A STUDY ON "AN EVALUATION OF AUTHENTICATION METHODS USED IN SMARTPHONES"

Roseland Peter Assistant Professor, Naipunnya Institute of Management and Information Technology, Pongam, Thrissur, Kerala
Dona Varghese. Student B.Com (Finance) Batch 2018-21, Naipunnya Institute of Management and Information Technology, Pongam, Thrissur, Kerala

Abstract: User authentication with Smartphone is more and more envisaged for applications on the internet and electronic transactions. A recent survey showed that over 50% of smartphone users grab it immediately after waking up. As smartphone embeds more and more personal information and is used as preferred device accesses, distant services a strong authentication is necessary for logical access control. PIN code authentication is a common solution is simple it does not constitute a strong identity proof as anybody looking at the user typing it could use it. In order to solve this problem biometrics is more and more used to increase the level of confidence of user authentication. Nevertheless, biometric data is sensitive and requires a particular attention in terms of security and privacy. The study is taken to assess commonly used user authentication mechanisms on smart phones focusing security and usability. Also to identify influence of new inventions in the screen lock authentication systems among different group of people.

Keywords: Authentication, smart phone

Introduction

Smartphone is used not only as a communication device but also for storing personal data, some of which are sensitive to be accessed by others. Therefore the smart phone manufactures provide some security features to protect smart phones from unauthorized accesses. The operating systems on smart phones such as Android, Blackberry OS, IOS, and Windows phone provide the unlock screen mechanism with various type of authentication methods that are different on each platform. There are difference in the behaviour and characteristics of users for different smartphones. Companies wanting their products and services to be widely used would need more information on the use of smartphones and the user's behaviour in order to be able to create strategies in a variety of mobile devices. The use of authentication methods on smartphones is important because among the factors which are considered when selecting a handset is the security features which occupy the second place after battery life. By knowing the characteristics of the users, smartphone companies will be able to customize the types of authentication methods offered to the users based on their needs. Currently, one of the most common authentication mechanisms is based on the use of passwords. This is due its ease of implementation for the Service Providers (SPs), cost effectiveness and its familiarity to end-users. Authentication and authorization are two of the most important security features for mobile transaction systems.

Statement of the problem

In this section we explain the ways to authenticate the users and the types of authentication mechanisms developed using them, in the context of smartphone. More specifically, we present the assessment of commonly used user authentication mechanisms on smartphones focusing on the security and usability.

Objectives of the study

- To determine the user behaviour based on the perceived security and convenience, as well as the preference for different types of authentication methods.
- To identify the influence of new inventions in the screen lock authentication systems among different group of people.
- The dependence on smart phones for storing important files secured by biometric authentication

Review of literature

1. Usman Naeem, Yasar Amin (2018): Smart phones are inescapable devices, which are becoming more and more intelligent and context aware with emerging sensing, networking, and computing capabilities.

They offer a captivating platform to the users for performing a wide variety of tasks including socializing, communication, sending or receiving emails, storing and accessing personal data etc. at anytime and anywhere. Commonly used approaches for searching mobile devices are password, PIN, pattern lock, face recognition and fingerprint

2. M Inoue, T Ogawa (2018): Security technology on mobile device is increasingly more important as smartphones are becoming more versatile and, thus, store more sensitive information. Among the three indispensable factors of owner authentication technologies on mobile devices, security, usability and system efficiency, usability is considered the key factor.

3. Jose Maria Jorquera Valero, Pedro Miguel (2018): Continuous authentication systems for mobile devices focus on identifying users according to their behavior patterns when they interact with mobile devices. Among the benefits provided by these systems, we highlight the enhancement of the system security, having permanently authenticated the users; and the improvement of the user's quality of experience, minimizing the use of authentication credentials.

Research Methodology

Both primary and secondary data are used for the study. A well- structured questionnaire is used for collecting primary data. Secondary data is collected from journals, articles, books and E-sources. Non – Probability samples used in this research is the convenience sampling .Percentage analysis is used for analysing the data..

Data Analysis and Discussion

Sl NO	Data Analysis		Frequency	Percentage
1	Age	10-20 Years	13	21.6
		20-30 Years	46	76.7
		30-50 Years	Nil	Nil
		Above 50 Years	1	1.7
2	Mobile Phone Brands used by respondents	Nokia	1	1.7
		Samsung	12	20
		i Phone	6	10
		Asus	1	1.7
		Vivo	4	6.7
		Oppo	5	8.3
		Redmi	15	25
		Honor	1	1.7
		Ingnix	1	1.7
		Others	14	23.2
3	Period of usage of smart phone	Less than 1 Year	14	23.3
		1-2 Year	12	20
		2-4 Year	15	25
		Above 4 Years	16	26.7
		Others	3	5
4	Additional measures used to protect the smart phones in particular situations	I leave my phone in a safe place	12	20
		I conceal my phone in my clothes	4	6.7
		Others	11	18.3
5	The type of screen lock used by respondents	Pin/Password/Pattern	25	41.7
		Finger Print	28	46.7
		Face lock	3	5
		Others	4	6.6
6	Whether storing important data in smart phones is a	Yes	37	61.7
		No	23	38.3

	good thing			
7	The quality of payments through smart phones	Good	55	91.7
		Bad	5	8.3
8	The medium for payment through smart phones	Application	41	68.3
		Website	12	20
		Others	7	11.7
9	Application used for payments	Google Pay	27	45
		Phone Pay	9	15
		Pay tm	7	11.7
		Not even used any	9	15
		Others	8	13.3
10	The authentication methods to protect these applications	Pin/Password/ Pattern	39	65
		Finger print	14	23.3
		Face lock	3	5
		Others	4	6.7
11	The usability and security of following Pin/Password pattern	Usability		
		High	21	35
		Medium	33	55
		Low	6	10
		Security		
		High	25	42
		Medium	29	48
		Low	6	10
12	The usability and security of following Biometric Security System	Usability		
		High	22	36.7
		Medium	30	50
		Low	8	13.3
		Security		
		High	20	33.3
		Medium	31	51.7
		Low	9	15
13	The system where fingerprint authentication carried by	Knowledge based System	11	18.3
		Biometric System	34	56.7
		Don’t Know	15	25
14	Whether respondent use forgot password facility while unlocking the smart phones	Yes always	8	13.3
		Sometimes	25	41.7
		Never	27	45
15	The accessibility of pin/password by the respondents	Yes	38	63.3
		No	3	5
		Maybe	19	31.7
16	The period of changing the password	Daily	12	20
		Weekly	4	6.7
		Monthly	15	25
		More than 1 month	29	48.3
17	The problems faced by respondents while unlocking the pattern	Device getting locked for 30 seconds or more	23	38.3
		It may be hang for sometimes	8	13.3
		No problems faced	29	48.4
18	Whether any difficulties	Yes	13	21.7

	faced while using face lock	No	18	30
		Sometimes	29	48.3
19	The problems faced while unlocking face lock	It will not open while using spectacles	6	10
		When eyes closed	14	24
		When smiling	4	6
		Others	36	60

- From the above table it can be understood that 21.7% of the respondents are in the age group of 10-20 years, 76.7% of respondents are in age group of 20-30 years, zero percentage in 30-50 age group and the remaining 1.7% are in the age group of above 50 years.
- From this table, it is understand that the brands of smartphones, used by the respondents. Out of 60 respondents 1.7 percent of the respondent are using Nokia, 20 Percent of them using Samsung, 10 percent of them are using IPhone, 1.7 percent are using Asus, 6.7 percent are using Vivo, 8.3 percent are using Oppo, 25 percent are using Redmi, 1.7 percent of the respondent are using Honor, 1.7 percent are using Infinix, 23.2 percent of the respondents are using other brands.
- From this table, it shows the period of usage of the smartphone. It shows, 23.3 percent of respondents are under below 1 year category. 20 percent of them are under the category of 1 to 2 years. 25 percent are come under the category of 2 to 4 years, 26.7 percent of them are under the category of above 4 years and the remaining people are come under the category of others.
- This table shows the additional measures used in smartphone for protection in particular situation. 20 percent of the respondents leave in their phone in a safe place before going somewhere. 55 percent of them enable a screen lock for this situation. 6.7 percent of them conceal their smartphone in their clothes or in a bag. And the remaining 18.3 percent of them take other measures other than these.
- The above table shows 41.7 percent of the respondents use Pin/Password/Pattern as their screen lock. 46.7 percent of them uses finger print as their screen lock .5 percent of of them uses face lock and 6.6 percent uses others as their screen lock.
- The table shows storing important files in smartphone is a good thing or not. 61.7 percent of the respondent's support it, 38.3percent neglects it.
- The table above shows the quality of online payment through smartphone. 92 percent of them make good response and the remaining 8 percent shows bad response.
- From the above table we can see that 45.2 percent of respondent are using Google Pay application for online payment. 15.5 percent of them uses Phonepe application. 11.9 percent of them uses Paytm application 14.3 percent of the people did not use any application. And 13.1 percent uses other application other than these.
- In the above table we can understand that 68.3 percent of the respondents use application and 20 percent respondent's uses website for payment and the remaining 11.7 percent are using other.
- It shows the authentication methods used to protect the applications used for online payment. Out of the 60, 65 percent of them are using Pin/Password/Pattern 23.3 percent of them uses fingerprint 5 percent uses face lock and the remaining 6.7 percent of them uses other techniques or not used.
- From the above table it can understand that 35 percent of the respondents says that the usability of Pin/Password/Pattern is high, 55 percent of respondent says that the usability is medium and 10 percent says that usability is low. Then, it can understand that 42 percent says that the security of Pin/Password/Pattern is high, 48 percent says medium and 10 percent says it is low.
- From the above table, it can understand that, 36.7 percent of respondents say that the usability of biometric system is high, 50 percent of them says usability is medium and 13.3 percent of them says it is low. Then, 33.3 percent of respondents say that the security of biometric authentication system is high, 51.7 percent says security is medium and 15 percent says it is low.
- In the above table shows the respondents knowledge on the fingerprint authentication system 18.3 percent of them chooses knowledge based system 56.7% of them chooses biometric system and 25% of them did not know about it.

- In the above table shows whether the respondent forgot password facility while unlocking the smartphone. 13.3 percent of the respondent always uses the facility, 41.7 percent of them uses that for sometimes only. 45 percent of them never uses that facility.
- In the table shows the easy accessibility and remaining of Pin/Password by the respondents 63.3 percent them can easily access and remember their password. But 5 percent of them cannot easily access and remember their password. And 31.7 percent of them are not sure about it.
- In the above table shows the period of changing the password. 20 percent of respondents daily change the password. 6.7 percent of them weekly changes the password. 25 percent of them monthly changes the passwords. 48.3 percent of them uses a password more than 1 month.
- In the above table shows the problems faced by the respondents while unlocking the pattern. 38.3 percent of the respondent's device getting locked for 30 seconds or more. 13.3 percent of them tells that their phone may hang for sometimes. 48.4 percent of them says there is no problems faced by them while unlocking the pattern.
- In the above table, it shows whether the respondents face any difficulties. 21.7 percent of them face difficulties. 30 percent face no difficulties and 48.3 percent of them are facing difficulties for sometimes.
- In the table shows the problems faced while unlocking face lock. 10 percent of them says that their face lock will not open while using spectacles, 24 percent of them says that it will not open when eyes closed. 6 percent of them says that will not open when smiling. 60 percent of them says that they are facing other problems.

Findings

- Majority of the respondents are come under 20-30 year's age category.
- Out of 60 respondents most of them are using Redmi.
- It can be understood that most of them are using smartphone come under the category of above 4 years and less than 1 year.
- From the 60 respondents, half of them are enable screen lock and choose a harder pattern as additional measures to protect the smartphone in particular situations.
- Out of 60 respondents, majority of them are using fingerprint authentication as screen lock and Pin/Password/Pattern also a commonly used method.
- From the details, almost 61.7% of the respondents say that storing important files in smartphone is good thong.
- Most of the respondent in the 60, says that online payments through mobile phone is good and it has good quality also.
- 68.3% of the respondents choose application for payment through smartphones.
- Google pay is the commonly used application for mobile payment and some of them did not use these application.
- Out of the 60 respondents, most of them use pin/password/pattern authentication methods to protect these applications.
- Out of 60 respondents, most of them says that the usability and security of pin/password/pattern is medium.
- Majority of the 60 respondents, says that the usability and security of biometric system is medium.
- From the 60 respondents, most of them uses screen lock security system for both purpose of convenience and security.
- From the 60 respondents, most of them say that fingerprint system come under biometric system.
- Under the 60 respondents, almost every one of them says that their pin/password/pattern is memorable and accessible one.
- From the 60 respondents, most of them says that they never used the 'forgot password' facility in their smartphone.
- Out of the 60 respondents, most of them uses a password more than one month.

- Out of the 60 respondents, most of them not faced any problems while unlocking the pattern.
- Majority of them uses the face lock for sometimes.
- While users face the problem that face lock will not open because of other problems.

Conclusion

In this context, it is clearly identified that in this modern world the protection of a smartphone is very necessary. From the study it is understand that almost 90% of people are using smartphone consider valuable property because they store their important files and everything in the smartphone.so, it must be protected. For this purpose, there are some authentication methods are available. There is Pin lock, Password, Pattern lock, fingerprint authentication, face lock, voice lock etc.to protect smartphone. People can select proper screen lock for protection. Although multimedia smartphones have become very popular among the general public thanks to their simple portability and various convenient features, the risk of important data loss due to phone loss or theft by a third party has also increased. For these reasons, uses of multimedia smartphones employ the built in locking features in the multimedia smartphone. However, typical locking features have low security strength and are vulnerable to the shoulder surfing and smudge attacks, where passwords can be determined easily.

References

1. Ametinger J and Roland S 2012 Secure and Usable Authentication on Mobile Devices MoMM, 10th International Conference on Advances in Mobile Computing & Multimedia, 257-262

Ben-Asher N et al 2011 On the Need for Different Security Methods on Mobile Phones. Proc. 13th Int'l Conf. Human Computer Interaction with Mobile Devices and Services (MobileHCI), 465-473

2.Final Report-INFS5261 Hans –Joachim,Jelana Mirkovie, Ivika Milanovic, Oyvind Bakkeli ―Authentication Methods

3. http://www.uio.no/studier/emner/matnat/ifi/INF5261/v10/studentprojects/ authentication- methods/ FinalReport Authentication Methods.pdf

4. https://wjst.wu.ac.th/index.php/wjst/article/view/864

5. https://pubmed.ncbi.nlm.nih.gov/28878177/

6. https://www.researchgate.net/publication/322668916_One_tap_owner_authentication_on smartphones

7. J. M. Jorquera Valero, P. M. S´anchez Snchez, L. Fern´andez Maim´o,A. Huertas Celdr´an, M. Arjona Fern´andez, S. De Los Santos V´ılchez, and G. Mart´ınez P´erez: "Improving the Security and QoE in Mobile Devices through an Intelligent and Adaptive Continuous AuthenticationSystem," Sensors, vol. 18, no. 11, pp. 3769, November 2018. DOI10.3390/s18113769View publication statsView publication stats

8. A Hang, F Hennecke, S Löhmann, M Maurer, H Palleis, S Rümelin, EV Zezschwitz, AButz and H Hussmann. User Behavior, Technical Report. University of Munich, 2012. researchgate.net/publication/333661358_A_Review_of_Improving_the_Security_and_QoE_in_Mobile_Devices_through_an_Intelligent_and_Adaptive_Continuous_Authentication_System

9. Ali, Z., Payton, J. & Sritapan, V., 2016a. At Your Fingertips: Considering Finger Distinctness in Continuous Touch-Based Authentication for Mobile Devices. In Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016. pp. 272–275.

10. Anon, 2003. Four grand challenges in trustworthy computing. November 2003. Available at: http://www.cra.org/resources/researchissues/four_grand_challenges_in_trustworthy_computing/ [Accessed April 5, 2015].

11. Anon, 2005. President's Information Technology Advisory Committee. Cyber security: A crisis of prioritization. February. Available at: https://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf [Accessed April 5, 20

12. Botha, R.A., Furnell, S.M. & Clarke, N.L., 2009. From desktop to mobile: Examining the security experience. Computers and Security, 28(3–4), pp.130–137. Available at: http://dx.doi.org/10.1016/j.cose.2008.11.001.

13. Braz, Christina; Seffah, Ahmed and MRaihi, D., 2007. Designing a Trade-off between Usability and Security: A Metrics Based Model. Human Computer Interaction – Interact. , pp.114–126.

14. Burr et al., 2013. Archived NIST Technical Series Publication Superseding Publication(s) Electronic Authentication Guideline.

15. Chaffey, D., 2016. Mobile Marketing Statistics compilation. Smart Insights, pp.1–37. Available at: http://www.smartinsights.com/mobile-marketing/mobile-marketinganalytics/mobile-marketing-statistics/.

16. Chong, Y.-Y., Franklin, J.M. & Greene, K.K., 2016. Usability and Security Considerations for Public Safety Mobile Authentication. National Institute of Standards and Technology Interagency Report 8080. Available at: http://dx.doi.org/10.6028/NIST.IR.8080

