Random Graphic User Password in Mobile Device

Prajakta Bhangale [1], Crystal Wilson Dsouza[2], Jasmine Angel Stalin[3]& Mary Elizabeth Sundaraj[4]
[1]Project Guide,[2,3,4]Students
[1,2,3,4]Mumbai University, FR. Conceicao Rodrigues College of Engineering,

Abstract : Nowadays, smart phones are used, so authentication is necessary here. So to keep the system secure, we have come up with an idea of random graphic pattern generator. Just like smart phones there will be patterns, user allows drawing their pattern on a two-dimensional 3 X 3 matrix using more than one lines. There will be pin and patterns. The pin will remain same but number sequence will keep changing. To make a system more secure random graphic pattern is used. The user needs to first select a pin (minimum 4 digit). Then based on the pin the user needs to draw a pattern. Next time if the user logs-in, the pin remains same, but number sequence keeps changing (by randomly changing the fixed position of the digital graphics that shows on the touch screen). To login to the system one time, the user will get only 5 chances after 6th entry of the password the system will get blocked automatically.

Keywords: Authentication, Password, Security, Graphical Pattern, Smart Phone, secured system.

I. Introduction

Nowadays, mobile devices like smartphones are used everywhere, so authentication plays an important role here[1]. There should be security too. Weak pin has some disadvantage. We have come up with an idea of random graphic pattern. In this case, just like smart phones there will be patterns, user allows drawing their graphical password on a two-dimensional 3 X 3 matrix using more than one lines. Our idea is to propose a new graphic pattern for system i.e. mobile as well as a system, by randomly changing the fixed positions of the digital pattern that shows on the system, the user will be able to draw different pattern by clicking on the digital graphic pattern everytime based on the same unique pin. The user usually enters in the password based on his or her personal details or draws a simple graphic pattern on the touch screen as passwords for unlocking the lock screen. Although this might help the user to remember the password but, nowadays technology has so much developed that anyone can hack the system. To make a system secure random pattern is used. The user needs to first select a pin. Then based on the pin the user needs to draw a pattern. Next time if the user logs-in, the pin remains same, but number sequence keeps changing (by randomly changing the fixed position of the digital graphics that shows on the touch screen). To login to the system one time, the user will get only 5 chances after 6th entry of the password the system will get blocked automatically. Data and information on devices are maintained confidentially. Easy to remember, hard to guess. Secures the bank account from hackers by blocking the account, when the phone is lost. Graphical passwords removes different attack. used in application's like Banking and accessing accounts. Emails. Although graphical authentication has advantages compared to password methods, however the shoulder surfing problem. Networks and databases of companies and industries. Personal systems. ATM machines. Web-login applications. The pin will remain same but number sequence will keep changing

II. Problem definition

Nowadays, smart phones are used, so authentication are important here. So to keep the system secure, we have come up with an idea of random graphic pattern generator. just like smart phones there will be patterns, user allows drawing their pattern on a two-dimensional 3 X 3 matrix using more than one lines. There will be pin and patterns. The pin will remain same but number sequence will keep changing. The user usually enters in the password based on his or her personal details or draws a simple graphic pattern on the touch screen as passwords for unlocking the lock screen[1]. Although this might help the user to remember the password but, nowadays technology has so much developed that anyone can hack the system. To make a system secure random pattern is used. The user needs to first select a pin (minimum 4 digit). Then based on the pin the user needs to draw a pattern. Next time if the user logs-in, the pin remains same, but number sequence keeps changing (by randomly changing the fixed position of the digital graphics that shows on the touch screen). To login to the system one time, the user will get only 5 chances after 6th entry of the password the system will get blocked automatically.

III. existing system

One of the proposed based on the pin authentication but also uses one-time password of pattern [1] mobile as well as a system, by randomly changing the fixed positions of the digital pattern that shows on the system, the user will be able to draw different pattern by clicking on the digital graphic pattern everytime based on the same unique pin. The user usually enters in the password based on his or her personal details or draws a simple graphic pattern on the touch screen as passwords for unlocking the lock screen. Although this might help the user to remember the password but, nowadays technology has so much developed that anyone can hack the system. To make a system more secure random graphic pattern is used. The authorized user needs to select a pin (minimum 4 digit). Then based on the pin the user needs to draw a pattern. Next time if the user logs-in, the pin remains same, but number sequence keeps changing (by randomly changing the fixed position of the digital graphics that shows on the touch screen). To login to the system one time, the user will get only 5 chances after 6th entry of the password the system will get blocked automatically. Data and information on devices are maintained confidentially. Easy to remember, hard to guess. Secures the bank account from hackers by blocking the account, when the phone is lost. Graphical passwords removes different attack. To provide authentication, if the user log's-in next time the password will be same but, pattern will keep changing. To login to the system one time, the user will get only 5 chances after 6th entry of the password the system will get blocked automatically.

IV. PROPOSED SYSTEM

Smart phones are used nowadays, so authentication is important here. So to keep the system secure, we have come up with an idea of random graphic pattern generator. just like smart phones there will be patterns, user allows drawing their pattern on a two-dimensional 3 X 3 matrix using more than one lines. There will be pin and patterns. The pin will remain same but number sequence will keep changing. To make a system more secure random graphic pattern is used. The user needs to first select a pin (minimum 4 digit). Then based on the pin the user needs to draw a pattern. Next time if the user logs-in, the pin remains same, but number sequence keeps changing (by randomly changing the fixed position of the digital graphics that shows on the touch screen). To login to the system one time, the user will get only 5 chances after 6th entry of the password the system will get blocked automatically.

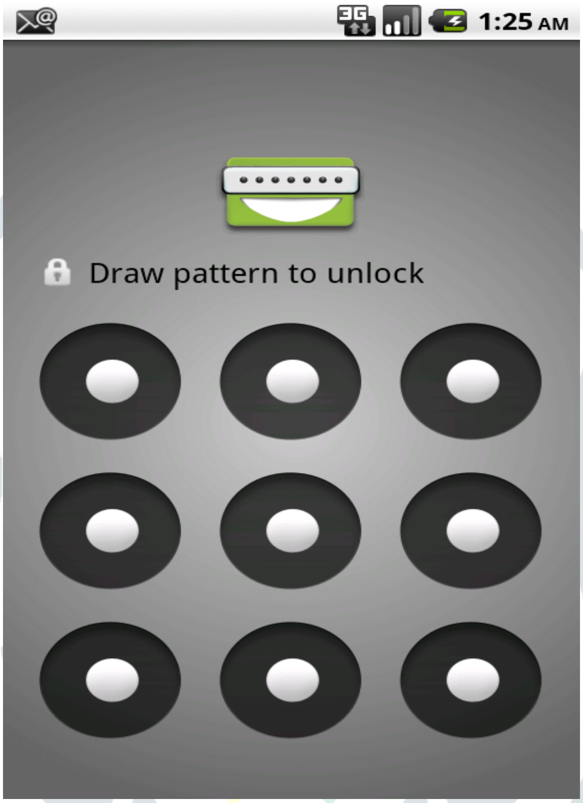

Figure 1 Keypad [1]

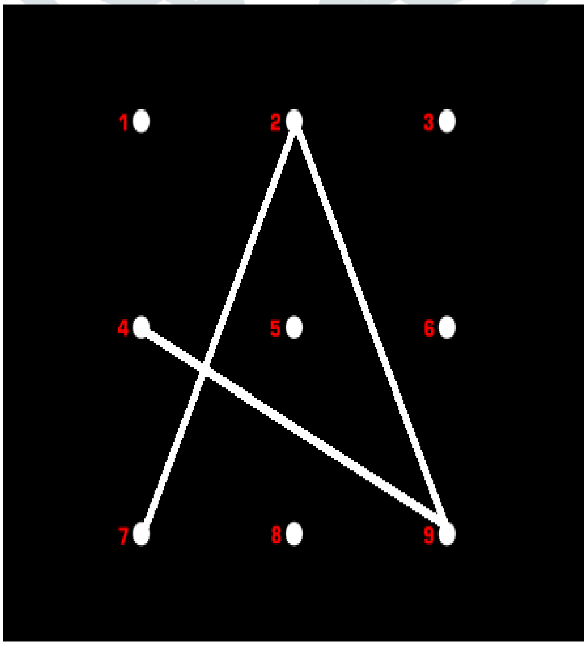

Figure 2 graphical user interface keypad [1]

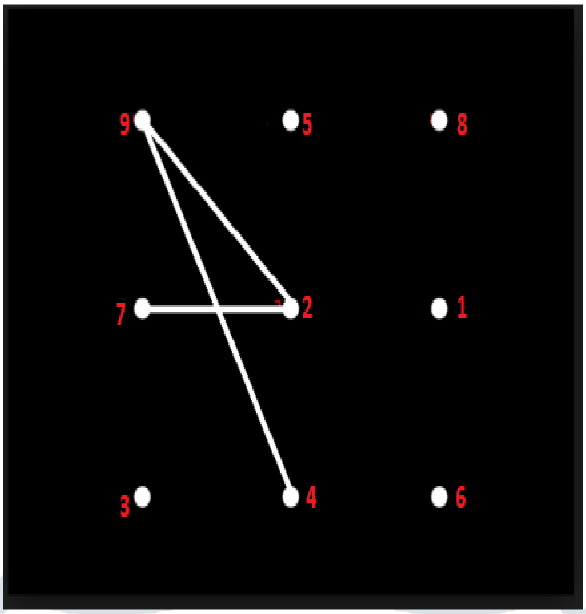

Figure 3 Graphical user interface keypad

V. OBJECTIVES

Our idea is to propose a new graphic pattern for protection of system, by randomly changing the fixed positions of the pattern that shows on the system, the user will be able to draw different pattern by entering the pin everytime based on the same unique pin. Then a user allows drawing their graphical password on a 3 X 3 matrix using more than one lines.. Authentication phase can provide the strong protection against various attack because of the uncertainty of digit number position in 3 X 3 matrixs which generated one-time pattern[2]. Meanwhile, the user graphical pattern can be calculated by the mobile device fornot much of the processing time. To provide authentication, if the user log's-in next time the password will be same but, pattern will keep changing. To login to the system one time, the user will get only 5 chances after 6th entry of the password the system will get blocked automatically. Data and information on devices are maintained confidentially. Easy to remember, hard to guess. Secures the bank account from hackers by blocking the account, when the phone is lost. Graphical passwords removes different attack. used in application's like Banking and accessing accounts. Emails. Although graphical authentication has advantages compared to password methods, however the shoulder surfing problem. Networks and databases of companies and industries. Personal systems. ATM machines. Web-login applications. The pin will remain same but number sequence will keep changing.

VI. CONCLUSION

The goal of the security measure is to create a pattern which will ensure the safety of the Users resources by just adding a pin and the number sequence for pattern will keep changing. This is the main concern for any organization and users too which wants to protect their confidential data from intruders. So, we have taken up the project of random Graphical patterns. These types of patterns are a trend which will be replacing the textual passwords by graphical patterns.

VII. REFERENCE

[1] Shen, S.-S., Kang, T.-H., Lin, S.-H., & Chien, W. (2017). *Random graphic user password authentication scheme in mobile devices. 2017 International Conference on Applied System Innovation (ICASI). IEEE Access,* doi:10.1109/icasi. 2017.7988123

[2] Sudha, R., & Shanmuganathan, M. (2017). *An Improved Graphical Authentication System to Resist the Shoulder Surfing Attack. 2017 International Conference on Technical Advancements in Computers and Communications (ICTACC). IEEE Access,* doi:10.1109/ictacc.2017.23

[3] Gupta, D. (2017). *A new approach of authentication in graphical systems using ASCII submission of values. 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE Access,* doi:10.1109/iwcmc. 2017.7986483

[4] Kaja, S., & Gupta, D. (2017). *Graphical password scheme using persuasive cued click points. 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon).*doi:10.1109/smarttechcon. *IEEE Access,* 2017.8358450

[5] Alhothaily, A., Hu, C., Alrawais, A., Song, T., Cheng, X., & Chen, D. (2017). *A Secure and Practical Authentication Scheme Using Personal Devices. IEEE Access, 5, 11677–11687.*doi:10.1109/access.2017.2717862