BioPrivacy: A Behavioral Biometrics Continuous Authentication System based on Keystroke Dynamics and Touch Gestures.

Ioannis Stylios[1], Andreas Skalkos[1], Spyros Kokolakis[1] and Maria Karyda[1]

[1]University of the Aegean, Greece
{istylios,ask,sak,mka}@aegean.gr

Abstract. This paper is an extended version of SECPRE 2021 paper and presents a research on the development and validation of a BBCA system that is based on users keystroke dynamics and touch gestures on mobile devices. Session authentication schemes establish the identity of the user only at the beginning of the session, so they are vulnerable to attacks that tamper with communications after the establishment of the authenticated session. Moreover, smartphones themselves are used as authentication means, especially in two-factor authentication schemes, which are often required by several services. Whether the smartphone is in the hands of the legitimate user constitutes a great concern, and correspondingly whether the legitimate user is the one who uses the services. In response to these concerns, Behavioral Biometrics (BB) Continuous Authentication (CA) technologies have been proposed on a large corpus of literature. This paper presents a research on the development and validation of a BBCA system (named BioPrivacy), that is based on the user's keystroke dynamics and touch gestures, using a Multi-Layer Perceptron (MLP). Also, we introduce a new behavioral biometrics collection tool, and we propose a methodology for the selection of an appropriate set of behavioral biometrics. Our system achieved the best results for keystroke dynamics which are 97.18% Accuracy, 0.02% Equal Error Rate (EER), 97.2% True Acceptance Rate (TAR) and 0.02% False Acceptance Rate (FAR).

Keywords: Machine Learning, Behavioral Biometrics, Continuous Authentication, Mobile Devices, Multi-Layer Perceptron (MLP).

1 Introduction

User authentication technology plays a critical role in securing access to online services. Authentication systems identify users only when the session is initiated (entry point authentication model), thus leaving them exposed to attacks that take place after the initial authentication process [1, 7, 8, 9, 10, 39, 41]. These systems defend themselves against such attacks by performing an additional authentication step at critical points in the session but are not popular with users due to the inconvenience caused by repetitive authentications. Also, smartphones are used as authentication means, especially in two-factor authentication schemes, which are often required by several electronic services. Whether the smartphone is in the hands of the legitimate user constitutes a great concern, and correspondingly whether the legitimate user is the one who uses the services. In addition, mobile devices are vulnerable to smudge attacks [40], i.e., the mark of the fingerprints left by our finger on the screen, as it is easy to reveal the touch pattern or the PIN of the device. Thus, stealing a device carries the risk of granting full access to personal data and crucial applications. Moreover, smartphone users are unaware of privacy and security threats and keep large amounts of private information including PINs, credit card numbers, etc., stored in their mobile devices [1].

For the above reasons, Behavioral Biometrics (BBs) and Continuous Authentication (CA) are employed by a new method of user authentication which is also based on the "something that the user is" paradigm [2, 3, 4, 5, 6, 7, 9]. The technological advancement of mobile devices has led to the efficient capture of user behavior via their incorporated sensors, thus enabling the authentication of users based on their behavioral biometrics [11, 12, 13, 14, 15]. The incorporated sensors of mobile devices are used to enroll BB templates [7, 14, 16]. The BBs that may be employed are walking gait, touch gestures, keystroke dynamics, hand waving, user profile, and power consumption. The advantage of BBs is that they use some characteristic feature of a single individual and provide continuous authentication [7]. Alongside the initial login process CA technology represents an extra security mechanism since it monitors user behavior and re-authenticates continuously the user's identity throughout a session [5, 17, 18, 19, 20]. Finally, the work of [10, 22, 23, 58, 59] showed the eagerness of users to adopt biometric authentication methods in order to protect their privacy.

This paper is an extended version of SECPRE 2021 paper [49] and presents a research on the development and validation of a BBCA system, named BioPrivacy, that is based on users keystroke dynamics and touch gestures on mobile devices. We aim at building a system that will continuously authenticate the user of a smartphone. We start with an experimental biometric data collection process via mobile smartphones. The main objective is to propose a methodology and a data collection tool (BioPrivacy Collection Tool) for the selection of an appropriate set of behavioral biometrics. In this experiment, we recorded users' keystroke dynamics and touch gestures. Also, the present research aims to designing and evaluating new approaches to Continuous Authentication (CA) by developing and using a Multi-Layer Perceptron (MLP).

The structure of this paper is as follows: In Section 2, we present an overview of the keystroke dynamics, the Multi-Layer Perceptron (MLP) and the evaluation metrics. In Section 3 we present a recent state-of-the-art literature review focusing on keystroke dynamics and touch gestures. In Section 4, we present the BioPrivacy System Architecture. Specifically, we present the biometrics collection architecture by which we can collect the biometric data of the users, and the data preparation for introduction to machine learning algorithms. In Section 5, we present the data collection process, via mobile smartphones and the BioPrivacy collection tool, by which we recorded users keystrokes and touch gestures. In Section 6, we present the results of our research and in Section 7, we make a discussion, and we present the contributions and limitations of our paper. Finally, in Section 8, we present our conclusions and future research.

2 Background

In this section, we present an overview of the keystroke dynamics, the Multi-Layer Perceptron (MLP) and the evaluation metrics.

2.1 Keystroke dynamics

The procedure of recording the typing keyboard inputs of an individual on a mobile device and the effort to identify him via an analysis based on his tapping habits is called keystroke dynamics [7]. Some researchers on keystroke dynamics collect data from predefined texts, for example during the typing of a text message, or during the log-in session when entering passwords. Others conduct their research by collecting data not restricted on predefined sentences or passwords. In both cases the results are of high accuracy [7].

2.2 Touch gestures

The smartphone touch screen sensor is used for collecting touch data. Actions of input associated with parameters such as speed, velocity, size, length, direction or pressure, are converted into a gesture output template. These parameters are different between users and indicate the behavior of each, thus consisting the basis of the touch gesture authentication systems [7, 14].

2.3 Multi-Layer Perceptron (MLP)

Artificial Neural Networks (ANNs) are structures inspired by human brains' function. These networks can estimate model functions and handle linear/nonlinear functions by learning from data associations and generalizing to previously unknown scenarios. Multi-Layered perceptron (MLP) is a widely used Artificial Neural Network approach (ANNs) [46]. Specifically, a feedforward artificial neural network called a Multi-Layer Perceptron (MLP) is a type of Feedforward Artificial Neural Network (FANN). Each

unit in an MLP neural network performs a biased weighted sum of its inputs and then passes this activation level through a transfer function to generate output [57].

MLP networks typically include three layers: input, hidden, and output. The number of neurons in the input layer is equal to the number of parameters affecting the problem. Almost all problems can be solved with just one hidden layer. The number of neurons in the hidden layer or layers should be arbitrarily chosen [47]. This is a powerful modeling tool that employs a supervised training procedure with data examples with known outputs. Training for the MLP approach is accomplished in two steps. In the first step, the training data set is fed by a randomly picked input vector. The activated neurons output is subsequently propagated from hidden layer(s) to the output layer. The back propagation step, begins by calculating the gradient descent error and then propagates it backwards to each neuron in the output layer, followed by the hidden layer. The neural network's weights and biases are recomputed at the end of the second step. These two steps are repeated until the network's total error is less than a predetermined rate or the maximum number of epochs is reached [47]. Although, MLP network is a widely-used ANN approach, the MLP network still has certain limitations, such as time-consuming issues in reaching a solution [48].

2.4 Evaluation metrics

The basic metrics applied to evaluate an authentication system depend on the error rates. As suggested by Stylios et al., [7] research works should include at least the FAR, TAR, FRR, EER, and Accuracy when evaluating the performance of their approach. In this way, a comparison between the different approaches will be feasible. Following, we discuss some basic metrics used to calculate authentication errors [7, 31, 32, 33]:

- True Acceptance Rate (TAR) is the conditional probability of a pattern to be classified in the class “Genuine” given that it belongs to it. TAR is given by the formula:

$$TAR=TA/(TA+FR) \tag{1}$$

- False Acceptance Rate (FAR) is the conditional probability a pattern to be classified in the class “Genuine” given that it does not belong to it. FAR is given by the formula:

$$FAR=FA/(FA+TR). \tag{2}$$

- False Reject Rate (FRR) is the conditional probability a pattern not to be classified in the class “Genuine” given that it belongs to it. FRR is given by the formula:

$$FRR=FR/(FR+TA) \tag{3}$$

- Accuracy is defined as the probability of correct classification of a pattern. Accuracy is given by the formula:

$$\text{Accuracy} = (TA+TR)/(TA+TR+FA+FR) \quad (4)$$

- Equal Error Rate (EER) is the error rate that is achieved by tuning the detection threshold of the system such that FAR and FRR are equal [28].

3 Related Work

In this section we present a recent state-of-the-art literature review focusing on keystroke dynamics and touch gestures.

3.1 Keystroke dynamics

The majority of keystroke dynamics methods are restricted to using a specific context with a prearranged text. In the work of Clark and Furnell [24], the authors employed the typing patterns of users when entering telephone numbers and text messages, to authenticate them. They used Multi-Layer Perceptron (MLP), Radial Basis Functions (RBF), and General Regression Neural Network (GRNN) classifiers. The best results achieved were 12.8% average EER with the Multi-Layer Perceptron (MLP) classifier.

In the work of Draffin et al. [4], the authors conducted a real-world study and collected 86000 keystrokes from 13 participants in three weeks. Keystrokes were not restricted to the use of prearranged text or passwords. They used Feed Forward Neural Network for classification and achieved 86% accuracy after 15 keypresses with 2.2% FRR, and 14% FAR.

In the work of Darren and Inguanez [25], they collected typing data while users were entering 15 prearranged text sentences during four different scenarios, namely, One-Handed stationery, Two-handed stationery, One-Handed moving, and Two-handed moving. The participants were free to choose one of the four scenarios, while the smartphone owner had to complete all 4 activities. The authors used a Least Squares SVM classifier with RBF kernel and the one-handed scenario achieved the best results, namely, 0.44% EER, 100% accuracy, 0% FAR, and 1% FRR, while all their results achieved around 1% EER.

In the work of Krishnamoorthy [26], the classification of users was based on keystroke dynamics, by applying concepts of machine learning. The participants of this study were asked to type a specific password and their typing characteristics were recorded. Krishnamoorthy effectively identified each one of the 94 users and achieved 98.44% identification accuracy with the Random Forest classifier.

In Table 1, we present the performance of machine learning models on keystroke dynamics. For each system, there is at least one of the five basic metrics, namely FAR, TAR, FRR, EER, and Accuracy.

Table 1: A literature review on keystroke dynamics

Method	Works	Platform	Classification	Performance (%)				
				FAR	TAR	Accuracy	FRR	EER
Keystroke Dynamics	[24] in 2006	Smartphone	MLP					12.8
	[4] in 2013	Smartphone	FFNN	14		86.0		22
	[4] in 2013	Smartphone	SVM	0		100	1	0.44
	[25] in 2018	Smartphone	Random Forest			98.44		2.2

As we can see in Table 1, RF and SVM classifiers have achieved very good results while the performance of the MLP and the FFNN is relatively low. We believe that further research is necessary to see if FFNN and MLP can have better performance. By applying a new design approach to MLP, using the BioPrivacy collection tool dataset, we will see if we have an improvement in the performance. In case a high performance is achieved, we will apply MLP in our system.

3.2 Touch Gestures

Buriro et al. [50] built a system that profiled users based on their finger movements on the touchscreen while signing or writing and the movements of the device. They tested their mechanism on a dataset of 30 volunteers and achieved a True Acceptance Rate (TAR) of 95% with a False Acceptance Rate (FAR) of 3.1% by using a Multilayer Perceptron (MLP). Filippov et al. [51] built an authentication system using the data that resulted from the interaction of twenty-one users with the touch screen of a smartphone. They gathered 2000 features from seven different gesture types of swipe while users interacted with the smartphone. Their system was evaluated by using the Isolation Forest method and achieved values of FRR and FAR equal to 6.4% and 7.5%, respectively. Moreover, their system detected the illegitimate user in seven performed actions.

Shen et al. [52] collected touch data from 102 subjects during three different operation scenarios. The best performance among all three operation scenarios was achieved when participants hold the smartphone and performed touch actions while sitting or standing still. More specifically, the FAR was 3.98%, the FRR 5.03%, and the EER 4.71%. Debard et al. [53] proposed the Convolutional Neural Networks, which used 2D filters for the recognition of touch gestures on a touch surface. They used a dataset of 6591 touch gestures from 27 individuals. They compared the performance of their method to the performance of the methods provided by Hochreiter et al. [54] and Liu et al. [55] who used the LSTM classifier. The Convolutional Neural Networks classifier used by Debard et al. [53] achieved 89.96% accuracy while the LSTM classifier achieved 73.10% in the work of Hochreiter et al. [54] and 87.72% in the work of Liu et al. [55].

Yang et al. [56] used behavioral biometrics of touch and based on anomaly detection they developed a CA method for security-sensitive mobile applications named Behave-Sense. They used touch gestures of click and slide. For classification they used Isolation Forest and One-class SVM Method. For the sequence of touch operation their method achieved an average accuracy of 95.85% when considering 9 touch operations.

In Table 2, we present the performance of machine learning models on touch gestures. For each system, there is at least one of the five basic metrics, namely FAR, TAR, FRR, EER, and Accuracy.

Table 2: Touch gestures modality research works.

Method	**Publications**	**Platform**	**Classification**	**Performance (%)**				
				FAR	**TAR**	**Accuracy**	**FRR**	**EER**
Touch Gestures	[50] in 2016	smartphone	MLP	3.1	95			
	[51] in 2018	smartphone	Isolation Forest	7.5			6.4	
	[52] in 2018	smartphones	HMM	3.9			5.03	4.71
	[53] in 2018	touch surface	CNNs			89.96		
	[56] in 2019	smartphone	Isolation Forest			95.85		

As we can see in Table 2, the MLP classifier in [50], the Isolation Forest in [51], and the HMM in [52] performed well, achieving 3.1%, 7.5% and 3.9% FAR, respectively. The HMM also achieve EER 4.71%. The CNN achieved 89.96% accuracy in [53], while the Isolation Forest achieved 5.85% accuracy in [56]. We will apply a new design approach to MLP to see if we can achieve a better performance.

4 Experimental setup

In this part we present the BioPrivacy System Architecture. Specifically, we present the biometrics collection architecture by which we can collect the biometric data of the users, and the data preparation for introduction to machine learning algorithms.

4.1 Bioprivacy's collection tool

Bioprivacy's collection tool is an Android application for collecting cell phone sensor values. For the needs of our research, we collected the touch gestures and keystroke dynamics, however the application can collect the following biometric features:

- *Walking gait:* Measurement records are captured by the accelerometer and gyroscope sensor. There is also a pacemaker that records the time between steps.
- *Touch gestures:* This approach records the unique user touch features, such as finger pressure and orbit, speed and acceleration of motion as the individual interacts with the mobile device.
- *Keystroke dynamics:* With this method, users are identified by the way they type on the device keyboard.
- *Hand waving:* Hand waving records are collected by the following sensors: accelerometer, gyroscope.
- *GPS Location:* The application collects geographic location.

The BioPrivacy Application sends the data to an API that stores the data in an online MySQL database. This API is an online application running at all times (24/7). It is built to retrieve data from the application and store it in the online database. Each operation is performed on different files so that if one file has an error it will not affect the other. Each of the files receives different input parameters. The online database is designed to allow multiple users to store their sensor data at any time. Thus, there is no concern about data separation and synchronization. The application apriori covers all the possible malfunctions of multiple communication with the base.

A software system must be sustainable and scalable. For this reason, the structure of the application is such that it significantly enhances the creation of an architecture that could accommodate all possible types of expected changes. The project was developed in Android Studio. To use the source code of the program, as well as for compile and redistribution, developers who might want to extend the code should use the latest version of Android Studio with the latest version of the Android SDK installed.

4.1.1 User Interface

In fig. 1a we see the navigation menu of the application. From the graphical viewpoint in the six options (Accelerometer, Gyroscope, Gestures, Pressure, GPS, Keystroke), users view the corresponding information according to the corresponding view. By selecting the accelerometer and/or gyroscope, users see a graph showing the values of the sensors. The axes' measurements are perspective. However, the graph of the accelerometer and the gyroscope may appear as follows in the application (fig. 1b).

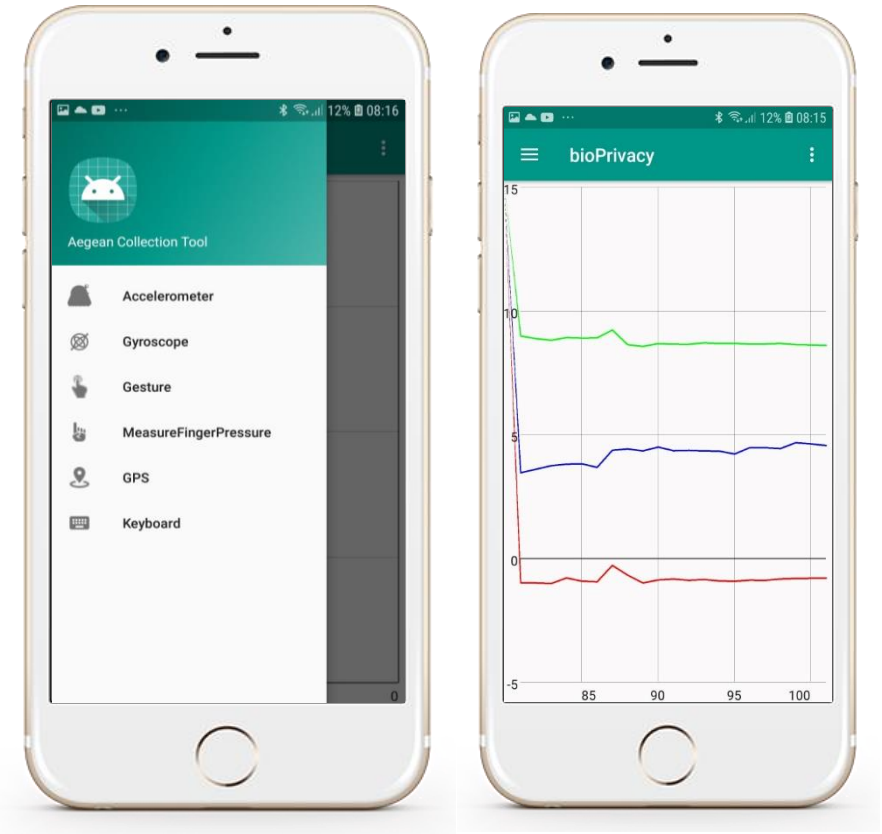

Fig. 1: a) The application menu. b) Interface measurements of the accelerometer or gyroscope.

In fig. 2a we see the BioPrivacy interface for touch gesture modality. It shows the state of the application (running or not) as well as the X and Y coordinate and the pressure applied to each of the fingers touching the screen. Finally, in fig. 2b we see the keystroke recording interface. For keystroke, the application opens its keyboard and displays on-screen details including finger positions, hold time and inter-key time.

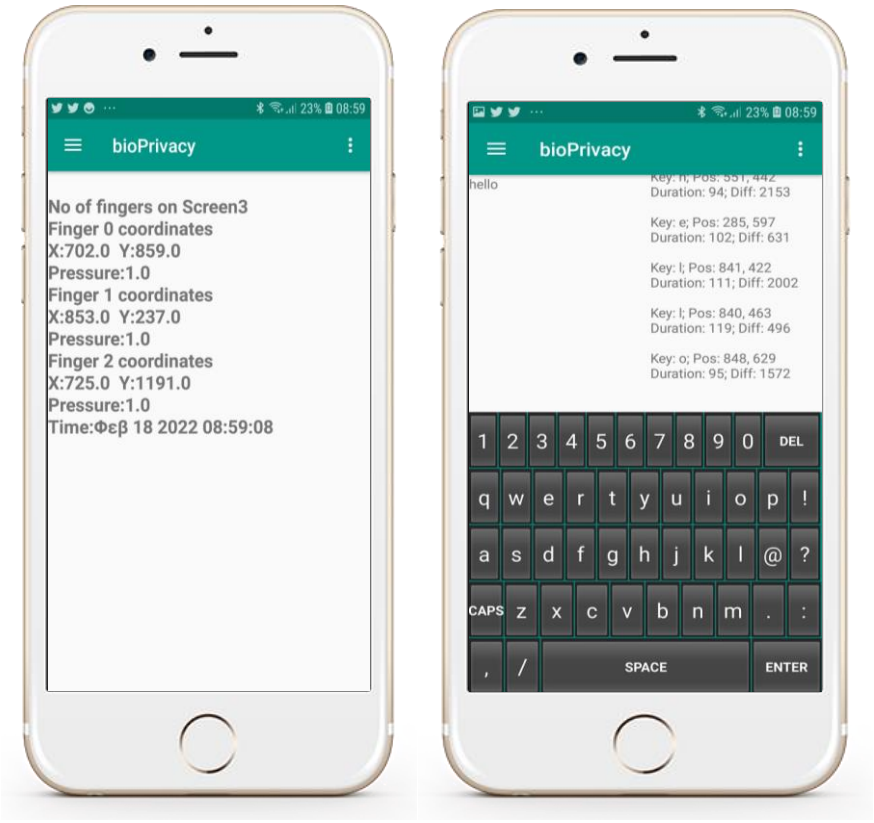

Fig. 2: a) Touch gesture recording interface. b) Keystroke interface

4.1.2 Data Collection and Features Extraction

Regarding keystroke dynamics and touch gestures BioPrivacy collects data and creates features in specific ways. Following, we will provide a detailed description of the ways that the BioPrivacy collects the data and creates the features of keystroke dynamics and touch gestures.

4.1.2.1 Keystroke dynamics

When a user types on the BioPrivacy's keyboard, the inputs are recorded and analyzed in order to identify him based on his tapping habits [7, 34]. The BioPrivacy application extracts the duration and latency of the pressure on keys and the location points of fingers as described [7, 29, 35, 36, 37]:

- *Duration*: is the time period between pressing and releasing a key.

- *Latency*: is the time period between releasing a pressed key until pressing the next key.
- *Pressure*: is the pressure on a key.
- *Location*: are the location points (xi, yi) of the finger on the screen.

4.1.2.2 Touch Gestures

The gesture of touch is a single or multiple strokes or a swipe on the touch screen of the mobile device made by the finger. The BioPrivacy application extracts the location points, the time stamps and the pressure of touch. Each of them can be encoded as a series of vectors [49]:

$$S_i = (x_i, y_i, t_i, p_i), i = \{1, 2, \dots, N\}, \textit{(1)}$$

where x_i, y_i are the location points, and $t_i, p_i$are the time stamps and the pressure on screen, respectively. Here, N is the total number of swipes.

4.2 BioPrivacy system architecture

There is a set of basic modules included in the BioPrivacy system (see fig. 3). We ended-up in this set of basic modules according to the literature [7, 38]. The registration process, which is the first step of the BioPrivacy system, involves collecting the biometric sample, processing the biometric data to extract the reference sample, and storing it for further use. The efficiency and accuracy of a biometric system are directly dependent on the registration process. During the life cycle of a biometric, it is sometimes necessary to re-record, taking into account the normal as well as the unexpected change or evolution of biometric characteristics.

1. *Data acquisition:* Sample acquisition: To acquire biometric data we must use the appropriate sensor.

2. *Feature extraction:* The raw data must be preprocessed before extracting the distinctive features. More specifically, we must identify and extract outliers and improve the quality of data, especially in cases where data are collected in uncontrolled environments from uncooperative users. The set of discriminative features are extracted once the data is cleaned and processed.

3. *Feature templates:* This is a repository database containing a concatenation of the extracted feature vectors for a particular user (i.e., the device owner). It is created during the enrollment phase and used during the recognition phase to be compared with the captured feature sample and verify the claimed identity.

4. *Decision-making:* This is used only during the recognition process. This step compares the template that is currently being extracted with the saved template to generate a matching score and make a decision. The decision validates the

claimed identity to see if it is done by the legitimate user (genuine) or an impostor.

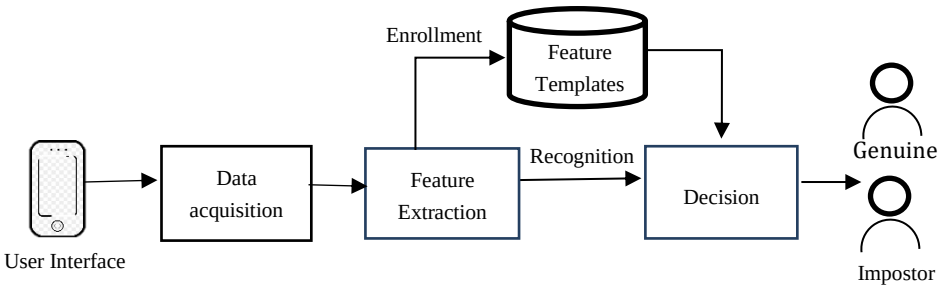

Fig. 3. BioPrivacy system architecture.

5 Methodology

In this section, we present the data collection process, via mobile smartphones and the BioPrivacy collection tool, by which we recorded users keystrokes and touch gestures. We have a sample of 39 individuals. All the participants are smartphone owners and familiar with the experimental part of the process.

For the keystroke, the data collection process consists of 16 sessions in total and each session lasts 2 minutes approximately. During the sessions, a predefined sentence or a sequence of numbers were displayed on the screen and participants had to either memorize and input them or input them immediately after they were displayed. In this way, we have two kinds of inputs, one that the participants must read, memorize, and then write and another that the participants must read and then immediately write. We select one individual from the 39 participants of our sample as Genuine user and the rest 38 as impostors.

For the touch gestures, the data collection process consists of 16 sessions in total and each session lasts 2 minutes approximately. We collect gestures such as swipe left/swipe right, swipe up/ swipe down which are widely used. Also, we collect some special gestures such as single or multiple fingers touches and swipe up or down in a specific area, because they can be used for continuous authentication [37].

Finally, we evaluate the performance of our system, which is based on the Multi-Layer Perceptron, by calculating the FAR and TAR metrics, Accuracy and Equal Error Rate.

6 Results

In this section we present the results of our research. First, we present the results from the bioprivacy's collection tool regarding keystrokes dynamics and touch gestures. Following, we present the machine learning results achieved regarding keystrokes dynamics and touch gestures data by applying the MLP classifier.

6.1 Bioprivacy's collection tool results

Following, we will see a detailed presentation of the BioPrivacy's collection tool results. Firstly, we present the results from the BioPrivacy's collection tool regarding keystroke dynamics where we describe the features of duration, latency, pressure, x and y values. Following, we present the results from the BioPrivacy's collection tool regarding touch gestures where we describe the features of x and y values, time and pressure. These data are collected from 39 participants. The data collection process consisted of 16 sessions and each session lasted approximately 2 minutes.

6.1.1 Keystroke Dynamics

In Table 3 we see records in the database regarding keystroke dynamics. The features are duration, latency, the pressure on keys, and the location points (x, y) of the finger. The data received from the database were in accordance and consistent with the theoretical framework presented in Section 4.1.

Table 3. Keystroke dynamics data

Sensor	Key	Duration	Latency	Pressure	X_value	Y_value
Touch Screen (Keyboard)	p	134	189	1.0	943.0	404.0
	u	96	176	1.0	637.0	417.0
	f	57	358	0.50	339.0	243.0

From the data collected with the BioPrivacy collection tool, we created a dataset that consists of 39 individuals and 1488 Instances. We separated the users into 2 classes (Genuine – Impostor), one individual as a Genuine user and the rest 38 individuals as impostors. We also inserted a data preprocessing step by applying Normalize with scale 1.0.

6.1.2 Touch gestures

As mentioned above, BioPrivacy collects touch gestures. Table 4 shows the database entries sent by the application regarding touch gestures.

Table 4: Touch gestures data.

Sensor	Action	X_value	Y_value	Time	Pressure
Touch Screen (Gestrures)	Action_Down	646.8269	1248.5352	20	0.1
	Action_Move	652.2571	1227.4142	10	0.5
	Action_Up	790.6092	1199.5518	30	0.5

From the data collected with the bioprivacy collection tool, we created a dataset that consists of 39 individuals and 28071 Instances. We separated the users into 2 classes (Genuine – Impostor), one individual as a Genuine user and the rest 38 individuals as impostors. We also inserted a data preprocessing step by applying Normalize with scale 1.0.

6.2 Machine learning Results

In this section we evaluate the performance of our system, which is based on the Multi-Layer Perceptron, by calculating the FAR and TAR metrics, Accuracy and Equal Error Rate. The MLP classifier is applied on keystroke dynamics and touch gestures data. The results achieved by our system are presented below.

6.2.1 Keystroke Dynamics results

We applied the MLP classifier with the following configurations: L 0.3 -M 0.2 -N 500 -H 3. The learning rate (L) is set to 0.3, the Momentum to 0.2, the training time (N) to 500, and we used 3 hidden layers (H). Our system achieved 97.18% Accuracy and 0.02% Equal Error Rate. In Table 5, we summarize the accuracy and EER.

Table 5: Accuracy and EER

Accuracy	Equal Error Rate
97.18%	0.02%

In Table 6, we present the detailed results by class. In the class Impostor, we achieved 94.5% True Acceptance Rate (TAR) while we have 0% False Acceptance Rate (FAR). In the class Genuine, we achieved 100% True Acceptance Rate (TAR) while the False Acceptance Rate (FAR) is 0.05%. Finally, in the Weighted Average, we have 97.2% TAR and 0.02% FAR.

Table 6: Detailed results By Class

Classifier	TA Rate	FA Rate	Class
MLP	94.5%	0%	Impostor
	100%	0.05%	Genuine
Weighted Avg.	97.2%	0.02%	

6.2.2 Touch Gestures results

We applied the MLP classifier with the following configurations: L 0.3 -M 0.2 -N 500 -H 3. The learning rate (L) is set to 0.3, the Momentum to 0.2, the training time (N) to 500, and we used 3 hidden layers (H). Our system achieved 91.36% Accuracy and 0.02% Equal Error Rate. In Table 7, we summarize the accuracy and EER.

Table 7: Accuracy and EER

Accuracy	Equal Error Rate
91.36%	1.9%

In Table 8, we present the detailed results by class. In the class Impostor, we achieved 97.9% True Acceptance Rate (TAR) while we have 55.3% False Acceptance Rate (FAR). In the class Genuine, we achieved 43.7% True Acceptance Rate (TAR) while the False Acceptance Rate (FAR) is 0.02%. Finally, in the Weighted Average, we have 91.4% TAR and 49.8% FAR.

Table 8: Detailed results By Class

Classifier	TA Rate	FA Rate	Class
MLP	97.9%	55.3%	Impostor
	43.7%	0.02%	Genuine
Weighted Avg.	91.4%	49.8%	

7 Discussion

This paper presents our research on the development and validation of a BBCA system (BioPrivacy) that is based on the user's keystroke dynamics using Multi-Layer Perceptron (MLP). Also, we introduce a new biometrics collection tool of the BioPrivacy system. We applied an experimental procedure of biometrics data collection where 39 individuals participated and completed the process. We received positive feedback on the application and users stated that they enjoyed the procedure. The data received from the database were in accordance and consistent with the analysis presented in the section 4.1 of the present paper.

Regarding the challenges of the keystroke dynamics collection methodology, they are based on something that the user must recall from his/her memory, like a password, and something that the user sees and types, like a captcha. In this way, we have two kinds of inputs, one that the participants must read, memorize, and then write and another that the participants must read and then immediately write. We created a dataset that consists of 39 individuals and 1488 Instances and 2 classes (Genuine – impostor). One individual as a Genuine user and the rest 38 individuals as impostors.

By applying a new design approach of the MLP and the BioPrivacy dataset we achieved an improved performance in relation to the literature. In [4] the performance of the FFNN is relatively low achieving FAR 14%, Accuracy 86% and EER 22%. In [24] the MLP achieved 12.8% EER. Our approach achieved Accuracy 97.18%, EER 0.02%, TAR 97.2% and FAR 0.02%.

In touch gestures the MLP had a very good performance achieving 0.02% false acceptance rate (FAR) in the Genuine class. That means, a good level of security against impostors. Our MLP achieved better FAR compared to: 3.1% with MLP in [50], 7.5% with Isolation Forest in [51], and 3.9% with HMM in [52]. The HMM also achieved EER 4.71%, our approach achieved EER 1.9%. Our MLP also achieved Accuracy 91.36% which is better than the 89.96% accuracy achieved with the CNN in [53]. Finally, in terms of usability the performance is lower since we achieved 43.7% TAR in the Genuine class.

The results show that keystroke dynamics perform better than touch gestures. Based on the high performance of the MLP in keystroke dynamics, we can conclude that a keystroke biometric system could be accepted by users and be successful. In contrast, in touch gestures, we have a relatively high FAR which means that its effectiveness is limited and further research is necessary.

7.1 Contribution

The principal contributions of this paper are as follows:

- We developed a new behavioral biometrics collection tool,named BioPrivacy Collection Tool, by which we can collect behavioral biometrics of users on mobile devices.
- We propose a methodology for the selection of an appropriate set of behavioral biometrics.
- We developed a BBCA System. We present the development of a BBCA system based on MLP.

7.2 Limitations

As suggested by Stylios et al. [7], CA systems need to be evaluated under the high effort approaches to see the actual performance of machine learning and deep learning models under the spectrum of today's possible threats. Therefore, our system should be evaluated against the Frog-Boiling attack [27], the Algorithmic attack [42], the Mimic attacks [43, 44], and the Snoop-forge-replay attack [45]. Finally, our system was tested in a sample of 39 individuals and we plan to evaluate it in a larger sample of users.

8 Conclusions and further research

Smartphones are used as a mean to authenticate individuals, particularly in two-factor authentication schemes, which are often obligatory by several electronic services. Whether the legitimate user possesses the smartphone constitutes a great concern, and correspondingly whether the services are used by the legitimate user. In this paper, we presented our research on the development and validation of a keystroke dynamics and touch gestures Continuous Authentication System, named BioPrivacy. In our paper, we present a new behavioral biometrics collection tool, named BioPrivacy Collection Tool and we propose a methodology for the selection of an appropriate set of behavioral biometrics. We applied an experimental test to examine the consistency of the collected data with the theoretical framework presented in section 4.1. Our results showed that the collected data are consistent and in accordance with the theoretical framework. In the present research we developed a BBCA system based on MLP. The best performance achieved by our system was on keystroke dynamics. More specifically, it achieved Accuracy 97.18%, EER 0.02%, TAR 97.2% and FAR 0.02%.

Our future research focuses on the extension of the BioPrivacy Collection Tool to include more behavioral modalities. Also, we will collect data from a larger population to create a dataset that will be publicly available. Finally, we will evaluate our model against possible attacks vectors and highlight relevant countermeasures.

Acknowledgments

This research is co-financed by Greece and the European Union (European Social Fund- ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning 2014-2020» in the context of the project “BioPrivacy: Development and validation of a Behavioral Biometrics Continuous Authenti-cation System” (MIS 5052062).

References

1. I. Stylios, S. Kokolakis, O. Thanou & S. Chatzis (2016). Users' Attitudes on Mobile Devices: Can Users' Practices Protect their Sensitive Data? 10th Mediterranean Conference on Information Systems, MCIS 2016.
2. P. Corcoran, C. Costache, "Biometric Technology and Smartphones: a consideration of the practicalities of a broad adoption of biometrics and the likely impacts, IEEE Consumer Electronics Magazine 5 (2) (2016) 70–78, https://doi.org/10.1109/MCE.2016.2521937.
3. F. Cherifi, B. Hemery, R. Giot, M. Pasquet, C. Rosenberger, Performance evaluation of behavioral biometric systems. Behavioral Biometrics for Human Identification: Intelligent Applications, IGI Global, 2010, pp. 57–74.
4. J. Zhu Draffin, J.Y. Zhang, KeySens: passive user authentication through microbehavior modeling of soft keyboard interaction, MobiCASE. (2013), https://doi.org/10.1007/978-3-319-05452-0_14.
5. Biometric authentication: the how and why [online]. Available: https://about-fraud.com/biometric-authentication, accessed on 21/2/2019.

6. B. Dorizzi, (2005). Biometrics at the frontiers, assessing the impact on society technical impact of biometrics, background paper for the institute of prospective technological studies, DG JRC - Sevilla, European Commission.
7. I. Stylios, S. Kokolakis, O. Thanou, S. Chatzis. (2021). Behavioral Biometrics & Continuous User Authentication on Mobile Devices: A Survey. Information Fusion, Volume 66, 2021, Pages 76-99, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2020.08.021.
8. M. Frank, R. Biedert, E. Ma, I. Martinovic, D. Song, Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication, IEEE Trans. Inf. Forensics Secur. 8 (1) (2013) 136–148, https:// doi.org/10.1109/TIFS.2012.2225048.
9. I.C. Stylios, O. Thanou, I. Androulidakis., E. Zaitseva, A review of continuous authentication using behavioral biometrics, in: Conference: ACM SEEDACECNSM, At Kastoria, Greece, 2016, https://doi.org/10.1145/2984393.2984403.
10. N.L. Clarke, S.M. Furnell, Authentication of users on mobile telephones – a survey of attitudes and practices, Comput. Secur. 24 (2005) 519–e527.
11. W. Shi, J. Yang, Y. Jiang, F. Yang, T. Feng, Y. Xiong, SenGuard: Passive user identification on smartphones using multiple sensors, in: International Conference on Wireless and Mobile Computing, Networking and Communications, 2011, pp. 141–148, https://doi.org/10.1109/WiMOB.2011.6085412
12. N.D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, A.T. Campbell, A survey of mobile phone sensing, IEEE Commun. Mag. Arch. 48 (9) (2010) 140–150. IEEE Press Piscataway, NJ, USA.
13. V.M. Patel, R. Chellappa, D. Chandra, B. Barbello, Continuous user authentication on mobile devices: recent progress and remaining challenges, IEEE Signal Process Mag. 33 (4) (2016) 49–61.
14. R. Murmuria, A. Stavrou, D. Barbara, D. Fleck, Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users, in: Proc. Int. Workshop Recent Adv. Intrusion Detection, 2015, pp. 405–424.
15. Introduction to android: sensors overview, android developers [online]. Available: https://goo.gl/MGWQy8, accessed on Feb., 21, 2020.
16. K. Jain, Y. Chen, M. Demirkus, "Pores and ridges: Fingerprint matching using level 3 features, Proc. Int. Conf. Pattern Recog. 4 (2006) 477–480.
17. D. Crouse, H. Han, D. Chandra, B. Barbello, A.K. Jain, "Continuous authentication of mobile user: fusion of face image and inertial measurement unit data, in: Int. Conf. Biometrics, 2015, pp. 135–142.
18. A. Abdulaziz, J.K. Kalita, "Authentication of smartphone users using behavioral biometrics, IEEE Commun. Surv. Tutor. 18 (2016) 1998–2026.
19. E.A. Ahmed, I. Traor´e, Continuous authentication using biometrics: data, models, and metrics, Hershey, IGI Global, PA, USA, 2011.
20. Z. Wu, Z. Chen, An implicit identity authentication system considering changes of gesture based on keystroke behaviors, Int. J. Distrib. Sens. Netw. 2015 (2015) 110–130.
21. P. Pons, P. Polak, Understanding user perspectives on biometric technology, Commun. ACM 51 (9) (2008) 115–118.
22. N.L. Clarke, S.M. Furnell, P.M. Rodwell, P.L. Reynolds, Acceptance of subscriber authentication methods for mobile telephony devices, Comput. Secur. 21 (3) (2002) 220–228.
23. S. Karatzouni, S.M. Furnell, N.L. Clarke, R.A. Botha, Perceptions of user authentication on mobile devices, in: Proceedings of the 6th Annual ISOnEworld Conference, April 11-13, 2007, Las Vegas, NV, 2007.
24. N.L. Clarke, S.M. Furnell, Authenticating mobile phone users using keystroke analysis, Int. J. Inf. Secur. 6 (1) (2007) 1–14.

25. C. Darren, F. Inguanez, Multi-Model authentication using keystroke dynamics for Smartphones, in: IEEE 8th International Conference on Consumer Electronics, Berlin (ICCE-Berlin), 2018.
26. S. Krishnamoorthy, Identification of user behavioural biometrics for authentication using keystroke dynamics and machine learning, Electron. Theses Dissertations (2018) 7440.
27. Z. Wang, A. Serwadda, K. S. Balagani and V. V. Phoha, (2012). "Transforming animals in a cyber-behavioral biometric menagerie with Frog-Boiling attacks," IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, pp. 289-296.
28. N. Samarin, (2018). A Key to Your Heart: Biometric Authentication Based on ECG Signals. 4th Year Project Report Computer Science, School of Informatics, University of Edinburgh.
29. I. Lamiche, G. Bin, Y. Jing, et al. (2019). A continuous smartphone authentication method based on gait patterns and keystroke dynamics. J Ambient Intell Human Comput 10, 4417–4430. https://doi.org/10.1007/s12652-018-1123-6
30. F. Cherifi, B. Hemery, R. Giot, M. Pasquet, C. Rosenberger (2010). Performance evaluation of behavioral biometric systems. In: Behavioral Biometrics for Human Identification: Intelligent Applications, pp. 57–74. IGI Global.
31. A. Lykas, (1999). "Computational Intelligence". University printing press, University of Ioannina, Greece.
32. S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic. 2017. Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17). Association for Computing Machinery, New York, NY, USA, 386–399. DOI: https://doi.org/10.1145/3052973.3053032
33. R. Dash & P. Dash, (2017). MDHS–LPNN: A Hybrid FOREX Predictor Model Using a Legendre Polynomial Neural Network with a Modified Differential Harmony Search Technique. Chapter 25. 10.1016/b978-0-12-811318-9.00025-9.
34. T-Y. Chang, C. J. Tsai, W. J. Tsai, C. C. Peng, & H. S. Wu, (2016). A changeable personal identification number-based keystroke dynamics authentication system on smartphones. Security and Communications Networks 2016; 9:2674–2685. Wiley Online Library (wileyonlinelibrary.com).
35. D. D. Alves, G. Cruz, and C. Vinhal, (2014). "Authentication system using behavioral biometrics through keystroke dynamics," in Proceedings of the IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM '14), pp. 181–184, IEEE.
36. H. Zhang, C. Yan, P. Zhao and M. Wang, (2016). Model construction and authentication algorithm of virtual keystroke dynamics for smart phone users, IEEE International Conference on Systems, Man, and Cybernetics (SMC), Budapest, pp. 000171-000175.
37. I. Stylios, S. Kokolakis, A. Skalkos, S. Chatzis, (2021), "BioGames: a new paradigm and a behavioral biometrics collection tool for research purposes", Information and Computer Security, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-12-2020-0196
38. A. Mahfouz, T. M. Mahmoud, A. S. Eldin, (2017). A survey on behavioral biometric authentication on smartphones. Journal of Information Security and Applications 37, (2017,) 28–37.
39. I. Androulidakis, V. Christou, N. G. Bardis, and I. Stilios, (2009). Surveying users' practices regarding mobile phones' security features. In Proceedings of the 3rd international conference on European computing conference (ECC'09). Tbilisi, Georgia, Pages: 25-30.

40. A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, J.M. Smith, (2010). Smudge attacks on smartphone touch screens. Proceedings of the 4th USENIX conference on Offensive technologies. pp. 1{7. USENIX Association.
41. D. M. Shila and E. Eyisi, (2018). Adversarial Gait Detection on Mobile Devices Using Recurrent Neural Networks, 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 316-321, doi: 10.1109/TrustCom/BigDataSE.2018.00055.
42. A. Serwadda and V. V. Phoha, (2013). Examining a Large Keystroke Biometrics Dataset for Statistical-Attack Openings. ACM Transactions on Information and System Security. 16.
43. P. Negi, P. Sharma, V. S. Jain, B.Bahmani, (2018). "K-means++ vs. Behavioral Biometrics: One Loop to Rule Them All. Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego, CA, USA ISBN 1-1891562-49-5
44. T. C. Meng, P. Gupta, and D. Gao, (2013). “I can be you: Questioning the use of keystroke dynamics as biometrics,” in Proc. NDSS, pp. 1–16.
45. K. A. Rahman, K. S. Balagani and V. V. Phoha, (2013). "Snoop-Forge-Replay Attacks on Continuous Verification with Keystrokes", in IEEE Transactions on Information Forensics and Security, vol. 8, no. 3, pp. 528-541.
46. H. Taud, J. F. Mas, (2018). Multilayer perceptron (MLP). In Geomatic Approaches for Modeling Land Change Scenarios (pp. 451-455). Springer, Cham.
47. M. Oral, E. Laptalı Oral, A. Aydın, 2012. Supervised vs. unsupervised learning for construction crew productivity pre-diction, Automation in Construction 22: 271–276. http://dx.doi.org/10.1016/j.autcon.2011.09.002
48. O. Arslan, O. Kurt, H. Konak, 2007. Yapay sinir ağlarının jeodezide uygulamaları üzerine öneriler [Suggestions on geodesy applications of artificial neural networks], in 11.Türkiye Harita Bilimsel ve Teknik Kurultayı, 2–6 April 2007, Ankara, Turkey.
49. I. Stylios, A. Skalkos, S. Kokolakis, M. Karyda, (2021). BioPrivacy: Development of a Keystroke Dynamics Continuous Authentication System. 5th International Workshop on SECurity and Privacy Requirements Engineering SECPRE 2021, 6 – 8 October 2021.
50. A. Buriro, B. Crispo, F. Delfrari, K. Wrona, (2016). Hold & Sign: A Novel Behavioral Biometrics for Smartphone User Authentication Conference: Mobile Security Technologies (MoST) 2016 in conjunction with IEEE Security and Privacy (S&P 16).
51. A. I. Filippov, A. V. Iuzbashev and A. S. Kurnev, (2018). User authentication via touch pattern recognition based on isolation forest, IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, pp. 1485-1489. doi: 10.1109/EIConRus.2018.8317378.
52. C. Shen, Y. Li, Y. Chen, X. Guan and R. A. Maxion, (2018). Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication, in IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 48-62.
53. Q. Debard, C. Wolf, S. Canu and J. Arne, (2018). "Learning to Recognize Touch Gestures: Recurrent vs. Convolutional Features and Dynamic Sampling," 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, pp. 114-121.
54. S. Hochreiter and J. Schmidhuber. Long short-term memory. Neural Comput., 9(8):1735–1780, 1997.
55. J. Liu, A. Shahroudy, D. Xu, and G. Wang. Spatio-Temporal LSTM with Trust Gates for 3D Human Action Recognition. 2016.
56. Y. Yang, B. Guo, Z. Wang, M. Li, Z. Yu, X. Zhou, (2019). BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. Ad Hoc Networks 84 (2019) 9–18. 1570-8705 Elsevier.

57. Singh, G., & Sachan, M. (2014, December). Multi-layer perceptron (MLP) neural network technique for offline handwritten Gurmukhi character recognition. In 2014 IEEE international conference on computational intelligence and computing research (pp. 1-5). IEEE.
58. Stylios, I., Kokolakis, S., Thanou, O. and Chatzis, S. (2022), "Key factors driving the adoption of behavioral biometrics and continuous authentication technology: an empirical research", Information and Computer Security, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-08-2021-0124
59. Skalkos A, Stylios I, Karyda M, Kokolakis S. Users' Privacy Attitudes towards the Use of Behavioral Biometrics Continuous Authentication (BBCA) Technologies: A Protection Motivation Theory Approach. *Journal of Cybersecurity and Privacy*. 2021; 1(4):743-766. https://doi.org/10.3390/jcp1040036