Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 22 (2013) 1319 – 1327

Procedia
Computer Science

17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems - KES2013

Toward Introduction of Immunity-based Model to Continuous Behavior-based User Authentication on Smart Phone

Yuji Watanabe*, Houryu, Tsutomu Fujita

Nagoya City University, 1 Yamanohata, Mizuho-cho, Mizuho-ku, Nagoya 467-8501, Japan

Abstract

Smart phone stores a lot of important private information, so that user authentication is increasingly necessary to prevent attacks by illegal users who are not the owner of the smart phone. Password authentication or biometrics can be generally applied only on login. After the authentication is passed, not only the legal owner but also illegal users freely use the smart phone. Therefore we are trying to develop a behavior-based user authentication system to continuously check the user activities after login. The developing system can extract many operational and behavioral features characteristic of user by multiple sensors; for example, touch screen, accelerometer, microphone, and GPS sensor. And then it can combine the authentication results from the multiple sensors because a single sensor may produce poor authentication accuracy. In this paper, we report the ongoing results of our system, that is, the experimental results from user authentication using touch operational features, and some features extracted from accelerometer. We also discuss the introduction of immunity-based model to our system to integrate the authentication results from the multiple sensors.

Keywords: Smart phone; Behavior-based user authentication; Multiple sensors, Immunity-based model

1. Introduction

Mobile devices, such as smart phones, tablets, and portable computers have been rapidly spread for the last decade. Because smart phone stores a large amount of important private information, user authentication is increasingly necessary to prevent attacks by illegal users who are not the owner of the smart phone. The most general user authentication is password authentication, which requires that the owner only memorizes a short password and inputs the password for login. However, there are some problems: (1) the password is probably

* Corresponding author. Tel.: +81-52-872-5037; fax: +81-52-872-5037.
E-mail address: yuji@nsc.nagoya-cu.ac.jp.

doi:10.1016/j.procs.2013.09.220

lost or forgotten and then it is illegally shared and used by attackers, and (2) because the password authentication can be generally applied only at the beginning of use, illegal users as well as the legal owner freely use the smart phone after login. Frequently retyping the password during a login session is extremely user-unfriendly to annoy smart phone user. Moreover, the assumption that the actual physical user is always the same as the login user may not be true in many practical environments. A continuous user authentication after login without frequent user involvement is needed.

Biometrics authentication based on the physiological characteristics, for example, fingerprint, face and voice [1] has some merits. First, it can achieve high authentication accuracy for the intrinsic characteristics. Second, the owner is free of memorizing the password. Third, the biometric characteristics cannot be lost or forgotten, so that it is hard to copy and share them. However, continuous authentication after login is troublesome the same as password, and then the problem (2) of the password authentication still remains. Furthermore, a dedicated device such as fingerprint scanner, which is required by the biometrics authentication, is not desirable in terms of cost, size, and power efficiency of smart phone.

Behavior-based biometrics authentication is a substitute approach. Since the 1990s, in personal computer environment, keystroke pattern, commands sequence, or mouse operation has been employed as user behavior which is difficult to be imitated (e.g. [2-4]). The behavior-based authentication system initially creates normal profiles of a legitimate user behavior. If the system observes the remarkable difference between the profiles and the current user activities, then it gives an alarm as illegal use. The behavior-based user authentication can check the user activities both on login and after login. Other advantage of the behavior-based authentication is the absence of dedicated devices.

Researches of behavior-based authentication on cell phone and smart phone are relatively new but have recently progressed, for instance, keystroke-based authentication [5-6], authentication using accelerometer [7-9], touch screen-based biometrics [10-11], and authentication using multiple sensors [12-13]. Although biometrics authentications during walk and jog using accelerometer can perform high accuracy, they are invalid for stillness. Other researches mainly pay attention to user authentication on login because login task is the same for every user. Since user's task after login is different, it becomes harder to identify a user. The continuous behavior-based user authentication after login is a challenging issue.

Therefore, we are trying to develop a behavior-based user authentication system to continuously check the user activities after login. The developing system can extract many operational and behavioral features characteristic of user by multiple sensors; for example, touch screen, accelerometer, microphone, and GPS sensor. And then our system can combine the authentication results from the multiple sensors because a single sensor may yield poor authentication accuracy. In our previous study [14], we focused on operational behaviors on touch screen at the first stage for the continuous behavior-based authentication system on smart phone. And we made a text browsing application to record fingers history on smart phone and extracted characteristic operational features, namely, the distribution of touched region, the speed of fingers and so on. The experimental results have shown that the distribution of region touched by fingers for each subject was interestingly different.

In this paper, we report the ongoing results of our system, that is, the authentication performance by touch operational features, and some features extracted from accelerometer. We also discuss the introduction of immunity-based model to our system to integrate the authentication results from the multiple sensors.

2. Related Work

Behavior-based authentication schemes on cell phone and smart phone can be classified based on employed sensors and behavior, namely, keystroke [5-6], accelerometer [7-9], touch screen [10-11], and multiple sensors [12-13].

Isohara et al [5] have proposed a simple and easy-to-use anomaly detection system on cell phone environment. Because the system was proposed for cell phone with severely limited calculation resources, it used only the key frequency for user authentication. However, since smart phone has more powerful calculation resources than cell phone, authentication based on other complicated characteristics can be applied on smart phone. Zahid et al [6] have evaluated the performance of the keystroke-based user identification for 25 users on smart phone and then achieved about 2% FAR (False Acceptance Rate) and 0% FRR (False Rejection Rate). An individual authentication using motions of a portable device with an acceleration sensor, 3D motion authentication, which is proposed by Ishihara et al [7], has obtained less than 1.5% FRR and less than 1% FAR with the user's own signature satisfying the guideline. However, frequent motions of the portable device are necessary for continuous authentication. Other accelerometer-based authentications [8-9] have used the data obtained by the accelerometer of a portable device on a belt or in a pocket while the users performed normal daily activities, such as walking, jogging and climbing stairs. Although they performed high accuracy during walk and jog, they were invalid when the user remains stationary.

For touch screen biometrics, Angulo and Wastlund [10] used Pattern Lock implemented in the Android OS, and Sae-Bae et al [11] made use of movement characteristics of five-fingers touch gestures. However, they coped with user authentication on login. Gesture authentication using a touch panel and an acceleration sensor proposed by Kenjo and Hayashibara [12] was also on login. SenGuard [13] was a passive user identification on smart phone using multiple sensors, similar to our system. SenGuard aims to continuously identify a user after login using multiple sensors, namely, accelerometer, microphone, cell ID location and touch screen. Although the evaluation results for accelerometer and location history were reported, the detection accuracy for microphone and touch screen are not shown yet. Furthermore, combined results by multiple sensors are still unexplained.

3. Touch Screen Biometrics

In our previous study [14], we focused on operational behaviors on touch screen at the first stage for the continuous behavior-based authentication system on smart phone. This section first reviews the text browsing application and the fingers history recorded by the application. Next it presents the feature extraction from the recorded fingers history. Finally we show new experimental results including the authentication performance by touch operational features.

3.1. Text browsing application and fingers history

Because we have developed some applications on iOS for some years, we created an application to record fingers history on iPhone, iPod touch and iPad (as a matter of course we started to develop on Android OS). It is preferable that user behavior is recorded in the background process. Because multitasking is supported for iOS through only seven background APIs: background audio, voice over IP, background location, push notifications, local notifications, task completion, and fast app switching, it is difficult to store operational behaviors in the background process on iOS.

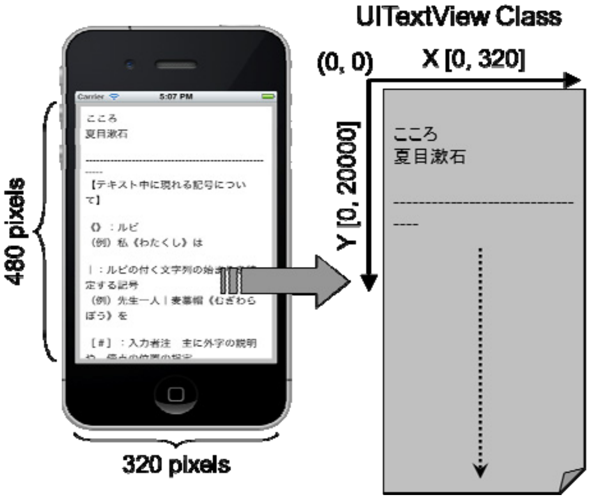
Because browsing is one of basic functions equipped with many applications on smart phone, as the first stage for touch screen-based authentication on smart phone, we made a simple text browsing application to record fingers history as shown in Fig.1 (a). The display size is 480 pixels high by 320 pixels wide (iPhone 4 and 4th generation iPod touch has 960 x 640 pixels, and iPad has 1024 x 768 pixels). So the text browser has only vertical scroll. A text is scrolled by the following fingers operations.

- *Flick*: users place a finger on the screen and quickly swipe it in the desired direction.

- *Drag*: users place a finger on the screen and move it in the desired direction without lifting it from the screen.

An extended application which can get other fingers operations such as tap and pinch is under construction.

Fig. 1 (b) illustrates that the origin is located at the top left corner of the screen, and the X and Y coordinates are specified. The UITextView Class which implements the behavior for a scrollable, multiline text region is used to display multiple lines of text, such as when displaying the body of a large text document. The class can get touched points not on screen but on text, so that the range of Y varies depending on the text document while the range of X is from 0 to 320. The Japanese text document in Fig. 1 (b) has Y ranging from 0 to 20000.



こころ
夏目漱石

【テキスト中に現れる記号について】

《》：ルビ
（例）私《わたくし》は

｜：ルビの付く文字列の始
定する記号
（例）先生一人｜麦藁帽《むぎわらぼう》を

［＃］：入力者注　主に外字の説明や、傍点の位置の指定

(a) (b)

Fig. 1. (a) screenshot of the simple text browsing application to record fingers history on iPhone and iPod touch.; (b) the origin and the X and Y coordinates on UITextView Class [14]

The fingers history continuously recorded by the text browsing application is in the form of {*event*, (*x*, *y*), *t*}, where *event* means one of 3 touch events as follows:

1. A finger is placed on the text.
2. The finger is moving without lifting from the text.
3. The finger is released.

And (*x*, *y*) is the coordinates of point touched by the finger, *t* is the touch event time. For example, when the finger is touched at 20 seconds from the start and is released at 25 seconds, we can obtain the fingers history like {{1, (200, 15), 20}, {2, (200, 16), 22}, {3, (200, 18), 25}}.

3.2. Feature Extraction

From the recorded fingers history, we should extract characteristic operational features suitable for user authentication. Because touch operation on smart phone is probably close to mouse operation on personal computer, referring to the previous research on mouse operation [4], we extract the following features.

1. The distribution of region touched by the finger
2. The X-coordinate of the finger (because the range of X is fixed)

3. The moving distance of the finger from the starting point (*event* 1) to the ending point (the corresponding *event* 3)
4. The speed of the finger (the above moving distance divided by the taken time)
5. The moving angle of the finger between the starting point and the ending point

First we calculate the average and the standard deviation of 4 features excluding feature 1, that is, the X-coordinate, the moving distance, the speed and the angle over all the history. Next, for the 4 features, we split the time series features into overlapping windows with window size *n* and then calculate a simple moving average of the features every windows for continuous user authentication.

3.3. Preliminary experimental results

We carried out preliminary experiments using the text browsing application on iPod touch to record fingers history. 5 subjects participated in this experiment (4 subjects already have smart phone). After the subjects were explained how to use iPod touch and the application, they were free to read the text document. When they finished reading, they returned iPod touch. We can get each recorded fingers history through iTunes.

Table 1 shows the number of detected touch events and detected moving distances for 5 subjects. Fig. 2 illustrates the distribution of region touched by fingers (X and Y coordinates of the entire detected events) for 5 subjects. From the results, subject A, C, D and E are accustomed to operation on smart phone while subject B may be not used to reading the text document on smart phone. In terms of subject A and E, the number of detected events is smaller, and the distribution of touch events is not scattered. Therefore subject A and E are especially accustomed to operation on smart phone. After experiment, we confirmed subject A and E had their own smart phone for over 2 year. The distribution can be one of promising characteristic operational features suitable for user authentication.

Table 2 depicts the average and the standard deviation of 4 features, namely, the X-coordinate, the moving distance, the speed and the angle of each subject's finger over all the history. The averages of the X-coordinate and the moving distance for subject B are similar to those for subject C. Indeed, there are no significant differences between subject B and C by Welch's *t* test. As for the average of the speed, we also verify no significant differences between subject A and B. Finally for the average of the angle, there are no significant differences between subject C and D. Although only one feature is invalid for biometrics authentication, the combination of features may make user authentication available.

To evaluate the authentication performance by the combination of features, we enter the moving averages of 4 features into two classification algorithms: decision trees (J48) and neural networks (NN) from the WEKA data mining suite [15], referring to the previous research on accelerometer-based authentication [9]. We use the default settings and the ten-fold cross validation. We also use two metrics: FRR (False Rejection Rate) and FAR (False Acceptance Rate) according to the previous studies.

Table 1. Number of detected events and detected moving distances for 5 subjects

Subject	**A**	**B**	**C**	**D**	**E**
# of detected events	**120**	2420	250	270	**110**
# of detected moving distances	7	339	72	52	24

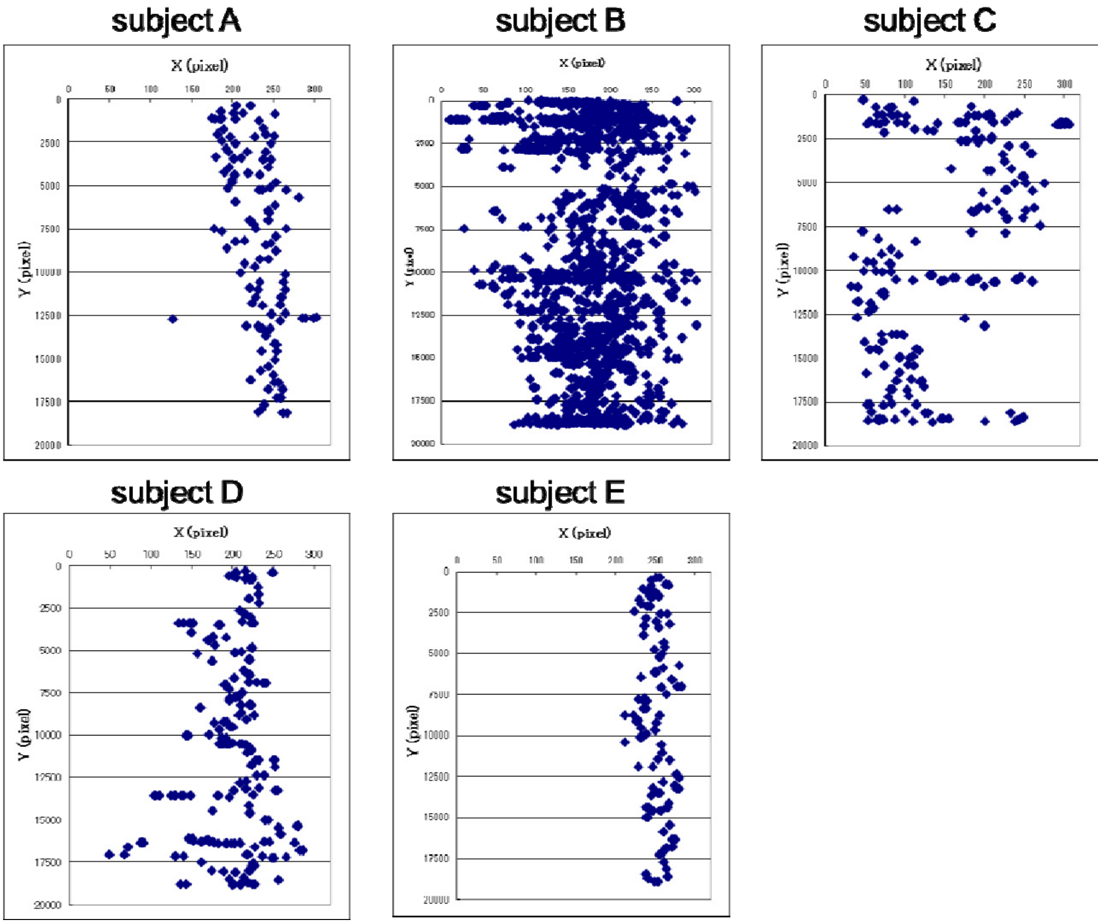


Fig. 2. The distribution of region touched by fingers for 5 subjects

Table 2. Average and standard deviation of 4 features over all the history for 5 subjects

Subject		**A**	**B**	**C**	**D**	**E**
X-coordinate	Ave.	231.6	**169.6**	**163.0**	197.4	251.1
(pixels)	S.D.	29.6	51.8	83.0	39.9	15.7
Moving distance	Ave.	7.4	**7.9**	**7.9**	7.6	9.2
(pixels)	S.D.	2.0	8.4	6.2	3.2	1.5
Speed	Ave.	**104.1**	**119.4**	53.1	86.9	168.0
(pixels/s)	S.D.	98.0	606.9	56.1	88.9	75.0
Angle	Ave.	-33.7	22.2	**-18.3**	**-20.9**	-42.6
(degrees)	S.D.	102.5	94.8	83.1	101.7	84.6

Table 3 and 4 show the metrics by decision trees (J48) and neural networks (NN) for each subject, changing window size 5 and 10, respectively. From the results in Table 3, FRR and FAR when window size is 5 are terrible, so that our user authentication is totally useless. As shown in Table 4, FRR and FAR for window size 10 become better than those for window size 5. However, compared with the performance of keystroke-based authentication [5-6] and authentication using accelerometer [7-9], our touch screen-based authentication needs to be gigantically improved changing some factors, for example, how to record finger history, how to extract operational features, window size, and classification algorithms.

Table 3. FRR and FAR by two classification algorithms for 5 subjects using window size 5

Subject		**A**	**B**	**C**	**D**	**E**	**Weighted Ave.**
Decision trees (J48)	FRR (%)	33.3	11	35.4	64.7	25	21.9
	FAR (%)	0.4	41	3.5	6.2	1.1	30.3
Neural networks (NN)	FRR (%)	100	6.6	75	80.9	35	25.9
	FAR (%)	0	65.5	1.9	3.4	2.2	47

Table 4. FRR and FAR by two classification algorithms for 5 subjects using window size 10

Subject		**A**	**B**	**C**	**D**	**E**	**Weighted Ave.**
Decision trees (J48)	FRR (%)	100	6.7	16.3	39.7	0	12.2
	FAR (%)	0	26.2	1.5	4.1	0.2	19.9
Neural networks (NN)	FRR (%)	100	6.4	20.9	27	6.7	10.8
	FAR (%)	0	22.1	1.5	3.9	0.2	16.8

4. Accelerometer-based Authentication

An alternative approach to improve the poor authentication accuracy by a single sensor is to use multiple sensors and combine the authentication results from the multiple sensors. So, we created an iOS application to record the 3 axes accelerometer data during walking. And we carried out preliminary experiments for 3 subjects. The subjects walked along a corridor for about 5 minutes while they carried the iPod touch in their pocket. We set the sampling frequency of 50ms, in other words, collected about 20 data per second. Fig. 3 shows an example of obtained 3 axes accelerometer data.

Referring to the previous study using accelerometer [9], we divide the raw time series data into non-overlapping windows with window size 200 and then generate features from the data contained in each window. Since acceleration data is collected for 3 axes about 20 times per second, there are 600 total data in about 10-second interval. The reason of non-overlapping windows unlike the touch screen biometrics mentioned in subsection 3.2 is that we can get a lot of acceleration data in short time. The accelerometer-based authentication can take about 10 second to clarify an illegal user, while the touch screen-based authentication may take more time, minute order to clarify.

We intend to extract a total of 43 features described below:

- Average for each axis: $\bar{x} = \sum_{i=1}^{200} x_i / 200$
- Standard deviation for each axis: $\sqrt{\sum_{i=1}^{200} (x_i - \bar{x}) / 200}$

- Average absolute difference for each axis: $\sum_{i=1}^{200}\left|x_i - \overline{x}\right|/200$
- Average resultant acceleration: $\sum_{i=1}^{200}\sqrt{x_i + y_i + z_i}\,/200$
- Time between peaks for each axis: Time in milliseconds between peaks in the sinusoidal waves associated with most activities
- Binned distribution for each axis: We determine the range of data (maximum – minimum), divide this range into 10 equal sized bins, and then record the fraction of the 200 data that fall within each of the bins.

where x_i, y_i, and z_i are i-th acceleration data for each axis in each window.

We are now extracting the features for each subject, so that we will show the results at conference site.

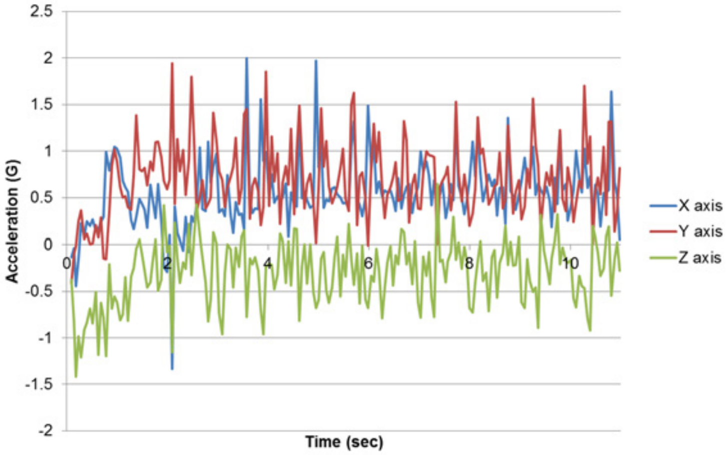


Fig. 3. An example of obtained accelerometer data

5. Discussion: Introduction of Immunity-based Model

If we complete each behavior-based authentication application for individual sensor on smart phone, we should consider how to combine the authentication results from the multiple sensors. Although SenGuard [13] similar to our system has not yet clarified detailed sensor fusion technique and results combined by multiple sensors, it uses a sliding window based classifier aggregator and then a majority based meta classifier for the final decision. Each sensor happens at certain time with its specific duty cycles. For example, accelerometer based authentication is triggered when user is walking, while touch screen based authentication takes place when user is touching screen. So SenGuard needs the sliding time window to aggregate all available outputs from each sensor-based classifier.

The concept of the sliding time window may be also useful for our system. However, we intend to differentiate ourselves from SenGuard by introducing immunity-based models to our continuous behavior-based authentication using multiple sensors. Ishida [16] has proposed the immunity-based diagnosis model. The diagnostic model, which is a variant of majority vote model, is performed by mutual tests among sensors and dynamic propagation of active states. Each sensor node has the capability of testing the linked nodes, and being tested by the adjacent others as well. Based on the test outcomes, each node calculates its own credibility. The immunity-based diagnosis model can be directly applied to our system. In the introduction of the immunity-based diagnosis model, each node is corresponding to single behavior-based authentication for each sensor on smart phone, and each test outcome is decided by authentication time, frequent and accuracy between the nodes.

Furthermore, Okamoto and Ishida [17] have proposed an immunity-based anomaly detection system with sensor agents based on the specificity and diversity of the immune system. Conventional systems have used only a single sensor to detect anomalies, while the immunity-based system makes use of multiple sensors, which lead to improvements in detection accuracy. The incorporation of the immunity-based system into our system may be possible.

References

[1] Jain A, Bolle R, Panakanti S. *Biometrics: Personal Identification in Network Society*. Kluwer Academic Publishers; 1999.

[2] Joyce R, Gupta G. Identity Authentication Based on Keystroke Latencies. *Communications of the ACM* 1990, **33(2)**:168-176

[3] Schonlau M, DuMouchel W, Ju W, Karr A, Theus M, Vardi Y. Computer Intrusion: Detecting Masquerades. *Statistical Science* 2001, **16(1)**:58-74

[4] Izumi M, Nagao W, Miyamoto T, Fukunaga K. User Identification System Using Feature of Mouse Operation. *IEICE Transactions on Communications* 2004, **J87-B(2)**:305-308

[5] Isohara T, Takemori K, Sasase I. Anomaly Detection on Mobile Phone Based Operational Behavior. *IPSJ Journal* 2008, **49(1)**:436-444

[6] Zahid S, Shahzad M, Khayam SA, Farooq M. Keystroke-Based User Identification on Smart Phones. *Proc. of the 12th International Symposium on Recent Advances in Intrusion Detection*, 2009, p. 223-243

[7] Ishihara S, Ohta M, Namikata E, Mizuno T. Individual Authentication for Portable Devices Using Motion of the Devices. *IPSJ Journal* 2005, **46(12)**:2997-3007

[8] Mantyjarvi J, Lindholdm M, Vildjounaite E, Makela SM, Ailisto H. Identifying users of portable devices from gait pattern with accelerometers. *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2005, p. 973-976

[9] Kwapisz JR, Weiss GM, Moore SA. Cell Phone-Based Biometric Identification. *Proc. of the 4th IEEE International Conference on Biometrics: Theory Applications and Systems*, 2010, p. 1-7

[10] Angulo J, Wastlund E. Exploring Touch-screen Biometrics for User Identification on Smart Phones. *IFIP Summer School*, 2011

[11] Sae-Bae N, Ahmed K, Isbister K, Memon N. Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-touch Devices. *The 30th ACM Computer-Human Interaction conference (CHI)*, 2012, p. 977-986

[12] Kenjo K, Hayashibara N. Input Method of Gesture Authentication for Mobile Devices using Touch Panel and Accelerometer. *IPSJ SIG Technical Report* 2012, **CSEC-56(8)**

[13] Shi W, Yang J, Jiang Y, Yang F, Xiong Y. SenGuard: Passive User Identification on Smartphones Using Multiple Sensors. *Proc. of IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications*, 2011, p. 141-148

[14] Watanabe Y, Ichikawa S. Extraction of Operational Behavior for User Identification on Smart Phone. *Proc. of the 17th International Symposium on Artificial Life and Robotics*, 2012, p. 333-336

[15] Witten I, Frank E. *Data Mining: Practical Machine Learning Tools and Techniques*. Morgan Kaufmann Publishers; 2005.

[16] Ishida Y. Fully Distributed Diagnosis by PDP Learning Algorithm: Towards Immune Network PDP Model. *Proc. of IJCNN*, 1990, p. 777–782

[17] Okamoto T, Ishida Y. An Immunity-Based Anomaly Detection System with Sensor Agents. *Sensors* 2009, **9(11)**:9175-9195