International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 01 | Jan 2021 www.irjet.net p-ISSN: 2395-0072

# A COMPARATIVE STUDY OF GRAPHICAL PASSWORD METHOD (I.E. PATTERN) AND ALPHANUMERIC PASSWORD METHOD(I.E. PIN) FOR MOBILE DEVICE AUTHENTICATION

**Shweta Shankar Wader**

*Student, Department of Information Technology, Keraleeya Samajam(REGD.) Dombivli's Model College, Maharashtra, India*

---

**Abstract -** *Authentication is the process that verifies the identity of a user or method(process). Authentication can be performed using alphanumeric passwords and graphical passwords. Alphanumeric passwords contains both letters and numbers as well as special characters whereas graphical passwords consists of an image used as a password. Mobile devices like smartphones and tablets are widely wont to perform security critical and privacy sensitive activities like mobile banking, mobile health care, mobile shopping, etc. Screen locks are utilized in mobile devices to guard sensitive in-formation. Graphical password and alphanumeric password are two common sorts of screen locking methods. The alphanumeric password scheme has shown some downside in terms of security and usability. For example, a user may pick a simple to recollect alpha-numeric password which will even be easy to guess. On the contrary, if as user picks a password that's hard to guess it's going to even be hard to recollect. Several alternative password mechanisms have been introduced. Graphical password is one among them, and it's supported pictures or patterns. However, graphical password is also vulnerable to certain types of security breaches and malware attacks. This study mostly takes a note of user's preferences and their behaviour towards these two methods .This is an comparative study of graphical password method i.e. pattern and alphanumeric password method i.e. PIN(Personal Identification Number) in terms of security, performance, usability and retention.*

***Key Words*: Authentication, Alphanumeric password, Graphical Password, Pattern, PIN, Usability**

## 1. INTRODUCTION

Humans are often considered the weakest link in ICT (information and communication technology) security. Patrick, Long, and Flinn (2003) [1] recognizes and pin points the three security areas for which human factor issues are very important: 1.authentication (passwords), 2. Security operations (intrusion detection) and 3. Developing secure systems (developing the security).

In order to build an efficient and feasible authentication there is a need to strike a balance be-tween usability and security. Generally user authentication consists of three factors: a. what the user knows; b. what the user has; and c. what the user is. The authentication methods in this study are based on what the user knows (knowledge-factor). Based on knowledge-factor, different authentication methods have been proposed over the years. Alphanumeric passwords are the most commonly used passwords but they have some flaws as well. Previous studies have shown that users have a tendency to choose short alphanumeric passwords which are easier to recall (Adams and Sasse 1999) [2] but these passwords can be easily guessed. On the other hand, if an alphanumeric password is hard to guess, then it is often hard to remember and retain as well (Suo, Zhu, and Owen 2005)[4]. Graphical password has been introduced as an substitute for alphanumeric password. The idea behind graphical password is that users can remember pictures better than text. Human psychology supports such assumption (Shepard 1967)[5]. At present, four-digit PIN(personal identification number) is considered the most popular password among device authentication methods. This method comes under the category of alphanumeric password scheme. Now-a-days pattern lock is getting popularity amongst the Android OS users (Aviv et al. 2010)[6] which is a graphical password scheme named which requires traversing an on-screen 3 × 3 grid of contact points. This paper presents a comparative study between graphical (Pattern) and alphanumeric password scheme in terms of performance and security. The primary question is as follows: Are graphical passwords competitive to alphanumeric passwords in terms of security, performance, usability and retention?

## 3. BACKGROUND/LITERATURE REVIEW

Mobile devices contain various type of sensitive personal
information such as SMS, text messages, mails, application, app
data, music, images, and so much more. This leads to security risk considering all the confidential information at one place. One way to avoid and

prevent the security breaches is to use the screen lock methods, which provides authentication on our mobile devices. Alphanumeric password scheme has some security and usability drawbacks such as: a difficult password is hard to retain, and a short password is easy to guess. Some researchers have developed graphical passwords as a substitute to text password to cover up the drawbacks of guessing attacks and making it easy to recall or retain but it has its drawbacks as well. This arises the question of which mobile authentication method serves the main purpose better in terms of usability and security as well as performance and retention. Chiang and Chiasson (2013)[7] also described the password length and password strength as security criteria. Persuasive cued click points (PCCP), is a technique proposed by Chiasson et al. (2012)[8]. They describe that graphical password is effective in terms of memorability and supply benefits over alpha-numeric passwords because images are often used as cues for various passwords. They also stated graphical pass-words are easy to find out but typically require longer login time. An extensive research has been wiped out the search for re-placing passwords for web authentication (Bonneau et al. 2012)[9]. This paper offers excellent and accurate information for comparative evaluation of authentication schemes. They enlist 11 sorts of alternative password methods, like biometrics recognition, graphical password (PCCP), etc. that can a good substitute for alphanumeric password. They categorize usability benefits of a perfect authentication scheme into 8 proper-ties: 1.memorywise-effortless, 2. scalable-for-users, 3. easy-to-learn, 4.efficient-to-use, 5. infrequent-errors, etc. Furthermore, a perfect authentication scheme should have following security benefits: a. resilient to physical observation, b. resilient to guessing, c. resilient to theft because the measurement to match each password scheme with alphanumeric password. A comparative study is required to work out advantages and drawbacks between graphical and alphanumeric password schemes on mobile devices.

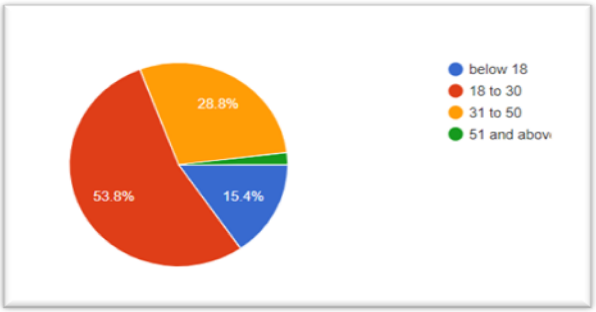
## 4. METHOD AND MATERIALS

Quantitative and qualitative methods were selected for this particular research. Primary and Secondary research method was performed for this paper. Secondary research or desk research is a type of research that involves using pre-existing data. Secondary research includes research material published in research reports, journals and similar documents. These documents are often made available online and offline by libraries, websites, online journals etc. . Secondary research method involves re-analysing, interpreting, or reviewing past data. Secondary research was performed using qualitive data sets. This type of secondary data is employed once you want the previously-collected information to tell your current research. It is particularly used when you want to test the information obtained through qualitative research by implementing a quantitative method. Questionnaire method was used for survey. Answers obtained through closed-ended questions with multiple choice answer options are analysis may involve pie-charts, bar-charts and percentages and answers obtained through open ended questions are involved in qualitative research. Qualitative method provides answers to 'why?' and 'how?'. Qualitative research discussions are determined by respondent's opinions, feedback and feelings .A Google form was used to collect data.

## 5. DATA AND RESULTS:-

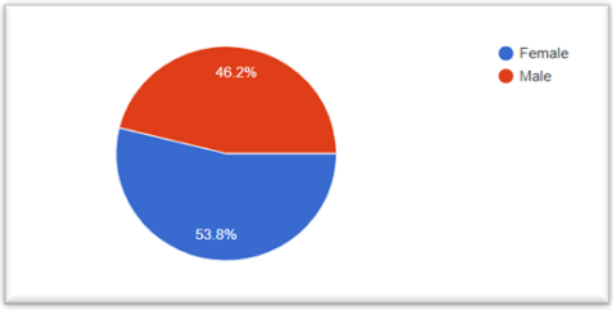
A small survey was conducted to analyze the preference of users between the two methods: Pattern and PIN and also the reason of their preference. There were total 52 participants in the survey which were of different age groups. Summary of the responses:

1. Age (52 responses): 8 participants belongs to age group below 18. 15 participants belong age group 31 to 50 .28 participants were 18 to 30 age group. 1 participant belong to age group 51 and above.



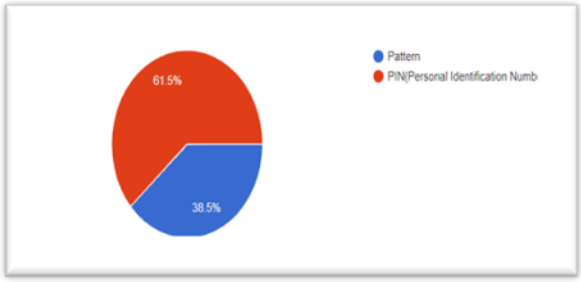

2. Gender(52 responses)

28 participants were female and 24 participants were male.




3. Which method do you prefer to lock your screen on your mobile (52 responses)

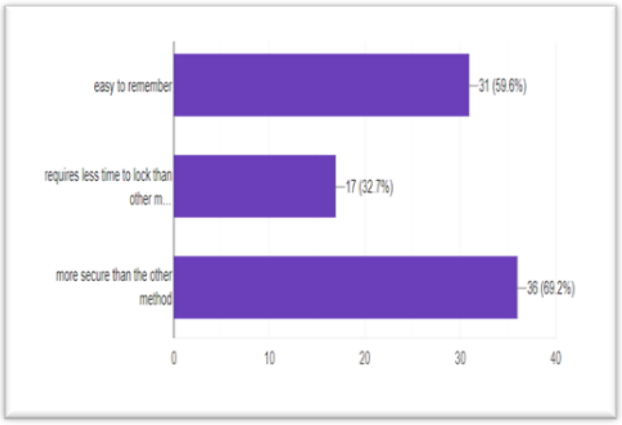
32 (61.5%) participants preferred PIN and 20(38.5%)preferred Pattern




4. Reason for your preference (52 responses)

This question included answers in checkboxes.

| Reason for your preference | Number of participants |
|---|---|
| Easy to remember | 31 |
| Requires less time than other method | 17 |
| More secure than other method | 36 |




The data collected from the survey which was conducted for the research paper "A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication" (Mohd Anwar and Ashiq Imran; Department of Computer Science North Carolina A&T State University) is also referred[3]. Analysis of data collected from user tasks and survey responses to spot usability issues and user preferences when using graphical passwords on mobile devices. Analyzing the effect of screen size on login performance by comparing differences between Android mobile devices and tablet on creation time and login time for every scheme. For the creation time and login time, t-tests were used to work out whether there are significant differences for various devices. All the t-tests are performed at 95% confidence interval (i.e., the α-value is about at 0.05). The password creation time is measured from the time between first touch on mobile devices to the touch the submit button. Comparison of pattern creation time and PIN creation time for both tablet and phone was conducted.. When calculated unpaired t-test of PIN creation time for both tablet and phone the result is not significant. . The pattern on the tablet takes the very best time among other comparison. The login time is measured because the time for successful login into the mobile device. Comparison for both pattern and PIN in mobile device of various size using unpaired t-test for four cases. Calculation of t-test of login time of pattern and PIN for separately and alongside tablet and phone. When measuring login time, user reset treated as fail attempts. Unsignificant result for login time between pattern and PIN schemes was observed. The results show the pattern takes slightly less time to log in on phone, and PIN takes slightly less time on tablet.

## 6. DISCUSSIONS

From the conducted survey is observed that majority participants(32 participants) opted for PIN and comparatively less people (20)opted for Pattern.

From the reason of preference question it is clear that majority people choose security over difficulty. This means that people were choosing difficult passwords to remember so as to not compromise with the security.

Less people were concerned about the time requirement as there was not significant difference between the both for the people.

Observations were drawn from the secondary research as well. Observations were as follows:

Login time is depends on the length of pattern password. The longer the pattern the more time it takes to login whereas PIN has fixed length of digits so it's login time is consistent

The creation time required for PIN password is slow when compared to the creation time of pattern in Android mobile phone.

Observations and data from secondary resources showed that, the majority of the people preferred security to usability. A brute-force attack against a specific password would involve exhaustively searching the password space( an indicator of the security strength of a password scheme is the total number of possible passwords, is called possible password space.).

The login time is less for people who use same pattern/PIN for different devices than people who use different pattern/PIN

## 7. CONCLUSION

In this paper, comparison of the security, performance, usability and retention of pattern and PIN passwords as screen lock methods is studied. In the paper through the survey, observations and secondary research it can be concluded that people prefer security over usability. In this paper secondary data is gathered about creation time and login time mobile devices(tablet and mobile phone). It was observed that more number of people were on the side of strong PIN and comparatively less people opted strong pattern.

Limitations and future work: Like any other study, there are is a limitation to this research that should be noted. ▪ Initially the link was sent to more than 80 people out of which only 52 responded. While the data is enough to make the conclusions which I did, the results should not be generalized. This study is limited to few research papers and online journals. In the future, a large-scale study can be conducted to check the criteria such as: usability, security, retention and performance.

Suggestions: No matter what screen lock method you implement there are chances of security breaches. So the best way to guard your phone is to use both PIN and Pattern. Also PIN and password is more reliable because it gives you much more space to create entropy (lack of order or predictability). For one, you have the full alphabet, all the numbers and various symbols at your disposal.

## 8. ACKNOWLEDGEMENTS

I would like to express my special thanks of gratitude to all my teachers for their able guidance and support in completing my research.

I also like to extend my gratitude to all respondents for their responses without which this study would not have been successful.

## 9. REFERENCES

[1] Patrick, A.S., Long, A.C., Flinn, S. 2003. HCI and security sys-tems. In Proceedings of the CHI 2004, 1056-1057, New York, NY: ACM Press.

[2] Adams, A., and Sasse, M.A. 1999. Users are not the enemy. Communications of the ACM 42(12): 40-46.

[3] Mohd Anwar and Ashiq Imran ;Department of Computer Science North Carolina A&T State University "A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication ".April 2015 Conference: Modern Artificial Intelligence & Cognitive Science Conference

[4] Suo, X., Zhu, Y., and Owen, G.S. 2005. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference (ACSAC), 463-472, Tucson, AZ: IEEE Press

[5]Shepard, R.N. 1967. Recognition memory for words, sentences, and pictures. Journal of verbal Learning and verbal Behavior 6(1): 156-163

[6]Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., and Smith, J.M. 2010. Smudge attacks on smartphone touch screens. In WOOT, 10, 1-7, Berkeley, CA: USENIX Association

[7] Chiang, H.-Y., and Chiasson, S. 2013. Improving user authentication on mobile devices: A touchscreen graphical password. In Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services, 251-260, Munich, Germany: ACM press.

[8] Chiasson, S., Stobert, E., Forget, A., Biddle, R., and Van Oorschot, P.C. 2012. Persuasive cued click-points: Design, im-plementation, and evaluation of a knowledge-based authentica-tion mechanism. Dependable and Secure Computing, IEEE Transactions on 9(2): 222-235.

[9] Bonneau, J., Herley, C., Van Oorschot, P.C., and Stajano, F. 2012. The quest to replace passwords: A framework for compara-tive evaluation of web authentication schemes. In Proceeding of Security and Privacy (SP) IEEE Symposium on, 553-567, San Francisco, CA: IEEE Press