ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

A Study on Keystroke Dynamics for Touch Screen

[1] Dr Sonali Vyas [2] Ms. Pragya Vaishnav
[1] Assistant Professor AIIT, [2] Research Scholer AIIT
[1] Amity University,Jaipur,India [2] Amity University Jaipur,India

Abstract: - **At present maximum people store private and sensitive data on their Smartphone. Consequently, the demand is growing for secure mobile authentication methods. Setting a password-based authentication is the most frequently used method to protect data from intruders. However, people tend to use password, which can be easily remembered, hence easy to crack. Therefore, an additional mechanism is needed to enhance the security of password based authentication. One such complementary method is to use the typing pattern of the user, known as keystroke dynamics. Keystroke dynamics or typing dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the pattern of typing on a keyboard. Keystroke dynamics is a behavioral biometric, Keystroke dynamics of mobile referred as Touch dynamics and refers to the process of measuring and assessing human touch rhythm on touchscreen mobile devices (e.g. smartphones and digital tablets). In this paper, we are mentioning the different patterns to authenticate the touch screen mobiles.**

I. INTRODUCTION

This is mobile world and the majority of the transactions are done using mobile devices that includes financial transactions, accessing various websites that need authentication etc. For mobile devices as well as many new laptops, desktops a touch screen acts as a keyboard. The keystroke dynamics that is a behavioral biometrics used as support authentication factor becomes more challenging due to dynamism of a touch screen. And hence becomes more challenging with varying sizes and types of available keyboards to capture the user behavior Keystroke dynamics refers to the process of measuring and assessing human's typing rhythm on digital devices, like computer keyboard, mobile phone, or touch screen panel. Person's typing on digital devices such as pressing keys and releasing keys, and attempt to identify them based on habitual rhythm patterns in the way they type. Some features that are used to measure or assess keystroke dynamics include timing information, e.g., the hold time and the flight time. When an imposter tries to use a Compromised password, it can be easily detected and access can be denied because of the variation in the typing pattern. Due to similar neurophysiologic mechanisms, the rhythms and patterns are idiosyncratic like handwriting or signatures. This technology is relatively cheaper than the fingerprint or retinal scan technology, which requires expensive and extra hardware for data collection. Keystroke dynamics do not require any extra hardware. duration of keystrokes, frequency error control, pressure of keystrokes, Rate of typing, statistics of text etc. To capture keystroke dynamics, it is necessary for users to type their own password a number of times during enrollment. The time duration of each key pressed, the keystroke latency between two successive keys and digraph, the time between key pressed and successive key pressed are measured using real time measurement in our experiment. The Mean and Standard Deviation of these measurements are found and the user profile is created.

Keystroke dynamics include several different measurements which can be detected when the user presses keys in the keyboard. Possible measurements include:

- Latency between consecutive keystrokes.
- Duration of the keystroke, hold-time.
- Overall typing speed.
- Frequency of errors (how often the user has to use backspace).
- The habit of using additional keys in the keyboard, for example writing numbers with the num pad.
- In what order does the user press keys when writing capital letters, is shift or the letter key released first.
- The force used when hitting keys while typing (requires a special keyboard).

Touch dynamics biometrics have their unique merits or useful features, while at the same time, they also introduce challenging issues. The sections below summarize the features and the challenging issues.

A touch dynamics authentication system can offer a number of useful features compared to the other types of biometrics authentication system. These are the following.

Continuous Monitoring: Touch dynamics biometrics can be used to verify the authenticity of a user beyond the initial authentication by constantly monitoring the user touch dynamics patterns. In other words, user reauthentication can be performed easily and non-intrusively throughout an active login session. In this way, security protection goes beyond initial login without compromising usability. This is one of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

the most notable advantages touch dynamics biometrics have over other physiological biometrics. Revocability: In an event when a passcode associated with a touch dynamics template is compromised, a new touch dynamics template can easily be generated when a new passcode is created. This is not the case for other physiological biometrics. For example, with iris or face biometrics, once they are compromised, there will be no replacement, and for fingerprints biometrics, the number of replacements is limited (humans have only 10 fingers to use after all). Non-dependency: A mobile device usually operates in an on-the-go manner, so the surrounding lighting condition and background noise level are, in most cases, constantly changing. In comparison with other biometrics features, such as face and voice biometrics, the feature acquisition of touch dynamics biometrics is less sensitive to these environmental factors. Therefore, it is more suited to, and can be more easily deployed to a mobile device. Transparency: Touch dynamics authentication system requires little or no additional interventions from a mobile device user. This is because the acquiring and processing of touch dynamics patterns can be carried out in the background while the user is using the device. Users may not be aware that their touch dynamics patterns are being captured, the captured data are being used for authentication, and the authentication is carried out periodically or they are protected by an extra layer of authentication. This is in a stark contrast to other biometrics Familiarity: The touch dynamics data used for authentication is acquired during mobile users' routine input activities. This is a process which mobile users are already familiar with, so the data acquisition operation tends to have a gentler learning curve with a higher usability level than other biometrics data acquisition cases. Cost Effectiveness: In contrast to other physiological bio-metrics authentication methods such as iris and fingerprint biometrics that typically require the use of specialized hard- ware, touch dynamics authentication system only uses built- in mobile sensors. This can reduce device costs and it is ideal for large-scale deployments.

II. LITERATURE REVIEW

Authentication is essential to secure access to sensitive data. Authentication is the process of determining whether someone is the one who is claims to be [6] [7]. The task of authentication becomes more complicated with the invent of smart phones. A more recent publication reported by [1] used early generation smart phone with touch sensitive screen, which could be interacted via finger or stylus (special pointing stick). The trend of applying keystroke dynamics biometrics to newer hardware technology should be encouraged, since the interaction method, processing capability, and availability of these devices open to new research dimension and opportunity. Passcode authentication method to achieve an enhanced level of security in user authentication and in the protection of mobile devices. This method can be implemented by employing existing sensors embedded in a mobile device, so it is comparatively cheaper than other biometrics authentication method. In addition, this method is non- intrusive and can operate in parallel with a person's normal mobile device usage activities (Shen et al., 2016). The existing passcode authentication method has a wide social acceptance, and the touch dynamics authentication method is also expected to be widely acceptable by the general public (Campisi et al., 2009). Touch dynamics biometrics refers to the process of measuring and assessing human touch rhythm on touch screen mobile devices (e.g. smartphones and digital tablets). A form of digital signatures is generated upon human interactions with these devices. These signatures are believed to be discriminative and unique for each individual, so may be used as a personal identifier. One of the earliest research works on keystroke dynamics authentication was conducted by Gaines et al.(1980). They carried out an experiment to try to recognize 6 professional secretaries by analyzing the way they typed three passages of texts consisting of 300 to 400 words each. Since then, many related efforts have been made. Crawford, Karnan et al. and Teh et al. have, independently, written surveys of the pub- lished works on keystroke dynamics authentication (Crawford, 2010; Karnan et al., 2011; Teh et al., 2013). However, these early works on Keystroke dynamics authentication largely focus on computer keyboards. With the rapid development of mobile communication technologies, more recent research efforts in this area have been focused on mobile devices with physical keypads (Campisi et al., 2009; Clarke and Furnell, 2007; McLoughlin and Naidu, 2009). Most recently, research activities are largely carried out in the context of touchscreen mobile devices. Fig. 2 summarizes the timelines of the touch dynamics biometrics research as influenced by technological developments in the sector. Touch dynamics biometrics have their unique merits or useful features, while at the same time, they also introduce challenging issues. The sections below summarize the features and the challenging issues.

III. METHODOLOGY

III.1. Working mode

The verification mode may operate in either a static or a dynamic manner. The static and dynamic working modes are complementary to each other, i.e. they may be deployed in-dependently, or alongside with each other to enhance the security protection level afforded to the deployed mobile device. In the following, we discuss the two working modes. Hereafter, we use the term, Verification-in-Static-Mode (ViSM), to refer to the verification mode being used in the

static working mode and, Verification-in-Dynamic-Mode (ViDM), to refer to the verification mode being used in the dynamic working mode.

III.1.1.Verification-in-static-mode (ViSM)

One application scenario of the ViSM is static authentication, which is also known as one-off authentication. In static authentication, a user attempts to authenticate himself /herself to a system at the beginning of a log-in session or at some pre- defined intervals during a session. For example, a touch dynamics authentication method may be integrated with an existing passcode authentication method, forming a so-called two-factor authentication system in which the passcode authentication method serves as the first factor and the touch dynamics authentication method serves as an additional, i.e. the second, authentication factor. This two-factor authentication system provides a stronger level of protection than any of the two authentication methods when they are used alone. In addition, the use of the second authentication factor can also prevent passcode sharing.

III. 1.2.Verification-in-dynamic-mode (ViDM)

An example of application scenario of the ViDM is dynamic authentication, also known as continuous authentication. A dynamic authentication method performs authentication checks on a user in an application or communication session (i.e. after the initial authentication is performed). The dynamics feature may be reflected by the use of information that is generated in real-time during the session to authenticate the user and/ or by the use of multiple instances of authentication in the session, but the intervals between the multiple authentication instances are not predefined, e.g. they may be determined by the occurrence of some touch events. A touch dynamics authentication system is particularly suited to this mode, as touch dynamics data can be acquired transparently over a period of time to revalidate the user's identity without user's intervention, and this may be done at any point during the session. Continuous authentication can reduce security risks in a number of ways such as unauthorized device sharing, device lost/theft, session hijacking, etc. Of course, as in the case of any biometrics authentication method, it is important to achieve a low FRR value to make the system more usable, as, other- wise, a legitimate user may be locked out of the service in the middle of a session. According to our literature survey, more papers have been published for static authentication (77%) than dynamic authentication (23%).

III.2 Timing feature (TM)

The timing feature is the most widely used feature in touch dynamic biometrics. A touch event (finger touching down or lifting up) on a virtual keyboard generates digital interrupts that can be detected by the mobile OS API function calls (Kambourakis et al., 2014). Each of these events can be coupled with a timestamp value. These timestamp values do not have semantic meaning and need to be further manipulated. Based on these timestamp values, two different types of timing feature with varied lengths can be extracted.

III.2.1Timing feature types

By performing mathematical operations on two touch event timestamp values, two types of timing feature types can be obtained. The first one is the Dwell Time (DT) and it refers to the time duration of a touch event with the same key. It is also known as interval, press or hold time in literature. This value can be obtained by subtracting a key release timestamp value from its key press timestamp value. The second one is the Flight Time (FT). It refers to the time interval between the touch events of two successive keys. It is also known as latency. According to Sheng et al. (2005), FTA may have a negative value. This scenario happens when a subject presses the next key before releasing the previous one. However, this scenario is more likely to happen when acquiring the timing feature using a computer keyboard rather than using a virtual keyboard. This is due to the difference in physical and geometrical size of virtual keys against physical keys; it is very rare for a subject to use multiple fingers simultaneously when providing their input on virtual keys. As a result, the chances of pressing the next key before releasing the previous one is significantly reduced or in some cases do not exist when using a virtual keyboard.

III. 2.1.1. Timing feature length

A timing feature can be extracted with different feature lengths. The shortest feature length is known as uni-graph, which is the timing feature extracted by taking the touch event time- stamp values of the same key. The timing features extracted from two or more keys are called di-graph and n-graph, respectively. Graph and di-graph are used. The only two exceptions were the experiments conducted by Giuffrida et al. (2014); Trojahn et al. (2013), where the n-graph with the size of 3 or larger were extracted. The reason why a large n-graph size is not commonly used is that a larger n-graph contains a lower feature granularity (Trojahn et al., 2013). This has been experimentally proven by Giuffrida et al. (2014). In their experiment, the authors compared the ac- curacy performances of different n-graph sizes. The comparison result showed that a larger n-graph size produces a lower ac- curacy performance.

III. 3 Spatial feature (SP)

A spatial feature is a characteristic associated with physical interactions between a fingertip and a device touch screen surface, and it can be acquired when a touch event is per-formed. The three most commonly reported spatial features in literature are touch size, pressure, and position. Visual examples of these three spatial features extracted using

anAndroid mobile device are reported in Y. Meng et al. (2014).

III.2.1. Touch size

The touch size represents an approximation of the screen area being touched in a touch event. Each touch event is associ- ated with a touch size value. The value is typically returned from an API function and is scaled to a value in the range between 0 and 1 (Zheng et al., 2014). This value is normally used as feature data without further manipulation. The touch size value captured from a subject is determined by the subject's fingertip size. For example, Nixon et al. (2014) observed that an adult male subject usually produces a larger touch size value than a child or an adult female subject. This means that it is hard for people with different fingertip sizes to mimic each other.

3.2.2. Touch pressure

The touch pressure is another feature that is often used along with the touch size. A touch pressure value measures the approximated force asserted on the screen upon each touch event. It is expressed in an abstract unit, with a value in the range between 0 (softer touch) and 1 (harder touch) (Zheng et al., 2014). Similar to the case for the touch size, a touch pressure value extracted by an API function can be used directly without further manipulation. A touch pressure value is linked to a sub- ject's finger muscle that is unique to each subject. Therefore, it is hard for one subject to imitate another subject's touch pres- sure purely by observations, making a touch dynamics authentication system that uses touch pressure feature highly resistant to shoulder surfing attacks(Feng et al., 2013.)

3.2.3. Touch position

The touch position is a two-dimensional matrix feature that captures a fingertip landing location on a device screen (or key). Each touch event can be associated with an x and y-coordinate measured in pixel units (Kolly et al., 2012). The touch position feature to identify a subject. This is further supported by the observations reported by among different subjects in their experiment. The touch position can be expressed using two different ways(i) as the absolute coordinates of a touch event relative to the entire Screen (Y. Meng et al., 2014), or (ii) as an offset to the center of a key used (Draffin et al., 2014). Also, by some mathematical manipulations, additional features can be derived. These include the distance (Buschek et al., 2015; Kambourakis et al., 2014), speed (Kambourakis et al., 2014), or angle (Serwadda et al., 2013), between two touch events. However, there is a concern with this coordinate representation of touch posi- tion values (Alotaibi et al., 2014); that is, the coordinate system of a screen is device dependent. Using different devices, the captured touch position values are not consistent. Therefore, touch position values should be normalized, unless data ac- quisition operation is conducted on a device with a similar model (Jain et al,,2014).

III.3. Motion Fetures (MO)

Modern mobile devices are embedded with two hardware motion sensors, the accelerometer and the gyroscope These sensors have been widely used in applications, such as device pairing and sleep cycle monitoring applica -tion, that make use of movement data or are movement dependent (Owusu et al., 2012). Each touch event usually inflicts a small amount of movement and/or rotation to the device. These motion features can be captured and used to identify a subject. The accelerometer sensor measures the linear movement rate applied to a device over time. It is designed to detect the movement along the x, y, and z-axis in both positive and negative directions. These three values are measured in the unit of m/s2 (Aviv et al., 2012). On the other hand, the gyroscope sensor measures the rotation rate applied to a device against the three axes: (i) tilt forward and backward (pitch), (ii) twist from side to side (roll), and (iii) turn from portrait to land- scape (yaw). These values are measured in the unit of rad/s (Giuffrida et al., 2014). Normally, raw motion data obtained from these two sensors are not readily usable as feature data. This is because each touch event generates more than one movement and rotation values. To make the data usable as feature data, we should apply some statistical computations, such as min, max, mean and variance, on the raw data, and the results of these computations can be used as meaningful feature data (de Mendizabal-Vazquez et al., 2014; Ho, 2013). Also, as Zheng et al. (2014) pointed out, both sensors are sensitive to tiny movement changes. There- fore, they chose to combine sensor values of x, y and z-axis into a vector of feature, instead of using them individually. Researchers are divided as to whether the accelerometer sensor actually provides a better discriminative property than the gyroscope sensor. For example, the experimental results from Giuffrida et al. (2014) show that the accelerometer data can better capture a subject's touch dynamics patterns than the gyroscope data. However, the observations made by Cai and Chen (2012) show a different result, i.e. the gyroscope data provide a better accuracy, especially if a subject uses the device while moving. In literature, a majority of the touch dynamics motion feature data are from both types of sensors. This is good because data from both types of sensors may complement each other, leading to a better accuracy in identifying a subject.

IV. CONCLUSION

Currently, mobile devices are used to not only make or receive a call, take photos, and play video games, but also give the special assistance in the business, such as providing

internet access, directing access to e-mail and cooperating data, transferring money, and managing bank account. As a consequence, the authentication of users for mobile devices has become an important issue. In mobile phones, people cannot avoid interaction with keystroke dynamics. However, each person may have different styles to press the key because the typing style is based on user's experience and individual skill which is difficult to imitate. A keystroke dynamics is based on the assumption that different people have unique habitual rhythm pattern in the ways they typed.
The touch screen mobile is our present. However, working on keystroke dynamics for touch screens poses multiple challenges. Our Future work will be to focus on identifying pattern and algorithm that will help in identifying a person uniquely in the below mentioned scenarios.

• The size of touch screen is not fixed and may vary from one mobile device to other. Hence finding pattern with changing size is a challenging task.
• In the case of touch screens the keyboard is not a separate hardware device but is driven by available different software solutions. A user may use different keyboards on the same mobile device. This is another issue that needs to be addressed for pattern identification in touch screen dynamics.

REFERENCE

[1] Pin Shen Teh,1 Andrew Beng Jin Teoh,2,3 & Shigang Yue1(2013) A Survey of Keystroke Dynamics Biometrics1School of Computer Science, University of Lincoln, LN6 7TS, UK 2School of Electrical and Electronic Engineering, Yonsei University, Seoul 120-749, Republic of Korea 3Predictive Intelligence Research Cluster, Sunway University, Bandar Sunway, 46150 P.J. Selangor, Malaysia

[2] Asma Salem Dema Zaidan Andraws Swidan Ramzi Saifan Amman, Jordan Amman, Jordan Amman, Jordan Amman, Jordan(2016) Analysis of Strong Password Using Keystroke Dynamics Authentication in Touch Screen Devices

[3] Stuti Srivastava Department of Physics and Computer Science Dayalbagh Educational Institute, Agra, India stuti.sri0210@gmail.com Prem Sewak Sudhish Senior Member, IEEE Department of Physics and Computer Science Dayalbagh Educational Institute, Agra, India(2016) Continuous Multi-biometric User Authentication

[4] Alotaibi N, Bruno EP, Coakley M, Gazarov A, Monaco V, Winard S,et al., 2014. Text input biometric system design for handheld devices. Proceedings of Student-Faculty Research Day. pp. B7.1–8.

[5] Antal M, Szabó LZ. 2014. Keystroke dynamics on Android platform. Proceedings of the 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, Romania, pp. 131–6.

[6] Shanmugapriya, D., & Padmavathi, G. (2011). An efficient feature selection technique for user authentication using keystroke dynamics. IJCSNS International Journal of Computer Science and Network Security, 11(10), 191-195.

[7] Witten, I. H., Frank, E., Trigg, L., Hall, M., Holmes, G., & Cunningham, S. J. (1999). Weka: Practical machine learning tools and techniques with Java implementations. Department of Computer Science, University of Waikato, New Zealand.