbers, the user can save or discard the setup.

➢ *View Setups*

This screen in fig 3 allows the experimenter to view the already created setups (if they exist) for experimentation. The setups are presented to the experimenter with the summary of the parameter for each of the setups.

➢ *Run Experiments*

The run experiment is a screen that facilitates the conduct of the experiments. It presents a list of all the setups created so far. The user taps on a displayed setup to immediately start an experiment as shown in fig 4. As the experiment commences, the app logs every bit of the user's activity into the device's storage in a CSV file that can be retrieved for analysis.

➢ *Room Database*

Room is a persistent database that provides an abstraction level on the conventional SQLite database used with Android apps. It lets app developers save app data efficiently and reliably [10].

The research was conducted with the help of a specially-developed Android app accessible via: https://drive.google.com/file/d/1GwWkerTtKyv1NKN9QJgwmAPOxkUFR7M4/view?usp=share_link.

IV. RESULTS AND DISCUSSION

We experimented with a total of 104 volunteers recruited mainly from the staff and students of Kebbi State Polytechnic Dakingari. The gender distribution of the volunteers is presented in Figure 2 below.

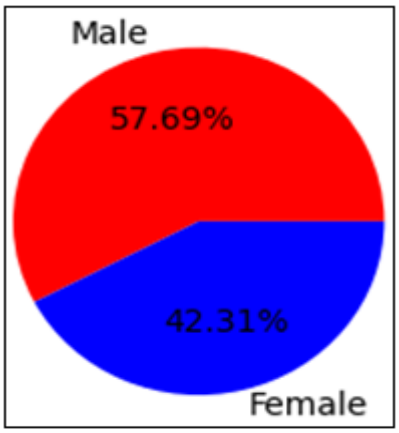

Fig 5 Gender Distribution of the Volunteers

ISSN No:-2456-2165

We asked each of the recruited volunteers to choose a 5-digit PIN of his/her choice in the first place. After four days of the selection, we requested a volunteer to attempt to log in to the phone on which the app was installed using the PIN s/he had chosen. We limited the number of attempts to 3 as it is the norm with the traditional 4-PIN system. A user may succeed to authenticate on either the first, second, or third attempt. A user may also fail to authenticate even after the third attempt. This is classified as an unsuccessful attempt. This is illustrated in Figures 3 and 4.

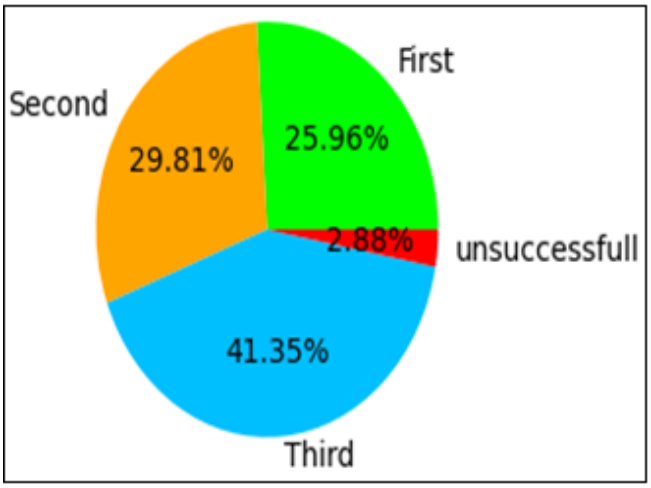

Fig 6 Percentages of Authentication with Regards to First, Second, Third, and Unsuccessful Attempts.

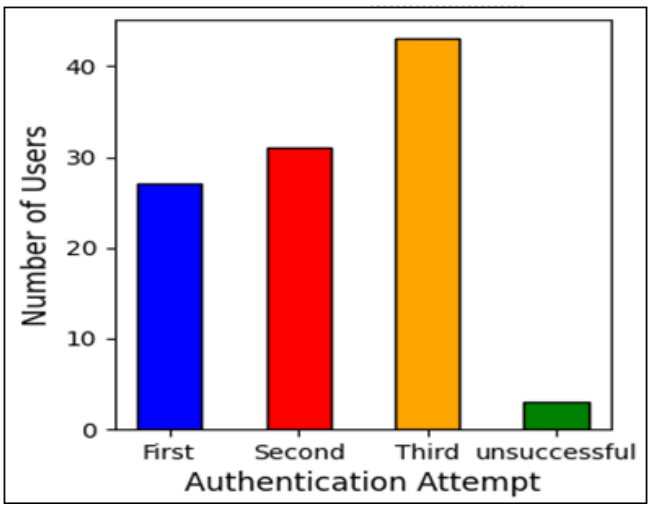

Fig 7 Distribution of users According to First, Second, Third, or Unsuccessful Attempt

We can notice from Figures 3 and 4 that a significant portion of the users succeeded only in the third attempt (about 42 out of the 104 users, which is approximately 41.35%) due to mistakes in entering the PIN. This could be attributed to the increase in the size of the PIN and may be due to the fact users could have haphazardly chosen their PINs with due consideration to the nature of the PIN. This significantly affects the usability of the system

However, the average authentication time was 9 seconds. This is a bit fair. But as people get used to the new scheme, the time to authenticate will reduce significantly.

V. CONCLUSION

The fact that a significant percentage of the users succeeded in the third attempt (41.35%) may be attributed to the increase in the size of the PIN. This affects the usability of the scheme but at the same time increases its security strength. Overall, 97.12% of users were able to authenticate. This is a little bit plus on the usability.

REFERENCES

[1]. R. Ryu, S. Yeom, D. Herbert, and J. Dermoudy, "The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction," ICT Express, 2023.

[2]. M. Cardaioli, M. Conti, G. Orazi, P. P. Tricomi, and G. Tsudik, "BLUFADER: Blurred face detection & recognition for privacy-friendly continuous authentication," Pervasive and Mobile Computing, vol. 92, p. 101801, 2023.

[3]. I. Olade, H.-N. Liang, and C. Fleming, "Story-based authentication for mobile devices using semantically-linked images," International Journal of Human-Computer Studies, vol. 171, p. 102967, 2023.

[4]. H. Khan, U. Hengartner, and D. Vogel, "Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying," presented at the Symposium on Usable Privacy and Security (SOUPS), Ottawa Canada, 2015.

[5]. W. H. Lee, X. Liu, Y. Shen, H. Jin, and R. B. Lee, "Secure Pick Up: Implicit Authentication When You Start Using the Smartphone," presented at the SACMAT'17, Indianapolis, IN, USA, 2017.

[6]. Y. Shin and S. S. Woo, "PasswordTensor: Analyzing and explaining password strength using tensor decomposition," Computers & Security, vol. 116, p. 102634, 2022.

[7]. P. Shrestha, H. Truong, P. Toivonen, N. Saxena, S. Tarkoma, and P. Nurmi, "Chirp-Loc: Multi-factor authentication via acoustically-generated location signatures," Pervasive and Mobile Computing, vol. 88, p. 101720, 2022.

[8]. D. Nyang, H. Kim, W. Lee, S.-b. Kang, G. Cho, M.-K. Lee, et al., "Two-Thumbs-Up: Physical protection for PIN entry secure against recording attacks," computers & security, vol. 78, pp. 1-15, 2018.

[9]. F. Binbeshr, M. M. Kiah, L. Y. Por, and A. A. Zaidan, "A systematic review of PIN-entry methods resistant to shoulder-surfing attacks," computers & security, vol. 101, p. 102116, 2021.

[10]. AndriodDev. (2023, 30/06/2023). Save data in a local database using Room. Available: https://developer.android.com/training/data-storage/room