Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.01 – 03

Continuous Authentication on Touch Devices using Behavioural Biometrics

Pranav Tiwari, Isha Agrawal, Leena Ahire, Arsh Khan

K. K. Wagh Institute of Engineering Education & Research, Nashik
pranav11.tiwari@gmail.com, agrawalisha1808@gmail.com, leenaahire5@gmail.com, arshkhan7000@gmail.com

Abstract— Authentication has become a part of our daily lives. We need authentication to log in to our emails, to log into our bank accounts, and now even devices. The need of authentication was born because the data stored on these devices or services has become more and more personal with every passing day. To prevent this private data to reach in the hands of wrong people, authentication plays an important role to make sure that the person accessing the data is the owner of the information or at least is authorized to view the information. Smartphones store a great deal of private information these days, from personal photos to sensitive documents. But the authentication on smartphones are inherently weak and do not follow the same standard as account passwords do. Account passwords require you to make your password difficult to some minimum requirements. But smartphones allow any type of passwords which may be weak. Apart from passwords, smartphones allow for PIN and pattern type of authentication which are again less secure than passwords. And all types of authentication techniques on touch devices are entry point authentication techniques including the ones mentioned above. This paper discusses an authentication technique that will actively monitor user behaviour to provide real time authentication to the user and thus potentially proving to be a better authentication technique.

Keywords— behavioural biometrics, active authentication, touch devices, security, user authentication

INTRODUCTION

Authentication is a technique to allow only an authorized user to view or modify the data. Authentication methods on touch based devices are primarily PIN, pattern and password. Out of which, PINs and patterns are widely popular because of the ease of use. Even though these methods offer significant security, the laziness of the user blemish the security offered. Users often keep overtly simple passwords, PINs and patterns because they're to be entered hundreds of times over the period of a day to unlock their device. These simple passwords and patterns are often easy to guess and/or shoulder surf.

There are other methods which are more secure than the regular entry point authentication systems such as fingerprint sensors, iris scanners, etc. These methods often require the usage of extra hardware which uses cost and space on the device. And despite that, since these only provide entry point authentication, the intruder may force the genuine user to unlock the device for him (For example, a thief who threatens the user to unlock the device for him) and then use it. In that case, an entry point authentication system fails in its entirety.

So as to avoid a scenario like the one previously described, continuous authentication must be used where the authentication takes place in real time and unlike entry point authentication techniques, it continuously monitors the user to check if it's the genuine user or if somebody else has started using the device.

This paper tries to mitigate the aforementioned problems by proposing a potential solution by using continuous authentication employing behavioural biometrics. The proposed solution will provide continuous authentication without any inference in the ergonomics of the device. Behavioural biometrics is used to provide an insight on the behaviour of the user. Every user has a unique behavioural trait that can be tracked, profiled and monitored to achieve this continuous authentication.

BACKGROUND AND RELATED WORK

Reference [1] was one of the first active authentication system developed. It was developed the US Defense Advance Research Project Agency's (DARPA) Active Authentication program for continuous authentication of users by using behavioural biometrics authentication systems, which does not depend on specific hardware or sensors. The authors build a biometric profile by observing the behaviours such as mouse movements, keystrokes and application usage. The aim was to determine if a regular office user would be able to use the system without hindrance which was proved. And the false user would be detected in a mean time of 18 seconds using keyboard, 2.4 minutes if using the mouse and 1.5 minutes by tracking application usage.

[2], [3] talk about the use of mouse for acquiring behavioural biometric data to detect intrusion, perform user verification and authentication. [3] mentions and analyses the hazard of using continuous authentication. It also gives experimental results and data from different computers to show how user behaviour varies from machine to machine. This that inspired our methodology to make sure that the system performs closely, if not identically, on various types of touch devices.

[4] discusses a similar approach that we will use in this paper by using touch input to perform authentication. The author uses the information from the stroke to classify the input. The classification algorithm is used to perform authentication and verify if the user is a genuine user or not.

METHODOLOGY

This paper aims to perform continuous authentication on a touch device by using behavioural biometrics. The biometric profile will be created using the user's behaviour data and the data from the device sensors. All touch devices, be it smartphones or tablets, now-a-days come with accelerometer and gyroscope. These sensors can be used to collect the reading when a touch operation is being performed along with the readings just before and after the touch operation is performed. All this data has to be extracted and stored and processed to create a profile first which will define the classes which will further go on to classify if the touch operations being performed are of a genuine user or an intruder.

A. Anticipation

We use the expectation maximization model to anticipate the next touch operation given that we have some sensor data that has previously occurred just before a specific kind of touch operation. We will be storing the features from the touch interaction in a vector [5]. Now, while we anticipate the touch operation, let this vector with unknown parameters be called Θ. Since it is given that we already have acquired some sensor data and are anticipating a touch operation, let's call X, as the set of data obtained from the sensors. And let Z be the latent discrete variable of unobserved values. We calculate marginal likelihood of an anticipated touch operation. This gives us a likelihood of the anticipated touch operation between 0 and 1.

B. Action and its Evaluation

As performed in [5], the touch operation's features will be extracted into the vector Θ and its features will be selected by using the selection parameters by checking the inter-class and intra-class scores. The selected features will be overwritten in the vector Θ, along with additional parameters that are, application name in which the action is being performed, and the sensor readings to denote the orientation of the device on which the touch operation is performed. This vector will be checked by a classification algorithm for each feature to generate a classification score. This classification score will depend upon the number of features selected during the stage of feature selection.

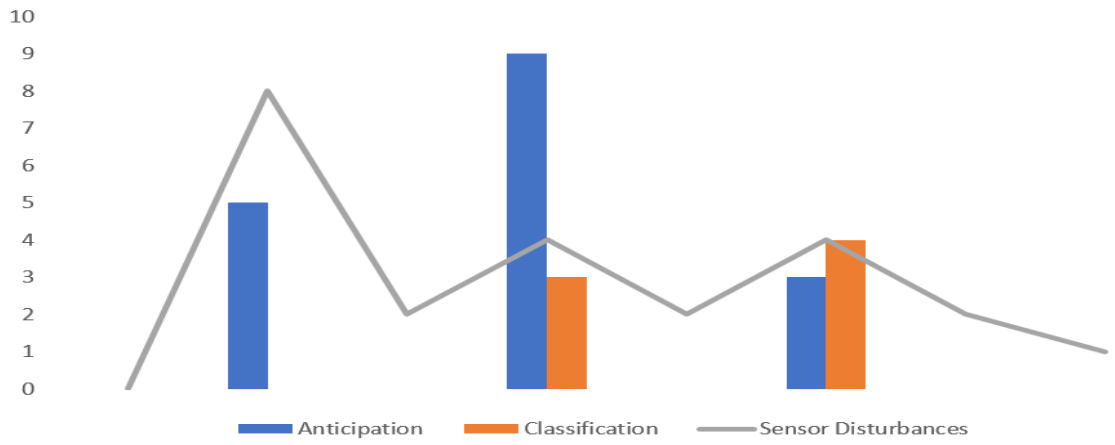

Fig. 1 Double-Tap Operation Readouts

Let us take an example of a double-tap touch operation on a smartphone. Now, during the anticipation of a double tap, there will be an observed spike (first spike in the above figure) in accelerometer reading as the user will clinch the phone due to contraction of the muscles on the base of the finger used to perform the action. Upon this observed sensor activity, it will start calculating the anticipation probability (marginal likelihood, in blue) for every known touch operation type. After which, when the first tap occurs (second spike), it will again anticipate another tap, since the sensor will read a slight jolt, with a marginally higher probability than for other type of operations due to the shorter than normal duration of the first tap (individual tapping duration in a double tap is marginally lower than normal tap durations). Figure 1 shows the example operation's reading behaviour and anticipation. It will also calculate the classification scores of both the taps performed. The classification score and the probability of anticipation of the next touch operation are added to give a final score which will determine if the operation performed is by an intruder or the genuine user.

CONCLUSION

This paper aims to give an idea about how the behavioral biometrics can be used to perform authentication continuously. This kind of authentication is far from perfect and is not meant to replace the existing entry point authentication systems but rather work in synergy with them. The idea of using behavioral biometrics for the purpose of authentication creates hurdles like gauging the proper distinction and variance between the behavior of different users. With the advancements in machine learning and natural language processing, we may find such behavioral biometrics potentially in every device that needs authentication. We are going to build the system proposed in this paper and add evaluation results in the future about how this system fairs against the existing methodologies.

REFERENCES

[1] *Active Authentication*, document DARPA-BAA-12-06, Defense Advanced Research Projects Agency, Arlington, VA, USA, 2012.

[2] N. Zheng, A. Paloski, and H. Wang, "*An efficient user verification system via mouse movements*," in Proceedings of the 18th ACM conference on Computer and communications security, ser. CCS '11. New York, NY, USA: ACM, 2011, pp. 139–150.

[3] Z. Jorgensen and T. Yu, "On mouse dynamics as a behavioral biometric for authentication," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 476–482.

[4] M. Frank, 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. Inf. Forensics Security*, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[5] Chao Shen, Yong Zhang, Xiaohong Guan, and Roy A. Maxion, "Performance Analysis of Touch-Interaction Behavior for Active Smartphone Authentication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 498–513, March 2016.

[6] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and I know it's you! Implicit authentication based on touch screen patterns," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, Austin, TX, USA, 2012, pp. 987–996.

