Pak. J. Biotechnol. Vol. 15 (Special Issue 1) Pp. 31-35 (2018) Lalithamani N. et al.,
www.pjbt.org, PISSN: 1812-1837, EISSN: 2312-7791

SURVEY ON NONOBSTRUCTIVE AND CONTINUOUS USER AUTHENTICATION ON MOBILE DEVICES

N.Lalithamani, Raam Balaji D and SVPKH Satya Dev

Department of CSE, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India,
n_lalitha@cb.amrita.edu, raam.balaji@gmail.com, satyadevsv@gmail.com

ABSTRACT

The use of mobile devices in our day to day life has increased drastically in the last ten years. Much of it can be contributed to the breakthrough in the field of communication. Since they contain most of our personal information, the constant worry of security and privacy has increased. In order to tackle this problem, non-obstructive and continuous user authentication has been proposed. This paper deals with the methods that have been proposed till now and the challenges that are yet to be overcome in this field.

Index Terms— Continuous, Authentication, Mobile, Progress, Non-obstructive.

I. INTRODUCTION

A common method of user authentication in mobile devices are based on knowledge which the user possess like a password, pattern or pin. Recently biometric authentication has been used to authenticate and authorize the user using traits such as a fingerprint. When the user uses password or pin, they tend to keep easy to remember thereby easy to remember the password. This leads to lax in security. Studies show that 34% of users use no form of authentication on their mobile devices and most of the mobile devices have no method to verify that the user who originally unlocked the device is still in the control of the device (Tapellini 2014, Khan et al., 2015). Thus, an unauthorized individual can access information which can be damaging for the user. To overcome this a continuous and non-obstructive is required.

II. BIOMETRIC PERFORMANCE EVALUATION

The performance of a biometric enabled system mainly depends on the accuracy of that system. In order to measure this, a large number of genuine and illegitimate attempts are made and the results that are obtained from this are saved and their performance is evaluated. A legitimate attempt is an attempt made by the genuine user to get authorized. An illegitimate attempt is made by an imposter trying to get authenticated.

Most of the biometric system gives a score after processing the biometric data. This score is used to determine whether the user is genuine or not. To do this a threshold value has to be fixed. If that value is too high, fewer illegitimate attempts get accepted but it may also reject some of the legitimate attempts of the user. This may be inconvenient for the user. If the threshold value is too low, the security provided by the biometric system would be lax.

The common measures in biometric system are as follows (Shyamala and Padmanabhan 2015):

- False Match Rate (FMR): Percentage of illegitimate attempts that are considered as a match.
- False Non-Match Rate (FNMR): Percentage of legitimate attempts that are falsely considered as a mismatch.
- Failure to Acquire Rate (FTA): Percentage of attempts that could not be processed by the system.
- False Acceptance Rate (FAR): Similar to that of false match rate. But in this metric, the failure to acquire rate is also considered. FMR takes the total number of attempts into consideration while FAR takes the total number of processable into consideration.

$$FAR = FMR * (1 – FTA)$$

- False Reject Rate (FRR): Similar to that of false non-match rate. But in this metric, the failure to acquire rate is also considered. FNMR takes the total number of attempts into consideration while FRR takes the total number of processable into consideration.

$$FRR = FTA + FNMR *(1 – FTA)$$

- Equal Error Rate (ERR): The point at which both the FAR and FRR are equal.

III. VARIOUS APPROACHES FOR CONTINUOUS AUTHENTICATION

In continuous authentication model, the various attributes of the users like their swipe pattern, gait, keystroke, facial patterns and even in some cases even their voice (Crouse et al., 2015). Then the gathered data are processed in real-time and the system determines if the user who is using the device is a legitimate user. If the system determines that the attributes it has processed do not match that of the legitimate user, it locks the mobile device and asks the user for the pre-set pin or password to authenticate them. All these functions have to be done in real-time for the system to be foolproof. In this paper, we look at the various methods proposed to implement this continuous authentication system.

A. Touch

Touch is one of the commonly evaluated biometric features in the continuous authentication system. This is because the data can be collected with reliably and without any need for any extra sensors. Screen gestures like the swipe of the finger and the pinch are used to create a profile of the user. A behavioral feature vector is obtained from this and this is used to authenticate the user continually when they are using the phone. Studies show that the way people swipe their finger to accomplish the same task varies significantly (Frank et al., 2013). This can be used to differentiate the user.

From a single swipe, six features can be obtained. They are – the start and the end points, time period,

device orientation, the pressure applied while swiping, phone orientation and the finger size (Frank et al., 2013). In one method, using these attributes a 30-dimensional feature vector was obtained and out of these 30, three of them were removed and the rest 27 were processed using a kernel support vector machine and k-nearest-neighbours classifiers. When a dataset containing 41 using were processed using this method, it achieved an equal error rate between 0% and 4% (Frank et al., 2013).

The above is under the assumption that only one finger is in contact with the screen. But in reality, most of the gestures in the mobile device involves using more than one finger such as pinch zooming and rotating. By obtaining the position coordinates of the area of contact of the finger, the direction in which the finger is moving, speed in which the fingers are moving, the pressure applied and the distance between the used fingers, features for multi-touch can be obtained (Feng 2012). In these multi-touch cases, a second-order auto-regressive model for modeling and mutual information-based metric for gesture recognition is used (Sherman 2014).

An image-based method called graphic touch gesture feature (GTFG) has also been proposed for analyzing the touch data. In this method, the swipe traits are changed to image space to model the dynamics of the swipes categorically (Zhao et al., 2013).

This method is applicable for single and multi-finger swipes. Using this method very low equal rejection rate has been obtained in some of the data sets. An equal error rate between 6.33% and 15.40% has been observed using this method (Zhao et al., 2014). These show the touch dynamics is important in continuous mobile device authentication.

B. Gait Analysis

Another behavioral trait that can be used to authenticate the user is the walking manner This is called as gait analysis. The data needed for gate analysis can be obtained from the gyroscopic and the accelerometer in the mobile devices. There are many methods that can be used to authenticate the user based on gait analysis (Thang et al., 2012, Muaaz and Mayrhofer 2013, Mantyjarvi, 2005, Zhong and Deng 2014, Juefei-Xu 2012). They all vary in the feature that is obtained from the data and the authentication method. Some of these methods include using dynamic time warping (Thang et al., 2012, Muaaz and Mayrhofer 2013. Another method uses frequency domain analysis, and distribution statistics of the obtained data (Mantyjarvi, 2005). This method has obtained an equal error rate of 7%. An another method which involves hidden Markov model is called gait dynamic images (GDIs) (Zhong and Deng 2014). In this method, the data that is collected from the accelerometer is taken and the cosine similarity of the data collected gives the GDI for data at the time t and a signal interval of i (Zhong and Deng 2014). This method has achieved an equal error rate between 3.88% and 7.22% when the nearest neighbor classifier is used to process the data. All the before mentioned method take into account the pace of the user. Several pace-independent methods have also been put forth (Juefei-Xu 2012). One method involving the usage of wavelets and SVM classifier has achieved a verification rate between 61.1% and 99.4% at 0.1% false acceptance rate (Juefei-Xu 2012).

C. Facial Feature Recognition

Face recognition is one of the important biometric features that can be considered when continually authenticating the device. This is because of the facial feature of individual are unique except in some cases like twins. Facial recognition for security purpose often involves three steps. First, the face is identified and extracted from the image that is obtained from the mobile device's camera. Second, the complete features are extracted from the face which is isolated. In the third step, the extracted features are given to a classifier to process it and verify the authenticity of the user. A different method to recognize and process the features which are extracted have been put forth. We will take a look at some of them.

Several methods have been put forward for identifying the face from the image. In one of the methods, a combination of Haar and Adaboost was used to detect the faces. However, it proved to be ineffective when the poses or illumination vary and when there are partial images (Hadid, et al., 2007, Viola and Jones 2004, Ojala, et al., 2002) Next method involves detecting the segment of faces and cumulating them to obtain the facial region (Mahbub et al., 2016). Another method involves the usage of the deep convoluted neural network (DCNN) (Sarkar et al., 2016).

One of the methods to implement face recognition involves usage of one-class SVM (Abeni et al., 2006). There are three steps to it. The first step involves face detection using Viola-Jones detector (Viola and Jones 2004). Next step involves normalizing the illumination of the image using histogram equalization. The final step involves providing the one-class SVM, the obtained features, to check for similarities. Face recognition is based on face and eye detection (Hadid, et al., 2007). This method has an average authentication rate between 82% and 96% under the following conditions Mobile used: Nokia N90, Processor used: ARM9, Size of the image: 40 × 40 and 80 × 80 (Hadid, et al., 2007).

Another way to go about face recognition involves extracting and identifying the attributes present in the face and comparing them to reach a conclusion (Samangouei 2015). A score-based technique was used to check the legitimacy of the user. It was combined with an LBP-based method of Hadid, et al., (2007) to increase the accuracy and performance. The one-class SVM and Fourier transform method achieved an equal error rate between 3.95% and 7.92% (Abeni et al., 2006), while attribute based model achieved an equal error rate between 13% and 30% (Hadid, et al., 2007).

D. Behavior- based Authentication

Behavioral-based Authentication involves authenticating the user based on their activity. A profile of the legitimate user is created by taking into consideration the application he/she uses, the number to which he/she dials, duration of the calls, services that he uses etc. [Li 2011, Li 2014, Basu 2015). After the profile has been established, the system continually monitors the acti-

vity of the user and it checks it against the created profile. If there are any drastic changes in the activity, the system considers the user to be not legitimate. This method has achieved an equal error rate between 5.4% and 13.5% (Li 2011). Since the activity of the user can change over time, the system should be adaptable to the change. For this, a dynamic profiling method has been proposed. This combined with rule-based classifiers and smoothening function has achieved an equal error rate of 9.8% (Li et al., 2014). An another way to profile a user based on their activity involves incremental training (Kayacik et al, 2014). The drawback of this is that the training takes a long time to complete A new method which includes monitoring the application data and trying to determine the user location based on Wi-Fi hotspots and nearby Bluetooth devices have been proposed (Neal 2015). This procedure has a recognition rate of 80% and 93% (Neal 2015).

E. Keystroke Analysis: This method involves profiling user based on their typing. This is a behavioral biometric, so it less accurate when compared to physiological biometric. In this, two parameters are taken into consideration namely, the time period between the press and release a key and the time period between two subsequent key presses. Various methods have been put forth to use this analysis in continuous authentication (Chang, et al., 2012, Ahmed et al., 2017, Clarke and Furnell 2006 and Gascon et al., 2014). But this alone will not be sufficient since the user will not be typing most of the time.

IV. Fusion Methods

Using a single type of biometric for continuous is not practical for the following reasons (Ross and Jain 2004):

- The data obtained may not be processable all the time.
- The data collected may not be valid all the time. For example, a users' touch dynamics may vary when his/her hand is injured.
- A particular sensor may be damaged/not present in the mobile device.

So a continuous authentication system which combines two or more biometric features is required for the system to remain practical. This results in the need to combine the data obtained from the various sensors in the mobile device. The most common method to combine the biometric features are as follows (Saravanan 2017):

- Sample-level: In this method, the data collected from various sensors are combined together before they are processed. For example, the fingerprint from all the fingers can be combined together to make it into a single sample and this sample can be further processed.
- Feature-level: In this method, the sample data from various sensors are processed separately and a vector representation of the data which can be used in decision making is made. This representation is referred to as feature or template set. These features are combined together to create a single feature set.
- Score-level: After a biometric feature has been processed, a score is established which determines whether the user is legitimate or not. This score is compared against the threshold value to determine the legitimacy of the user. Combining score from different biometric modality is called as score-level fusion.
- Decision-level: In this, each modality determines if the user is legitimate or not and then the fusion takes place. Weightage may be given to each modality in order to reach a final decision about the legitimacy of the user.

V. Summary

We have seen the various physiological and behavioral biometrics that can be used in the process of continuous authentication. As the results show, physiological biometric has higher accuracy than the behavioral biometrics. This is due to the fact that the behavioral character is bound to change as time goes on, and the dataset to compare against has to be constantly updated. This leads to decrease in performance and accuracy. While designing a continuous authentication system, a balance between performance and accuracy has to be maintained. For example, even though face recognition provides a more constant and secure way of authentication, the process of facial recognition can be resource consuming in mobile devices and hence cannot be done in real time. But trait like touch dynamics is more efficacious in terms of computational time. Thus, a combination of various biometric traits will be more powerful than a single biometric trait in the case of continuous systems.

The issue of usability and security is a cause for concern (Clarke et al., 2009, Crawford and Renaud 2014). In a continuous authentication system, there is usually a threshold value which determines whether a user is legitimate or not. An increase in threshold value would compromise the security of the system and a decrease in it would lead to the usability of the system. It comes down to figuring out which is more important – false rejection rate or false acceptance rate. In the viewpoint of a security system, high a false rejection rate may inconvenience a legitimate user but does not decrease the security provided. But a high false acceptance rate is a cause for concern as others may gain access to the device.

Several surveys have been conducted by other researchers to figure out the usability of a continuous authentication system in real time. In one survey, a model which incorporates the identification of voice, face and keystroke biometrics was given to a group of 27 people. In that, 92% of them consider this model to be more secure when compared to explicit authentication methods like PIN or password (Clarke et al., 2009). And another survey involving 37 participants was conducted in lab and field settings (Khan et al., 2015). It shows that 91% of the group felt that the non-obstructive and continuous method of evaluation to be more convenient than normal methods.81% of them felt that the level of security was satisfactory and 35% were inconvenienced with the false rejection. These studies

suggest that users are open to the idea of the continuous authentication method (Khan et al., 2015).

VI. Proposed Model

Our proposed model involves using multi-modal continuous authentication system which provides a higher level of security. In this model, we use a physiological biometric which is the face and a behavioral biometric which is the touch dynamics.

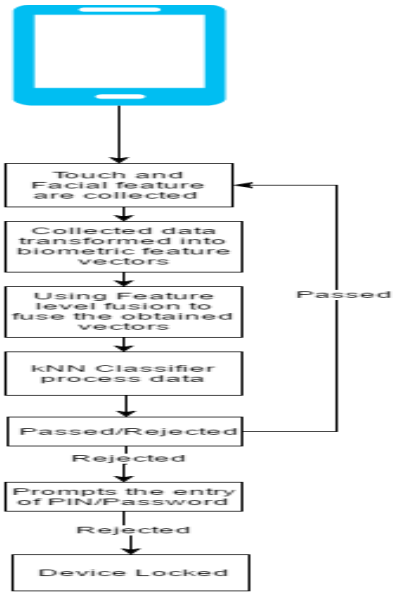

Figure 1: Proposed Model for continuous mobile authentic-cation using face recognition and touch dynamics.

The reason for selecting the touch module are as follows:

1. They have achieved low equal error rate.
2. We will be able to obtain reliable data at all time
3. Does not require additional hardware to obtain the data.

The reason for including the facial recognition module is because they are more accurate than behavioral biometric and the facial data can be obtained easily using the mobile device's front camera.

Next step involves extracting the features from the data obtained from the touch and the facial module. The obtained data can be fused together using feature level fusion. This will result in a new feature set which will represent the user. Then k-nearest-neighbour classifier (kNN) can be used to determine the legitimacy of the user. If the user is found to be legitimate, the phone remains unlocked and the whole process starts again. If the user is found to be illegitimate, then the user is prompted to enter a PIN or password to prove his identity to the system. If the user fails to do so, the phone gets locked.

VII. Conclusion and Future Work

This work was done based on the motivation of securing the mobile device which is now an integral part of our life with a higher level of security by including a system which continually checks for the legitimacy of the user. This work helps even the layman in under stating the usage of biometric features in the system of continuous evaluation. This would help in making the even more secure since the mobile devices contain data which can be damaging to the user if it is revealed to others. Future work of this survey would be an implementation part of the proposed work of securing the mobile device using touch and facial features.

VIII. Acknowledgement

We would like to thank our Guide, Ms. Lalithamani. N, Assistant Professor (SG), Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, for her guidance, valuable comments, and reviews which helped a lot in writing this paper. We also thank our friends for providing their valuable reviews and helpful suggestions.

References

Abeni, P., M. Baltatu and R. D'Alessandro, Nis03-4: Implementing biometrics-based authentication for mobile devices, Proc. IEEE Global Telecom-mun. Conf., Pp. 1-5 (2006).

Ahmed. I.A. Yousif1, A.M. Kikin and H. Mutaqin, Exploring endophytic bacteria origin from jatropha curcas l. and their potential to enhance plant growth in eggplant. Pak.J. Biotechnol. 14(2):238-244 (2017)

Bassu, D., M. Cochinwala and A. Jain, A new mobile biometric based upon usage context, Proc. IEEE Int. Conf. Technol. for Homeland Security Pp. 441–446 (2013).

Chang, T.Y., C.J. Tsai and J.H. Lin, A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. J. Syst. and Software 85(5): 1157–1165 (2012).

Clarke N.L. and S.M. Furnell, authenticating mobile phone users using keystroke analysis. Int. J. Inform. Security 6(1): 1–14 (2006).

Clarke, N., S. Karatzouni and S. Furnell, Flexible and Transparent User Authentication for Mobile Devices, Emerging Challenges for Security, Privacy and Trust, D. Gritzalis and J. Lopez, Eds. Berlin, Heidelberg: Springer Pp. 1-12 (2009).

Crawford H. and K. Renaud, Understanding user perceptions of transparent authentication on a mobile device. J. Trust Manage. 1(7): 1–28 (2014).

Crouse, D., H. Han, D. Chandra, B. Barbello and A. K. Jain, Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data, Int. Conf. Biometrics Pp. 135–142 (2015).

Feng, T., Z. Liu, K. A. Kwon, W. Shi, B. Carbunar, Y. Jiang and N. Nguyen, Continuous mobile authenticcation using touchscreen gestures, Proc. IEEE Conf. Technol. Homeland Security Pp. 451–456 (2012).

Frank, M., R. Biedert, E. Ma, I. Martinovic and D. Song, Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Inform. Forensics and Security 8(1): 136–148 (2013).

Gascon, H., S. Uellenbeck, C. Wolf and K. Rieck, Continuous authentication on mobile devices by analysis of typing motion behavior, presented at Proc. GI Conf. Sicherheit (Sicherheit, Schutz und Verlsslichkeit) (2014).

Hadid, A., J. Heikkila, O. Silven and M. Pietikai nen, Face and eye detection for person authentication in mobile phones, Proc. ACM/IEEE Int. Conf. Distributed Smart Cameras Pp. 101–108 (2007).

http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

Juefei-Xu, F., C. Bhagavatula, A. Jaech, U. Prasad and M. Savvides, Gait-ID on the move: Pace independent human identification using cell phone acc-elerometer dynamics, Proc. IEEE Int. Conf. Biome-trics: Theory, Applicat. and Syst. Pp. 8–15 (2012).

Kayacik, H.G., M. Just, L. Baillie, D. Aspinall and N. Micallef, Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors. CoRR, abs/1410.7743 (2014).

Khan, H., U. Hengartner and D. Vogel, Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying, 11th Symp. Usable Privacy and Security (SOUPS-15) Pp. 225–239 (2015).

Khan, H., U. Hengartner and D. Vogel, Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying, 11th Symp. Usable Privacy and Security (SOUPS-15) Pp. 225–239 (2015).

Li, F., N. Clarke, M. Papadaki and P. Dowland, Active authentication for mobile devices utilising behaviour profiling. Int. J. Inform. Security 13(3): 229–244 (2014).

Li, F., N. Clarke, M. Papadaki and P. Dowland, Behaviour profiling for transparent authentication for mobile devices, Proc. Euro. Conf. Inform. Warfare and Security Pp. 307–314 (2011).

Mahbub, U., V. M. Patel, D. Chandra, B. Barbello and R. Chellappa, Partial face detection for conti-nuous authentication, Proc. IEEE Int. Conf. Image Processing (2016).

Mantyjarvi, J., M. Lindholm, E. Vildjiounaite, S.M. Makela and H. Ailisto, Identifying users of port-able devices from gait pattern with accelerometers, Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 2: ii/973–ii/976 (2005).

Muaaz M. and R. Mayrhofer, An analysis of different approaches to gait recognition using cell phone based accelerometers, Proc. Int. Conf. Advances in Mobile Computing and Multimedia, Pp. 293:293–293:300 (2013).

Neal, T., D. Woodard and A. Striegel, Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits, Proc. IEEE Int. Conf. Biometrics Theory, Applicat. and Syst. Pp. 1–6 (2015).

Ojala, T., M. Pietikainen, and T. Maenpaa, Multi-resolution gray-scale and rotation invariant texture classification with local binary patterns, IEEE Trans. Pattern Anal. & Mach. Intell. 24(7):971-987 (2002).

Ross A. and A. K. Jain, Multimodal biometrics: An over view, Proc. Euro. Signal Processing Conf. Pp. 1221–1224 (2004).

Samangouei, P., V.M. Patel and R. Chellappa, Attribute-based continuous user authentication on mobile devices, Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst. Pp. 1-8 (2015).

Saravanan, D., Improved image searching using user input image fundamental feature technique. Pak. J. Biotechnol. 14(2): 233 – 237 (2017).

Sarkar, S., V. M. Patel and R. Chellappa, Deep feature-based face detection on mobile devices, Proc. IEEE Int. Conf. Identity, Security and Behavior Anal. (2016).

Sherman, M., G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvir-ta and T. Roos, User-generated free-form gestures for authentication: Security and memorability, Proc. 12th Annu. Int. Conf. Mobile Syst., Applicat., and Services, Pp.176-189 (2014).

Shyamala C.K. and T.R. Padmanabhan; An integrated distributed storage design offering data retrievability and recoverability using soft decision decoding of block codes. Journal of Computing and Information Technology 23(3): 191-210 (2015).

Tapellini D., Smartphone thefts rose to 3.1 million in 2013: Industry solution falls short, while legislative efforts to curb theft continue (2014)

Thang, H.M., V.Q. Viet, N.D. Thuc and D. Choi, Gait identification using accelerometer on mobile phone, Proc. Int. Conf. Control, Automation and Inform. Sci. Pp. 344–348 (2012).

Viola P.A. and M.J. Jones, Robust real-time face detection, Int. J. Comput, Vision 57(2): 137–154 (2004).

Zhao, X., T. Feng and W. Shi, Continuous mobile authentication using a novel graphic touch gesture feature, Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst. Pp. 1–6 (2013).

Zhao, X., T. Feng, W. Shi, and I. Kakadiaris, Mobile user authentication using statistical touch dynamics images, IEEE Trans. Inform. Forensics and Security 9(11): 1780–1789 (2014).

Zhong Y. and Y. Deng, Sensor orientation invariant mobile gait biometrics, Proc. IEEE Int. Joint Conf. Biometrics Pp. 1–8 (2014).