Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

AUTHENTICATION OF SMART PHONES USING BEHAVIOUR BIOMETRIC

[1]Mr.P.Mathivanan [2]A.Ajithkumar [3]R. Gowthaman [4]T. Thamizhselvan

[1]Assistant Professor and
[2 3 4]Student, Department of Information Technology,Manakula Vinayagar Institute of Technology, Puducherry, India

Abstract- *Smartphone's and tablets have become available at everywhere at cheap price and in hands of everyone in our daily lives. Smartphone's, in particular, have become more than personal assistants. The main features of the smartphone's and tablet provides users to play, work, and socialize whenever they want. Smartphone's are small in size, which is user friendly, and carry in user's pockets or purses. The main issue in mobile device is people store their personal and private data, where it can be easily prone to utilized by other unauthorized persons. One of the greatest concerns is the possibility of breaching security and privacy if the device is seized by an outside party. The data can be retrieved by unauthorized users in two ways; when their friends access their mobiles when they know the passwords or pin and the other is users lost their device, so that anyone can try to access the system. In this paper, analyzed the various techniques, approaches, attacks in the biometric behavior system and proposed a new framework that consist of three different techniques for security; keystroke, touch event, and gesture methodologies.*

1. Introduction

The recent revolution taking place in the field of technology is the smart phones and tablet because of the portability, cheap, smaller in size, and more features. Smartphone devices are characterized by expedient features, such as sophisticated operating systems that can allow users to browse the Internet; this is mainly used to listen, watch, record the video streams, navigation. These devices also have large internal storage that enables users to store gigabytes of valuable information, such as personal photos, contact details, call histories and private messages. The rapid evolution in the mobile technology results in the significant change in large number of consumers using smartphone devices instead of personal computers. According to the market research the quantity of smartphone sold is more compared to the laptops worldwide. The tremendous increase in the number of consumers who are buying smartphones has pushed the smartphones to hit the market, and they are leading all other electronic devices in terms of sales. According to the International Data Corporation (IDC), the total number of shipments in the second quarter of 2015 reached 337.2 million smartphones worldwide, an increase of 11.6% compared to the same quarter in 2014.

Smartphones provide more personal benefits for users every day. Many people have come to rely on smartphones for many common, personal and work-related communication tasks. Most users tend to store their passwords and private information on smartphones to efficiently perform these operations in a hassle-free manner. Consequently, potential threats to the accounts of owners have increased tremendously.

With the vast popularity of smartphones, privacy and security issues have become paramount. Due to the size of smartphones, they are quite prone to potentially being lost, stolen, or accessed easily by non-owners. Once an intruder has physical access to a device, he/she may be able to impersonate the original owner of the device for monetary or non-monetary gains and mischiefs; thus, smartphones are much more susceptible to theft than desktops. Attackers are likely to access Online Social Networks (OSNs), financial application and other applications on stolen devices. According to the total number of lost or stolen devices in the USA increased from 1.6 million in 2012 to 3.1 million in 2013. Breitinger and Nickel's survey of 548 subjects shows that only 13% of owners tends to use PIN or visual codes, which means that information contained in the smartphones of at least 87% of the owners is in danger once these devices are lost or stolen. 74% of the participants justify this by saying that they want quick access to their devices or that they do not think about security.

The main issue in the smartphones and the tablets is the users are likely stores their personal and confidential data in mobile phones. The security becomes the main question in the smartphones and the tablets. Even though are number of authentication system such as pin, password, pattern, etc still cracked by unauthorized users easily. In this paper, three different kind of authentication system is proposed based on the biometric behavior. The three authentication system is keystroke approach, touch event, wave gesture. The keystroke is based on the four digit pin number with the effective combination of random number and current time in smartphones. The touch event utilizes the graphical image where the

users have the set the three different regions by touching it. The wave gesture is based on the waving gesture of the hand sensed by the sensors. This improvises the security of the system better than the standard security system in usage.

2. Related Work

Biometric User authentication:
The main objective of the biometric authentication techniques on the touch enabled mobile phones are based on the five physiological and six behavioral characteristics. This framework[1] for establishing a reliable authentication mechanism by implementing a multimodel biometric user authentication system. The physiological biometrics is based upon a person's physical characteristics which are assumed to be relatively unchanging fingerprint, face, iris/retina, and hand/palm. The face feature recognition is categorized into three as traditional, three dimensional, skin texture. A generic biometric authentication system is constructed with the following process such as the biometric data is collected and processed through the sensor and pre-processor, and the feature is extracted from it, template generation, matcher, template storage. The main attacks are fingerprint attacks, spoofing attacks, synthetic attacks, mimic attacks, keystroke inference attacks.

Hand biometric system:
Hand biometric is one of the classical methods to identify the authorized person[2]. In Hand biometrics basically, user can be recognized based on hand shape (Hand Geometry) and a surface of the palm (Palm Print) [3]. Hand biometrics has unique features we can identify and extract the feature. Hand biometrics consists of fingerprint, palmprint, knuckle, vein these are the type of biometrics. In hand palm region consists more than 90 unique hidden features are found in our humans. Hand geometry is used to measure the size of the finger, width etc. In palmprint based the creases, we can able to detect and recognize the persons[4].

non-intrusive user verification framework:
The seven different types of behavioral biometrics are analyzed in as handwaving, gait, touchscreen, keystroke, voice, signature and general profiling. Along with this the amount of data the author use, the type of classifier the author choose, and the results the authors obtain. The authentication of the system is categorized into three as knowledge based, possession object based, and biometric. A non-intrusive user verification framework [5] is proposed in this system where the initial process starts by accessing the user tapping action, the tapping action is analyzed in order to time, acceleration, pressure, size, and then the one class learning system is based on the nearest neighbor distance, with the decision maker process based on the scoring scheme.

Due to the cheap cost and user friendly characteristics of smart phones, users store their private data on the mobile phones. The classical approach for securing this type of information on mobile devices is to authenticate users with mechanisms such as PINs, passwords, and fingerprint recognition. However, these techniques are vulnerable to user compliance and a plethora of attacks, such as smudge attacks. A novel authentication framework, which is based on recognizing the behavioral traits of smartphone [6] users using the embedded sensors of smartphone, such as Accelerometer, Gyroscope and Magnetometer is proposed. The proposed framework also provides a platform for carrying out multi-class smart user authentication, which provides different levels of access to a wide range of smartphone users. Micro-environment sensing is integrated with physical activity recognition to remove false positives arising due to the position sensitivity of smartphone inertial sensors, resulting in better user authentication.

3. Proposed Methodologies

Our framework contains three different ways of security such as keystroke, touch event, and gesture methodologies based on the behavioral biometrics. Behavioral biometrics, use behavioral traits of a subject like how one touches screen, walks, talks, signs a signature, and types to identify a subject. However, this behavior biometrics differs for each and individual based on the time duration, touching sense, swiping speed, and so many. The main advantage of the behavioral biometrics is that it can support in continuous and passive authentication without requiring additional hardware. The behavioral biometrics is quite cheaper and simpler than the physiological biometrics. These are based on touch screen behavior, gait, keystroke, hand waving, voice, profiling and signature. This can be avoiding number of attacks and user friendly.

Keystroke approach:
Keystroke technique analyzes the keystrokes to determine authorized and unauthorized. The speed of the keystrokes can be used to detect the authorized user based on his/her typing motion. The typing speed can be differentiated into two category as; static and dynamic typing. In static typing participants are asked to type a short and pre-defined text to analyze the motion

information, whereas in dynamic typing the subject is not required to type a specific string. A pin number authentication system is used to implement the keystroke along with the combination of the random number and the current time.

Initially, the user has to provide the default password as it is in the current android usage which will be used in case of emergency. Then the user has to select the random number which will be added with the current time stamp. The new four digit number remains as the pin number to unlock the smartphone. The random number remains static and the current time stamp as dynamic data where the user has to check the current time and added with the random number and enters the pin number. For example, the random number is 10 which are selected by the user and the current time of the user smartphone is 09:14 means then the new pin number is the combination of 0914 and 10 as 0924. This can avoid the shoulder surfing attack, incase someone see your password and they tries to open the smartphones means they can't unlock it.

Touch event technique:
The touch event can be categorized into single touch event, multi-touch event, duration time of the touch event, duration time of touch movements, duration time of the single touch, and duration time of multi-touch. This has the graphical user touch event where the users touch the graphical image at three different regions. So, if the users have to unlock the smartphone means then they have to touch the same region at the image. This cannot be easily accessed by the unauthorized users.

Wave Gesture technique:
Recently, the wave gesture gains more popularity in the authentication system. Hand waving behavior is the waving pattern of a person. In other words, the users can be distinguished from the authorized and the unauthorized based on the waving action. The movement of holding the phone and the waving varies for people. For example, many people use their hands to wave in a gentle way while others wave extremely rapid. The waving gestures can be traced based on speed, frequency, waving range and wrist twisting
.

4. Experimental Analysis

The experimental process is carried out in the android studio.

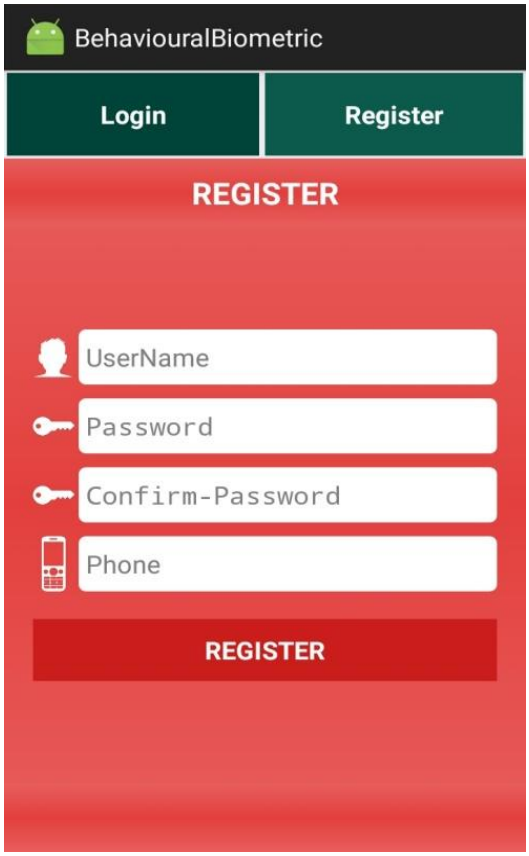

Fig. 1. Registration and login tab for the user to use their authentication information

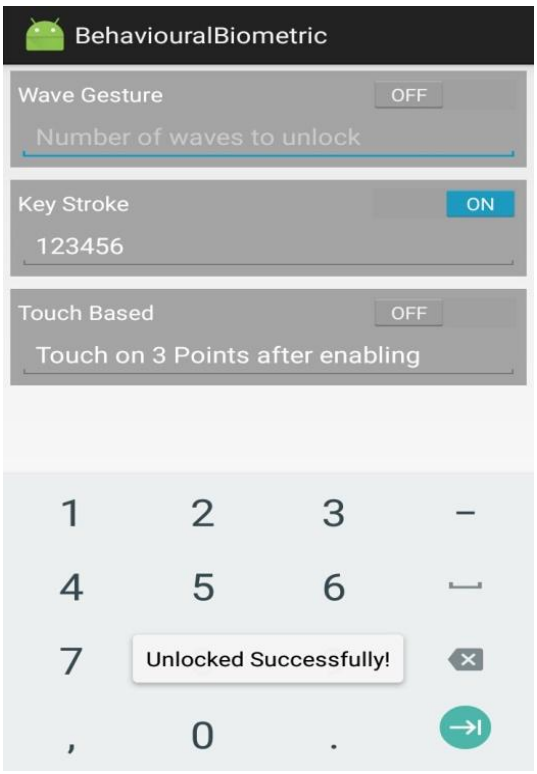

Fig. 2. Wave gesture, key stroke, touch based authentication system.

Conclusion:

The increased usage of the smart device results in the storage of private information in the smart phones and the tablets. Numerous problems arise due to security and privacy of the personal and confidential data. To overcome this issue, smart phones have the different type of security such as pin, pattern, etc. In this paper, the authentication system is proposed based on the user biometric behavior and analyzed the various biometric behavior analysis and attacks in it. The authentication system is based on the speed, duration, touching sense. The authentication system is categorized into three; keystroke, touch event, and wave gesture. Though these authentication can be tried three times to unlock the smartphones.

REFERENCE:

[1] W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones", IEEE Communications Surveys, 2015.
[2] E. GokulaKrishnan, G. Malathi, "A Survey on Multi-feature Hand Biometrics Recognition", Computational Vision and Bio Inspired Computing, pp 1061-1071, 2018.
[3] M. Faundez-Zanuy, "Biometric verification of humans by means of hand geometry", 39th Annual 2005 International Carnahan Conference on Security Technology CCST, pp. 61-67, 2005.
[4] Miguel A. Ferrer, Carlos M. Travieso and Jesus B. Alonso, "Multimodal Biometric System based on Hand Geometry and Palm Print Texture", 40th Annual IEEE International Carnahan Conferences Security Technology, pp. 61-67, 2006.
[5] Abdulaziz Alzubaidi and Jugal Kalita, "Authentication of Smartphone Users Using Behavioral Biometrics", Journal Of IEEE Communications Surveys And Tutorials, 2015.
[6] Muhammad Ehatisham-ul-Haq, Muhammad Awais Azam, Jonathan Loo, Kai Shuang, Syed Islam, Usman Naeem and Yasar Amin, "Authentication of Smartphone Users Based on Activity Recognition and Mobile Sensing", NCBI, Sensors, vol. 19, issue 9, 2017.
[7] Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M., "Smudge attacks on smartphone touch screens", In Proceedings of the 4th USENIX Conference on Offensive Technologies, Washington, DC, USA, 11–13, pp. 1–7, August 2010.
[8] Nan Zheng, Kun Bai, Hai Huang and Haining Wang, "You are How You Touch: User Verification on Smartphones via Tapping Behaviors", IEEE 22nd International Conference on Network Protocols, 2014.

[9] Derawi, M.O.; Nickely, C.; Bours, P.; Busch, C. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In Proceedings of the 2010 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Darmstadt, Germany, 15–17 October 2010; pp. 306–311.
[10] H. Crawford, "Keystroke dynamics: Characteristics and opportunities," in Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on. IEEE, 2010, pp. 205–212.
[11] N. Duta, "A survey of biometric technology based on hand shape," Pattern Recognition, vol. 42, no. 11, pp. 2797–2806, 2009.
[12] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," International Journal of Biometrics, vol. 1, no. 1, pp. 81–113, 2008.
[13] X. Zhang and Y. Gao, "Face recognition across pose: A review," Pattern Recognition, vol. 42, no. 11, pp. 2876–2896, 2009.
[14] A. K. Jain, "Biometric recognition: overview and recent advances," in Progress in Pattern Recognition, Image Analysis and Applications. Springer, 2007, pp. 13–19.
[15] M. Rogowski, K. Saeed, M. Rybnik, M. Tabedzki, and M. Adamski, "User authentication for mobile devices," in Computer Information Systems and Industrial Management. Springer, 2013, pp. 47–58.
[16] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: A survey," Communications Surveys & Tutorials, IEEE, vol. 15, no. 1, pp. 402–427, 2013.
[17] S. A. Hoseini-Tabatabaei, A. Gluhak, and R. Tafazolli, "A survey on smartphone-based systems for opportunistic user context recognition," ACM Computing Surveys (CSUR), vol. 45, no. 3, p. 27, 2013.
[18] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Computer security applications conference, 21st annual. IEEE, 2005, pp. 10–pp.
[19] L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones," in Proceedings of the 20th Network and Distributed System Security Symposium, NDSS, vol. 13, 2013, pp. 1–16.
[20] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," Proc. 4th USENIX Conf. Offensive technologies (WOOT ´ 10), vol. 10, pp. 1–7, 2010.

