ISSN 2395-1621

Graphical-Based Password Keystroke Dynamic Authentication System for Android/Touch-screen Phone

[#1]Pooja Paigude, [#2] Pooja Parekh, [#3] Samruddhi Taware, [#4] Raavi Vaidya

[1]Paigudepooja@gmail.com
[2]pooja2611994@yahoo.co.in
[3]samru.3011@gmail.com
[4]Raavi4116@gmail.com

[#1234]Department of Information Technology, Sinhgad Institute of Technology and Science
Savitribai Phule University of Pune
Narhe, Pune-41 India

ABSTRACT

Now-a-days, phone security is main concern. There are many traditional ways available to secure your phone. But traditional ways like Pin-Based authentication and physical biometric authentication methods are vulnerable to attacks. Many studies have employed behavioral and KDA (Keystroke Dynamic Authentication) systems which are more secure. KDA uses time feature to enhance security. In this paper, we are proposing a new graphical-based password KDA system for touch screen or android handheld mobile devices for screen size 130mm and 140mm.

Keywords— Keystroke Dynamics Authentication (KDA), security and authentication.

ARTICLE INFO

Article History

Received :20th January 2016

Received in revised form :

21st January 2016

Accepted :25th January , 2016

Published online :

27th January 2016

I. INTRODUCTION

Quick transfer of information or data is the basic necessity in this era. Hence, global access to information is important. That's when handheld devices like mobile phones or smart phones play an important role. Smart phones provide you with the ability to access data anytime and anywhere. But, such type of devices which give you the global access are most prone to attacks that may maliciously allow access to private information to the intruders. Smart phones now-a-days have many built-in authentication methods or the user is allowed to install such applications which allow security in form of Pin-based or physical form authentication. But, such applications are not enough to provide security to banking or any other e-commerce applications on the phone. Hence, studies are growing in biometric security techniques like Keystroke Dynamics Authentication, which are much more secure and reliable. In this paper, we have described the Keystroke Dynamic Authentication system which consists of two factors, the first is correctness of username and password and the second is correctness of typing rhythm. If both of these factors are correct then the user is authenticated. The task of Keystroke dynamics is to note KDA (Keystroke Dynamic Authentication) parameters which are the time intervals between different touches (press) and releases. KDA parameters also note the pressure of every touch. These biometric characteristics are unique for every person making this system more secure.

II. MAIN IDEA

The aim of this android application is to provide 3 levels in terms of security for transaction in banking applications and e-commerce applications. First we are making use of encryption for sending user id and password from the user's mobile phone. Once the user is authenticated he will be shown a graphical password screen. Secondly User is shown with sequence of images user has to select one block from each image. There will be 5 images displayed sequentially. Third, we measure KDA (Keystroke Dynamic-based Authentication) for each image touch. If the KDA parameters during login match with the KDA parameters

© 2015, IERJ All Rights Reserved

registered then the user is successfully authenticated. This paper proposes a new graphical-based password KDA system for touch screen handheld mobile devices. In addition, this paper explores a pressure feature, which is easy to use in touch screen handheld mobile devices, and applies it in the proposed system. This way we would improve security by using graphical authentication in mobile banking applications and e-commerce applications.

III. APPROCHES AND ALGORITHM

A. Registration Phase

Initially the first time user has to register to the system with a username and password. Then a set of 5 images is displayed one by one. Each image will contain an instruction

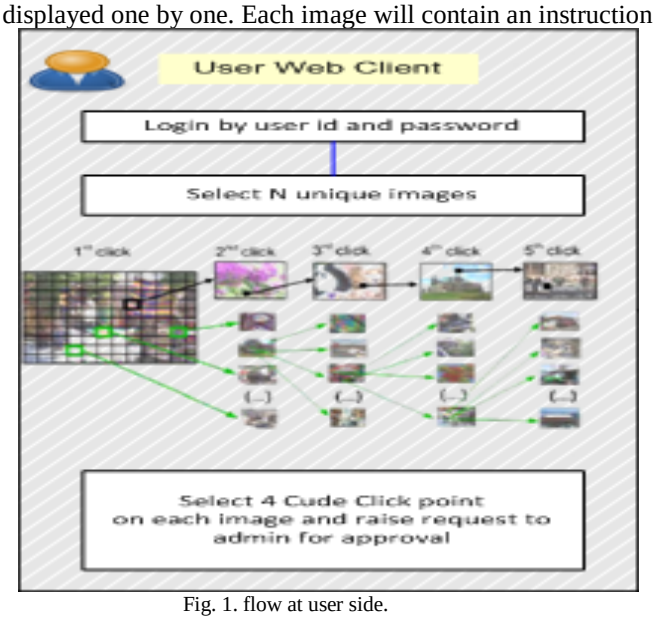

Fig. 1. flow at user side.

to touch (click) on a particular point on the image. Such points on the image are called as Cued Click Points. During this process, when a user's finger presses the touch screen of the handheld mobile device at thumbnail photo 'j' the system captures a pressure feature. In the interval between the press and release of the photo 'j', it will have four kinds of time features. In the i^{th} training sample, the relationships between the features are shown in Fig. 2, where user clicks 'photo1, photo2, photo3, photo4 '.

(1) Down-Up (DU) time: In the i^{th} training sample, the time duration of press and release of photo 'j' is called DUi,j .

(2) Up-Down (UD) time: In the i^{th} training sample, the time interval between the release of photo 'j' and press photo'j+1' is called $UD_{i,j}$.

(3) Down-Down (DD) time: In the i^{th} training sample, the time interval between the press of photoj and press photo'j+1' is called $DD_{i,j}$.

(4) Up-Up (UU) time: In the i^{th} training sample, the time interval between the release of photo 'j' and release photo'j+1' is called $UU_{i,j}$.

(5) Pressure: In the i^{th} training sample, the pressure of th User pressing the screen for photo 'j' is called $P_{i,j}$.

There are (4k − 2) dimensional features. These features of the user's i^{th} training sample include 'k' DU time features, 'k' pressure features,' k – 1' UD time features, and 'k – 1' DD time features. They are denoted separately as DUi set, UDi set, DDi , and Pi set as follows:

$DU_i = \{DU_{i,1}, DU_{i,2}, \ldots, DU_{i,k}\}$

$UD_i = \{UD_{i,1}, UD_{i,2}, ..., UD_{i,k-1}\}$

$DD_i = \{DD_{i.1}, DD_{i.2}, ..., DD_{i,k-1}\}$

$P_i = \{P_{i,1}, P_{i,2}, \ldots, P_{i,k}\}$

These sets of the ith training sample are denoted as:

$feat_i = \{DU_i, UD_i, DD_i, P_i\} = \{X_{i,1}, X_{i,2}, \ldots, X_{i,4k-2}\}$

Note, every user in the system only needs to provide five training samples (i=1-5) in the enrolment phase.[2]

B. Classifier Building Phase

The classifier is built to verify the user's identity after obtaining the personal features. This paper employs a

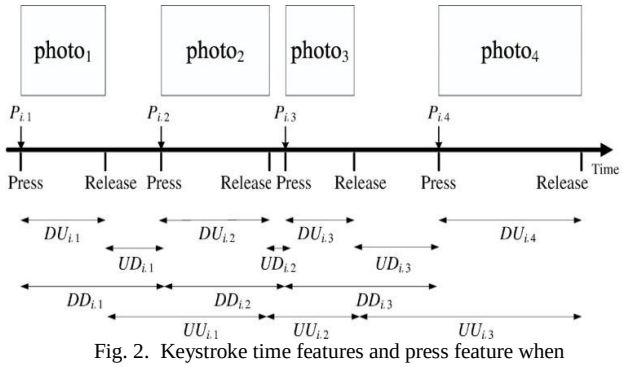

Fig. 2. Keystroke time features and press feature when a user enters a graphical password photo1, photo2, photo3, photo4

.

computation-efficient statistical classifier (Boechat et al., 2007). The mean f and the standard deviation f are calculated for each element in $feat_i$ by equations (1) and (2), respectively.

$$\mu_f = \frac{1}{5}\sum_{i=1}^{5} X_{i,f} \text{ , where } f = 1 \text{ to } 4k-2. \quad (1)$$

$$\sigma_f = \frac{1}{5-1}\sum_{i=1}^{5} \left|X_{i,f} - \mu_f\right| \text{ , where } f = 1 \text{ to } 4k-2. \quad (2)$$

The classifier does not require the impostors' patterns to build. Equations (1) and (2) can be calculated efficiently and are suitable for low-power mobile devices.[1]

C. Authentication Phase

In this phase, the classifier is used to verify the user's identity. After the user enters his or her graphical password, the system compares the sequence of it with the registered one in the registration phase. If it is inconsistent, the system rejects the user's login request.

© 2015, IERJ All Rights Reserved

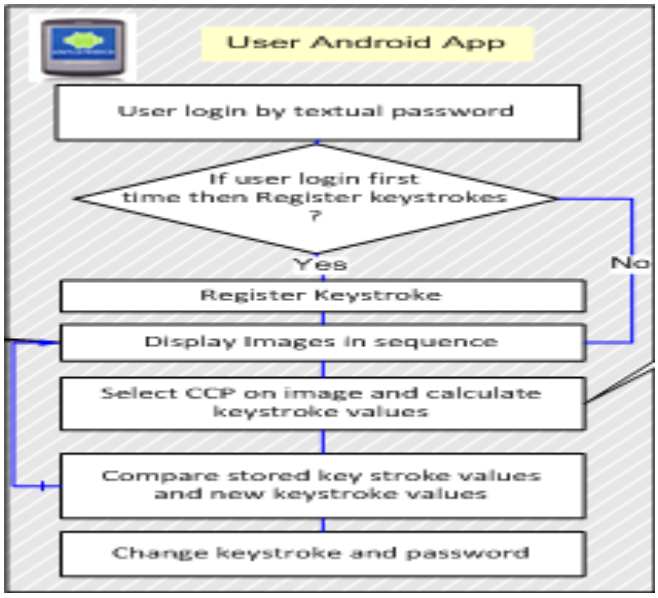

Fig. 3. flow-chart of android application

Otherwise, the corresponding features are examined. An unknown user's features are denoted as

$$feat_v = \{DU_v, UD_v, DD_v, P_v\} = \{X_{v,1}, X_{v,2}, \ldots, X_{v,4k-2}\}$$

and the system calculates the average distance 'D' between each element in $feat_v$ and $feat_i$ by equation (3). The system then accepts or rejects the user's login based on a threshold t. If D < = t, then the user is legitimate. Otherwise, the system rejects the user's login. That is, a user is able to login to a system only if he or she can be successfully authenticated via the graphical password and the KDA authentications.

$$D = \frac{1}{4K-2} \sum_{f=1}^{4K-2} \frac{X_{v,f} - \mu_f}{\sigma_f} \quad (3)$$

This phase only analyzes the distance between the user's login sample and the training samples. Even if the number of users increases, the time for finishing the authentication will not be affected. Similarly, computation in this phase is efficient.

IV. EXPERIMENTAL RESULTS

This paper provides a graphical-based password KDA system developed by Java language and implemented in Android by Android API MotionEvent function library. The press time and the release time were obtained by the getDownTime() and getEventTime() methods, respectively. The system calculates DU, UD, and DD time based on the press time and the release time. The keystroke time features were measured in ms(milliseconds). Android also provides the pressure value via the getPressure() method and it exerted on the device in kilopascals (Meier, 2010).[3] Fawcett (2006) pointed out the KDA system utility can be measured by a ROC (Receiver Operation Characteristic) curve. This paper uses Fawcett's method to calculate FRR and FAR to build the ROC curve and calculates EER to obtain the most balanced optimum threshold for the system. The EER is the system utility when the optimum threshold is obtained. The ROC curve is better than others if its southwestern point is close to the southwest (FAR is lower, FRR is lower, or both). Fig. 4 shows two ROC curves in the experimental results. The solid line denotes the result that uses time features and the dashed line denotes the result that uses time + pressure features. Fig. 4 shows the dashed line is close to the southwest; in other words, the pressure feature is useful for promoting system utility.[3]

V. CONCLUSION

In this paper, we proposed a graphical-based password KDA system for touch screen handheld mobile devices. A User enters his or her graphical password through an identical human–computer interface and therefore the user's keystroke features will not be affected if the user uses different devices. In the experiment, the novel pressure feature applied to touch screens could improve data quality and further promote KDA system utility.

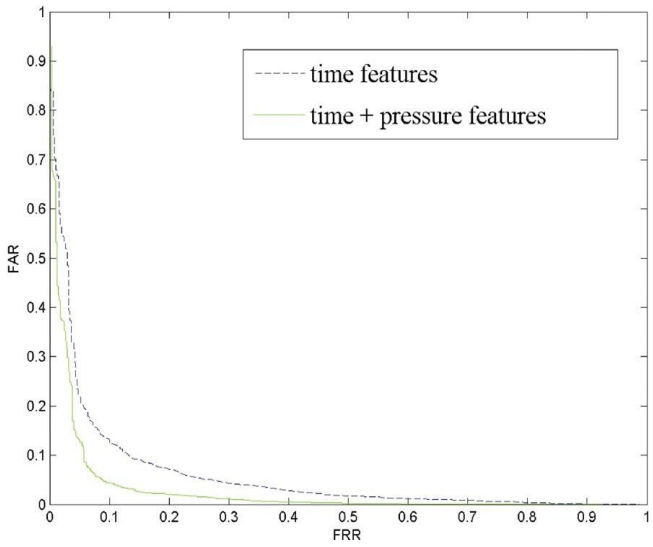

Fig. 4. Experimental Results by ROC

The time and pressure features are obtained when a user enters his or her graphical password so this system does not cause any extra burden on users. In our system, a user is able to login to the system when he or she can successfully authenticate via the graphical password and KDA authentications. Namely, even if the graphical password is revealed by a shoulder surfing attack, the probability of breaking the authentication is reduced. Finally, the performance of the proposed system is excellent, and is suitable for low-power mobile devices.

ACKNOWLEDGEMENT

We take this opportunity to thank all kind of support and help of many individuals and organizations. We would like to extend my sincere thanks to all of them. We are highly indebted to our project guide Prof. S. S. Telsang and Head of Department Dr. Tanaji Khadtare for their guidance and constant supervision as well as for providing necessary information regarding the project. We would like to express my gratitude towards our parents for their kind co-operation and encouragement. Our thanks and appreciations also go to people who have willingly helped us out with their abilities.

© 2015, IERJ All Rights Reserved

REFRENCES

[1] T. -Y. Chang, C. -J. Tsai and J. -H. Lin, "A Graphical-based Password keystroke Dynamic Authentication System for Touch Screen Handheld Mobile Devices", International Journal of Systems and Software, vol. 5, no. 85, (2012), pp. 1157-1165.

[2] Mahnoush Babaeizadeh ,Majid Bakhtiari, Mohd Aizaini Maarof," Keystroke Dynamic Authentication in Mobile Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 90 – No 1, March 2014.

[3] Mradul Shrivasatva,"Summer 2011 Keystroke dynamics for mobile devices –algorithm and authentication".

© 2015, IERJ All Rights Reserved