Continuous Authentication Using Mouse Clickstream Data Analysis

Sultan Almalki(✉), Prosenjit Chatterjee(✉), and Kaushik Roy(✉)

Department of Computer Science, North Carolina A&T State University, Greensboro, USA
{ssalmalki,pchatterjee}@aggies.ncat.edu,
kroy@ncat.edu

Abstract. Biometrics is used to authenticate an individual based on physiological or behavioral traits. Mouse dynamics is an example of a behavioral biometric that can be used to perform continuous authentication as protection against security breaches. Recent research on mouse dynamics has shown promising results in identifying users; however, it has not yet reached an acceptable level of accuracy. In this paper, an empirical evaluation of different classification techniques is conducted on a mouse dynamics dataset, the Balabit Mouse Challenge dataset. User identification is carried out using three mouse actions: mouse move, point and click, and drag and drop. Verification and authentication methods are conducted using three machine-learning classifiers: the Decision Tree classifier, the K-Nearest Neighbors classifier, and the Random Forest classifier. The results show that the three classifiers can distinguish between a genuine user and an impostor with a relatively high degree of accuracy. In the verification mode, all the classifiers achieve a perfect accuracy of 100%. In authentication mode, all three classifiers achieved the highest accuracy (ACC) and Area Under Curve (AUC) from scenario B using the point and click action data: (Decision Tree - ACC: 87.6%, AUC: 90.3%), (K-Nearest Neighbors - ACC: 99.3%, AUC: 99.9%), and (Random Forest - ACC: 89.9%, AUC: 92.5%).

Keywords: Mouse dynamics · Biometric · Continuous authentication · Behavioral biometric · Machine learning

1 Introduction

User authentication is a method that is used to determine whether a user is genuine ("allowed to access the system") or an impostor ("prohibited from access to the system") [1]. User authentication has three types of classes: knowledge based, object or token based, and biometric based. Knowledge-based user authentication is characterized by confidentiality; it is something that only the user would know. Object-based user authentication is characterized by control; it is something that the user has. Biometric-based user authentication relies on the user's physiological or behavioral characteristics; it is something the user is. While the weaknesses of knowledge-based and object-based approaches are that the user may lose or forget passwords and tokens,

G. Wang et al. (Eds.): SpaCCS 2019 Workshops, LNCS 11637, pp. 76–85, 2019.
https://doi.org/10.1007/978-3-030-24900-7_6

the advantage of a biometric-based approach is that it can uniquely identify an individual by using the individual's biological characteristics.

Although using biometric makes the authentication stronger and determines a user's identity uniquely, verification based on physiological biometrics such as iris, face, or fingerprint offers mainly a one-time static authentication [2, 3]. To avoid this drawback, behavioral biometrics such as mouse clickstream data can be used to continuously authenticate a user by monitoring the user's behavior [4]. In this work, an empirical evaluation of three classifiers is conducted on the Balabit dataset [5], which contains data for 10 users with a set of 39 behavioral features per user [6].

The rest of the paper is organized in four sections. Section 2 summarizes some previous research in this area. Section 3 describes the Balabit dataset and the feature extraction method. Section 4 describes the model and the experiments, followed by a discussion of the test results. Section 5 has concluding remarks and suggestions for future work.

2 Related Work

User behavioral analysis has been a focus of research for more than a decade. This section briefly presents some of the research on mouse-based authentication.

Antal et al. [6] applied a Random Forest (RF) classifier for each user using mouse movements for verifying impostor detection. They used the Balabit dataset [5], which includes 10 users. Each user has many sections and mouse actions. They segmented each session's data into three types of mouse actions: Mouse Movement (MM), Point Click (PC), and Drag and Drop (DD). The researchers extracted 39 features and obtained results of 80.17% average accuracy (ACC) and 0.87 average Area Under Curve (AUC). The highest accuracies achieved for users (7 and 9) were 93% and 0.97 AUC. The lowest accuracy achieved for a user (8) was 72% and 0.80 AUC.

Nakkabi et al. [7] proposed a user authentication scheme based on mouse dynamics. They collected mouse behavior data from 48 users and applied a fuzzy classification that relied on a learning algorithm for multivariate data analysis. They conducted an evaluation and achieved a False Acceptance Rate (FAR) of 0% and a False Rejection Rate (FRR) of 0.36%. Their experiments required more than 2000 mouse events in order to classify a user as legitimate.

Feher et al. [8] introduced a framework for user verification using mouse activities. The framework was divided into three parts: acquisition, learning, and verification. The first step is to capture user actions from the users' mouse activities. Then, classify each event type and store them in a database. The third phase is to send each event to the favorite classifier based on action type. The classifier has two layers: a prediction layer and a decision layer. The researchers conducted tests of multi-class classifier using a RF classifier. They collected the data from 25 volunteers. They obtained an Equal Error Rate (EER) of 1.01% based on 30 actions.

Gamboa et al. [9] developed a data acquisition system for collecting users' mouse activities. The system records all user interaction throughout the world wide web. The dataset was collected from 50 participants; each user has 400 strokes. A stroke is defined as a group of points between two actions. The authors proposed 58 behavioral

features extracted from the raw data using some mathematical operations. These features were used to identify a user based on how they interact with the system. Furthermore, Gamboa et al. developed a sequential classifier using statistical pattern recognition techniques in order to distinguish between users. The authors achieved an equal error rate of 0.7% per 100 mouse strokes.

Another biometric authentication approach based on mouse dynamics was introduced by Shen et al. [10]. They collected user behavioral data under a controlled environment using the software tool they developed. The software collected the events of "mouse move" or "mouse click" for about thirty minutes in each session. The dataset obtained had 15 sessions for each of 28 subjects. Based on a mining method, the researchers focused on using frequent and fixed actions as behavioral patterns for extracting user characteristics through pattern growth. They used an SVM and achieved an FAR of 0.37% and an FRR of 1.12%.

Schulz [11] collected a dataset from 72 volunteers using a software tool on their personal machines. The software tool presented a continuous authentication system using mouse events; it segmented a user's events into length of a movement, curvature, inflection, and curve straightness features, and then computed a user's behavioral signature using histograms based on curve characteristics. For the verification stage, the researcher used Euclidean distance for classification and computed the distance between a user's login and the mouse activities. An EER of 24.3% from a group of 60 mouse curves is obtained. In contrast, by using groups of 3600 mouse curves, the performance increased to an EER of 11.2%.

Bours et al. in [12] proposed a login system based on mouse dynamics. They collected data from 28 participants of different age groups. They used a technique called "follow the maze" in which the participants performed a task by following the tracks on their own computer. This task was performed five times per session in order to acquire sufficient data on mouse movements. The maze contained 18 tracks, divided into 9 horizontal and 9 vertical tracks. They measured the various distances using Euclidean distance, Manhattan distance, and edit distance algorithms. The results that they obtained were an EER of 26.8% in the case of the horizontal direction and an EER of 27.0% in the case of the vertical direction.

Hashia et al. [13] worked on mouse movement as a biometric. They proposed two authentication methods: the first method is for initial login of users (enrollment), and the second one is to monitor a computer for suspicious activities (verification). It required from the user about 20 s to complete each of two methods. For the enrollment phase, a user must be using the mouse and following a series of dots that showed one at a time on the user's screen. The purpose of this step is to record the coordinates of the mouse every 50 ms and then calculate the speed, deviation from a straight line, and angles. They used the data collected from the enrollment phase for the verification phase by comparing a user's credentials and the data collected in the enrollment phase. They tested their approach using 15 participants of age 22–30. They achieved an error rate of 20% when using 1.5 standard deviations of the average from the corresponding enrollment value, and an error rate of 15% using 1 standard deviation of the average from the corresponding enrollment value.

3 Description of Mouse Raw Data

This research used the Balabit Mouse Challenge dataset [5], obtained at the Budapest office of the Balabit company. The dataset contains raw data obtained from 10 users using remote desktop clients connected to remote servers. It has many sessions with characteristics of how a person uses a mouse. Each session includes a set of rows, where each row recorded a user action as (rtime, ctime, button, state, x, y): "rtime" is the elapsed time recorded since the start of the session using the network monitoring device, "ctime" is the elapsed time through the client computer, "button" is a mouse button, "state" is information about the button, and "x" and "y" are the Cartesian coordinates of the mouse location [6].

3.1 Extraction of Features

A mouse action is a set of sequential user actions that represent a movement of the mouse between two points. This study uses the user features extracted from the Balabit Mouse Challenge dataset [5]. This dataset divides the raw data into three types of actions: MM, PC, and DD. MM describes a movement between two screen positions; PC is a Point Click or Mouse click; DD is a drag-and-drop event. The dataset presents 39 features extracted from an individual's mouse actions. A detailed description of features is found in [6].

4 Mouse Dynamics Model and Experimental Results

In this research, supervised machine-learning techniques were utilized to monitor the behavior of users in order to distinguish legal users from illegal users [14]. Three machine-learning algorithms were evaluated: Decision Tree Learning (DT), k-Nearest Neighbors (k-NN), and Random Forest (RF). The Scikit-learn software tools were used for the analysis of mouse clickstream data [15]. A significant step in the classification was to prepare the training data in CSV format, so that it could be interpreted by the classifiers. In the model, if a user's mouse dynamics are the same as the characteristics stored in the system's database, then the system lets the user continue working on the device; otherwise, the system must log out the user (see Fig. 1). Specifically, the following steps describe how the model works:

- Data Collection Phase: Raw data of the users are collected.
- Features Extraction Phase: Meaningful features, such MM, PC, and DD, were extracted using the method reported in Antal et al. [6].
- Data Preparation Phase: For the training phase, all the users' data was aggregated and put in random order. The training dataset was then split into two parts: the first part (70% of the data) was used for training, and the second part (30% of the data) was used for testing the model's performance. For every experiment, the balance of training sets and evaluation sets remained the same in order to avoid classifier bias.

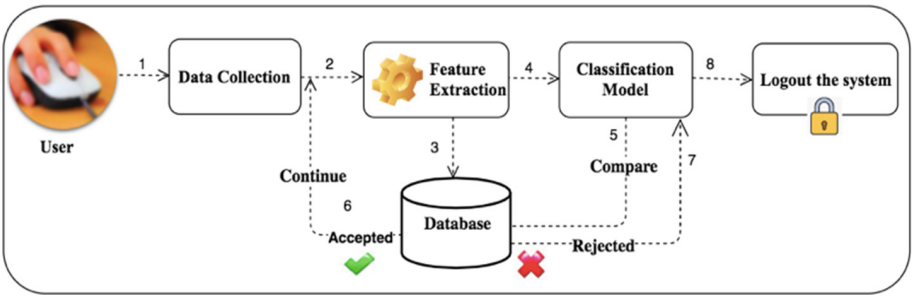

Fig. 1. User behavioral biometrics model

- Select a Classifier Phase: DT, RF, and KNN were utilized to show the ability of the proposed model to determine whether a user was genuine or an impostor from a user's mouse clickstream data.
- Training Data Phase: The training process began by reading the characteristics of all the users from the training dataset and then loading them into the three classifiers to train the model. This step was a significant step, since the training data contained the user behavior itself and a class label.
- Testing Data Phase: After completion of the training step, the model was tested on the new data that was never used for training, to categorize whether the user as a genuine user or an impostor.

The experiment was conducted in two stages: (i) a verification stage, and (ii) an authentication stage. The evaluations were measured using classifier accuracy (ACC) and area under curve (AUC). Another important evaluation to examine the classifiers is to plot the receiver operating characteristic (ROC). The ROC curve plots the True Positive Rate (TPR) against the False Positive Rate (FPR) [16].

4.1 Verification Stage

In this stage, all three classifiers were first trained using the data that only contained the genuine user's actions (positive). Each user has many sessions; all users' sessions data were placed in one Excel file. Then, the experiment was conducted by doing training and testing for each user using the DT, K-NN, and RF classifiers. The goal of the verification stage was to verify whether the mouse data was related to a given user. After testing all the users using three classifiers, a perfect score of 100% verification rate was achieved.

4.2 Authentication Stage

In this stage, each user is in one of two classes: genuine (positive) and impostor (negative). The impostor actions were selected from the other users. Then, we assigned the positive action as {1} and the negative action as {0}. The classifiers are responsible for determining the probability that the user belongs to the genuine class or imposter class. Therefore, all classifiers were tested based on these two scenarios:

A. A single user's data with all actions (MM, PC, DD)
B. All the users' data with a single action (MM, PC, DD)

Scenario A: A Single User's Data with All Actions. In scenario (A), an experiment was conducted for a single user (35, 7, 9, 12, 15, 16, 20, 21, 23, and 29) with all actions (MM, PC, and DD), using the three classifiers. The DT, K-NN, and RF classifiers achieved average accuracies of 91.9%, 94.4%, and 79.7%, respectively. The highest average accuracies were achieved for user (9): (ACC: 91.8%), DT 96.2%, KNN 99.2%, and RF 80.1%. The lowest average accuracies were achieved for user (12): (ACC: 85.6%), DT 90.1%, KNN 91.5%, and RF 75.2%. Table 1 reports the results in detail for each user. The AUC value is computed based on the FPR and the TPR. ROC curves are given in Figs. 2, 3, and 4.

Table 1. Scenario A: single user, all actions (MM, PC, DD)

User	Decision tree		K-nearest neighbors		Random forest	
	ACC%	AUC	ACC%	AUC	ACC%	AUC
35	84.9	92.1	96.6	99.4	88.3	91.2
7	92.4	93.8	88.7	92.2	85.8	88.1
9	96.2	97.1	99.2	99.1	80.1	81.0
12	90.1	97.5	91.5	99.2	75.2	79.7
15	92.6	98.1	99.7	99.3	80.5	82.5
16	88.6	91.0	97.3	99.4	84.9	86.7
20	93.8	97.2	90.1	99.0	75.6	80.5
21	95.6	97.9	92.4	99.3	72.8	77.3
23	91.1	96.4	95.2	99.3	82.2	84.9
29	94.5	96.5	93.5	99.8	71.7	74.4
Avg	91.9	95.7	94.4	98.6	79.7	82.6

Scenario B: All Users' Data with a Single Action. In scenario (B), the dataset was initially separated into three groups of mouse actions: MM, PC, and DD. Each group contained all users (35, 7, 9, 12, 15, 16, 20, 21, 23, and 29). Training and testing of the three classifiers were then conducted on each group based on the single action. The results are reported in Table 2 (MM), Table 3 (PC), and Table 4 (DD). The highest accuracies were achieved with the PC action compared to MM and DD, as shown in Table 3 (PC): (DT: ACC: 87.6%, AUC: 90.3%), (KNN: ACC: 99.3%, AUC: 99.9%), and (RF: ACC: 89.9%, AUC: 92.5%). Also, ROC curves are given in Figs. 5, 6 and 7 for (MM), Figs. 8, 9, and 10 for (PC), Figs. 11, 12 and 13 for (DD).

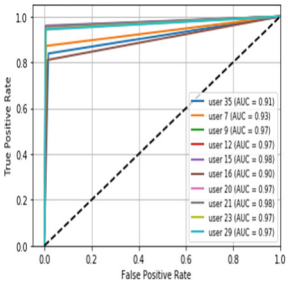

Fig. 2. ROC curve for DT, single user, all actions

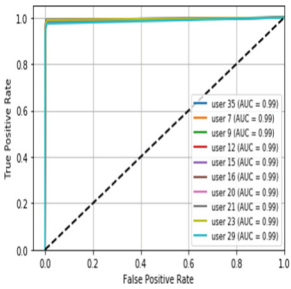

Fig. 3. ROC curve for KNN, single user, all actions

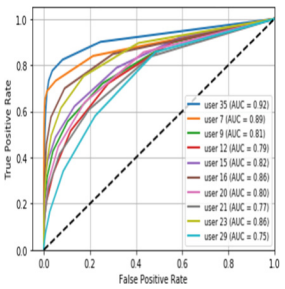

Fig. 4. ROC curve for RF, single user, all actions

Table 2. Scenario B: all users, single action (MM action)

User	Decision tree		K-nearest neighbors		Random forest	
	ACC%	AUC	ACC%	AUC	ACC%	AUC
35	92.9	95.8	99.5	100	97.3	99.0
7	95.4	98.1	99.7	100	98.8	99.8
9	83.2	86.7	99.2	99.9	85.1	87.6
12	81.1	84.0	99.5	99.6	86.2	89.9
15	80.6	83.0	99.7	99.9	88.5	91.9
16	93.6	96.3	99.3	99.8	93.9	95.2
20	80.8	84.4	99.1	100	87.6	90.7
21	78.6	80.6	99.4	99.6	80.8	84.5
23	75.7	78.1	99.2	99.7	85.2	89.6
29	79.5	81.2	99.5	99.4	82.7	85.3
Avg	84.1	86.8	99.4	99.8	88.6	91.3

Table 3. Scenario B: all users, single action (PC action)

User	Decision tree		K-nearest neighbors		Random forest	
	ACC%	AUC	ACC%	AUC	ACC%	AUC
35	93.9	95.7	98.6	99.9	91.3	94.4
7	95.4	97.6	99.7	100	98.8	99.7
9	85.2	88.7	99.2	100	89.1	92.4
12	90.1	93.4	99.5	99.9	86.2	89.9
15	84.6	86.5	99.7	99.9	88.5	91.0
16	91.6	94.8	99.3	100	95.9	97.1
20	86.8	89.1	99.1	99.9	88.6	91.4
21	82.6	85.0	99.9	99.9	89.1	91.0
23	83.1	87.8	99.2	99.8	89.2	92.3
29	82.5	84.7	98.9	99.8	82.7	85.5
Avg	87.6	90.3	99.3	99.9	89.9	92.5

Table 4. Scenario B: all users, single action (DD action)

User	Decision tree		K-nearest neighbors		Random forest	
	ACC%	AUC	ACC%	AUC	ACC%	AUC
35	92.3	94.5	98.6	99.4	98.3	99.0
7	93.9	95.5	95.7	97.9	95.8	97.8
9	82.5	86.9	98.2	99.7	87.1	91.8
12	85.3	89.3	98.5	99.5	89.2	93.5
15	88.1	90.5	99.7	100	90.5	93.1
16	87.6	89.6	98.3	99.6	91.9	94.4
20	85.8	88.2	98.1	99.5	89.6	92.1
21	85.6	89.2	96.4	98.2	79.8	82.8
23	85.2	87.8	98.2	99.5	93.2	96.0
29	82.8	85.0	98.5	99.6	80.7	84.4
Avg	86.9	89.7	98.0	99.3	89.6	92.5

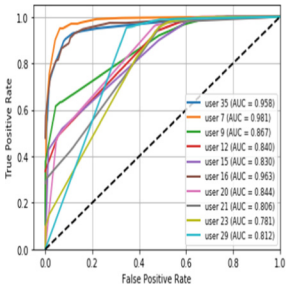

Fig. 5. ROC curve for DT, all users, MM action

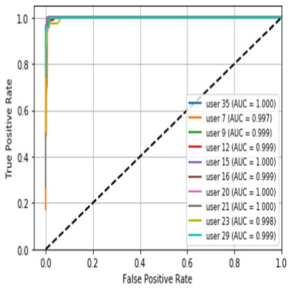

Fig. 6. ROC curve for KNN, all users, MM action

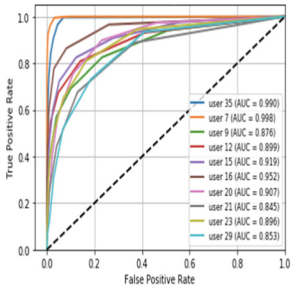

Fig. 7. ROC curve for RF, all users, MM action

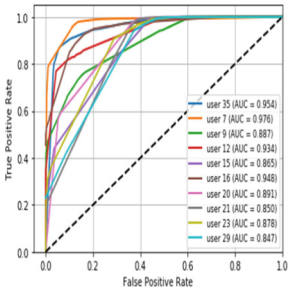

Fig. 8. ROC curve for DT, all users, PC action

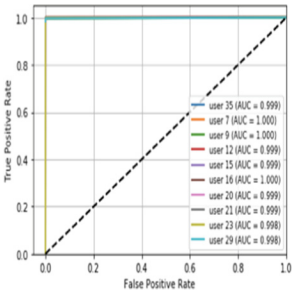

Fig. 9. ROC curve for KNN, all users, PC action

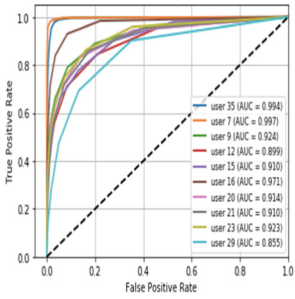

Fig. 10. ROC curve for RF, all users, PC action

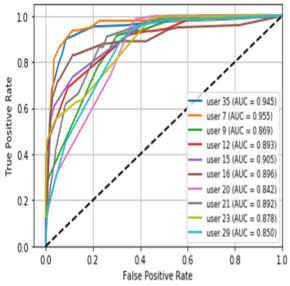

Fig. 11. ROC curve for DT, all users, DD action

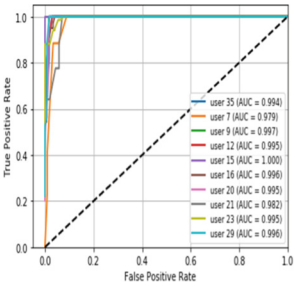

Fig. 12. ROC curve for KNN, all users, DD action

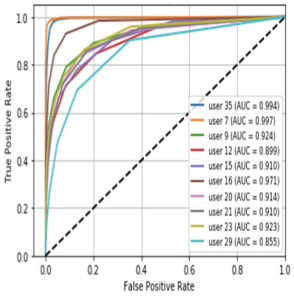

Fig. 13. ROC curve for RF, all users, DD action

5 Conclusion

This paper provides a continuous user authentication model based on mouse click-stream data analysis. Each of three machine-learning classifiers used 39 features of mouse actions MM, PC, and DD. The classifiers were able to determine a genuine user from an impostor with reasonable accuracies and AUC.

In the verification phase, the model was able to recognize the user with an accuracy of 100%. In the authentication phase, data containing genuine and impostor actions were examined using two scenarios: (A) a single user with all actions, and (B) a single action with all users. The best results were obtained from scenario B using the PC action: (DT - ACC: 87.6%, AUC: 90.3%), (KNN - ACC: 99.3%, AUC: 99.9%), and (RF - ACC: 89.9%, AUC: 92.5%). In the future, a deep learning model will be constructed using the MM, PC, and DD actions, and its performance will be compared with the traditional classifiers.

Acknowledgment. This research is partially supported by the Army Research Office (Contract No. W911NF-15-1-0524).

References

1. Pisani, P.H., Lorena, A.C., de Carvalho, A.C.: Adaptive biometric systems using ensembles. IEEE Intell. Syst. **33**(2), 19–28 (2018)
2. Hameed, S.M., Hobi, M.M.: User authentication based on keystroke dynamics using backpropagation network. Int. J. Adv. Res. Comput. Sci. **3**(4), 35–40 (2012)
3. Gorad, B.J., Kodavade, D.V.: User identity verification using mouse signature. IOSR J. Comput. Eng. (IOSR-JCE) **12**(4), 33–36 (2013)
4. Shen, C., Cai, Z., Guan, X., Du, Y., Maxion, R.A.: User authentication through mouse dynamics. IEEE Trans. Inf. Forensics Secur. **8**(1), 16–30 (2013)
5. Fülöp, Á., Kovács, L., Kurics, T., Windhager-Pokol, E.: Balabit Mouse Dynamics Challenge data set (2016). https://github.com/balabit/Mouse-Dynamics-Challenge
6. Antal, M., Egyed-Zsigmond, E.: Intrusion detection using mouse dynamics. arXiv preprint arXiv:1810.04668 (2018)

7. Nakkabi, Y., Traoré, I., Ahmed, A.A.E.: Improving mouse dynamics biometric performance using variance reduction via extractors with separate features. IEEE Trans. Syst. Man Cybern.-Part A: Syst. Hum. **40**(6), 1345–1353 (2010)
8. Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., Schclar, A.: User identity verification via mouse dynamics. Inf. Sci. **201**, 19–36 (2012)
9. Gamboa, H., Fred, A.: A behavioral biometric system based on human-computer interaction. Biom. Technol. Hum. Identif. **5404**, 381–393 (2004)
10. Shen, C., Cai, Z., Guan, X.: Continuous authentication for mouse dynamics: a pattern-growth approach. In: 2012 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 1–12, June 2012
11. Schulz, D. A.: Mouse curve biometrics. In: 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, pp. 1–6, September 2006
12. Bours, P., Fullu, C.J.: A login system using mouse dynamics. In: Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2009, pp. 1072–1077, September 2009
13. Hashia, S., Pollett, C., Stamp, M.: On using mouse movements as a biometric. Proceeding Int. Conf. Comput. Sci. Its Appl. **1**, 5 (2004)
14. Luzbashev, V., Filippov, A.I., Kogos, Konstantin, A.G.: Continuous user authentication in mobile phone browser based on gesture characteristics, pp. 90–95 (2018). https://doi.org/10.1109/WorldS4.2018.8611589
15. Jovic, A., Brkic, K., Bogunovic, N.: An overview of free software tools for general data mining. In: 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1112–1117, May 2014
16. Salman, O.A., Hameed, S.M.: Using mouse dynamics for continuous user authentication. In: Proceedings of the Future Technologies Conference, November, pp. 776–787 (2018)