Hidden Monitoring Based on Keystroke Dynamics in Online Examination System

E. A. Kochegurova* (ORCID: 0000-0003-4473-528X) and R. P. Zateev** (ORCID: 0000-0001-8852-0737)

aNational Research Tomsk Polytechnic University, pr. Lenina 30, Tomsk, 634050 Russia
*e-mail: kocheg@mail.ru
**e-mail: roma-zateev@mail.ru

Received June 22, 2022; revised July 4, 2022; accepted July 6, 2022

Abstract—The COVID-19 pandemic has accelerated the development of distance learning technologies, where online tests and exams play an important role. In online testing, the detection of various types of academic fraud, including cases where the examinee is falsely represented by another person, is of particular importance. Continuous biometric (behavioral) authentication can be a solution to counter unauthorized access. This paper proposes an authentication technology based on keystroke dynamics and hidden monitoring. An application for collecting and updating keystroke dynamics profiles of domain users and their continuous authentication is developed. The efficiency of reducing the dimension of the keystroke feature space based on the frequency of alphabetic letters is demonstrated. Results of popular performance metrics (FAR, FRR, ERR, ROC, and DET) are significantly improved already when evaluating only metric distances. For instance, ERR is reduced from 10.1% to 0.79%, which is comparable to the estimates provided by the kNN method for its optimal parameters.

DOI: 10.1134/S0361768822060044

1. INTRODUCTION

The COVID-19 pandemic has had a significant impact on almost all spheres of everyday life. To reduce the infection rate, many companies and organizations transferred their employees to remote jobs and implemented other restrictive measures. Thereby, they accelerated the progress in digitalization, distance learning, telemedicine, online commerce, etc.

However, the positive technological impetus to the development of the IT industry has inevitably led to the growth of cybercrime. In the year the pandemic began (2020), a sharp increase in the number of cybercrimes, both throughout the world and in Russia, was recorded. According to Data Economy, an autonomous non-profit organization, in 2020, 363 thousand cybercrimes were reported in Russia, which is 77% more than in the previous year [1]. The statistics published by InfoWatch also indicates, in addition to the increase in the number of attacks by hacker groups, the emergence of new risks associated with remote work [2]. In 2021, a sharp increase in the number of intentional information leaks (82% of the total number) and leaks resulted from actions of cybercriminals (up to 63%) was recorded worldwide. Russia’s share in the number of global information leaks is quite impressive and amounts to 16.9%.

According to Ivideon, the number of cyber attacks in 2021, as compared to the previous year, increased by 40% worldwide and by 54% in Russia.

Even though information security has always been one of the highest priorities for any organization, this problem becomes especially important under the current conditions.

The education sector is one of the most vulnerable sectors in terms of cybersecurity, which is due to the mentality of students and circulation of large amounts of confidential information. This makes universities attractive targets for hackers. In September 2021 alone, there were more than 10 incidents involving ransomware that targeted personal data of students and teachers [3].

On the other hand, the pandemic has had a significant impact on the traditional system of higher and school education. According to UNESCO [4], the crisis has affected almost 1.6 billion students in more than 190 countries on all continents. The closure of schools and other educational institutions affected 94% students worldwide. Even though the number of partially or completely closed educational organizations decreased to 7.5% in September 2021 [5], the forms and methods of education have significantly transformed towards distance learning. However, uni-
Universities are still not ready for full-scale implementation of distance learning. In the context of higher education, online learning is often reduced to webinars, video/audio conferences, and use of e-learning platforms (Moodle, WebTutor, and iSpring Learn).

Online tests and exams are of great importance for e-learning. Tests allow the teacher to receive feedback from each student, estimate the academic progress, and improve the learning process. However, students sometimes resort to a number of academic fraud methods during online tests, including impersonation [6, 7]. Currently, there are no efficient methods for detecting this type of fraud.

2. ACADEMIC INTEGRITY OF ONLINE LEARNING

Academic integrity is a problem not only for the education sector but also for the whole society. Academic integrity violations negatively affect the educational environment, skills acquired by students, and the overall image of the university.

The global transition of higher education to online technologies inevitably activated many traditional forms of academic fraud: plagiarism, falsification of results, unauthorized collaboration, impersonation, etc. In addition to organizational means used to counteract these types of fraud (the university code of conduct for students and administrative sanctions for academic integrity violations), there are also methodological recommendations for teachers. For online classes, it is recommended to

- increase the individuality and specificity of test assignments;
- reduce the factological part of assignments and augment their conceptual part to develop thinking skills;
- increase the number of synchronous checks of answers in online mode;
- increase the number of small and simple assignments and use free forms, e.g., an essay, for large assignments.

The proposed measures [8] partially reduce the number of academic integrity violations; however, they significantly increase the workload on the teacher.

Continuous authentication by hidden monitoring can be a solution to counter unauthorized cooperation and impersonation.

3. KEYSTROKE AUTHENTICATION AND IDENTIFICATION

To protect a computer system from unauthorized access, two-step verification is generally used:

- primary identification: establishing the identity of a user, i.e., confirming the legitimacy of an authorized user;
- dynamic (continuous) authentication: the continuous confirmation of the identity of the legitimate user.

3.1. Authentication Methods

Authentication is a process of comparing the data provided by the user with the data stored in a directory services database. If these data match, then the user is given access to protected resources; otherwise, access is denied [9].

There are several methods for user authentication (see Fig. 1). These methods can be divided into three main groups based on the following paradigms [10]:

- something you know (e.g., password or PIN): knowledge-based authentication;
- something you have (e.g., token or smart card): attribute-based authentication;
- something you are, i.e., physiological and behavioral biometrics.

The “something you are” paradigm uses biometric features: physiological (fingerprint, face, iris, etc.) and/or behavioral (handwriting or keystroke patterns, gait, etc.) [19].

User recognition based on keystroke dynamics is quite attractive to organizations because it has lower implementation cost in comparison to other biometric methods, as it does not require any additional hardware. In addition to a standard keyboard, a highly efficient software application is required. While being rather accurate, this method is also capable of recognizing users in hidden mode, which is comfortable and does not distract users. Individual keystrokes, rhythm, and typing speed determine the keystroke dynamics (KD) of a user. All behavioral characteristics, including the KD, can gradually change with time; however, the probability of stealing or imitating these data is significantly lower than that for physiological data. That is why the KD can be useful for identification and authentication [11, 12]. The advantages, disadvantages, and examples of the authentication methods considered above are summarized in Table 1.

3.2. Authentication Modes

Hidden continuous monitoring is the most reasonable (for recognition systems) and comfortable (for users) identification method. According to the global security survey published by IBM (2018), 44% of the respondents considered biometrics to be the most secure authentication method, while 65% found that biometrics facilitates the authentication process [13].

The KD, as a biometric behavioral characteristic, is dynamic in nature. It includes constant and random components. The constant component is due to
human physiology, i.e., the user’s ability and skills in working with a keyboard. The random component depends on the psycho-emotional state of the user.

For the recognition, the dynamic behavioral features of the KD are more complex than the physiological ones. However, it is the behavioral features that are difficult to fake [10], which improves the effectiveness of impersonation detection.

Depending on the type of text (fixed or free), two main authentication modes can be distinguished [14]:
- static authentication (primary or by event);
- dynamic authentication (continuous).

It is continuous authentication that makes it possible to organize hidden identity verification of users during the entire session in any application. The recognition system captures keystrokes and compares them with an available template [6, 11, 17–19].

Static authentication can supplement the initial login procedure, or it can be activated when suspecting an intrusion [15, 16].

Both static and continuous authentications provide the second level of security when the user is already logged in. Meanwhile, dynamic authentication is aimed at continuous verification of the users or their psycho-emotional states.

This study is devoted to user authentication by continuous monitoring of KD features in online exam applications. More specifically, we focus on the following problems:
- collecting and updating KD samples for domain users;
- extending well-known static identification approaches to the case of dynamic identity recognition based on free and long texts;
- reducing the dimension of the space of extracted keystroke features to improve the selective properties of KD samples and the efficiency of continuous authentication.

3.3. Authentication Lifecycle

KD-based continuous authentication has a registration stage and an authentication stage (see Fig. 2).

At the registration stage, the system receives keystroke data. Then, keystroke features (hold time, flight time, etc.) are extracted, a keystroke profile (template) is formed or modified in the database, and user authentication is carried out.

Thus, the lifecycle of continuous authentication includes four main steps.

Table 1. Characteristics of authentication methods

| Method       | Advantages                                      | Disadvantages                        | Examples         |
|--------------|------------------------------------------------|--------------------------------------|------------------|
| Password     | 1. Easy to implement                           | 1. Can be forgotten or stolen        | 1. Password      |
|              | 2. Unambiguous recognition                     |                                      | 2. PIN           |
| Attribute    | 1. Easy to implement                           | 1. Can be lost or stolen             | 1. Key           |
|              | 2. Low cost                                    |                                      | 2. Smartcard     |
| Biometrics   | 1. Uniqueness                                  | 1. Implementation cost               | 1. Fingerprint    |
|              | 2. Impossible to forget/lose                    | 2. Data variability regardless of a person | 2. Voice         |
|              |                                                 |                                      | 3. Keystroke pattern |
I. Collection of KD data is a continuous process when the user works with a keyboard in any application. In Windows, the message interception mechanism is used. The Windows hook makes it possible to detect any keystroke event [20]. The OS captures the ANSI code and timestamps of key presses (Down/Press) and key releases (Up/Release). The accuracy of keystroke measurements is up to milliseconds.

II. Extraction of classification features. The raw keystroke data must be cleaned of outliers and invalid values; in some cases, they need to be normalized. Based on these data, more significant KD features (typing rhythm, typing speed, flight time, etc.) can be obtained, which reflect the unique behavioral characteristics of the user. There are many KD features with the most popular ones among researchers being digrams (digraphs): timestamps of two key states [17, 21–23]. The main KD features are as follows:

- hold (dwell) time;
- flight time;
- typing speed;
- number of typing errors;
- degree of arrhythm when typing;
- specific use of service keys.

Figure 3 shows some of the most commonly used time and frequency features.

- DU: dwell time (DT) is a time interval between a key press (down, press) and a key release (up, release).
- UD: flight time (F-RP) is a time interval between the release of the previous key and the press of the next key.
- UU, F-PP or DD, F-RR are intervals between pressing or releasing one key and pressing or releasing the next key, respectively.

Subsystems for preprocessing timestamp data and extracting KD features form a set of desired features for each keystroke. Using this set, a keystroke profile (template) of the user is generated and placed in the database.

As a result of KD feature extraction, we obtain a bank of profiles, which requires adaptation. Being a biometric behavioral characteristic, the keystroke profile is variable and needs to be updated. For this purpose, the sliding window technique can be employed [49]. The bank of profiles is used to train the classifier and at the stage of identity recognition.

III. User recognition.

To protect a computer system from unauthorized access, two-step verification is generally implemented:

- primary identification: the identification of the user;
- dynamic (continuous) authentication: the continuous confirmation of the identity of the legitimate user.

Authentication is a task of classifying users registered in the system.

The basic methods and algorithms for user classification (recognition) are the same for static and continuous (dynamic) authentication. They can be divided into three groups:

- statistical;
- based on closeness estimates;
- machine learning.

The use of these methods and the main representatives of each group are considered in detail in [20].

Historically, the works on keystroke dynamics recognition dealt with predefined and structured texts, i.e., with static authentication. According to different authors [22, 24], the number of studies devoted to continuous authentication is still small and does not exceed 10–15% of all works on keystroke recognition. The first fruitful investigation of continuous authentication is the work by Gunetti, published in 2005, where recognition accuracy exceeded 90% [25]. For comparison, the accuracy of the very first recognition methods on free texts (Monrose, 1997) was 23%.
The reviews on keystroke recognition published in the last decade made it possible to generalize the data on the effectiveness of continuous authentication (the main results are presented in Table 2). In addition to the references, the table includes the classification parameter, recognition method, and performance indicators. The data were borrowed from our own studies [20, 26] or adapted from the reviews [17, 22, 24, 27–33].

Finally, we should note the conditional nature of KD-based approaches to user recognition. These approaches generally include a model and training methods; however, their combinations can be different.

IV. Decision making on user’s legitimacy.

This step fully depends on a particular applied problem and recognition performance indicators.

In the case of dynamic identification, the main goal of continuous monitoring is to provide permanent access to network resources for a user registered in the domain, as well as to prevent access for an unregistered user.

Generally, the probabilities of the corresponding false events are estimated: a false denial of access for a registered user and a false provision of access for an unregistered user. By analogy with estimates in statistical radio engineering, the following errors are most commonly used in keystroke dynamics studies [17, 20, 21, 36, 38].

- False rejection rate (FRR), which is a type I error that estimates the false denial of access to a legitimate (registered) user:

\[
\text{FRR} = \frac{\text{FR}}{\text{TA} + \text{FA} + \text{TR} + \text{FR}}.
\]

- False acceptance rate (FAR), which is a type II error that estimates the false provision of access to an illegitimate user:

\[
\text{FAR} = \frac{\text{FA}}{\text{TA} + \text{FA} + \text{TR} + \text{FR}}.
\]

Here,

- true accept (TA) is the number of valid accepts of legitimate users;
- true reject (TR) is the number of valid rejects of illegitimate users;
- false acceptance (FA) is the number of cases where access was granted to an illegitimate user;
- false rejection (FR) is the number of cases where access was denied to a legitimate user.

Table 2. Dynamic identification methods

| Year | Work, author | Parameter | Method | Efficiency |
|------|--------------|-----------|--------|------------|
| 2005 | [25] Gunetti | FT        | Distance, R/A | FAR-0.005%, FRR-5% |
| 2010 | [32] Shimshon|            | Clustering   | FAR 3.47%, FRR 0% |
| 2011 | [33] Messerman|           | Statistical  | FAR-2.02%, FRR-1.84% |
| 2011 | [37] Solami |            | Clustering   | Accuracy 100% |
| 2013 | [27] Alsultan| digraph    | Fusion       | FAR-21%, FRR-17% |
| 2014 | [35] Ahmed   | digraph    | Neuronal network | FAR-0.015%, FRR-4.82% |
| 2014 | [39] Antal   | DT, FT     | Statistical  | Accuracy 93.04% |
| 2014 | [40] Locklear|            |             | EER 4.55–13.37% |
| 2015 | [41] Kang    | DT, FT     | Clustering, distance | EER 3.8% |
| 2015 | [42] Matsubara| digraph, DT| Distance    | Accuracy 99% |
| 2016 | [23] Morales | digraph, n-graph | kNN, distance | Accuracy 90% |
| 2017 | [31] Alsultan| digraph, DT| Support vector machine | FAR 0.169, FRR 0.423 |
| 2017 | [36] Goodkind| contextual features | Naive Bayes | Accuracy 82.2% |
| 2017 | [30] Ali     |            | kNN         | EER 3.7% |
| 2021 | [34] Chang   | DT, FT     | CNN-GRU     | Accuracy 99%, EER 0.0690 |
false accept (FA) is the number of invalid accepts of illegitimate users;

false reject (FR) is the number of invalid rejects of legitimate users.

The denominators of (1) and (2) contain the total number of attempts.

FRR and FAR depend on the adjustable threshold or sensitivity of the algorithm (see Fig. 4).

FRR, FAR, and ERR are sufficient for making a decision on the acceptance or rejection of the user. If the goal of the monitoring system is to provide a high level of security, then low thresholds should be used, which correspond to a large percentage of false rejects (FRR). Large FRR values provide higher security and more difficult access to the system for everyone, both insiders and outsiders. For a high threshold and low sensitivity of recognition algorithms, access becomes easier; however, FAR and the number of falsely accepted users increase. The tradeoff between FRR and FAR has to be determined individually in each case.

Another popular indicator that does not depend on the threshold is the equal error rate (EER). EER values correspond to equal values of FRR and FAR, which makes EER a universal performance indicator for any authentication system.

These three metrics (FRR, FAR, and EER) are most widely used for decision making in monitoring and authentication systems. Studies on keystroke dynamics also frequently employ the receiver operating characteristic (ROC), which is a ratio between TA and FA for different thresholds. ROC reflects the limiting capabilities of algorithms, which is especially important when investigating various classifiers.

4. HIDDEN MONITORING IN ONLINE EXAMINATION SYSTEMS

The COVID-19 pandemic has accelerated the introduction of the blended learning model, and many universities have implemented learning management systems. The main contribution to the final assessment of students' performance in these systems is made by online exams and tests. However, it is these forms of online learning that are most prone to academic fraud because the online environment allows students to work with little or no control. According to some researchers [43–45], the success of online exam systems is due to the use of biometric control and continuous monitoring during online exams. Keystroke dynamics makes it possible to organize the hidden monitoring of the identity of a legitimate student (who has passed primary identification) in a mode comfortable for him or her.

The main problems of keystroke dynamics—lifecycle, components, and efficiency—are discussed in Section 3. A specific use of these technologies is considered in Sections 4.1–4.4.

4.1. Authentication Lifecycle

The principles of continuous authentication outlined above are used to confirm the legitimacy of a student in the process of online testing.

The capabilities of continuous authentication in solving this problem are investigated by computational experiment. The experiment is conducted in accordance with the block diagram of the system shown in Fig. 5, which includes three main subsystems:

- registration;
- adaptation or template updating;
- user authentication.

In the case of distance learning, each subsystem operates in continuous mode. As shown in Fig. 5, the common steps of registration and authentication are data collection, data processing, and keystroke feature extraction.

4.1.1. Data collection in the experiment. The development of a continuous authentication system and its
performance testing are carried out using some keystroke dataset, statistical or locally collected one.

There are several public datasets based on fixed texts (Buffalo and BiosecurID) and free texts (Clarkson II and Villani-2010) [18, 23, 46, 47]. Some fixed datasets (CMU and WEBGREYC) [46] form templates by using login and password, which is not acceptable for dynamic authentication. In addition, these datasets do not include templates for Russian texts. When recognizing Russian users, English-language templates are of interest only for primary identification and static authentication based on password data.

In this work, local data collection is carried out using a special application developed for Windows. The application has client–server architecture. On the client side, keystroke data are collected locally in the background.

The target audience of this study is the university domain whose users have above-average computer skills. Using the keyboard input interception mechanism implemented in Windows, the so-called hook traps, all keyboard events are recorded. For each event, an array is formed that contains the following data:

- user login in the domain;
- key code;
- event (key pressed/released);
- timestamp.

The collected data are represented in the text format as follows (see Fig. 6).

The other functions of the application are implemented on the server. This reduces the risk of stealing the keystroke data from less secure client machines.

4.1.2. Data preprocessing. The raw data collected during the user session are preprocessed in the system to eliminate outliers, unreasonable hold times (30–200 ms), unpaired events, and short sessions.

The most important part of the preprocessing is the choice of the duration of the session. Mathematically, this corresponds to the choice of time windows into which the flow of keyboard events is partitioned. The sizes of the windows can differ at the stages of registration and authentication. There are various methods used for this purpose [18]:

- partitioning based on the duration of the user session or on the number of clicks;
- sliding windows.

This study uses a sliding window of 500 characters in continuous authentication mode. The size of the data sample must be large enough to ensure the representativeness of individual characters in the window, as well as guarantee that their estimates are statistically significant and unbiased. However, it is well known that the keystroke pattern tends to change due to the psycho-emotional component. That is why the time window should be sliding. The sliding window is also opposed by the possibility of reverse biometrics: the possibility of compromising long unprotected templates. By combining these two methods, we select the minimum sample size for the consistent estimate of the average values for Russian letters.

4.1.3. Extraction of KD features and generation of keystroke templates. The dimension of the resulting

![Fig. 5. Continuous authentication architecture (block diagram).](image-url)

![Fig. 6.](image-url)
The feature space in the continuous authentication problem is quite high. This is due to the size of the Russian alphabet and the large number of KD features.

The analysis of the researches devoted to keystroke features showed that the most popular ones are DU and UD (dwell time and flight time): according to [12, 20], the frequency of using each of them ranges from 30% to 40% in applied research.

In our study, the keystroke data from the last session of each user are sent to the server in the text format.

Then, the statistical characteristics DU and UD are computed for each letter during a user session. The result is an updated keystroke template, adapted after the last session and saved in a JSON file.

4.1.4. Vector parameter generation. The keystroke template stores the processed and reliable data on the keystroke dynamics of users in the last session in terms of the selected KD features (average dwell values for each key).

To improve the informativity and reliability of the generated templates, additional metrics and tools can be used to derive an aggregate KD indicator.

Dimensionality reduction based on extraction of stable features.

Reducing the dimension of the feature space is an important problem for keystroke dynamics, especially in the context of distance education and online testing, where the confirmation of the legitimacy of a student must be carried out as quickly as possible to detect impersonation.

On the one hand, the extraction of stable KD features contributes to the reduction of the feature space. On the other hand, it improves the selective properties of the templates.

When extracting stable features, we can improve the informativity of the KD features themselves [49]. The idea of these methods is to narrow timestamp ranges based on some rule, most often, by using statistical criteria. In this case, the narrowing technique can be applied to individual sessions, individual users, etc.

In addition, to improve the informativity of KD features, heuristic methods can be employed. In this study, this method is associated with the frequency of alphabetic letters in texts. According to the Russian National Corpus (https://ruscorpora.ru), the frequency of Russian letters (expressed in %) decreases from 10.985 (letter О) to 0.9965 (letter X) and 0.0375 (letter Ъ) (see Fig. 7a). Therefore, to obtain consistent estimates for all Russian letters, we need a very large sliding window, which is unacceptable in online authentication. A way to reduce the size of the window is to use a letter frequency threshold as a stable feature. For the threshold selected in this study (0.55), this means that the user template does not include the rarely used letters Й, Ћ, Є, І, Є, Ь, and Ё (see Fig. 7b).

The KD feature vector includes the features (the average DU values of the last session) of 27 Russian letters with the weight coefficients corresponding to the frequency of these letters in texts (see Fig. 7b).

4.1.5. Recognition of legitimate users. Static authentication and dynamic authentication are both aimed at confirming the legitimacy of the user who has already passed the initial registration. The difference is only in the type of the generated text. In the case of dynamic (continuous) authentication, the user creates free text in any OS application at any time; in the case of static authentication, the text and time of its generation are predetermined by the security system.

It should be noted that the confirmation of the user’s legitimacy based on his or her keystroke dynamics is a one-class classification problem. This problem is more complex than multiclass classification because the data of an illegitimate user are not available to the recognition system. The classifier is trained on objects of one class; in the process of testing, the algorithm determines whether a new object belongs to this class. The data of registered users are stored in the system in the form of dynamically updated templates. They can be considered objects of the same class (that of legitimate users).

In online learning systems, one-class classification can be carried out to recognize unregistered users, i.e., malefactors.

In online testing, one-class classification prevents impersonation of students.

Even though dynamic authentication is much more complex than static authentication, the recognition methods are similar. A brief review of the dynamic...
The classification of recognition methods is quite conventional; however, it is possible to distinguish machine learning methods, statistical methods, and methods based on metric distances [20].

In this work, the most popular recognition methods are chosen as classifiers in each of the three groups for the one-class classification problem:

- support vector machines (SVM) [17, 21, 34];
- k-nearest neighbors (kNN) algorithm [17, 21, 27, 34, 46];
- Euclidean and Manhattan metrics.

The basic idea of a one-class support vector machine (OCSVM) is to detect the boundaries of one class, rather than to separate objects of several classes as in the multiclass problem [48]. In addition, one-class classification is also known as an anomaly detection problem, which consists in finding patterns in data that do not conform to expected behavior [49], e.g., when the psycho-emotional state of the user changes under the influence of alcohol, etc.

The OCSVM maps feature vectors to a higher-dimensional space by using a kernel function. In the case of a radial basis function (RBF) kernel, there is a hyperplane that separates the majority of objects of a given class (in our case, legitimate users) from the origin. Exceptions are objects that lie closer to the origin than the hyperplane.

A one-class kNN (OckNN) algorithm estimates the distance between class objects. A new object is considered an exception if the majority of the objects (e.g., their \(p\)th part) of the entire class are at a distance exceeding \(D\) from the new object. The distance is computed using a selected metric in the feature space (\(p\) and \(D\) are the parameters of the method).

The OCSVM and OckNN algorithms are quite easy to implement. Their main requirement is the representativeness of the source dataset.

|                      | Euclidean | Manhattan | kNN | SVM |
|----------------------|-----------|-----------|-----|-----|
|                      | frequency | frequency |     |     |
| ERR, (0-100)\%       | 10.8      | 0.99      | 10.1| 0.79| 0.54| 3.72|
| threshold (FAR=FRR), ms | 4.8      | 2.3       | 4.8 | 2.2 | 15  |
| Accuracy, (0-100)\%  | 90.87     | 99.20     | 83.41| 99.4| 99.45|
| Precision, (0-1)     | 0.83      | 0.98      | 0.73| 0.98| 0.98|
| Recall, (0-1)        | 0.71      | 0.83      | 0.74| 0.94| 0.98|

5. RESULTS

The main processes of the continuous authentication lifecycle in online learning are data registration and student authentication (see Fig. 2). In the process of registration, the continuous collection of keystroke data with subsequent extraction of keystroke features is carried out (Fig. 5).

The templates (profiles) of domain users are dynamic; they are formed by continuous monitoring of keystroke dynamics and do not depend on any particular application. The keystroke data for each domain user are collected in the sliding window and the template is formed using Russian and English letters. The study was carried out in the domain of a national Russian university. The window size was 500 clicks, upon accumulation of which the data were transferred to the server component of the program for preprocessing and KD feature extraction. As the number of clicks grew, the window was shifted and the next set of data was transmitted to the server, thus enabling continuous data registration in the current user session.

The server component of the program computes the average dwell times in the current session for each character and updates the template stored in the bank. For each user, the bank stores templates for the last 10 sessions, which makes it possible to track changes in keystroke dynamics, which are due to fatigue, psycho-emotional state, etc.

The identification capabilities of templates generated for different users can be estimated visually and statistically. Figure 8 shows templates of six random users of the university domain for Russian letters. The Y-axis represents the dwell time (in ms). The individual lines depict the typing rhythm and determine the keystroke pattern of each user.

Typing rhythms and speeds differ for different users, which results in different keystroke dynamics. This difference of KD features is also confirmed statistically, e.g., by the type and parameters of the distribution density (see Fig. 9).
For instance, the distribution for User3 is characterized by a small dispersion and average typing speed (expectation), which is in complete agreement with Fig. 8 and is confirmed by small deviations between the mode and median of the series (large and small dashed lines).

Figures 8 and 9 show that the average values for User4 and User1 are approximately equal. However, the distribution for User1 is heavy-tailed. The mode and median for this series differ significantly from one another, as in the case of User06. For a representative sample and high typing speed, this can be a discriminative feature of an altered psycho-emotional state.

User5 also has a high typing speed. In this case, the distribution density is bimodal, which corresponds to good typing skills. For this user, there are typing overlaps when the next key is pressed while the previous one is not released.

The next stage of recognition is the confirmation of the legitimacy of the student. For this purpose, the template of the registered user from the bank is compared with the current template (see Fig. 5). When confirming the legitimacy of the user, there are two possible outcomes:

– the template of the last session matches the template from the bank for the registered user;
– the templates do not match.

The pattern matching is analyzed using SVM, kNN, Euclidean metric, and Manhattan metric. The choice of these methods is substantiated in Section 4.1.5.

The most important characteristic for any method is the decision threshold. The threshold is selected (assigned) by the security system based on priorities of tasks. Small thresholds correspond to small differences between the basic and current templates and complicate access to the corporate network for everyone, including legitimate users. Large thresholds (low sensitivity) correspond to easy access for everyone.
Type I and II errors for the Manhattan metric are shown in Fig. 10 depending on threshold values.

In Fig. 10b, FAR, FRR, and EER are plotted taking into account the letter frequency; in Fig. 10a, without taking it into account.

It can be seen that there is a significant decrease in the errors, by an order of magnitude on average at different threshold values. For instance, on the data from Table 3, these values are 10.85 and 0.995 for the Euclidean metric. In Table 3, for all selected methods, the EER values are given for a threshold at which FAR = FRR.

The authentication features based on the Manhattan and Euclidean metrics are almost identical with respect to the frequency of alphabetic letters. However, they have certain differences when the frequency is not taken into account. The kNN method has a slightly better performance, ERR = 0.545, at a slightly higher threshold 15 ms. However, this requires a time-consuming selection of algorithm parameters and does not guarantee that parameter adjustment would not be necessary under real-world conditions. The lack of optimal parameter values explains the low authentication results of the SVM method.

A confusion matrix is also a useful tool for analyzing the events that occur when recognizing legitimate and illegitimate users (see Table 4). The intersections of its rows and columns contain true (T) or false (F) outcomes of recognition: accept (A) or reject (R). The columns correspond to the recognition results, while the rows correspond to the real users.

The performance indicators shown in Table 3 are computed as follows:

\[
\text{Accuracy} = \frac{TA + TR}{TA + FA + TR + FR}.
\]  

(3)

\[
\text{Precision} = \frac{TA}{TA + FA}.
\]  

(4)

\[
\text{Recall} = \frac{TA}{TA + FR}.
\]  

(5)

These three indicators reflect the quality of authentication of legitimate users from different angles.

\textit{Accuracy} estimates the correct accepts and rejects for all possible legitimate and illegitimate users.

\textit{Precision} is the ratio of correctly accepted users to all users accepted by the system.

\textit{Recall} reflects the number of correctly accepted users out of all legitimate ones. \textit{Recall} is also referred to as sensitivity of a recognition model.

\textit{Accuracy} is usually expressed as a percentage, while \textit{Precision} and \textit{Recall} vary from 0 to 1.

The last tools for authentication quality assessment are the DET and ROC curves shown in Fig. 11.

These curves confirm the similar performance of the kNN method and the methods that are based on the similarity of templates and take the letter frequency into account.

CONCLUSIONS

In this paper, we have considered the approach to confirming the legitimacy of students in the process of distance learning by hidden monitoring of KD features.

It has been found that the hidden identification of students is possible on the basis of continuous moni-

| Table 4. Confusion matrix |
|---------------------------|
| Actual user               | Recognized user |
|                           | legitimate | illegitimate |
| 1.                             | TA        | FR          |
| 2.                             | FA        | TR          |
Monitoring of keystroke data for any software application. As a result, the following conclusions can be made.

1. Correction (adaptation) of KD samples by using a sliding window is required, which allows one to dynamically track changes in the user’s keystroke pattern and psycho-emotional state.

2. Selection of stable keystroke features contributes to the dimensionality reduction of the KD feature space, which improves selective properties of the templates.

3. In this study, as a stable feature, we have used the frequency of alphabetic letters in texts according to the Russian National Corpus (https://ruscorpora.ru). The exclusion of six letters with frequencies below 0.5% from the templates has led to a significant change in all performance indicators. For instance, ERR has decreased by an order of magnitude, on average from 105 to 15, while Accuracy, Precision, and Recall have increased by 6–135 on average, reaching 98% for both the Euclidean and Manhattan metrics.

4. The kNN method has showed slightly better results for optimal parameters: ERR = 0.545 (versus 0.795), Accuracy = 99%, and Precision = 0.98.

5. Combining simple distance estimation algorithms with letter frequency leads to the absence of complex parameter optimization procedures, as in machine learning methods (kNN), while providing similar performance.

With the recognition performance being a key factor in continuous authentication, parameter adaptation significantly reduces the overall efficiency of user validation.

REFERENCES

1. Klyuchevskaya, N., Information security and COVID-19: Recommendations for businesses and citizens. https://www.garant.ru/article/1421147.
2. Analytics of the information security industry. https://www.infowatch.ru/analytics/analitik.
3. Hackers attack universities and colleges: Leak digest. https://www.infowatch.ru/analytics/daydzhesty-i-obozory/khakery-atakuyut-universitety-i-kollzedzhi-daydzhest-utechek.
4. Education: From the closure of educational institutions to the resumption of their work. https://ru.unesco.org/covid19/educationresponse.
5. Education: From destruction to recovery. https://ru.unesco.org/covid19/educationresponse.
6. Fenu, G., Marras, M., and Boratto, L., A multi-biometric system for continuous student authentication in e-learning platforms, Pattern Recognit. Lett., 2018, vol. 113, pp. 83–92. https://doi.org/10.1016/j.patrec.2017.03.027
7. Ngqondi, T., Maoneke, P.B., and Mauwa, L., A secure online exams conceptual framework for South African universities, Soc. Sci. Humanit. Open, 2021, vol. 3, no. 1, p. 100132. https://doi.org/10.1016/j.ssaho.2021.100132
8. Lee, C., How to maintain academic integrity in distance learning. https://www.turnitin.com/ru/blog/kak-podderzhit-akademicheskuyu-chestnost-pri-distantionnom-obuchenii.
9. Al-Naji, F.H. and Zagrouba, R., A survey on continuous authentication methods in Internet of Things environment, Comput. Commun., 2020, vol. 163, pp. 109–133. https://doi.org/10.1016/j.comcom.2020.09.006
10. Dasgupta, D., Roy, A., and Nag, A., Advances in User Authentication, Springer, 2017. https://doi.org/10.1007/978-3-319-58808-7
11. Stylios, I., Kokolakis, S., Thanou, O., and Chatzis, S., Behavioral devices: A survey, Inf. Fusion, 2021, vol. 66, pp. 76–99. https://doi.org/10.1016/j.infus.2020.08.021
12. Toosi, R. and Akhacee, M.A., Time-frequency analysis of keystroke dynamics for user authentication, Future Gener. Comput. Syst., 2021, vol. 115, pp. 438–447. https://doi.org/10.1016/j.future.2020.09.027
13. IBM Security, Future of identity study. https://www.ibm.com/downloads/cas/QRBAY08NO.
14. Hazan, I., Margalit, O., and Rokach, L., Supporting unknown number of users in keystroke dynamics mod-
15. Parkinson, S., Khan, S., Crampton, A., Xu, Q., Xie, W., Liu, N., and Dakin, K., Password policy characteristics and keystroke biometric authentication, *IET Biometrics*, 2021, vol. 10, no. 2, pp. 163–178. https://doi.org/10.1049/bme.2.12017

16. Kochegurova, E.A., Gorokhova, E.S., and Mozgaleva, A.I., Development of the keystroke dynamics recognition system, *J. Phys. Conf. Ser.*, 2017, vol. 803, p. 012073. https://doi.org/10.1088/1742-6596/803/1/012073

17. Kim, J., Kim, H., and Kang, P., Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection, *Appl. Soft Comput.*, 2018, vol. 62, pp. 1077–1087. https://doi.org/10.1016/j.asoc.2017.09.043

18. Lu, X., Zhang, S., Hui, P., and Lio, P., Continuous authentication by free-text keystroke based on CNN and RNN, *Comput. Secur.*, 2020, vol. 96, p. 01861. https://doi.org/10.1016/j.cose.2020.101861

19. Dargan, S. and Kumar, M., A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities, *Expert Syst. Appl.*, 2020, vol. 143, p. 113141. https://doi.org/10.1016/j.eswa.2019.113141

20. Kochegurova, E.A. and Martynova, Y.A., Aspects of continuous user identification based on free texts and hidden monitoring, *Program. Comput. Software*, 2020, vol. 46, no. 1, pp. 12–24. https://doi.org/10.1134/S036716882001003X

21. Zaidi, A.Z., Chong, C.Y., Jin, Z., Parthiban, R., and Sadiq, A.S., Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities, *J. Network Comput. Appl.*, 2021, vol. 191, p. 103162. https://doi.org/10.1016/j.jnca.2021.103162

22. Teh, P.S., Teoh, A.B.J., and Yue, S., A survey of keystroke dynamics biometrics, *Sci. World J.*, 2013, vol. 2013, pp. 1–24. https://doi.org/10.1155/2013/408280

23. Morales, A., Fierrez, J., Tolosana, R., Ortega-Garcia, J., Galbally, J., Gomez-Barrero, M., Anjos, A., and Marcel, S., KBOC: Keystroke biometrics ongoing competition, *Proc. IEEE 8th Int. Conf. Biometrics Theory, Applications and Systems (BTAS)*, 2016. https://doi.org/10.1109/BTAS.2016.7791180

24. Pisani, P.H. and Lorena, A.C., A systematic review on keystroke dynamics, *J. Braz. Comput. Soc.*, 2013, vol. 19, no. 4, pp. 573–587.

25. Gunetti, D. and Picardi, C., Keystroke analysis of free text, *ACM Trans. Inf. Syst. Secur.*, 2005, vol. 8, no. 3, pp. 312–347. https://doi.org/10.1145/1085126.1085129

26. Kochegurova, E., Luneva, E., and Gorokhova, E., On continuous user authentication via hidden free-text based monitoring, *Adv. Intell. Syst. Comput.*, 2019, vol. 875, pp. 66–75. https://doi.org/10.1007/978-3-030-01821-4_8

27. Alsultan, A. and Warwick, K., Keystroke dynamics authentication: A survey of free-text methods, *Int. J. Comput. Sci.*, 2013, vol. 10, no. 4, pp. 1–10.

28. Mondal, S. and Bours, P., A study on continuous authentication using a combination of keystroke and mouse biometrics, *Neurocomput.*, 2017, vol. 230, pp. 1–22. https://doi.org/10.1016/j.neucom.2016.11.031

29. Zhong, Y. and Deng, Y., A survey on keystroke dynamics biometrics: Approaches, advances, and evaluations, *Recent Adv. User Authentication Using Keystroke Dyn. Biom.*, 2015, vol. 2, pp. 1–22. https://doi.org/10.15579/gcsr.vol2.ch1

30. Ali, M.L., Monaco, J.V., Tappert, C.C., et al., Keystroke biometric systems for user authentication, *J. Sign. Process. Syst.*, 2017, vol. 86, pp. 175–190. https://doi.org/10.1007/s11265-016-1114-9

31. Alsultan, A., Warwick, K., and Wei, H., Non-conventional keystroke dynamics for user authentication, *Pattern Recognit. Lett.*, 2017, vol. 89, no. 5, pp. 53–59. https://doi.org/10.1016/j.patrec.2017.07.020

32. Shimshon, T., Moskovich, R., Rokach, L., and Eloviçi, Y., Continuous verification using keystroke dynamics, *Proc. Int. Conf. Computational Intelligence and Security (CIS)*, 2010, pp. 411–415. https://doi.org/10.1109/CIS.2010.95

33. Messerman, T., Mustafic, T., Camtepe, S.A., and Albayrak, S., Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics, *Proc. Int. Jt. Conf. Biometrics (JCB)*, 2011, pp. 1–8. https://doi.org/10.1007/IJCB.2011.6117552

34. Chang, H.C., Li, J., Wu, C., and Stamp, M., Machine learning and deep learning for fixed-text keystroke dynamics, 2021. https://doi.org/10.48550/arXiv.2107.07409

35. Ahmed, A.A. and Traore, I., Biometric recognition based on free-text keystroke dynamics, *Cybern. IEEE Trans.*, 2014, vol. 44, no. 4, pp. 458–472. https://doi.org/10.1109/TCYB.2013.2257745

36. Goodkind, A., Brizan, D.G., and Rosenberg, A., Utilizing overt and latent linguistic structure to improve keystroke-based authentication, *Image Vision Comput.*, 2017, vol. 58, pp. 230–238. https://doi.org/10.1016/j.imavis.2016.06.003

37. Al Solami, E., Boyd, C., Clark, A., and Ahmed, I., User-representative feature selection for keystroke dynamics, *Proc. 5th Int. Conf. Network and System Security (NSS)*, 2011, pp. 229–233. https://doi.org/10.1109/IC-NSS.2011.6060005

38. Eberz, S., Rasmussen, K.B., Lenders, V., and Martinovic, I., Evaluating behavioral biometrics for continuous authentication: Challenges and metrics, *Proc. ACM Asia Conf. Computer and Communications Security (ASIA CCS)*, 2017, pp. 386–399. https://doi.org/10.1145/3052973.3053032

39. Antal, M., Szabo, L.Z., and Laszlo, I., Keystroke dynamics on Android platform, *Procedia Techn.*, 2015, vol. 19, pp. 820–826. https://doi.org/10.1016/j.protcy.2015.02.118

40. Locklear, H., Govindarajan, S., and Sitowa, Z., Continuous authentication with cognition-centric text production and revision features, *Proc. IEEE/IAPR Int. Jt. Conf. Biometrics (IJCB)*, 2014. https://doi.org/10.1109/BTAS.2014.6996227
41. Kang, P. and Cho, S., Keystroke dynamics-based user authentication using long and free text strings from various input devices, *Inf. Sci.*, 2015, vol. 308, pp. 72–93. https://doi.org/10.1016/j.ins.2014.08.070

42. Matsubara, Y., Samura, T., and Nishimura, H., Keyboard dependency of personal identification performance by keystroke dynamics in free text typing, *J. Inf. Secur.*, 2015, vol. 6, pp. 229–240. https://doi.org/10.4236/jis.2015.63023

43. Wang, X., Yan, Z., Zhang, R., and Zhang, P., Attacks and defenses in user authentication systems: A survey, *J. Network Comput. Appl.*, 2021, vol. 188, p. 103080. https://doi.org/10.1016/j.jnca.2021.103080

44. Muzaffar, A.W., Tahir, M., Anwar, M.W., Chaudry, Q., Mir, S.R., and Rasheed, Y., A systematic review of online exams solutions in e-learning: Techniques, tools, and global adoption, *IEEE Access*, 2021, vol. 9, pp. 32689–32712. https://doi.org/10.1109/ACCESS.2021.3060192

45. Jagadamba, G., Sheeba, R., Brinda, K.N., Rohini, K.C., and Pratik, S.K., Adaptive e-learning authentication and monitoring, *Proc. 2nd Int. Conf. Innovative Mechanisms for Industry Applications (ICIMIA)*, 2020, pp. 277–283. https://doi.org/10.1109/ACIMIA48430.2020.9074955

46. Iapa, A. and Cretu, V., Shared data set for free-text keystroke dynamics authentication algorithms, 2021. https://doi.org/10.20944/preprints202105.0255.v1

47. González, N., Calot, E.P., Ierache, J.S., and Hasprué, W., On the shape of timings distributions in free-text keystroke dynamics profiles, *Heliyon*, 2021, vol. 7, no. 11, p. e08413. https://doi.org/10.1016/j.heliyon.2021.e08413

48. Mhenni, A., Cherrier, E., Rosenberger, C., and Essoukri Ben Amara, N., Analysis of Doddington zoo classification for user dependent template update: Application to keystroke dynamics recognition, *Future Gener. Comput. Syst.*, 2019, vol. 97, pp. 210–218. https://doi.org/10.1016/j.future.2019.02.039

49. Kazachuk, M.A., Dynamic user authentication based on keystroke dynamics analysis, *Cand. Sci. (Phys.–Math.) Dissertation*, Moscow, 2019.

50. Alpar, O., Biometric keystroke barcoding: A next-gen authentication framework, *Expert Syst. Appl.*, 2021, vol. 177, p. 114980. https://doi.org/10.1016/j.eswa.2021.114980

51. Yang, Y., Guo, B., Wang, Z., Li, M., Yu, Z., and Zhou, X., BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics, *Ad Hoc Networks*, 2019, vol. 84, pp. 9–18. https://doi.org/10.1016/j.adhoc.2018.09.015

*Translated by Yu. Kornienko*