© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718702

Comparative Analysis of Usability and Security Performance of Android Graphical Authentication Mechanisms

UMAR ISAH[1], HASSAN UMAR SURU[2], HUSSAINI UMAR SURU[3]
[1]*Department of Computer Science Education Adamu Augie College of Education Argnugn*
[2] *Department of Computer Science Abdullahi Fodio University of Science and Technology Alerue*
[3]*SLT Department Petroleum Training Institute Effurun, Warri Delta State*

Abstract- ***Mobile authentication systems play a critical role in protecting sensitive information stored on smartphones and other portable devices. Among graphical authentication methods, Android Pattern Lock has gained widespread adoption because of its simplicity and ease of use. However, concerns regarding usability, predictability, and vulnerability to observation attacks continue to raise questions about its effectiveness. This study presents a comparative usability and security analysis of Android Pattern Lock and the Draw-A-Secret (DAS) graphical password scheme based on human characteristics. The study also evaluates the impact of visible and invisible joining node configurations on authentication performance. A mixed-method approach involving questionnaire-based evaluation and experimental analysis was adopted. Data were collected from 60 participants using usability metrics such as authentication time, login success rate, error rate, and perceived ease of use, alongside security metrics including password space, resistance to shoulder surfing, and observability. The results indicate that Android Pattern Lock provides superior usability performance, while DAS demonstrates stronger theoretical security. Visible joining nodes significantly improved usability, whereas invisible joining nodes enhanced perceived security by reducing observation-based vulnerabilities. The findings confirm the existence of a usability and security trade-off in graphical authentication systems and highlight the importance of human-centered considerations in authentication design. The study recommends that mobile authentication mechanisms should balance usability and security to improve both user experience and protection.***

Keywords: Android Pattern Lock, Draw-A-Secret, Graphical Passwords, Usability, Security, Human Characteristics, Mobile Authentication

I. INTRODUCTION

As a result of rapid technological advancement mobile phones have improved in terms of capability, interaction and context of use. The use of mobile phone today isn't limited to simple communication only, but the mobile phone is a multipurpose device where sensitive data are stored that need protection from unauthorized user. The main purpose of an authentication system is to allow access only by legitimate users and prevent unauthorized access.

Authentication therefore serves as a means to determining who gains access to a certain system or resource (Shammee et. al., 2020). User authentication in the area of computing has been a cornerstone of computer security for decades (Conklin et al, 2004).

The exponential growth in technology has made the matter of security a major concern, given the prevalence of attackers, hackers, crackers, scammers and spammers (Pirim et al, 2008). Authentication is therefore a key area in security research and practice (Gao et al, 2009; Velásquez et. al., 2018).

Passwords are the most widely used technique for remote user authentication (Das et al, 2004). A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (Devika & Backiyalakshmi, 2014). It is a preferred method by the majority because it is highly usable and it is relatively inexpensive compared to other means of user authentication e.g. graphic authentication and biometric authentication which is the most secure form of user authentication.

Text-based authentication suffers from both security and usability disadvantages, as increasing number of using multiple account users adopted the habits of reusing single password to multiple accounts for the favor of remembrance which sacrificed security.

Some studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked (Devika & Backiyalakshmi, 2014).

The alternative techniques are graphical passwords and biometrics. But Biometrics techniques have their own disadvantages such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive.

Graphical passwords or graphical authentication systems are password systems that use images rather than characters or numbers in user authentication (Suru & Murano, 2019). Graphical passwords emerged as an alternative solution to textual passwords and it involves a user selecting images or points on an image in a particular order or sequence.

Images are known to create a good user experience (Ajilore et. al., 2021). Android pattern lock screen urges the user to draw a pattern within the limits of a 3×3 nodes grid in order to unlock the device. Users swipe their fingers connecting at least 4 nodes to form their graphical passwords (Andriotis et al., 2016).

Despite their global use and acceptance, Android developers claim that it is possible to bypass the authentication method if USB Debugging Mode is enabled. Android pattern lock suffers from vulnerabilities that can be exploited by popular attacker. The pattern lock screen is getting more popular, which increases the interest to examine its vulnerabilities.

As smartphones contain a large amount of personal and business data, privacy and confidentiality can be breached if an adversary breaks the authentication method. Authentication in mobile devices is inherently vulnerable to attacks and has the weakness of being susceptible to shoulder-surfing attack. Shoulder-surfing attack is a type of attack that uses direct observation techniques such as looking over someone's shoulder to get information (Alsuhibany, 2021). Authentication is therefore a key area in security research and practice (Gao et al, 2009; Velásquez et. al., 2018).

Usability is an essential component of authentication system acceptance and effectiveness. According to Nielsen (1993), systems that are easy to learn, efficient, memorable, and satisfying are more likely to be accepted by users. Similarly, Cranor and Garfinkel (2005) emphasized that authentication systems should achieve a balance between usability and security.

This study therefore investigates the usability and security performance of Android Pattern Lock and DAS while considering the influence of human characteristics and node visibility configurations.

II. LITERATURE REVIEW

2.1 Concept of Graphical Authentication

Authentication is the process of validating the identity of someone or something. It uses information provided to the authenticator to determine whether someone or something is in fact who or what it is declared to be. In private and public computing systems, for example, in computer networks, the process of authentication commonly involves someone, usually the user, using a password provided by the system administrator to logon.

The user's possession of a password is meant to guarantee that the user is three-step process. Firstly, users identify themselves to the mechanism, then they must authenticate themselves and the mechanism authenticates itself.

Lastly, users request information technology resources and the actions they will take and the mechanism will either permit or deny the request based on information held on files that denote the resources and actions a user is permitted to undertake. The means by which users make themselves known to the system is typically through a unique identifier such as a name or an account number. Once the access control mechanism

establishes that it has a valid user, authentication of that user is undertaken (Bryant & Campbell, 2006).

Authentication in mobile devices is inherently vulnerable to attacks and has the weakness of being susceptible to shoulder-surfing attack. Shoulder-surfing attack is a type of attack that uses direct observation techniques such as looking over someone's shoulder to get information (Alsuhibany, 2021). Authentication is therefore a key area in security research and practice (Gao et al, 2009; Velásquez et. al., 2018).

2.2 Text Base Passwords

Text base password is the most common authentication mechanism use to prevent unauthorized users from gaining access to a system. The text base password is PIN and alphanumeric; PIN mostly consist of 4-digit complexity and the latest update 6 digit while Alphanumeric are combination of letters and numbers or specials character which is require from user before authentication.

Text and PINs continue to be the dominant authentication methods in spite of the numerous concerns by security researchers of their inability to properly address usability and security flaws and to effectively combine usability and security (Suru & Murano, 2019). Textual passwords were first popularized in the 1960s as a way to address security concerns that became evident as the first multi-user operating systems evolved.

Though the use of textual passwords has the advantage of usability amongst others, they are susceptible to attacks such as dictionary attacks, brute force attack, hidden cameras and shoulder surfing. This is due to the fact that users tend to choose simple and easy passwords which make it easy for attackers to penetrate access (Preußner et al., 2009).

Even in cases where users choose complex textual passwords especially where there is a need for unique and multiple ones, there is the challenge of memorability (Medlin et al., 2008). The memorability issues experienced in textual passwords have made many users keep the same password across various platforms, which isn't really safe. In a recent study, over 50% of respondents confirm to use same password across platforms/applications (Arogundade et. al., 2020).

The password-based approach to user authentication has a number of shortcomings that can undermine the efficacy of computer system security (Bryant & Campbell, 2006).

There are many different methods used to compromise password security, some of which are unsophisticated requiring little or no technical knowledge while others require a high level of technical expertise. Unsophisticated techniques include guessing, observing, viewing written records, being told, tricks and artifice and even sifting through rubbish bins. Other methods that require a high level of expertise include keyboard monitoring, packet interception, keystroke interception, host emulation and so on.

As a result of the drawbacks associated with the use of textual passwords, Greg Blonder in 1996 introduced the concept of graphical passwords (Blonder, 1996).

2.3 Graphical Based Authentication Techniques

Graphical password techniques have been proposed to address shortcomings of traditional text-based password techniques since images are more straightforward to recall than texts (Yahia et al., 2021). In Graphical Based Authentication Technique, a user creates a password by first entering a picture he or she chooses at the time of registration.

The pictures are stored in the database. As soon as the option of pictures is clicked, they are retrieved from the database and are displayed to the user.

The user chooses one of the images from number of images band then chooses several points of interest regions in the image. Each point of interest, is described by a circle (center and radius).

For each point of interest, the user types a word or phrase which will be combined with points of interest. If the user does not type any text after selecting POI then that POI is combined with an empty string. The user can choose either to enforce

the order of selecting POIs (stronger password), or to make the order insignificant.

Graphical password techniques demonstrate that the techniques can be grouped into four categories. A Recognition-based technique, Pure Recall-Based techniques, Cued Recall-Based and Hybrid (Perrig et al., 1999)

2.3.1 Recognition Based Technique

Recognition based graphical authentication systems are graphical systems that depend on the user's ability to recognize images selected earlier from a large collection of images at the registration stage (Suru & Murano, 2019).

In each round of authentication, the user is presented with many images from which one is expected to recognize and correctly select the images that represent one ‘s chosen password. Several recognition-based schemes have been developed and evaluated Dunphy and Yan, (2007) proposed a graphical authentication scheme based on the Hash Visualization Technique (Perrig et al., 1999).

Figure 2.1 Déjà vu (Touraj, 2015)

In their system, users are prompted to select a specific number of images from a set of randomly generated pictures. Subsequently, users must identify these pre-selected images to complete the authentication process. The study revealed a success rate of 90% for participants using this technique, surpassing the 70% success rate achieved with traditional text-based passwords.

However, it's crucial to note certain weaknesses in this approach. One notable drawback is the requirement for the server to store the seeds of users' portfolio images in plain text, posing potential security risks. Additionally, the process can be perceived as tedious and time-consuming.

From a security standpoint, recognition-based systems might not be optimal replacements for traditional text passwords, given their password space's cardinality, comparable to that of 4- or 5-digit PINs. This assumes the use of a set of images with a reasonable cardinality concerning usability. Proposed recognition-based systems employ various image types, including faces, random art, everyday objects, and icons.

Passfaces concept was developed by Real User Corporation (2007) is a graphical password authentication system that relies on users recognizing human faces as a means of authentication. Instead of traditional alphanumeric passwords or PINs, Passfaces presents users with a grid of faces during login, and the user must identify a pre-selected set of faces to gain access.

While Passfaces has been considered as a potentially more secure alternative to traditional password systems, like any authentication method, it has its own set of strengths and weaknesses. The effectiveness of graphical password systems, including Passfaces, may depend on factors such as the size of the face grid, the variability introduced during authentication, and user preferences. Passfaces is not suitable for individuals with prosopagnosia (face-blindness).

Logging in with Passfaces typically requires more time compared to textual passwords. Comparative studies conducted by Davis et al. (2004) revealed that users' choices in Passfaces are significantly influenced by factors such as gender, race, and the attractiveness of the faces. This influence makes Passfaces passwords potentially predictable to attackers.

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718702

Figure 2.2: Passfaces system (Davis 2004)

2.3.2 Pure Recall-Based Graphical Passwords

The pure recall-based systems also called draw metric systems. The system requires users to memorize and reproduce their secret drawings which were drawn or selected earlier on a blank canvas or on a grid during the registration process (Robert et al., 2012).

In pure-recall systems, passwords are usually generated and recalled without memory cue. There are a number of graphical password algorithms which are designed by using pure recall-based methods. Pure recall-based schemes are many in literature today and vast majority of these schemes were presented as improvements of Draw-A-Secret (DAS) which is the first of its kinds.

In DAS, password is a free-form drawing produced on a 5x5 grid and the same secret drawing is recalled and reproduced during authentication to gain access to secure resource. Since both registration and authentication processes simply depend on drawings, DAS system is said to be alphabet independent and as such the scheme is accessible to users of any language for applications.

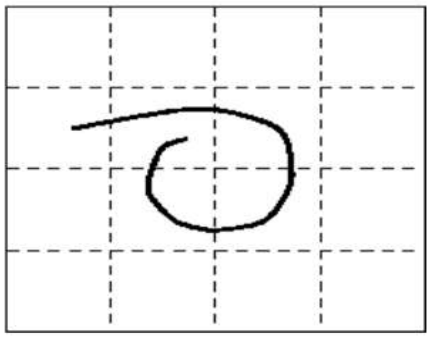

Figure 2.3: Jermyn et al (1999)

Draw A Secrete: Jermyn et al. proposed a scheme; known as Draw a secret (DAS) is a representative graphical password scheme. Rigorous theoretical analysis suggests that DAS supports an overall password space larger than that of the textual password scheme (Dunphy & Yan, 2007) the system is based on a two-dimensional grid, in which users are required to draw something to represent their password and each of the grid's coordinates is stored in the order drawing was made. For authentication, user needs to redraw the picture with the proper sequence at the same grids' coordinates, before authentication.

The advantage of these techniques Users is provided with a freedom to draw a password as long as they wish moreover there is no need to transfer images through network thereby reducing traffic loads, and the server-side graphical database storage.

Password space of grid-based schemes is better than traditional textual passwords. The weakness of this technique is vulnerable to guessing attack, shoulder surfing attack.

Thorpe and van Oorschot (2004) conducted an analysis of the memorable password space associated with the graphical password scheme introduced by Jermyn et al. They introduced the concept of graphical dictionaries and explored the potential vulnerability to brute-force attacks using such dictionaries. The researchers established a length parameter for DAS-type graphical passwords and demonstrated that DAS passwords with a length of 8 or more on a 5 x 5 grid might be less susceptible to dictionary attacks compared to textual passwords.

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718702

Additionally, they highlighted that the space of mirror-symmetric graphical passwords is considerably smaller than the full DAS password space. Given that people tend to recall symmetric images better than asymmetric ones,

Figure 2.4. Draw A Secrete

It was anticipated that a significant portion of users would opt for mirror-symmetric passwords. This observation raised concerns about the security of the DAS scheme, suggesting that it might be substantially lower than initially perceived. To address this issue, employing longer passwords is a viable solution.

Thorpe and van Oorschot's research indicated that the size of the space of mirror-symmetric passwords, with a length of about L + 5, surpasses that of the complete password space for corresponding lengths of L <= 14 on a 5 x 5 grid. Furthermore, Thorpe and van Oorschot delved into the impact of password length and stroke-count as complexity properties of the DAS scheme. Their findings highlighted that stroke-count has the most substantial influence on the DAS password space.

The size of the DAS password space experiences a significant reduction with fewer strokes for a fixed password length. While the length of a DAS password also plays a significant role, its impact is not as pronounced as the stroke-count. To enhance security, Thorpe and van Oorschot proposed a technique known as "Grid Selection." This involves an initially large, fine-grained grid from which the user selects a drawing grid a rectangular region to zoom in on—wherein they can enter their password. Implementing this technique could notably increase the DAS password space.

SIGNATURE TECHNIQUES

Syukri et al., (1998) propose techniques where a user will draw his signature, this technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature. After that, the system conducts verification using geometric average means and a dynamic update of the database.

The disadvantage of this technique is the forgery of signatures. Drawing with mouse is not familiar to many people; it is difficult to draw the signature in the same perimeters at the time of registration. (Robert et al., 2012)

Figure 2.5: Signature Techniques (Syukri et al., 1998)

2.3.3 Cued-Recall Systems

Cued-recall systems typically require that users remember and target specific locations within an image. This feature, intended to reduce the memory load on users, is an easier memory task than pure recall (Robert et al. 2012).

This memory task differs from simply recognizing an image as a whole. Some exiting research shows that people retain accurate, detailed, visual memories of objects to which they previously attended in visual scenes; this suggests that users may be able to accurately remember specific parts of an image as their password if they initially focused on them. In an ideal design, the cue in an authentication system is helpful only to legitimate users (not to attackers trying to guess a password).

2.4 Mobile Devices Authentication

Mobile authentication is the verification of a user's identity through the use of a mobile device and one or more authentication methods for secure access. Mobile devices become more powerful and compact; they have become a necessity for modern users.

Because of the devices' portability, users are able to use them to handle their daily tasks such as managing bank accounts, accessing social media, answering personal e-mails, or connecting to a virtual private network (VPN) when they are away from their desks.

Many of these tasks involve accessing of private information; therefore, mobile devices are often protected with passwords to prevent others from accessing the information. Android devices require a secure authentication scheme in order to control access to the device. The most common Authentication schemes for android mobile device include pin, pattern-based authentication, biometric authentication.

2.4.1 Biometrics Authentication Scheme

Biometric systems refer to use of any human traits and characteristics such as fingerprints, palm scan, iris scan, facial scan and DNA in authentication. Gait and gaze based biometric systems have also been developed (Suru & Murano 2019). The term biometrics refers to any variety of identification techniques, which are based on some physical, or behavioural characteristics of the individual, contrasted with those of the wider population Coventry et al. (2003). Unique digital identifiers are created from the measurement of the characteristic.

Physiological biometrics techniques include those based on the verification of fingerprint, hand and/or finger geometry, eye (retina or iris), face, wrist (vein), and so forth. Behavioural techniques include those based onvoice, signature, typing behaviour, and pointing. New voice biometrics would place it in the physiological rather than behavioural category.

All biometrics approaches follow a similar operation: a digital template is created during an enrolment process, then the template is stored in a database. On attempted verification, the relevant template is extracted and compared with the data input, say in the form of a fingerprint, or an acquired iris image, for positive identification.

Biometric authentication is often referred to as the secret weapon of authentication mechanism, due to the fact that it cannot be forgotten (Coventry et al.2003). Biometrics have recently become a popular authentication option for smartphones (De Luca et al., 2015). While they solve many of the security and usability problems of previous authentication mechanism, they also have some shortcomings.

Besides privacy issues, rearchers showed that some biometric systems can be tricked with relatively simple methods (Findling & Mayrhofer, (2013). In addition, users may perceive these systems as being insecure or awk- ward to use in specific situatio. Thus, getting biometrics right is hard and important: if a mechanism is seen as low-effort and secure, users may be motivated to protect their devices when they otherwise would not (De Luca et al. 2015).

The alternative techniques are graphical passwords and biometrics. But Biometrics techniques have their own disadvantages such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted.

The major drawback of this approach is that such systems can be expensive and the identification process can be slow to address these issues which lead to the proposal for graphical passwords (Harbach et al., 2016). There has also been significant research effort to solve existing security problems of smartphone authentication. However, for any of these alternative methods to be successfully adopted, a detailed understanding of how users interact with existing smartphone authentication mechanisms is highly needed (Harbach et al. 2016).

2.4.2 Android Graphical Authentication

The android smartphone has emerged as an excellent platform for graphical passwords because its intuitive interaction with the touch screen in contrast to text-based passwords on mobile devices. Graphical passwords on mobile devices seem like a natural fit, as they often require direct manipulation of visual elements.

For avoiding unwanted access on smartphones, different locking mechanisms are provided. The history of locking mechanisms was often a solution solely to prevent accidental use while current mobile phones require protection to secure the potentially vast amount of private data that we keep on our smartphones. The situation of our active use of

mobile phones, as well as its well-suited platform for using a graphical password, makes authentication on mobile devices an interesting field of study.

The Android operating system are being known for the graphical password called Pattern Lock released by Google in 2008. (Andriotis et al., 2016) This graphical password scheme is at this time available on all Android devices, as well provided on other mobile operating.

The Android Pattern Lock is one of the commonly used screen locks mechanisms on Android devices. For unlocking a device using pattern lock, the user is asked to draw a user-defined sequence of connected dots on a 3×3 grid. Such path is called a lock pattern and is presented in. When creating a pattern, Google has designed several rules for creating a pattern: the Pass-Go scheme Tao and (Adams, 2008).

The method is based on the introduction of nodes (indicators) that help users to form edges and well-defined lines (very similar to the pattern lock). Recent proposals aim to enhance the security of graphical passwords facilitating haptic parameters such as pressure and velocity to the final authentication schema (Orozco, et al., 2006).

Others try to distinguish different drawing styles based on the user's personality (Gao, et al.,2008). The rules for the creation of an Android pattern are simple. The pattern must connect atleast 4 nodes.

Its length cannot exceed 9 nodes given that a node can be visited only once. In addition, the pattern will always connect the first node, which is along its path. This means that it is not feasible to 'jump' over a node. Finally, a pattern can cross an already visited node to connect a neighbour node. Some vulnerabilities of the Android pattern lock screen were exposed in (Aviv, et al.,2010).

With the use of a camera, smudge attacks were performed on smartphone screens to recover traces and oily residues left by their owners. The overall password space of the authentication scheme was also calculated. (Using brute force methods).

The authors in (Andriotis, et al., 2013) replicated these experiments and were particularly interested in human factors that might affect the choice of a pattern. They investigated the occurrence of specific attributes such as sub-patterns and starting points and combined smudge attacks with their conclusions to reveal patterns drawn on smartphones.

Uellenbeck et al., (2013) studied the actual user choices of patterns with a large-scale user study. They evaluated the strength of the patterns and argued that even a small change in the pattern layout can make the authentication more secure.

2.5 Usability and Security

As the joke's continuing popularity demonstrates, many people believe that there is an inherent tradeoff between security and usability. A computer without passwords is usable, but not very secure. On the other hand, a computer that requires you to authenticate every 5 minutes with your password and a fresh drop of blood might indeed be very secure, but nobody would want to use it.

The human Characteristics of the intended users must be taken into account when designing or selecting an appropriate authentication mechanism. The expertise level of target users may dictate the acceptable complexity of the interaction, and the level of training required or expected (Robert et al., 2012).

The frequency of use may also have a significant influence on usability. Frequently accessed systems should be quick to use, and may rely more heavily on users' memory, as frequent repetition aids memory. If passwords are used for infrequently accessed systems, they must be especially memorable since memory decays.

Security mechanisms are designed to make things difficult for attackers: thus, any system that improves usability must ensure security. As design goals, security and usability have many aspects in common. Both require a holistic approach and a vision that system architects, developers, and marketers share.

Rarely is security or usability successfully sprinkled on at the end of a product's development: instead, both must be designed and built in from the

beginning. But because security and usability are different skills, it's generally harder and more expensive to build systems that are both secure and usable In recent years, there has been a growing realization that usability problems are hindering security efforts.

A small but growing group of researchers have dedicated themselves to working at the interface between security and usability an interface that has come to be called human-computer interaction and security (HCI-SEC).

Interaction Conference was perhaps the first formal event devoted to discussions of usable security. This was followed by a birds-of-a-feather session at the 2003 Usenix Security conference and a July 2004 Workshop on Usable Privacy and Security Software (WUPSS) held at Rutgers University's DIMACS center.

These events show that HCI-SEC is gaining legitimacy as a separate and legitimate field of study.

More than 80 researchers and students attended WUPSS, which included two days of formal presentations along with a third day of informal, smallgroup discussions.

Participants came from a variety of disciplines, including security, privacy, software engineering, HCI, and psychology. Speakers identified numerous open problems and suggested a variety of approaches ranging from preliminary proposals to examples of implemented systems. Virtually all computer users come face-to-face with a leading HCI- SEC problem when they try to use an ATM, listen to messages on their cell phone's voicemail system, or access their email: an increasing proliferation of passwords.

Individuals are asked to remember dozens of unique passwords, all of which are supposed to be difficult to guess, yet easy to remember, to make matters worse, they're often frequently required to change their passwords have been proposed as another possible solution to the password problem. But little work has been done to demonstrate that graphical password schemes are actually secure and usabble.

2.6 Human Characteristics and Authentication Performance

Human characteristics play an important role in authentication usability and security. Factors such as age, experience, familiarity with mobile devices, and cognitive ability influence user interaction with authentication systems.

Card et al. (1983) emphasized that human performance is strongly affected by cognitive processing and interaction design. Recent research has also shown that experienced smartphone users generally authenticate faster and commit fewer errors compared to inexperienced users.

The influence of human characteristics on authentication performance highlights the need for user-centered authentication design.

III. METHODOLOGY

A mixed-method research design combining experimental evaluation and questionnaire-based data collection was adopted for this study. The mixed-method design ensures both quantitative reliability and qualitative depth, providing a comprehensive understanding of how human characteristics influence Android lock usability and security (Creswell & Creswell, 2018; Yin, 2022).

Sixty participants were selected using purposive sampling. Participants were required to perform authentication tasks using Android Pattern Lock and DAS under visible and invisible joining node conditions.

Usability metrics measured include:

- Mean creation time
- Mean login time
- Login success rate
- Error rate
- Perceived ease of use

Security metrics measured include:

- Password space
- Resistance to shoulder surfing
- Observability
- Smudge attack vulnerability
- Perceived security

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718702

Data collected were analyzed using descriptive statistics including mean scores, percentages, and comparative analysis.

IV. RESULTS AND DISCUSSION

Table 1: Comparative Usability Analysis of Android Pattern Lock and DAS

The table 1 presents a comparative analysis of key usability metrics between Android Pattern Lock and the Draw-A-Secret (DAS) graphical password scheme. The comparison focuses on performance indicators such as creation time, login time, success rate, error rate, and perceived ease of use, in order to evaluate the relative efficiency and user-friendliness of the two authentication methods.

Table 4.1: Comparison of Usability Metrics

Metric	Android Pattern Lock	DAS (Draw-A-Secret)
Mean Creation Time (sec)	4.21	6.35
Mean Login Time (sec)	2.37	3.89
Login Success Rate (%)	94%	86%
Error Rate (Avg.)	0.3	0.9
Ease of Use (5-point scale)	4.3	3.5

The results indicate that Android Pattern Lock outperformed DAS in all usability metrics.

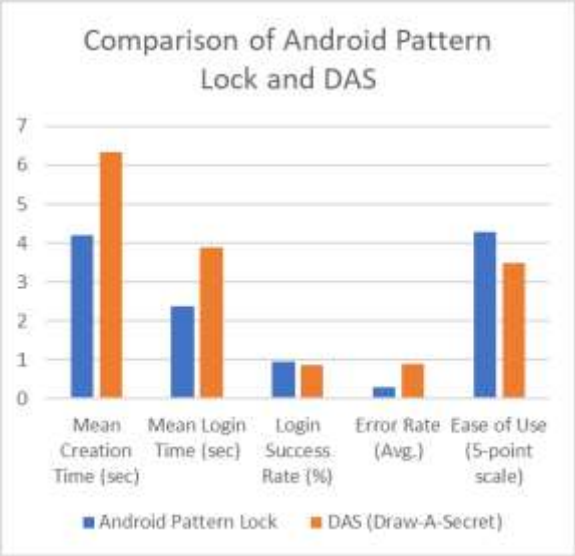

Figure 4.1 Comparison of Android Pattern Lock and DAS

Android Pattern Lock recorded a mean creation time of 4.21 seconds, whereas DAS recorded 6.35 seconds. This indicates that participants were able to create authentication patterns more quickly using Android Pattern Lock than DAS. The shorter creation time suggests that Android Pattern Lock is easier to learn and configure. This may be attributed to its structured 3×3 grid layout and users' prior familiarity with the system. In contrast, DAS requires free-form drawing, which increases the cognitive effort needed during password creation.

The mean login time for Android Pattern Lock was 2.37 seconds, compared to 3.89 seconds for DAS. This shows that participants authenticated more quickly using Android Pattern Lock. Faster login time reflects better usability and efficiency. The higher login time in DAS suggests that recalling and reproducing free-form drawings is more time-consuming than tracing a structured pattern. Android Pattern Lock achieved a login success rate of 94%, while DAS recorded 86%.

This indicates that users were more successful in correctly authenticating using Android Pattern Lock. A higher success rate reflects better memorability and ease of use. The lower success rate in DAS suggests that users experienced more difficulty recalling their passwords accurately.

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718702

The average error rate for Android Pattern Lock was 0.3, whereas DAS recorded 0.9. This implies that users made fewer mistakes when using Android Pattern Lock. The higher error rate in DAS further supports the notion that free-form drawing introduces complexity, making it more prone to user errors.

On a 5-point Likert scale, Android Pattern Lock recorded a mean score of 4.3, while DAS recorded 3.5. This shows that participants perceived Android Pattern Lock as easier to use compared to DAS. According to the scale interpretation, Android Pattern Lock falls within the "high usability" range, while DAS falls within the "moderate usability" range.

4.2 Security Comparison Table: Pattern Lock vs DAS

Table 4.2: Comparative Analysis of Security Performance

Metric	Android Pattern Lock	DAS (Draw-A-Secret)
Password Space	Limited (3×3 grid, constrained patterns)	Large (free-form drawing space)
Resistance to Brute-Force Attack	Moderate	High
Resistance to Shoulder Surfing	Moderate	High
Pattern Predictability	High (common patterns)	Low (less predictable)
Smudge Attack Vulnerability	High	Moderate
Observability (Trace Visibility)	High	Low
Perceived Security (5-point scale)	3.4	4.2

The Table 4.2 presents a comparative evaluation of the security performance of Android Pattern Lock and the Draw-A-Secret (DAS) graphical password scheme. Android Pattern Lock demonstrates moderate security due to its limited password space and predictable pattern structures. The use of a fixed 3×3 grid restricts the number of possible combinations, making it more susceptible to brute-force and guessing attacks.

Additionally, the visibility of pattern traces during input increases its vulnerability to shoulder-surfing and smudge attacks. In contrast, DAS exhibits stronger security characteristics. Its free-form drawing mechanism allows for a significantly larger password space, which enhances resistance to brute-force attacks. The absence of structured constraints makes user-created passwords less predictable, thereby reducing the likelihood of successful guessing attacks.

Furthermore, DAS provides better protection against observation-based attacks such as shoulder-surfing, as patterns are less visually traceable compared to Android Pattern Lock. This is supported by the lower observability and reduced pattern trace visibility associated with DAS. Overall, the results indicate that DAS provides higher theoretical and perceived security than Android Pattern Lock, although this comes at the cost of reduced usability.

The perceived security ratings also indicate that participants considered DAS to be more secure than Android Pattern Lock. This perception may be influenced by the complexity and flexibility of the DAS system.

Table 2: Comparative Analysis of Visible and Invisible Joining Nodes

Metric	Visible Joining Nodes	Invisible Joining Nodes
Mean Creation Time (sec)	5.21	6.08
Mean Login Time (sec)	2.37	3.12
Login Success Rate (%)	94%	87%
Error Rate (Avg.)	0.3	0.8
Ease of Use (5-point scale)	4.4	3.6

The mean creation time for visible joining nodes was 5.21 seconds, while invisible joining nodes recorded 6.08 seconds. This indicates that participants were able to create patterns more quickly when visual feedback was available.

The shorter creation time suggests that visible nodes reduce cognitive effort during pattern formation. In contrast, invisible nodes require users to rely more on memory and spatial recall, leading to increased time during pattern creation. The mean login time for visible joining nodes was 2.37 seconds, compared to 3.12 seconds for invisible joining nodes.

This shows that authentication is faster when users can see the pattern being traced. Visible nodes provide immediate visual guidance, allowing users to complete authentication efficiently. The increased login time in the invisible condition reflects the additional mental effort required to recall and reproduce the pattern without visual cues. Visible joining nodes achieved a success rate of 94%, whereas invisible joining nodes recorded 87%. This suggests that users were more successful in correctly authenticating when visual feedback was present.

The lower success rate in the invisible configuration indicates that the absence of visual cues negatively affects memorability and accuracy. The average error rate for visible joining nodes was 0.3, while invisible joining nodes recorded 0.8.

This demonstrates that users made significantly fewer errors when using visible nodes. The higher error rate in the invisible configuration further confirms that lack of visual feedback increases the likelihood of mistakes during authentication. On a 5-point Likert scale, visible joining nodes recorded a mean score of 4.4, while invisible joining nodes recorded 3.6. This indicates that participants perceived the visible configuration as easier to use. Based on the scale interpretation, visible nodes fall within the high usability range, whereas invisible nodes fall within the moderate usability range.

Metric	Visible Joining Nodes	Invisible Joining Nodes
Resistance to Shoulder Surfing	Moderate	High
Pattern Trace Visibility	High	Low
Perceived Security (5-point scale)	3.5	4.3
Observation Attack Risk	Higher	Lower

The invisible joining node configuration demonstrated higher perceived security compared to the visible mode. Participants believed that invisible nodes offer better protection against shoulder surfing attacks due to the absence of visible pattern traces.

Visible joining nodes, while easier to use, expose the pattern path during authentication, making them more vulnerable to observation attacks.

V. JUSTIFICATION OF FINDING

The lower usability performance of the Draw-A-Secret (DAS) scheme can be explained by its reliance on free-form recall, which increases cognitive effort. This supports earlier work by Jermyn et al. (1999) and is reinforced by more recent findings that recall-based graphical passwords often introduce usability challenges despite offering stronger theoretical security (Yahia et al., 2021).

Furthermore, the higher perceived security associated with DAS is justified by its larger password space and less predictable structure. This aligns with security principles emphasizing complexity as a defense against brute-force and guessing attacks (Anderson, 2008). Recent research also highlights that users often associate complexity with higher security, even when usability is reduced (Golla et al., 2017; Uellenbeck et al., 2013).

The findings on node visibility configurations are also supported by both classical and contemporary

studies. Visible joining nodes improve usability by providing visual feedback, while invisible nodes reduce the risk of shoulder-surfing attacks by minimizing observable traces (Aviv et al., 2010; Andriotis et al., 2016). This reinforces the usability–security trade-off concept widely discussed in usable security research (Cranor & Garfinkel, 2005; Alqahtani & Mohammad, 2020).

VI. SUMMARY

This study examined the usability and security performance of Android graphical authentication mechanisms through comparative analysis and experimental evaluation. The study focused on Android Pattern Lock, Draw-A-Secret (DAS), and visible joining node and invisible joining node configurations.

The findings revealed that Android Pattern Lock demonstrated higher usability performance than DAS across several metrics, including authentication time, login success rate, error rate, and perceived ease of use. Participants were able to create and recall patterns more efficiently using Android Pattern Lock due to its structured design and familiarity.

The study further showed that DAS provides stronger theoretical security because of its larger password space and lower predictability. However, its usability was lower due to increased cognitive effort required for pattern recall and reproduction.

The comparison between visible and invisible joining nodes indicated that visible nodes improve usability by reducing authentication time and error rate. Invisible nodes, on the other hand, improve perceived security by reducing pattern visibility during authentication.

VII. RECOMMENDATIONS

Based on the findings of this study, the following recommendations are proposed:

1. Mobile device developers should prioritize authentication mechanisms that balance usability and security to improve user acceptance and protection.
2. Android Pattern Lock should be enhanced with additional security measures to reduce vulnerabilities associated with predictable patterns and observation attacks.
3. Invisible joining node configurations may be recommended for security-sensitive environments where protection against shoulder-surfing is important.
4. User education should be encouraged to improve awareness of secure pattern creation practices and reduce the use of predictable authentication patterns.
5. Mobile authentication systems should incorporate adaptive security mechanisms that adjust according to user context and risk level.

CONCLUSION

This study evaluated the usability and security performance of Android graphical authentication mechanisms through a comparative analysis of Android Pattern Lock, Draw-A-Secret (DAS), and node visibility configurations. The findings revealed that Android Pattern Lock provides superior usability performance compared to DAS.

Participants completed authentication tasks more quickly, achieved higher login success rates, committed fewer errors, and reported greater ease of use when using Android Pattern Lock. These results suggest that structured graphical interfaces improve efficiency and user interaction.

In contrast, DAS demonstrated stronger theoretical security due to its larger password space and reduced predictability. However, its free-form drawing mechanism introduced greater cognitive load, resulting in lower usability performance. This indicates that higher security complexity may negatively affect user convenience and task performance.

REFERENCES

[1] Alsuhibany, S. A. (2021). A Camouflage Text-Based Password Approach for Mobile Devices against Shoulder-Surfing Attack. Security and Communication Networks, 2021. https://doi.org/10.1155/2021/6653076

[2] Alqahtani, F., & Mohammad, R. (2020). Usability and security evaluation of graphical password authentication methods. International Journal of Advanced Computer Science and Applications, 11(6), 451–460. https://doi.org/10.14569/IJACSA.2020.0110657

[3] Andriotis, P., Oikonomou, G., Mylonas, A., & Tryfonas, T. (2016). A study on usability and security features of the Android pattern lock screen. Information and Computer Security, 24(1), 53–72. https://doi.org/10.1108/ICS-01-2015-0001

[4] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge attacks on smartphone touch screens. Proceedings of the 4th USENIX Workshop on Offensive Technologies, 1–7.

[5] Bryant, K., & Campbell, J. (2006). User Behaviours Associated with Password Security and Management. Australasian Journal of Information Systems, 14(1). https://doi.org/10.3127/ajis.v14i1.9

[6] Card, S. K., Moran, T. P., & Newell, A. (1983). The psychology of human-computer interaction. Lawrence Erlbaum Associates.

[7] Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability and biometric verification at the ATM interface. Conference on Human Factors in Computing Systems - Proceedings, 153–160. https://doi.org/10.1145/642611.642639

[8] Creswell, J. W., & Creswell, J. D. (2022). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (6th ed.). Sage Publications.

[9] De Luca, A., Hang, A., Von Zezschwitz, E., & Hussmann, H. (2015). I feel like i'm taking selfies all day! towards understanding biometric authentication on smartphones. Conference on Human Factors in Computing Systems - Proceedings, 2015-April (April), 1411–1414. https://doi.org/10.1145/2702123.2702141

[10] Devika, S., & Backiyalakshmi, R. (2014). Design and Analysis of User Identification for Graphical Password System. 5(1), 486–489.

[11] Dunphy, P., & Yan, J. (2007). Do background images improve "draw a secret" graphical passwords? Proceedings of the ACM Conference on Computer and Communications Security, 36–47. https://doi.org/10.1145/1315245.1315252

[12] Findling, R. D., & Mayrhofer, R. (2013). Towards secure personal device unlock using stereo camera pan shots. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8112 LNCS (PART 2), 417–425. https://doi.org/10.1007/978-3-642-53862-9_53

[13] Golla, M., Dürmuth, M., & Karame, G. (2017). On the security of smartphone unlock patterns. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 37–52. https://doi.org/10.1145/3133956.3133982

[14] Harbach, M., De Luca, A., & Egelman, S. (2016). The anatomy of smartphone unlocking a field study of android lock screens. Conference on Human Factors in Computing Systems - Proceedings, 4806–4817. https://doi.org/10.1145/2858036.2858267

[15] Nielsen, J. (1993). Usability engineering. Academic Press

[16] Preußner, J., Rudnik, Y., Brehm, H., Völkl, R., & Glatzel, U. (2009). Original Research Article. International Journal of Plasticity, 25(5), 973–994. http://www.sciencedirect.com/science/article/pii/S074964190800065X

[17] Real User Corporation, Passfaces TM http://www.realuser.com, Accessed on January 2007.

[18] Robert, B., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4). https://doi.org/10.1145/2333112.2333114

[19] Shammee, T. I., Akter, T., Mou, M., Chowdhury, F., & Ferdous, M. S. (2020). A Systematic Literature Review of Graphical Password Schemes. Journal of Computing Science and Engineering, 16(4), 163–185. https://doi.org/10.5626/JCSE.2020.14.4.163

[20] Syukri, A. F., Okamoto, E., & Mambo, M. (1998). A user identification system using

signature written with mouse. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1438(January 1998), 403–414. https://doi.org/10.1007/bfb0053751

[21] Uellenbeck, S., Dürmuth, M., Wolf, C., & Holz, T. (2013). Quantifying the security of graphical passwords: The case of Android unlocks patterns. Proceedings of the ACM Conference on Computer and Communications Security, 161–172. https://doi.org/10.1145/2508859.2516700

[22] Umar Suru, H., & Murano, P. (2019). Security and User Interface Usability of Graphical Authentication Systems – A Review. International Journal of Computer Trends and Technology, 67(2), 17–36. https://doi.org/10.14445/22312803/ijctt-v67i2p104

[23] Yahia, H. S., Zeebaree, S. R. M., Sadeeq, M. A. M., Salim, N. O. M., Kak, S. F., AL-Zebari, A., Salih, A. A., & Hussein, H. A. (2021). Comprehensive Survey for Cloud Computing Based Nature-Inspired Algorithms Optimization Scheduling. Asian Journal of Research in Computer Science, 8(2), 1–16. https://doi.org/10.9734/ajrcos/2021/v8i230195

[24] Zhang, Z., Wu, D., Li, L., & Gao, D. (2022). On the Usability (In)Security of In-App Browsing Interfaces in Mobile Apps. arXiv. https://arxiv.org/abs/2209.01568