Comparison between Usability and Security in Android Pattern System

Musa Ibrahim Kamba[1]; Anas Shehu[2]; Zauwali Sabitu Paki[3]

[1]Department of Computer Science, Waziri Umaru Federal Polytechnic Birnin Kebbi
[2]Department of Computer Science, Kebbi State Polytechnic Dakingari
[3]Department of Computer Science, Northwest University, Kano

Publication Date: 2025/03/15

Abstract: The research evaluates the usability and security of different Android patterns across 3x3, 3x4, and 4x4 grids on smartphone authentication mechanisms. Through an experiment with 90 volunteers using a specially created Android application, this study examines the security and usability of the Android pattern lock system. The results show that roughly 70% of participants authenticated on their first try, while only 13% failed to authenticate on their first, second, and third try, indicating that they failed to remember their pattern supply during the experiment, although the Android pattern lock is generally user-friendly, there are significant security concerns, as indicated by the failure rate. The findings advocate for the adoption of larger grid sizes to mitigate brute force and guess-based attacks while maintaining acceptable usability levels.

Keywords: *Usability, Security, Pattern Lock, Smudge Attack, Observation Attack.*

How to Cite: Musa Ibrahim Kamba; Anas Shehu; Zauwali Sabitu Paki. (2025). Comparison between Usability and Security in Android Pattern System. *International Journal of Innovative Science and Research Technology*, 10(3), 83-88. https://doi.org/10.38124/ijisrt/25mar041.

I. INTRODUCTION

The pattern lock mechanism has several security flaws despite its widespread use. Predictability, studies have revealed that users frequently form easily anticipated, basic patterns, including beginning from a corner or forming well-known shapes. This pattern may be exposed to attackers due to finger oil residue on the touchscreen, a vulnerability called a "smudge attack" [17]. The primary goal of this work is on the usability and security of Android authentication mechanisms, and the authentication strategy is to grant access to a smartphone's content only to authorized users, ensuring that unauthorized individuals cannot gain entry. Security is typically evaluated based on how difficult it is for an attacker to bypass the system without prior knowledge of its workings.

However, On the other hand, usability refers to how easy or difficult it is for users to interact with the authentication system. This includes various software-related elements such as menus, dialogs, and displays. To explore this aspect, an Android application was developed to simulate the authentication mechanism, adjusting certain parameters to identify the optimal balance between security and usability[1].

Beyond pattern-based authentication, several other methods are used to protect smartphone content, including fingerprint biometrics, facial recognition, passface, and passwords. Additionally, implicit authentication (IA) [2], which leverages behavioral biometrics to verify users based on actions like how they pick up their phone, has gained increasing attention in research. This method can be integrated into a two-factor authentication system to enhance security.

II. RELATED WORK

Several mechanisms exist for securing smartphone content beyond those mentioned earlier. This section reviews some of the commonly used authentication methods.

A. *Alphanumeric Password*

Alphanumeric passwords are widely used for user authentication across devices and services. These passwords typically include a combination of letters, numbers, and special characters, with many platforms mandating at least one uppercase letter, a numeral, and a special character to enhance security [3]. Such combinations improve the protection offered to the device, software, or service being secured.

B. *Facial Recognition*

Face recognition technology enables the identification of individuals through facial images. It operates by first detecting the face [4] and then extracting distinctive facial features for authentication. The human face contains several unique characteristics that form the basis of this recognition process [5]. Recently, this technology has been integrated into smartphones, allowing users to unlock their devices simply by looking at the screen instead of entering a PIN or drawing a pattern. This method is particularly beneficial for individuals who struggle with memorability. Originally, facial recognition was developed for crime prevention, with security agencies in the United States deploying surveillance cameras to identify individuals on watchlists [5].

C. Fingerprint

Fingerprint recognition identifies individuals by analyzing the unique patterns on their fingertips [6]. The system captures the user's fingerprint through a sensing device and stores the extracted features in a database. During authentication, the fingerprint is scanned again and compared with the stored template to verify the user’s identity[7]. Fingerprint biometrics can function in two modes: verification and identification [8]. In verification mode, the user claims an identity, and the system performs a one-to-one comparison with the corresponding stored template [7]. In identification mode, the system scans the fingerprint without any prior identity claim and searches the entire database for a match, making this process more time-consuming.

Fingerprint authentication is widely accepted due to its reliability, affordability, and robustness. It has long been used for secure identification and is now a common alternative to PIN codes or patterns in smartphones [9-11]. Since fingerprint authentication relies on biological characteristics, users do not need to memorize anything, making it a convenient and secure option [12].

D. PIN Code

The PIN code remains one of the most commonly used authentication methods for smartphones [13]. Users enter a four-digit PIN to unlock their devices, but PIN authentication extends beyond smartphones to applications like ATMs, POS systems, NFC payments, and SIM card locks. If a user enters an incorrect PIN, they are allowed two more attempts before the system locks access.

Since PIN authentication is so prevalent, researchers have explored its usability by increasing the PIN length from four to five digits. A study conducted through an Android app showed that only 2.88% of participants failed authentication after three attempts, while 41.45% succeeded on the third attempt. Although alphanumeric passwords offer greater security, they are less commonly used on smartphones due to their complexity [14].

E. Passfaces

Passfaces is an alternative authentication method where users select specific images as their password. This approach was developed to address the memorability challenges associated with traditional passwords. Since the human brain can recognize familiar faces within milliseconds, Passfaces authentication eliminates the need to remember complex passwords. Users simply recognize and select the correct images.

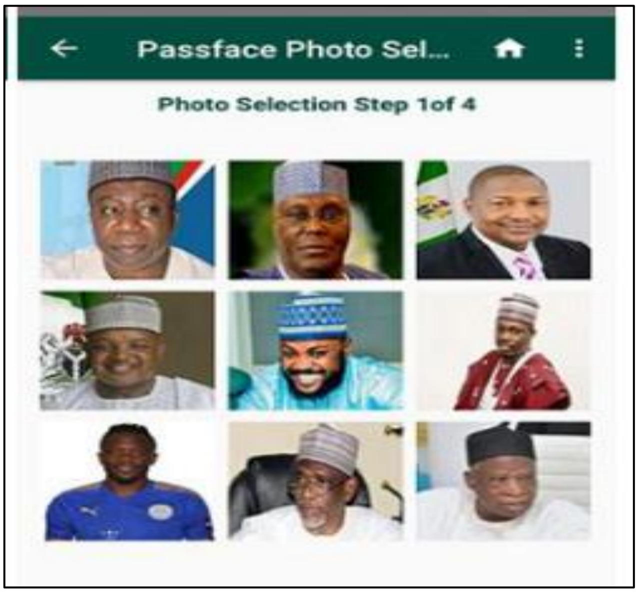


Fig 1: Passfaces Grid of 3x3 Tiles for a User to Select One

It should be noted that new authentication mechanisms are emerging such as authentication via voice (voice biometrics). Also, [15] developed a special Android app that simulated the Passfaces technology, The results reveal that Passfaces of size 4 is more usable with the least average authentication time and minimal errors, and overall, 80% of the volunteers could authenticate in the first attempt, about 10% and 3% authenticated in the second and third attempts, respectively. Another form of authentication is implicit authentication which can be used to create a two-factor authentication scheme [16, 17]. It is a kind of behavioral biometrics that allows for securing a smartphone by how the user picks his/her phone.

F. Android Pattern System

Google launched the Android pattern lock system in 2008 as a graphical authentication technique to protect mobile devices. With the use of a 3x3 dot grid, users can connect at least four dots to create a custom pattern without going back or raising their finger. An easy-to-use substitute for conventional PINs and passwords is provided by this technique [18].

➢ *Adoption and Usability*

Because of its physical and visual appeal, it got widespread use. According to studies, almost 40% of Android users favor pattern locks above other security features. The design of the system prioritizes usability, allowing for rapid device access while preserving a certain amount of security [19].

➢ *Aspects of Security*

The pattern lock mechanism has several security flaws despite its widespread use: Predictability: Studies have revealed that users frequently form easily anticipated, basic patterns, including beginning from a corner or forming well-known shapes. The pattern may be exposed to attackers due to finger oil residue on the touchscreen, a vulnerability called a "smudge attack" [20]. *Observation Attacks:* Using techniques like shoulder surfing or video recording, patterns can be improved and Substituted. Researchers have suggested several changes to solve these security issues: *Double Patterns:* This technique greatly increases complexity and decreases guessability by entering two consecutive patterns on the same grid. *M-Pattern Scheme:* A sophisticated pattern-based authentication system that adds more intricate pattern requirements to improve security [21].

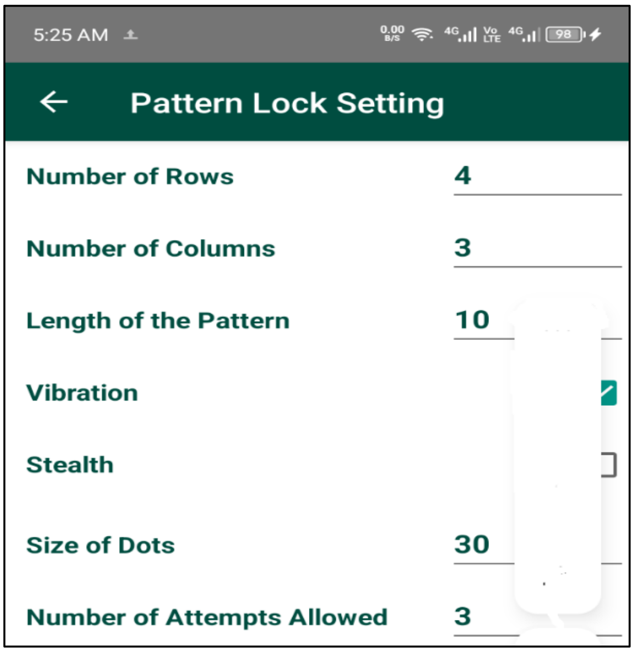
Other authentication options include passwords, PINs, and biometric choices like fingerprint and facial recognition, each of which strikes a different balance between convenience and security. This enables attackers to rebuild the pattern by examining hand movements. Users should be mindful of the security limitations of the Android pattern lock system, even if it offers an easy-to-use authentication option. Device security can be improved by using more intricate patterns or different authentication techniques.

III. MATERIAL AND METHOD

In this section, we will discuss the research procedure used to conduct the experiments for this research. It outlines the tools used and the different configuration parameters utilized to prepare the setups for the performed simulations.

- *Tools for the Experiments*

The research used an Android app developed by [22] to compare the usability and security of different access control systems on Android devices. It allows a researcher to specify different security parameters for the experiment as shown in Figure 2.

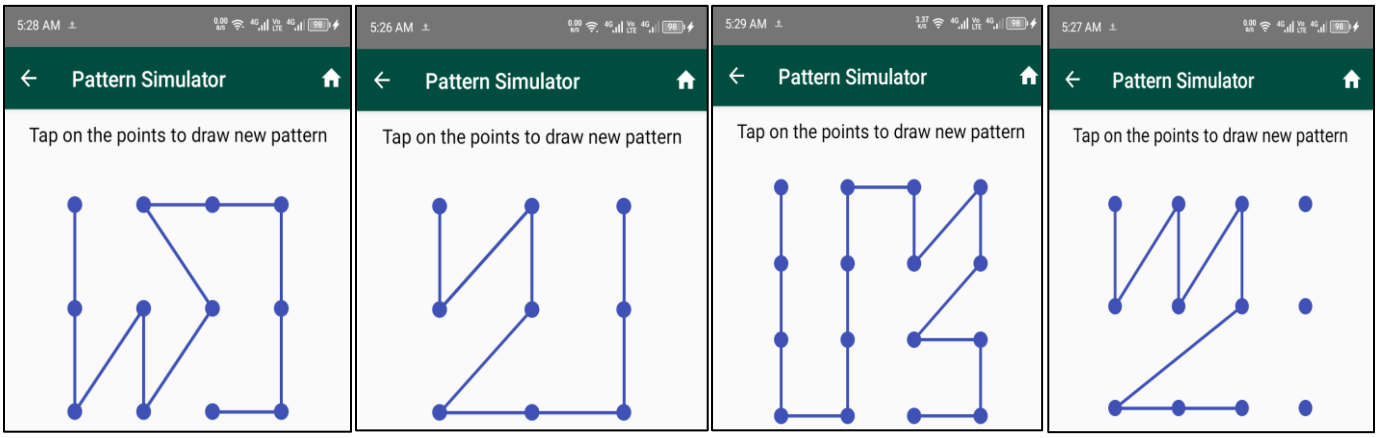


Pattern Lock Setting

Number of Rows	4
Number of Columns	3
Length of the Pattern	10
Vibration	☑
Stealth	□
Size of Dots	30
Number of Attempts Allowed	3

Fig 2: Parameter Setting for Simulation Setup.

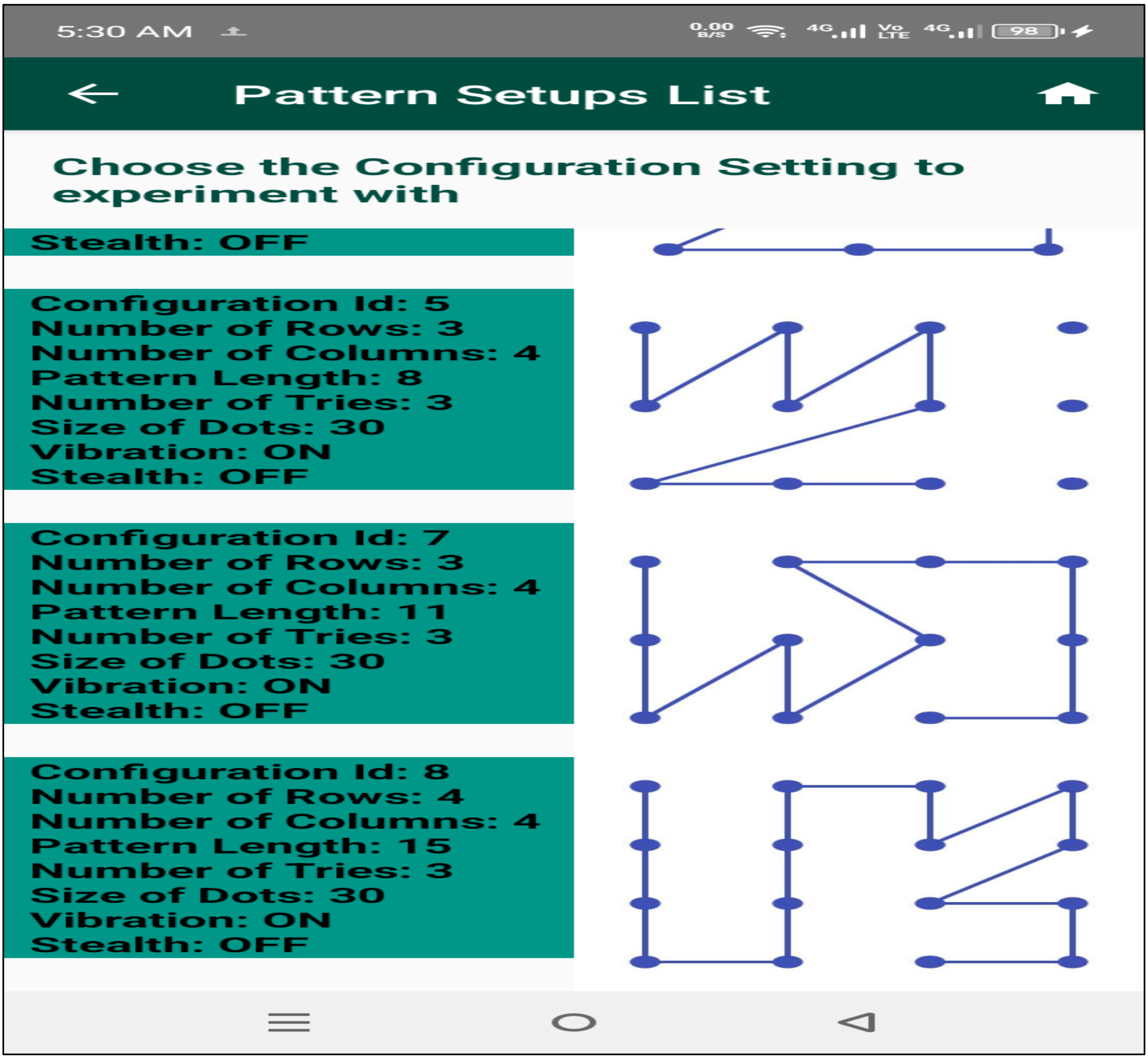
After setting the needed parameters, the next thing is to create the pattern for the simulation. Figure 3 shows samples of created setups.



5:28 AM
Pattern Simulator
Tap on the points to draw new pattern
5:26 AM
Pattern Simulator
Tap on the points to draw new pattern
5:29 AM
Pattern Simulator
Tap on the points to draw new pattern
5:27 AM
Pattern Simulator
Tap on the points to draw new pattern

Fig 3: Samples of Pattern Setups for Simulations

After creating the setups for the simulations, a researcher then proceeds to run the simulations. All the available setups created can be accessed from one screen as shown in Figure 4 below.



Pattern Setups List

Choose the Configuration Setting to experiment with

Stealth: OFF

Configuration Id: 5
Number of Rows: 3
Number of Columns: 4
Pattern Length: 8
Number of Tries: 3
Size of Dots: 30
Vibration: ON
Stealth: OFF

Configuration Id: 7
Number of Rows: 3
Number of Columns: 4
Pattern Length: 11
Number of Tries: 3
Size of Dots: 30
Vibration: ON
Stealth: OFF

Configuration Id: 8
Number of Rows: 4
Number of Columns: 4
Pattern Length: 15
Number of Tries: 3
Size of Dots: 30
Vibration: ON
Stealth: OFF

Fig 4: List of Created Setups for the Conduct of Simulations

The list of parameters for the simulations are shown in Table 1 below.

Table 1: List of Available Parameters for the Setup

Name of Parameter
Number of rows
Number of columns
Length of pattern
Size of dots
Shealth
Number of attempts
Vibration

IV. RESULT

In this work, 90 volunteers were recruited for the experiments; 27 volunteers ran on a 3x3 grid, 29 on a 3x4 grid, and 34 ran on a 4x4 grid. Each volunteer was allowed to have a maximum of 3 attempts. If a volunteer fails after the third attempt, the result is considered unsuccessful. Figure 5 gives the results of the simulations for the 90 volunteers.

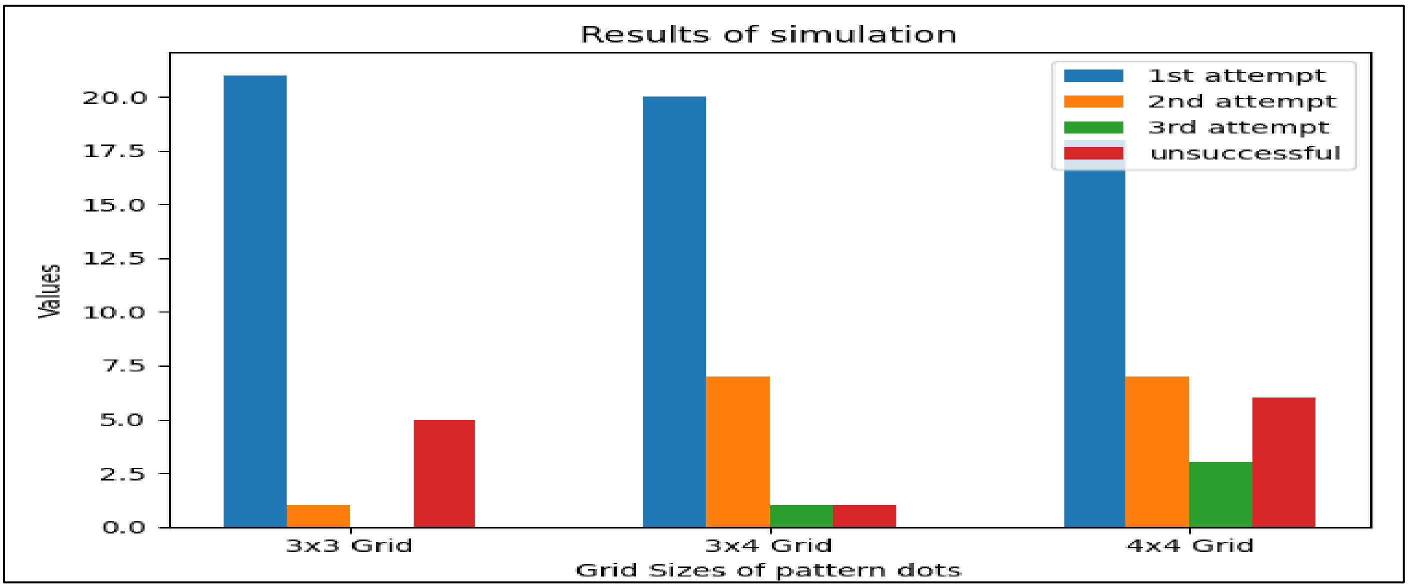


Fig 5: Results of Experiments for the Different Sizes of the Pattern

V. DISCUSSION

Looking at Figure 5, the results show that approximately over 6o percentage of the users were successful in the first attempt in all the grids of 3x3, 3x4, and 4x4. This shows that regardless of the grid size, users still succeed in authenticating. Though the number of unsuccessful attempts is a bit high, still it is approximately below 13 percent (12 users). This indicates the Android pattern lock is generally user-friendly, but there are significant security concerns, as indicated by the failure rate.

VI. CONCLUSION

It is clear from Figure 5 that users are encouraged to create their pattern lock on a high dimensional grid even if the size of the pattern is as small as 4. This will help avert guess and brute force attacks as the number of trials and errors will be highly impracticable. This approach balances usability since users can still create short, memorable patterns with the increased security that comes from making attacks impractical due to the sheer volume of possibilities.

REFERENCES

[1]. H. Khan, U. Hengartner, and D. Vogel, “Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying,” in Symposium on Usable Privacy and Security (SOUPS), Ottawa Canada, 2015.

[2]. W. H. Lee, X. Liu, Y. Shen, H. Jin, and R. B. Lee, “Secure Pick Up: Implicit Authentication When You Start Using the Smartphone,” in SACMAT’17, Indianapolis, IN, USA, 2017.

[3]. F. Schaub, R. Deyhle, and MichaelWeber, “Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms,” in MUM ’12, Ulm, Germany, 2012.

[4]. E. Hjelmas, and B. K. Low, “Face Detection: A Survey,” *Computer Vision and Image Understanding*, no. 83, pp. 236–274, 2001.

[5]. K. Bonsor, and R. Johnson. "How Facial Recognition Systems Work," 15/06/2022, 2022; https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm.

[6]. S. Liu, and M. Silverman, “A Practical Guide to Biometric Security Technology,” *IT Pro*, pp. 27-32, February 2001, 2001.

[7]. X. Jiang, "Fingerprint Classification," *Encyclopedia of Biometrics*, A. Maraikayar, ed., Springer-Verlag Berlin Heidelberg, 2009, pp. 439-446.

[8]. S. C. Dass, and A. K. Jain, “Fingerprint-Based Recognition,” *Technometrics*, vol. 49, no. 3, pp. 262-276, 2007.

[9]. DigitalPersona, "Best Practices for Implementing Fingerprint Biometrics in Applications," *Digitalpersona Camera Manual*, 2009].

[10]. Neurotechnology. "Neurotechnology Company Brochure," 15/05/2022, 2022; https://download.neurotechnology.com/Neurotechnology_Brochure_2022-02-17.pdf.

[11]. V. A. Sujan, and M. P. Mulqueen, “Fingerprint identification using space invariant transforms,” *Pattern Recognition Letters* pp. 609 – 619, 2002.

[12]. C. H. Park, and H. Park, “Fingerprint classification using fastFourier transform and nonlinear discriminant analysis,” *Pattern Recognition*, no. 38, pp. 495–503, 2005.

[13]. M. Harbach, A. D. Luca, and S. Egelman, “The Anatomy of Smartphone Unlocking A Field Study of Android Lock Screens,” in CHI 2016, San Jose, CA, USA, 2016, pp. 12.

[14]. A. Bello, S. Anas, S. Shamsu, and S. P. Zauwali, “Evaluation of the Effectiveness of PIN Code Authentication on Android Smart Devices,” *International Journal of Innovative Science and Research Technology*, vol. 8, no. 10, pp. 483-486, 2023.

[15]. M. D. Nasiru, S. Anas, S. P. Zauwali, and S. Shamsu, “Assessment of the Usability and Acceptability of Passface Authentication Mechanism on Android Phones,” *International Journal of Innovative Science and Research Technology,* vol. 7, no. 11, pp. 2456-2165, 2022.

[16]. H. Khan, U. Hengartner, and D. Vogel, "Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying."

[17]. C. Yongkiatpanich, and D. Wichadakul, “Extractive Text Summarization Using Ontology and Graph-Based Method,” in 2019 IEEE 4th International Conference on Computer and Communication Systems, 2019, pp. 105-110.

[18]. P. Andriotis, T. Tryfonas, and G. Oikonomou, “Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method,” *Information Security Journal: A Global Perspective,* vol. 23, no. 3, pp. 127-137, 2014.

[19]. T. J. Forman, and A. J. Aviv, “Double Patterns: A Usable Solution to Increase the Security of Android Unlock Patterns.,” *arXiv preprint arXiv:2008.10681*, pp. 1-7, 2020.

[20]. A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge Attacks on Smartphone Touch Screens. Proceedings of the 4th USENIX Conference on Offensive Technologies,” in Proceedings of the 4th USENIX Conference on Offensive Technologies, 2010, pp. 1-7.

[21]. J. Zheng, and X. Zhang, “M-Pattern: A Novel Scheme for Improving the Security of Android Unlock Patterns.,” *Journal of Information Security and Applications,* vol. 46, pp. 1-9, 2019.

[22]. K. Boudaoud, M. Winckler, Z. S. Paki, and P. Phalanque, “A Testbed Tool for Comparing Usability and Security of Mobile Authentication Mechanisms,” in 7th International Workshop on ADVANCEs in ICT Infrastructures and Services., Praia, Cape Verde Faculdade de Ciências e Tecnologias" of the University of Cape Verde (UNICV), 2019.