Tracing One's Touches: Continuous Mobile User Authentication Based on Touch Dynamics

Completed Research

Dongsong Zhang
The University of North Carolina at Charlotte
dzhang15@uncc.edu

Lina Zhou
The University of North Carolina at Charlotte
lzhou8@uncc.edu

Sailakshmi Pisupati
University of Maryland, Baltimore County
pika1@umbc.edu

Abstract

Despite that tremendous progress has been made in mobile user authentication (MUA) in recent years, continuous mobile user authentication (CMUA), in which authentication is performed continuously after initial login, remains under studied. In addition, although one-handed interaction with a mobile device becomes increasingly common, one-handed CMUA has never been investigated in the literature. There is a lack of investigation of the CMUA performance between one-handed and two-handed interactions. To fill the literature gap, we developed a new CMUA method based on touch dynamics of thumb scrolling on the touchscreen of a mobile device. We developed a mobile app of the proposed CMUA method and evaluated its effectiveness with data collected from a user study. The findings have implications for the design of effective CMUA using touch dynamics and for improvement of accessibility and usability of MUA mechanisms.

Keywords

Mobile user authentication, one-handed interaction, touch dynamics, security

Introduction

Recent advances in sensing and wireless communication technologies have propelled the ubiquitous and pervasive use of touch-screen mobile handheld devices (e.g., smartphones) in daily work and life activities, resulting in fast-growing mobile applications such as mobile payment, banking, ride-sharing, and m-Health. The number of smartphone users worldwide increased from 1.57 billion in 2014 to 2.53 billion in 2018. Mobile devices are transforming the way that businesses are done and services are delivered. According to the Internet Retailor 2017 Mobile 500 Guide, mobile commerce accounts for 38% of U.S. e-Commerce and grows faster than traditional e-Commerce. More and more consumers make purchases, payments, stock trading, check deposit, and wire transfer, etc. through their mobile devices. Workers also become increasingly mobile nowadays, with many enterprises allowing their employees to use mobile devices to do their work at office, home, or while traveling.

Due to convenience, ubiquity, and portability of mobile devices, an increasing amount of personal, important, or sensitive data and information is stored on those devices, ranging from personal contact information and medical reports to classified work-related documents. Those important data and information are exposed to high security risks. First, mobile devices can easily get lost or stolen. According to Statista[1], 10 percent of U.S. survey respondents lost or had a smartphone stolen in 2015. A stolen phone may be hacked, in which the personal information stored on the phone could be accessed illegally. According to a Pew Research Center Report, 28% smartphone owners do not use a screen lock or other security features to access their phone. Second, even though a mobile device is password-protected, passwords can be stolen through video surveillance or shoulder-surfing when people use a device in public. Therefore, securing mobile devices through effective user authentication is critical for preventing unauthorized misuse or abuse of information stored on those devices. Here we define mobile user authentication (MUA) as the process of verifying a user's legitimate right to access a mobile device (Abdulhakim and Abdul, 2014).

Authenticating users of a mobile device or application effectively and non-intrusively can be challenging. Current common MUA methods such as passwords, pins, and secret patterns are often ineffective and insufficient, and suffer from several limitations. First, studies have shown that users tend to choose a simple password like '12345' for their mobile devices because of relative difficulty in password entry (Patel et al. 2016), which can be compromised easily. Verizon's 2013 Data Breach Investigations Report confirmed that weak or default passwords and reused credentials were still the main source of mobile device security breaches. Second, if one does not exercise adequate vigilance such as shoulder-surfing attacks after an initial login authentication, then someone may be able to gain access to his/her device. Third, although non-password MUA methods such as physiological biometrics and gait-based methods have emerged, they often require special hardware or certain body movements that are easily observable. Fourth, current MUA methods mainly focus on login authentication while paying less attention to continuous authentication after initial login.

Continuous MUA (CMUA), particularly implicitly CMUA, has potential to address the above-mentioned limitations. To this end, this research proposes an implicit CMUA method that relies on touch dynamics of swiping behavior on a mobile device touchscreen. The swipe gesture brings several distinct advantages to implicit CMUA because of its common use, support of one-handed interaction, and rich information (e.g., its direction and duration). In addition, this study compares the performance of the proposed model between one-handed and two-handed interactions for the first time. The results of empirical evaluation not only demonstrate the effectiveness of the proposed approach to CMUA for both one-handed and two-handed interactions, but also provide insights into the impact of swipe direction (i.e., vertical and horizontal) on the performance of CMUA. The findings of this study offer both research and practical implications for improving the security, usability, and accessibility of CMUA.

The rest of the paper will be organized as follows. It first provides the research background and introduces related work on CMUA. Next, it presents the design of the proposed implicit CMUA approach, followed by reporting the results of the empirical evaluation. Finally, it summarizes major findings and discusses research contributions, practical implications, and future research opportunities.

Background and Related Work

Continuous mobile user authentication (CMUA) requires the user to re-authenticate or re-verify his/her identity after initial login. CMUA is of paramount importance because any user who gains unauthorized access to a device can do whatever he/she wants.

Technically, MUA methods designed for point-of-entry authentication can be re-purposed for CMUA. However, they generally require users to attend to explicit authentication behavior, which would lead to interruptions of their ongoing activity. Additionally, it is challenging to determine the frequency of deploying CMUA when applying point-of-entry MUA methods. Furthermore, those methods have their own limitations. For example, password-based authentication (e.g., text or image password), despite being the most popular method for point-of-entry MUA, faces a significant tradeoff between security and usability. In other words, simpler passwords are easier to remember but more insecure, while complex passwords are more secure but difficult to remember and enter. Additionally, passwords are easy to be hacked or stolen. Physiological biometrics based authentication methods, such as fingerprints, iris scan, and face, voice, or palm recognition (e.g., Chen et al. 2011; Trewin et al. 2012; Memon et al. 2017), are accurate, but raise privacy concerns and are vulnerable to replay (e.g., finger residue) and spoof (e.g., iris copy) attacks.

[1] https://www.statista.com/statistics/441650/items-lost-stolen-while-traveling/

The state-of-the-art CMUA methods are aimed to implicitly determine whether the current user is authenticated or not in a continuous manner. Here implicit MUA refers to the process of authenticating a user by employing the patterns of his/her mobile device use instead of by explicitly requiring deliberate actions from the user. Implicit MUA typically uses sensors and accessories built in a mobile device, such as gyroscope, touch screen, accelerometer, orientation sensor, and pressure sensor, to monitor a user's activities and device movement in a continuous yet transparent manner. Those sensors are capable of providing raw data with high precision and accuracy. According to Crawford and Renaud (2014), 73% of their participants felt that implicit authentication based on behavioral metrics would be more secure than traditional explicit methods such as passwords. Therefore, implicit authentication is much more suitable for CMUA than explicit authentication.

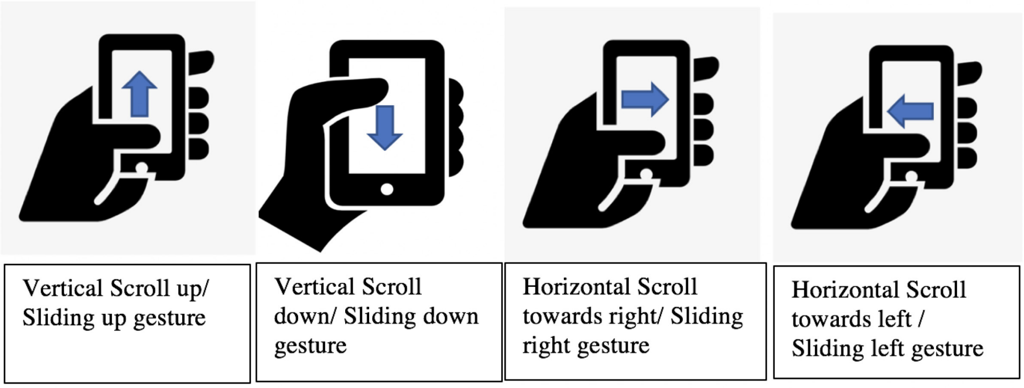
The performance of implicit CMUA methods heavily rely on the consistency, robustness, and effectiveness of user behavioral features used for building authentication models. Based on the types of features, existing CMUA methods can be classified into the following categories:

- Touch-dynamics based methods. They authenticate users based on their touch gestures and finger movements on the touch screen of a mobile device while performing certain basic operations, such as swiping (Zhou et al. 2016; Feng et al., 2012; Frank et al. 2013; Zhang et al. 2015).
- Keystroke dynamics based methods. They utilize features extracted from a user's keypad behavior on a mobile device (i.e., typing and key event patterns) (Krishnamoorthy et al. 2018; Patel et al. 2016). The assumption of this approach is that keystroke patterns should have the same neurophysiologic factors that make hand-written signatures unique. The downside of the keystroke dynamics based approach is its low accuracy caused by the difficulty in interacting with tiny soft keyboards on mobile devices. With special lighting and high-resolution photos, one can easily deduce a secret pattern by tracing oily residues or smudges on the screen of a mobile device. In addition, keystroke dynamics based authentication can only work when a user is using a keyboard on a mobile device.
- Gesture based methods. They distinguish users based on certain gestures (e.g., body or hand gestures) (Liu et al 2017). For example, users can be identified by their hand gestures when they are holding mobile devices (Guerra-Casanova et al. 2012).
- Gait based methods. They rely on characteristics of one's distinctive way of walking for authentication (Cola et al. 2016). Data used by this type of method is often collected or measured by the accelerometer and gyroscope sensors within mobile devices, or cameras or separate sensors placed in an environment. Given the nature of gait and gesture-based approaches, they can be easily observed and learned by others.
- Context-based methods. They build models based on user routines, such as location, phone calls, and application usage, and assign a positive or negative score to each user's routine (Shi et al. 2010). However, such context-based (e.g., location and time) approaches to MUA raise privacy concerns (Preuveneers and Joosen, 2015).

The literature review shows that touch dynamics holds great promise for CMUA for two main reasons: 1) touchscreen has become a defacto component of modern mobile devices. Users are constantly engaged in touch behavior while interacting with mobile devices; and 2) touch behavior does not pose significant privacy and security risks as exposed by other alternative methods. Thus, our design of CMUA method is based on touch dynamics, particularly on one of the most frequently used touch gestures — swipe. Mobile users commonly use swipe to navigate content on a mobile touchscreen. We selected swipe gestures in our method design also because it introduces a diverse (e.g., horizontal vs. vertical direction) and rich (e.g., stroke and pressure based) set of features, which can facilitate CMUA. In addition, a user can easily perform a swipe using his/her thumb during one-handed interaction, i.e., using the same hand to hold a device and perform a swipe gesture simultaneously. Prior research (Karlson and Bederson, 2008; Lai and Zhang, 2015) has suggested that users prefer one-handed interaction with mobile devices so that they can free the other hand for something else, let alone those users who have hand or arm impairments. It can be argued that a user's interactive behavior on a mobile device screen in one-handed interaction can vary significantly from that in two-handed interaction. However, none of the existing studies on CMUA has investigated and made a comparison between the models of one-handed and two-handed interactions. In addition, we did not find any studies that investigated the effectiveness of different types of swipes (e.g., vertical vs. horizontal) separately on CMUA. To address the above-mentioned limitations, this study proposes to use swipe dynamics to develop models for implicit CMUA and evaluate and compare model performances between one-handed and two-handed interactions. The proposed method has significant implications for improving usability and accessibility of CMUA.

Method

We propose an implicit approach to CMUA based on thumb swipes. Among thumb-based swipe gestures, we selected four common types: vertical scroll-up, vertical scroll-down, horizontal scroll-left, and horizontal scroll-right (see Figure 1).


Vertical Scroll up/ Sliding up gesture

Vertical Scroll down/ Sliding down gesture

Horizontal Scroll towards right/ Sliding right gesture

Horizontal Scroll towards left / Sliding left gesture

Figure 1. Four Swipe Gestures

CMUA can be viewed as a binary classification task – to classify a current mobile device user either as an authentic or as an unauthentic user based on a set of input features. Given a rich set of features that swipe gesture induces, we extracted input features from different levels: touch point, swipe, and hand.

A touch point *tp* is the point on the touchscreen that the user touches using his/her thumb or finger. This touch point is measured by several key features, such as x and y coordinates on a touchscreen, pressure applied by the thumb on the screen, size of the thumb at the time of touch, and the duration of touch. The measurement of (x, y) coordinates is in reference to the upper-left corner of the touch screen of a mobile device (see Figure 2(a)).

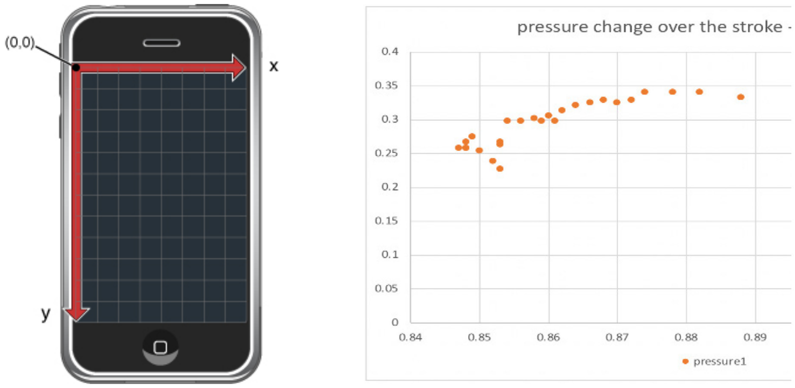


Fig. 2(a). (x, y) coordinates of a screen

Fig. 2(b). Variation in Pressure

Figure 2. Predictive Behavioral Features

A swipe is a set of sequential touch points between the first thumb press on a touch screen and the point where the thumb is lifted up from the touchscreen. It can be represented as $<t_1, t_2, t_3, ...t_n>$, where t_i is a touch point. We extracted the following swipe-level features:

- The slope of a swipe trajectory, which is the angle from the point (x_s, y_s) where the thumb first touches the touchscreen to the end point (x_e, y_e) where the thumb is lifted up from the touchscreen.

- Swipe curvature: it is computed based on the arc formed by a thumb trajectory while swiping on a touchscreen as tan_inverse $(y_e - y_s)/(x_e - x_s)$.
- Swipe length is the total number of touch points in a swipe.
- Pressure variation: When a user swipes his/her thumb on a touchscreen, he/she is unlikely to apply a uniform pressure across all swipe gestures, but decrease it towards the end of the swipe (Figure 2(b)). To keep track of touch dynamics, we measured pressure at 4 quartiles of a swipe gesture, including the 1st (1qp), 2qp, 3qp, and 4qp quarter pressure.

Measurements of the above features result in a total of 40 second-level features. The hand used to hold the phone can be either left or right hand. Users may interact with a mobile device using both hands (i.e., with one hand holding the device and the other interacting with it) or a single hand (i.e., using the same hand that holds the device to interact with it).

In order to examine the effect of different types of swipe gestures, we constructed three types of CMUA models – one vertical stroke model (Model 1), one horizontal stroke model (Model 2), and one combined model that integrated both vertical and horizontal stroke features (Model 3). The development of those CMUA models went through two stages – user enrollment and verification. During the enrollment stage, we collected data about users' swipe dynamics. During user verification, we built classification models based on features extracted from swipe dynamics. In this study, we chose four common machine learning techniques to build authentication models, including Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), and Support Vector Machines (SVM).

Evaluation

A total of 15 participants voluntarily participated into this study. They were recruited from a public university at the east coast of the U.S. The participants consisted of 6 males and 9 females between 22 and 27 years of ages. They all owned touch-screen smartphones. All participants were right-handed except for two. Two-thirds of the participants were Android users and one-third were iPhone users. Prior to enrollment, the participants went through a training session in a research lab, in which they were asked to interact with Samsung Galaxy S6 smartphones with a 5.1-inch touch screen, which were the same devices as they would use in the formal study. Given that the swiping activities should be identical between Android phones and iPhones, the participants owning iPhones did not report any discomfort or problems while interacting with the Samsung phones.

In the enrollment stage, the participants were asked to perform two types of tasks: vertical scrolling and horizontal scrolling (e.g., browsing a designated webpage), among others. In the vertical-scrolling tasks, the participants were asked to navigate the content of webpages via scrolling up and down. In the horizontal-scrolling task, the participants were asked to view a sequence of images via left and right scroll. In the verification phase, we trained models of swipe dynamics for individual participants using data collected from the enrollment phase.

In order to compare the constructed CMUA models between single-handed and two-handed interaction, which has never been investigated before, the participants were asked to first use the same dominant hand to hold the phone while performing the above tasks (i.e., single-handed CMUA), then switch to the non-dominating hand to hold the phone while using the dominant hand to perform similar activities (i.e., two-handed CMUA). The participants created 180 strokes on average across single-handed and two-handed CMUA and across vertical and horizontal swipes.

We used 10-fold cross-validations to evaluate the performance of CMUA based on some common metrics, including accuracy and Equal Error Rate (EER). Accuracy is measured as the percentage of authentication decisions that were made correctly. EER is defined as the rate at which FAR and FRR are equal (Zhou et al. 2016). False Acceptance Rate (FAR) is defined as the percentage of authentication decisions when a CMUA model incorrectly allows an access attempt by an unauthorized user, as represented in Equation (1). False Rejection Rate (FRR) is defined as the percentage of authentication decisions when the access of an authentic user is denied, as shown in Equation (2). For a CMUA model, maintaining a low FAR has always been preferred over a low FRR.

$$FRR = \frac{|Rejected\ authentic\ cases|}{|authentic\ cases|} \qquad (1)$$

$$FAR = \frac{|accepted\ authentic\ cases|}{|imposter\ cases|} \qquad (2)$$

Results

The accuracies of the models with different classification algorithms are reported in Table 1. They are the average accuracies of 10-corsss validation. The results show that 1) the touch dynamics of vertical swipes or horizontal swipes alone can serve as a promising source for building CMUA models; 2) compared with horizontal swipe, vertical swipe based models are generally more effective for CMUA; and 3) combining features of touch dynamics of vertical and horizontal swipes resulted in worse performance than using that of vertical or horizontal swipe separately.

Classifiers	Model 1 (vertical swipe features only)	Model 2 (horizontal swipe features only)	Model 3 (Combined features)
Decision Tree	96.70	94.05	93.07
Naïve Bayes	94.73	88.41	70.20
Random forest	96.7	96.36	95.03
SVM	97.41	88.41	84.55

Table 1. Accuracy (%) of one-handed CMUA models

Because the models with vertical swipes produced the best CMUA performance, as shown in Table 1, we further compared the performances of one-handed vs. two-handed CMUA models with vertical swipe features in terms of EER, aiming to examine whether there is any potential difference between the two types of interactions. The results show that the models built with vertical swipe features extracted from two-handed interactions produced significantly lower EERs (0.0041) than those built with features from one-handed interactions (0.0309).

Discussion

This study enriches the literature on CMUA by developing and comparing CMUA models based on swiping dynamics on a mobile device touchscreen. The findings of this study reveal that touch dynamics from vertical swiping is more effective for CMUA than its horizontal counterpart, while combining both does not result in performance improvement. These findings suggest that vertical swiping carries more important and unique behavioral characteristics of individual users, and mixing the touch dynamics of horizontal swipe gestures into the same model may introduce noise or present conflicting information for CMUA. These findings have theoretical and technical implications for how to improve the security of CMUA methods.

This research makes three primary research contributions to the field of MUA. First, it proposes and develops swipe dynamics based models for implicit CMUA. Although implicit CMUA is essential to the security and access control of mobile devices, it has been under studied. This study investigates the effectiveness of swipe dynamics on the touchscreen of a mobile device for implicit CMUA. The best-performed CMUA models in this study outperform alternative models that have leveraged touch dynamics by previous studies (e.g., Zhou et al. 2016; Li et al. 2013). The proposed CMUA method contributes to a growing body of literature on behavioral biometrics based user authentication. Additionally, given the frequent use of swiping on a mobile touchscreen, the proposed implicit CMUA models are generalizable to other contexts where users interact with the touchscreen of mobile devices.

Second, the results show that both vertical and horizontal swipe features can be used for effective MUA, although the former set of features is generally more effective. The finding implies that a CUMA model may incorporate vertical (or horizontal) features with other touch dynamics features, but may not combine features of both swipe types in one model together.

Third, the proposed CMUA model supports one-handed interaction, which has significant implications for improving usability and accessibility of CMUA. Prior research suggests that people prefer to use one hand to hold and interact with a mobile device (i.e., one-handed interaction) so that the other hand can be freed for something else (Karlson and Bederson, 2008). This is especially helpful when a user has situational impairment (e.g., when holding an umbrella or a cup of coffee in one hand), or has hand or arm impairment. This study is the first one that examines CMUA models under both two-handed and one-handed authentication conditions. Despite that the performance of the one-handed vertical swiping model is encouraging, the results show that the CMUA models built based on two-handed touch dynamics still led to better performance. This finding is not completely surprising in that securing a mobile device with a separate hand allows the user to create more stable and consistent touch dynamics in comparison to using the same hand for both holding and interacting with a device. The finding provides new evidence for addressing the security-usability tradeoff. Although one-handed CMUA is more usable and accessible than its two-handed counterpart, the former may be less accurate than the latter.

There are a few limitations of this study that provide future research opportunities. The combined models in this study integrated input features extracted from both vertical and horizontal swipe behavior. It is worthwhile to explore alternative ways of combining input features such as ensemble models where the classification results of two or more learners (e.g., one based on vertical swipes, and another based on horizontal swipes) can be integrated to generate better final classification results. The data used in this study were collected mainly from swipe dynamics only. A mobile device user mostly likely interact with the touchscreen via a mixture of touch gestures such as interweaving swipe, tap, and pinch. Thus, a natural extension of this study would be to investigate whether incorporating diverse types of touch gestures can further improve the performance of CMUA. In addition, the current experiment data were collected from one lab session. In view that touch dynamics may vary with usage context, it would be interesting to explore the stability and robustness of swipe dynamics for CMUA over time in future research. Finally, the sample size of this study is relatively small. It would be beneficial to conduct a future study with a larger sample size.

ACKNOWLEDGEMENTS

This research was supported in part by the National Science Foundation (Award #s: CNS 1704800 and SES 1527684). Any opinions, findings or recommendations expressed here are those of the authors and are not necessarily those of the sponsor of this research.

REFERENCES

Abdulhakim, A. and Abdul, M. (2014). "Touch Gesture Authentication Framework for Touch Screen Mobile Devices," *Journal of Theoretical & Applied Information Technology*, 62, 493-498.

Chen, C., Lee, C., and Hsu, C. (2011). "Mobile device integration of a fingerprint biometric remote authentication scheme," *International Journal of Communication Systems*. https://doi.org/10.1002/dac.1277

Chiang, H. & Chiasson, S. (2013). "Improving user authentication on mobile devices: a touchscreen graphical password," *MobileHCI'13*, August 27-30, 2013, Munich, Germany. 251-260

Cola, G., Avvenuti, M., Musso, F., and Vecchio, A. (2016). "Gait-based authentication using a wrist-worn device," MOBIQUITOUS 2016: Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. Hiroshima, Japan, November 28-December 01, 2016. 208-217

Crawford, H. and Renaud, K. (2014). "Understanding user perceptions of transparent authentication on a mobile device," *Journal of Trust Management*, 1, 1-28.

Feng, T., Liu, Z., Kwon, K.A., Shi, W., Carbunar, B., Jiang, Y., Nguyen, N. (2012). "Continuous mobile authentication using touchscreen gestures," *IEEE Conference on Technologies for Homeland Security* (HST), 451-456.

Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D. (2013). "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," *IEEE Transactions on Information Forensics and Security*, 8, 136-148

Guerra-Casanova, J., Sánchez-Ávila, C., Bailador, G., de Santos Sierra, A. (2012). "Authentication in mobile devices through hand gesture recognition," *International Journal of Information Security*. 11(2), 65-83.

Karlson, A. and Bederson, B. (2008). "One-handed Touchscreen Input for Legacy Applications," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1399–1408

Krishnamoorthy, S., Rueda, L., Saad, S., and Elmiligi, H. (2018). "Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning," *Proceedings of the 2nd International Conference on Biometric Engineering and Applications*. Amsterdam, Netherlands, May 16-18, 2018. 50-57

Lai, J. and Zhang, D. (2015). "ExtendedThumb: A Target Acquisition Approach for One-Handed Interaction with Touch-Screen Mobile Phones," *IEEE Transactions on Human-Machine Systems*. June 2015, 362-370.

Li, L., Zhao, X., and Xue, G. (2013). "Unobservable Re-authentication for Smartphones," *Network and Distributed System Security Symposium*, Feb. 24-27, 2013. San Diego, CA, USA. 1–16

Liu, C., Clark, G., and Lindgvist, J. (2017). "Where usability and security go hand-in-hand: robust gesture-based authentication for mobile systems," *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver, Colorado, USA. May 6-11, 2017. 374-386

Memon, Q., Alkassim, Z., AlHassin, E., Omer, M., Alsiddig, M. (2017). "Audio-visual biometric authentication for secured access into personal devices," *Proceedings of the 6th International Conference on Bioinformatics and Biomedical Science*. Singapore, Singapore, June 22-24, 2017. 85-89.

Patel, V., Chellappa, R., Chandra, D., Barbello, B. (2016). "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges," *IEEE Signal Processing Magazine*, 33, 49-61.

Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., and Ben-David, S. (2012). "Biometric authentication on a mobile device: a study of user effort, error and task disruption," *Proceedings of the 28th Annual Computer Security Applications Conference*. Orlando, Florida, USA. December 03-07, 2012, 159-168

Zhang, P., N., Beng, A., Teoh, J., and Chen, K. (2015). Recognizing your touch: towards strenthening mobile device authentication via touch dynamics integration. *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia*. Brussels, Belgium, December 11-13, 2015. 108-116

Zhou, L., Kang, Y., Zhang, D., Lai, J. (2016). "Harmonized authentication based on ThumbStroke dynamics on touch-screen mobile phones," *Decision Support Systems*. 92, 14-24.