Continuous Authentication in Smartphones: An Analysis on Robust Security Practices

Sajjad
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan
ciit.sajjad@gmail.com

Adnan Zeb
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan
adnanzeb933@gmail.com

Hussain Ahmad
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan
hamadnig@gmail.com

Munam Ali Shah
Department of Computer Science
COMSATS Institute of Information Technology, Islamabad, Pakistan
mshah@comsats.edu.pk

Sana Akram
Department of Computer Science
Bahria University
Islamabad, Pakistan
sana.ak889@gmail.com

Muhammad Sikander Zamir
Department of Computer Science
Bahria Universty
Islamabad, Pakistan
maliksunny111@yahoo.com

***Abstract*—The current authentication systems in smart phones are classified as static or one shot authentication schemes in which the user is validated at a single point. The existing authentication systems cannot recognize the difference between an intruder and a legitimate user if the security credentials like passwords have been leaked. This issue is addressed in continuous authentication schemes where the system constantly monitors the user by different procedures to detect the user as genuine or intruder. Continuous authentications schemes can be deployed using different methods such as behavioral, gestural and facial, etc. In this paper, we critically analyze the different continuous authentication schemes. We evaluate the robustness and failure free operation of each approach. We aim to provide a precise knowledge about different continuous authentications schemes which help the user to determine the appropriateness of the underlying model adapted by each approach.**

Keywords—Continuous authentication; security; mobile sharing; TIPS; SenGuard; SilentSense; GeoTouch; gestures; key strokes

I. INTRODUCTION

The increasing popularity of mobile and smart phones has made human life more easy and serviceable. The reason is its affordability and ability in managing their personal information like contacts, emails, images, etc. and private information such as bank accounts, passwords, etc. The day to day advancement in information technology now focuses on mobile devices as compared to PC's. Government and non-government organizations allow their employees to stay connected with their networks and work remotely using mobile applications. However, along with such convenience, mobile phones are easy to get lost or stolen. According to a survey, on a national scale 30-40% looting is associated with smart phones and tablets [1]. This unlawful act gives two assumptions: 1) The device itself is valuable; 2) The information in device is valuable to the robber. With the increasing capabilities of storing sensitive data on mobile phones, information leaking is the main concern to the whole information society. Recent studies [12] have demonstrated that leakage of sensitive information from smart phones can cause severe damage to the users.

Well-known methods for authenticating a user on cell phone are: password, pattern or facial recognition and fingerprint etc. These methods are called one shot authentications or static authentication [2]. In such methods, a user must pass a single point of entry to access the smart phone as shown in Fig. 1.

As mobile phones are more exposed to the risk of being lost or stolen thus protecting the sensitive data within the smart phones is the prime objective which is not possible with traditional methods as one shot authentication methods are more exposed to steal or loss. Passwords are easy to predict as most people use easy passwords to memorize. In a study of 6,000,000 passwords, 91% passwords were related to a group of 1,000 code words [3]. Similarly, 8.5% of users choose 123456 or password as their password.

Furthermore, in iPhone 4-digit the most commonly used three pass codes are 1234, 0000 and 2580 [4]. In addition, screen taps can easily be detected using accelerometer and gyroscope readings to derive the passwords on touch screens [4]. Finger spoofing [5] in case of fingerprints, picture to cheat the front camera in case of facial recognition and Smudge [6] attack can also break entry points in authentication schemes. The topmost shortcoming of such schemes is that once the smart phone is authenticated it cannot verify the user as legitimate user or attacker and the mobile is exposed to access all information stored in it. An example of such situations is mobile sharing [7] where a person gives his/her phone to a guest user to make a call, take a picture or access an application, in this manner the personal data of the smart phone owner can be breached. In the same way parents allow their children to play a game or for entertainment purposes and the children mistakenly delete their emails or make an online transaction. In such situations, the smart phone owner

does not want the leaser to violate the limits. However, the smart phones cannot verify the user as the owner or leaser. To sum up, traditional authentication methods cannot validate the user as owner or attacker if password is compromised. Security to access applications can be easily provided in smart phones; in addition, these situations can also be avoided by virtualization [29].

However, such scenario can make the smart phones user unfriendly. Imagine a circumstance where a user is asked to verify itself every time it access messages or emails. Authentication to access every application consumes more power and annoys the user. A survey [8] determined that password limitations are more annoying to user as compared to network loss, small screen low voice quality, etc. suggesting that implicit validation with barely user participation is a needed characteristic in smart phones.

In preference to static or one shot authentication methods, continuous authentication [9] uninterruptedly monitor users after successful login to the device using behavioral authentication. Behavioral authentication includes touch gestures, keystrokes, gait or any combination of those [10]. In touch gestures the user's involvement with the device reveals the user finger pressure, movement, trajectory of moment, etc. Mostly, a smart phone possesses touch sensor as "800 million mobiles were expected to be touch enabled by 2014" [11]. The data is stored in touch sensor and after successful login if any different activity is recorded than the normal behavior the smart phone should ask to user to verify itself. Accelerometers sensor [7] can record user's activities that can also be helpful to provide continuous authentication.

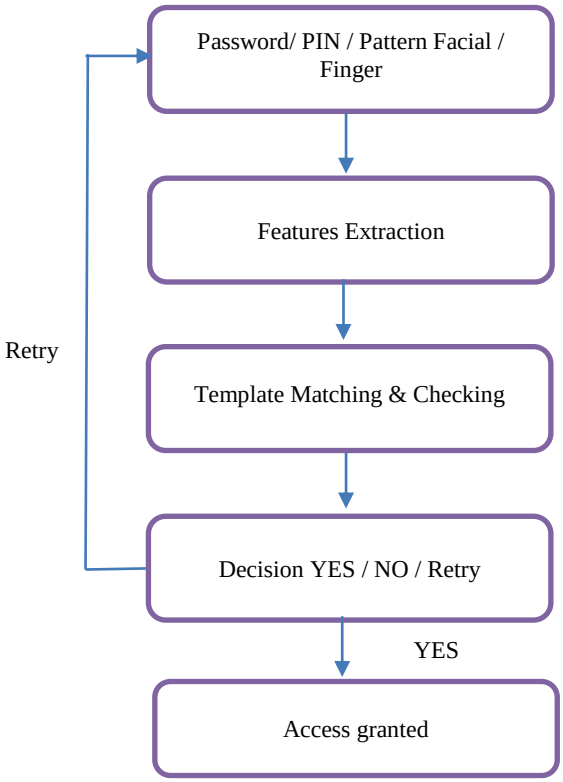

Fig. 1. Static or one shot authentication.

Continuous authentication in smart phones provide an additional defensive mechanism with no user friendliness but advantages such as: *1)* Providing additional security; *2)* the multifunctional sensor in the mobile devices can detect such activates. Whenever the system senses a different user it must recall the conventional authentication system asking the user to validate itself. The fact that mobile is personal computing device cannot be ignored. Thus, security is of main concern in smart phones. Continuous and implicit authentication schemes should be adopted in smart phones authentication as it complements one shot authentication with continuous monitoring of smart phone without interrupting the user. Our contribution to the research involves a survey to find out the best methods for continuous authentication in smart phones to optimized accuracy, power efficiency and user-friendliness. The comparison is based on the following attributes:

Universality: All peoples must have the attribute.

Commonness: Should not be common even must be unique in every individual.

Suitability: It must suit people and should be accepted easily.

Measurability: It must be easy to measure.

Performance: It must possess high accuracy level and should be fast enough.

Constancy: It must be constant enough and not to be change with passage of time.

Circumvention: It must avoid the illegal or unlawful access.

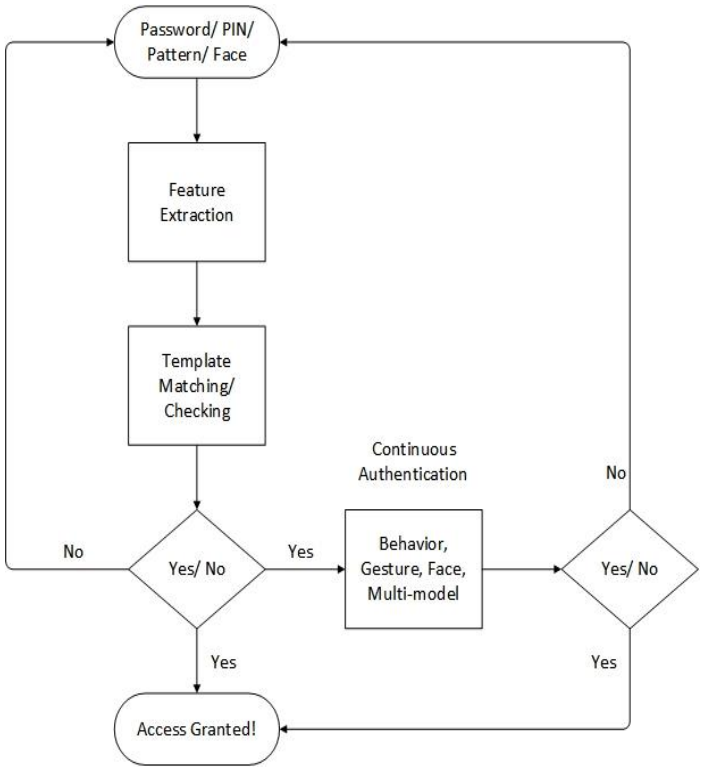

Fig. 2. Overview of continuous and static authentication.

The rest of this paper is organized as follows:

In this paper, we investigate the continuous authentication techniques for smartphones and evaluate the performance on different parameters. The remainder of the paper is organized as: Section II contains critical analysis of different continuous authentication schemes. Section III provides the performance comparison in graphical and tabular form. We discuss the open issues in Section IV and the paper is concluded in Section V.

II. Related Work

In this section, we review continuous authentication techniques using numerous aspects, presented by several authors for continuous authentication. Fig. 1 and 2 shows a brief overview static/one shot and continuous authentication.

A. Behavioral

Gait is defined as the movement of animal limbs however, the walking pattern of human beings on a solid surface is also considered as gait [13]. Gait is a behavioral biometric technique that is not distinct and changes with passage of time. Due to these limitations, it provides a low accuracy rate and can be implemented only where low level of security is required [14]. In gait based biometric the body features such as height, distance between pelvis, feet and head and distance between feet are measured during walk. Gait is a distant biometric technique in which a camera from a distance captures the walking style of an individual. These captured images and videos are then used to extract the gait features to be used for recognition of an individual. As videos processing is involved in feature's extraction [15], [16]. This technique is considered heavy and costly. N. Kunnathu [17] proposed that every person has a distinctive way of using the phone in a phone call. The minute differences in the viewpoint of the small activities made during the phone call can be relatively different among two persons. The Accelerometer provides a useful method of calculating the phone activities and the change in orientation of the phone. The experiment was performed on seven members who ended five test phone calls each enduring for a slight above 5 seconds showing excellent results. W. Shi *et al* proposed SenGuard [8] that collects data from the multiple available sensors in the smart phones. First prototype of SenGuard was built up using Voice, multi-touch, Locomotion and Location. SenGuard is considered as a crucial component of complete user authentication in smart phones. Users can also be recognized by recording the gestures and then checking the user pattern with the saved gestures on runtime [18].

B. Using Gestures

N. Zheng *et al*. [19] proposed that data from acceleration, time, size and pressure retrieved from sensors of smart phone, can form a non-interfering user verification procedure to verify if a validating user is the real possessor or an intruder who is familiar with the security code. Using a sample data of 80 users, several experiments were performed to authenticate efficiency of the offered system. The trial results demonstrated that the verification system attained a high precision around EER of down to 3.65%.

C. Bo *et al*. [20] proposed SilentSense, a framework that validate the existing user is genuine owner or not using behavioral biometrics. Behavioral biometrics includes walking patterns. Silent sense verifies the user using a model and novel method without interrupting the user with great sureness. FAR and FRR can be as short as less than 1% with 10 actions. Silent sense mix movement based biometrics for each user with earlier touch-based biometrics. The extensive assessments of silent sense on android phones can achieve an accuracy of 99%. T. Feng *et al*. proposed TIPS [21] which validates users by constantly examining touch screen gestures in the perspective of an application executing in background. TIPS evaluate data composed from 23 phone holders in a real-life environment and installed thirteen of them with hundred guest users. TIPS can reach above 90% accuracy in real-life natural environments. A. Jain *et al*. [22] proposed an approach by developing an application that collects data from smart phones' sensors, while user is interacting with the phone. To check the performance of this approach, the application was installed on two different devices and checked with user gestures of (Data Set I and Data Set II) 104 and 30 users' respectively. The experimental result showed 0.31% FRR on Data Set I. Data Set II also showed a similar trend to Data Set.

A. Kumar R. C *et al*. proposed Statistical methods [23] for continuous authentication using Touch gestures can archives Continuous authentication. TGSI continuously validates the user by verifying touch traces made on screen. TGSI was tested on data set collected from daily use of smart phones. The experimental results have demonstrated that TGSI can enhance the mobile security to a greater level. Their research work also presented how to convert touch gesture to statistical image and its verification for authorization. J. Shing *et al*. [24] proposed that every user has a different manner of using touch screen, .i.e., the explicit location pressed on the screen, the pressure applied and the movement of fingers on screen while rolling up and down can be unique. Furthermore, the quickness of the Gesture Segment (GS) is distinct to extract a meaningful velocity segment. Using and SVM algorithm with behavioral biometrics experimental results get an accuracy of 98.58%.

H.M. Reis [25] developed Interactive Geometry software for gestures to form geometric objects in GI application for smart phones. Numerous gestures were suggested and calculated by mathematicians. For implementing the proposed software GeoTouch, a team of five experts conducted the tests. The results showed that gestures decrease both the amount of errors and their harshness. C. Shing *et al*. [12] presented an approach based on four common types of touch operations. Using distance measurement technique and multiple decision procedure the efficiency of this approach was validated in physical life application scenarios. Experimental results proved that this approach is competitive and promising with a FAR of 4.68% and FRR 1.17 in few cases. M. Trojahn *et al*. [27] mixture of a handwriting and keystroke based authentication method has many benefits. Joint with knowledge factor and two-factor verification with no need of extra hardware the system has a FRR of 19 % and FAR of 21%. T. Feng *et al*. [28] proposed FAST, "Finger Gesture authentication system with touch screen". FAST

complements continuous authentication by extracting touch data from touch screens smart phones of 40 users and achieves FAR 4.68% and FRR of 0.13% indicating FAST provides reliable post login security without interrupting User.

C. Face

Face recognition is an important biometric technique currently used for continues authentication in smart phones [44]. For facial recognition first a face is scanned to extract its features which are then compared to the stored features patterns in the database. If matched, the individual is identified, else rejected. The database contains the features patterns of the user's facial image.

For face recognition, the system first recognizes the position and boundary of face, height and width of eyes, nose distances between eyes and nose and some other objects and area of face in the image, then the characteristics are extracted and matched with the stored patterns for identification. Front image and profile image are the two kinds of images that are used for the extraction of features. Most of the concentration is on front image because it contains more information which helps in accurate face recognition. Several differences and uniqueness exists between people's face, that's why they can't be categorized generally. The algorithm used for face recognition is grouped in to two approaches. First one is the geometric approach that searches for unique or dissimilar features, positions and shapes of the facial objects just like nose, eyebrows, eyes, chin, lips distance between them and other correlations among them. The second approach is photometric that distills an image into its values and compares the image to its value and removes variations [30]. Face recognition system can be fooled by different types of attacks such as by showing valid user's image, video or 3d facial replica [31]. Recently a huge number of bogus faces attacks have been observed frequently. These kinds of attacks generally involve video attacks, cut photo attack and warped photo attack. In video attack a high-resolution video is used to make the system feel it's a valid live user and the system is made fooled. In warped attack, copper papers are used for high resolution print of image and the attacker in a cautious and calculated manner wraps a whole photo to simulate facial motion [32]. Cut photo attacks are carried out in the same fashion as warped attacks but the section of the eye is cut to show blink behavior. However, continuous authentication using face has given tremendous results and can be applied as a background process to check the identity of the person using the smart phone without interruption.

D. Iris

Studies have revealed the possibility of using iris information for smart phones authentication. Continuous authentication using Iris recognition pipeline containing segmentation is implemented on smart phones. Each individual eye is considered for iris based recognition as each individual person has two unique patterns [42].

Iris as a biometric technique was first suggested in 1987 for authentication [33]. In 1993, J. Daughman successfully implemented iris as a biometric technique in authenticating for the first time [34]. Iris is a small, trim and rounded object and present as an internal part of the eye bordered by pupil and sclera which controls volume and diameter of pupil and flow of light to retina. In the initial two years of life, some changes occur to iris but after two years it becomes constant. Because of its uniqueness in every human being Iris was proposed for authentication. Iris of all people are different from one another, even iris of twins are different just like the finger prints [30], [35]. Iris based recognition systems are considered very secure because its algorithm is strong and it first checks the internal and external limits of iris in the eye image. Thus, it is easy for the system to distinguish the fake or non-natural iris from the original and natural iris. In addition, it is complex to modify the texture of iris. For iris based recognition system a watchful balance of light, focus, contrast and resolution is needed [36], [37]. Factors that affect the performance of iris based identification system are change in resolution, angle of rotation of eye, light, contrast and image focusing. Biometric techniques have been implemented using Iris recognition method. However, currently continuous authentication scheme in smart phones using Iris is not available.

E. Multimodal

Uni-modal biometric systems are those which use only one step or character for identification. However, every biometric technique has some boundaries. Some of them are universally unique where as some are exposed to attacks. None of these techniques can be completely trusted as environmental factors have a deep impact on them. Therefore, a more reliable identification, multimodal biometric was introduced to overcome these boundaries [38]. In multimodal biometric system two or more biometric techniques are combined to form a strong authentication system [39]. Multimodal are more secure as it is much difficult for an attacker to attacks with more than two fake features. It is difficult to make fool a system having multiple techniques of identification. Various features from physical or behavioral or from both are combined to make a multimodal identification system [39]. Face and voice [40], face and finger prints and so many others. In [41] Cormorant is a multimodal authentication framework using voice and face. CORMORANT is multi-modal, risk-aware cross device verification framework that allows transparent non-interfering authentication for smart phones. [42] presented a multimodal authentication technique using Face periocular, Iris and Characteristics with an EER of 0.68% confirming the strong performance of their offered system. Due to the combination of different techniques into one system makes multimodal a complex system [43].

III. Performance Comparison

In this section, different continuous authentication techniques are compared in tabular and graphical form. We compare the performances against application area, acceptance rates and accuracy level, etc.

A. Application Area

Table 1 shows the continuous authentication techniques and their application area.

TABLE I. APPLICATION AREA

Biometric	Application Area
Behavioral	Sensor for detection: Usage pattern in call, voice, motion, locomotion, multi-touch.
Gestures	In the form of background application constantly checking the touch strokes.
Face	In the form of application checking randomly or after fixed intervals by scanning user through front camera.
Iris	Application proposed in static however no experiments conducted for continuous authentication.
Multimodal	Multiple models proposed, However no experimental results in continuous authentication.

B. *FAR and FRR*

Table 2 shows the false acceptance rate (FAR) and false rejection rate (FRR) against each continuous authentication technique (best case only and N/A for not available).

TABLE II. FAR & FRR

Biometric Technique	FAR	FRR
Behavioral [17]	5.7%	8.0%
Using Gestures [20]	1%	0.99%
Face [44]	--	--
Iris	N/A	N/A
Multimodal	N/A	N/A

C. *Accuracy Level*

Table 3 represents the highest accuracy achieved against each technique. The best case in every technique has been taken and referred. N/A is used for techniques that don't have experimental results in continuous authentication.

TABLE III. ACCURACY LEVEL

Continuous Authentication Technique	Highest Accuracy Level achieved
Behavioral [17]	>90%
Using Gestures [20]	99%
Face [44]	>74.9%
Iris	N/A
Multimodal	N/A

D. Fig. 3 shows the graph created on data available in Table 3. The x-axis presents the technique whereas the y-axis shows the percentage.

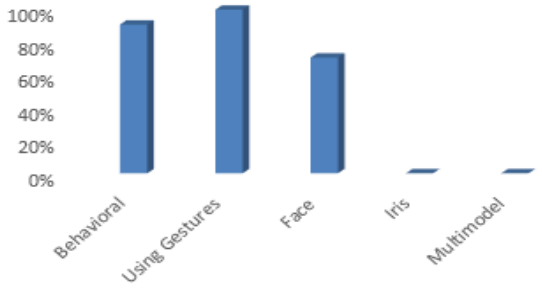

Fig. 3. Best case graphs.

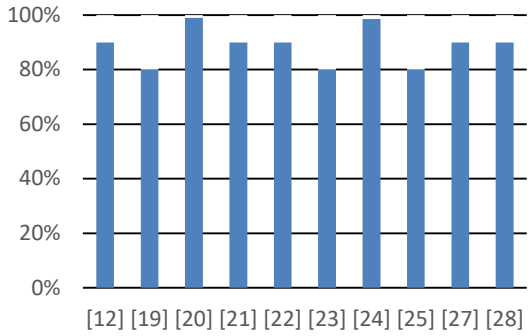

Fig. 4. Accuracy graph.

TABLE IV. LEVEL OF ACCURACY ACHIEVED USING GESTURES

Accuracy achieved using Gestures			
References	**Accuracy Achieved**	**FAR**	**FRR**
[12]	**90%**	4.68%	1.17
[19]	**>80%**	3.65%	1.13%
[20]	**99%**	1%	0.99%
[21]	**90%**	1%	1%
[22]	**>90%**	1%	0.31%
[23]	80%	3.36%	1.7%
[24]	98.58%	1.6%	1.3%
[25]	>80%	2.6%	1%
[27]	90%	21%	19%
[28]	>90%	4.68%	0.13%

E. Table 4 shows the Accuracy level achieved by using gestures along with their FAR and FRR against each reference.

F. Fig. 4 shows the accuracy graph plotted on data from Table 4. X-axis represents the reference whereas; Y-axis represents accuracy achieved in percentage.

G. *Performance Comparison*

Table 5 represents the overall comparison of the continuous authentication schemes developed or under research depending of the key factors included in the table. H, M and L represent high, median and low, respectively.

IV. DISCUSSION AND OPEN ISSUES

In this paper, we investigated different continuous authentication techniques for smart phones that are in practice or are under research. We critically analyzed the features, recognition techniques, application areas, and the accuracy levels etc. Based on universality, commonness, constancy, permanence, measurability and acceptability, the continuous authentication using gestures can result in a very secure and user friendly authentication system. However, along with such convenience it may not please the real owner as well. Example of such cases can be in touch gestures where the smart phone of a real user is trained on the gestures of its right hand. In case of any injury to its right hand, the smart phone cannot

justify the gestures from the left hand of the real user and may result in identifying the legitimate user as intruder. Similarly, in behavioral biometric techniques like activity recognition, if a user changes its daily activities because of its change in job, jogging or exercises will also affect the real user. In addition to gestures and gait recognition, to continuously authenticate a user, the facial recognition has a direct impact on user hair style and shaving or face covering cloths or hat, etc.

TABLE V. PERFORMANCE COMPARISON OF DIFFERENT TECHNIQUES

References	Characteristics	Universality	Uniqueness	Suitablity	Measurability	Performance	Acceptability	Avoidence	Advantages	Disadvantages
[13][15][16]	Behavioral	H	L	L	M	L	M	H	high universality	Low measurability, and need a large database to store video, spoofed easily
[8][17]		H	H	M	H	M	M	H		
[20][24]	Using Gestures	H	H	H	H	H	H	H	High uniqueness	Computational cost and battery Use
[12][21][22] [27][28]		H	H	H	M	H	M	H		
[19][23][25]		M	H	H	L	H	L	H		
[31][32]	Face	H	M	M	H	M	M	H	High universality and measurability	Spoofed
[44]		H	H	H	H	H	H	H		
[33][34] [36][37]	Iris	H	H	H	M	H	L	L	Low error and reliable	Low acceptability
[42][35]		H	H	H	H	H	M	L		
[34][38] [39][43]	Multimodal	H	H	M	M	H	H	L	High performance	Measurability
[40][41]		H	H	H	M	H	H	M		

V. CONCLUSION

A robust and reliable authentication technique is required for authentication in smart phones. Static authentication system with Password, Pin, Facial and patterns failed to provide high security and has no mechanism of identifying the real owner or intruder. Using continuous authentication techniques such as Gestures, behavioral etc. the difference between the real owner and intruder can be easily identified as every person has a unique way of using smart phones. However smart phones are still at risk if the intruder has the password or pin to unlock the smart phone. To secure the smart phone a security system is needed that dynamically selects a new password every time it records an activity that is not from the real user. Our future work involves building a dynamic security system for the smart phones to create a password every time the system detects an intruder. Such system along with continuous authentication can guarantee that even if password is compromised no one can unlock the smart phone but the real owner.

REFERENCES

[1] Z. Syed, J. Helmick, S. Banerjee, and B. Cukic Effect of User Posture and Device Size on the Performance of Touch-based Authentication Systems IEEE 16th International Symposium on High Assurance Systems Engineering 2015

[2] A.Jain,and V.Kanhangad Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touch gestures. Patternrecongnition letters 68(2015) 351-360

[3] T. Feng, Z. Liu, K.-An Kwon, W. Shi_, B. Carbunary, Y. Jiangz and N. NguyenContinuous Mobile Authentication using Touchscreen Gestures 978-1-4673-2709-1/12/$31.00 ©2012 IEEE

[4] N. Zheng, K. Bai, H. Huang and H. Wang You are How You Touch IEEE 22nd International Conference on Network Protocols 2014

[5] https://srlabs.de/spoofing-fingerprints, accessed: 21st February 21, 2016.

[6] http://www.alphr.com/news/security/360220/touchscreensopen-to-smudge-attacks Accessed 21st February 21, 2017

[7] T. Feng, X. Zhao, N. DeSalvo, Z. Gao, Xi Wang and W. Shi Security after Login: Identity Change Detection on Smartphones Using Sensor Fusion 978-1-4799-1737-2/15/$31.00 ©2015 IEEE

[8] W. Shi, J. Yang , Y. Jiang, F. Yang, and Y. Xiong. SenGuard: Passive User Identification on Smartphones Using Multiple Sensors IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) 2011

[9] R. P. Guidorizzi Active authentication.Security: IEEE IT Professional Magazine, 15(4):4–7, 2013.

[10] Rahman F, Gani MO, Ahamed S I. Seeing beyond visibility: A Four Way Fusion of User Authentication for Efficient Usable Security on Mobile Devices. Presented at the Eighth International Conference on Software Security and Reliability - Companion 2014; pp. 121-129.

[11] Smartphone Continuous Authentication based on Keystroke and Gesture Profiling J. Shing, W. Chih-Ta, L. Wan-Ching Lin, and Te En Wei. The

49th annual IEEE International Carnahan Conference on Security Technology 2015

[12] Chao Shen, Yong Zhang, Zhongmin Cai, Tianwen Yu, Xiaohong Guan Touch-Interaction Behavior for Continuous User Authentication on Smartphones 978-1-4799-7824-3/15/$31.00 ©2015 IEEE

[13] H. Iwama, D. Muramatsu, Y. Makihara, and Y. Yagi "Gait-based Person-Verification system for forensics,", pp. 113–120, 2012.

[14] A. N. Kataria, D.M. Adhyaru, A.K. Sharma, and T.H. Zaveri, A survey of automated biometric authentication techniques, Nirma Univ. Int. Conf. Eng. NUiCONE 2013, pp. 1–6, 2013.

[15] D.S. Matovski, M.S. Nixon, S. Mahmoodi, and J.N. Carter,The effect of time on gait recognition performance vol. 7, no. 2, pp. 543–552, 2012.

[16] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietik, J. Bustard, and M. Nixon, "Can gait biometrics be Spoofed ?" pp. 3280–3283, 2012.

[17] N. Kunnathu Biometric User Authentication on Smartphone Accelerometer Sensor Data,pp. 131-139 2014

[18] T. Feng, Xi Zhao, N. DeSalvo, T.Hua Liu, Z. Gao, X. Wang and W. Shi An Investigation on Touch Biometrics: Behavioral Factors on Screen Size, Physical Context and Application Context IEEE 2015

[19] N. Zheng, K. Bai, H. Huangand H. Wang You are How You Touch: User Verification on Smartphones via Tapping Behaviors 2014 IEEE 22nd International Conference on Network Protocols 2014

[20] C. Bo, L. Zhang, X.Yang Li, Q. Huang, Yu Wang.Silent Sense: Silent user identification via touch and movement behavioral biometrics. 2013.

[21] T. Feng, J. Yang, Z. Yan, E. Munguia Tapia and W. Shi TIPS: Context-Aware Implicit User Identification using Touch Screen in Uncontrolled Environments 2014

[22] A.Jain and,V.Kanhangad Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touch screen gestures Pattern Recognition Letters 68 (2015) 351–360

[23] A. Kumar R C and Dr. Sanjay Chitnis, Continous user authentication using touch screen gestures statistical images for Smartphone international Journal of Research computer application and robotics 2015,

[24] J.Shing Wu, C.Ta Lin W.Ching Lin,and T.En Wei, Smartphone Continuous Authentication based on Keystroke and Gesture Profiling: The 49th annual IEEE International Carnahan Conference on Security Technology 2015

[25] H. M. Reis, S. Isotani, I. Gasparini and R. Mizoguchi, A Dictionary of Gestures for Multitouch-based Interactive Geometry Software IEEE 15th International Conference on Advanced Learning Technologies 2015

[26] D. Sathya G. Paolo G. Kiran and S. Balagani Secure Privacy-Preserving Protocols for Outsourcing Continuous Authentication of Smartphone Users with Touch 2013.

[27] M. Trojahn and F. Ortmeier. Toward Mobile authentication with keystroke dynamics on mobile phones and tablets 27th international conference on advanced information networking and applications workshops 2013.

[28] T. Feng, Z. Liu, K.An Kwon, W. Shi, B. Carbunar, Y. Jiang and N. Nguyen Continuous mobile authentication using touchscreen Gestures. IEEE 2012.

[29] Shah MA, Kamran M, Khan H, Javaid Q. Vdroid: A lightweight virtualization architecture for smartphones. Future Technologies Conference (FTC) 2016 Dec 6 (pp. 1290-1296). IEEE.

[30] A. Heydarzadegan, M. Moradi and A. Toorani "Biometric recognition systems : A survey,", vol. 6, no. 11, pp. 1609–1618, 2013.

[31] A.D.S. Pinto, H. Pedrini, W. Schwartz, and A. Rocha, "Video-based face spoofing detection through visual rhythm analysis," 25th SIBGRAPI Conf. Graph. Patterns Images, pp. 221–228, August. 2012.s

[32] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S.Z. Li, "A face anti spoofing database with diverse attacks," pp. 2–7, 2012.

[33] D.M. Rankin, B.W. Scotney, P.J. Morrow, and B.K. Pierscionek, "Iris recognition failure over time : The effects of texture," Pattern Recognition, vol. 45, no. 1, pp. 145–150, 2012.

[34] "Multimodal biometric recognition using iris feature extraction and palmprint features," H.S, D. of E. Assistant Professor, S.C. of Engineering, I. Trichy, Tamilnadu, Prabakar.T.N, D. of E. Professor, and O. E. College, pp. 174–179, 2012.

[35] S. P. Fenker, N. Dame, and K. W. Bowyer, University of Notre Dame University of Notre Dame "Experimental Evidence of a Template Aging Effect in Iris Biometrics," pp. 232–239, 2010.

[36] A. Uhl and Y. Holler "Iris-sensor authentication using camera PRNU fingerprints," 2012 5th IAPR Int. Conf. Biometrics, pp. 230–237, March. 2012.

[37] C. Rathgeb, A. Uhl, and P. Wild, "Iris-biometric comparators: Exploiting comparison scores towards an optimal alignment under Gaussian assumption," 5th IAPR Int. Conf. Biometrics, pp. 297–302, March. 2012.

[38] P.S. Sanjekar and J.B. Patil, "A review of multimodal biometrics," vol. 4, no. 1, pp. 57–64, 2013.

[39] M.B.R.P.L. Correia and L.D. Soares, "Hand-based multimodal identification system with secure biometric template storage," pp. 165–173, November 2012

[40] Y.M. Fouda "Fusion of face and voice : An improvement,", vol. 12, no. 4, 2012.

[41] D. Hintze, E. Koch, R. D. Findling, R. Mayrhofer and Muhammad Muaaz CORMORANT: Towards Continuous Risk-Aware Multi-Modal Cross-Device Authentication 2015

[42] K. B. Raja R. Raghavendra M. Stokkenes and C. Busch Multi-modal Authentication System for Smartphones Using Face, Iris and Periocular" in Biometrics (ICB), 2015 International Conference on 2015.

[43] V. Subbarayudu and M. Prasad, "Multimodal biometric system," Emerg. Trends., vol. 1, no. 1, pp. 58–63, 2012.

[44] M. E. Fathy, V. M. Patel and Rama Chellapa, "Face based active authentication on Mobile Devices, ICASSP IEEE 2015, pp.1687-1691.