E-Learning: the Problem of Reliable Student Authentication and Information Security*

Rena R. Timirgaleeva[1][0000-0002-3078-1050], Igor Yu. Grishin[1][0000-0001-5839-1858] and Maxim V. Mironov[2]

[1] V.I. Vernadsky Crimean Federal University, Yalta, Russia
[2] Kuban State Technological University, Krasnodar, Russia
igugri@gmail.com

Abstract. Both electronic and remote learning is becoming common learning technologies for modern universities. Based on advances in the information technology field, educational institutions widely use e-learning systems; new educational standards also require their use in the educational process. However, the issues of information security of such systems are not well developed. Opponents of e-learning argue that the impossibility of an e-learning environment to reliably identify a student is the main problem with the use of such systems. The work is devoted to the most important problem of remote and e-learning - student authentication in the system. Different approaches to authentication are considered, their comparative analysis is carried out, the advantages and disadvantages of various authentication methods are revealed, it is established that biometric authentication methods are the most effective for solving educational tasks. The author's approaches are proposed based on dynamic authentication using the trainee's handwriting and static authentication using a manipulator mouse with a built-in ultrasound scanner. The proposed student authentication model solves the problem of strong authentication and provides the possibility of effective electronic assessment and electronic exams. The results obtained are confirmed by the results of simulation modeling and real experiments with students.

Keywords: Remote learning (distance), e-learning, teacher, learner, information technology, authentication methods, dynamic authentication, static authentication, information security, biometric features.

1 Introduction

In the last decade, the use of Internet technologies has expanded significantly in modern applications such as Big Data, newsgroups, and especially in e-learning and distance learning systems. E-learning systems are becoming increasingly attractive for the active acquisition of the required competencies both by people who upgrade their skills and by students of higher educational institutions who take online courses with interest and great benefit.

In recent years, more and more educational institutions in Russia are introducing various e-learning platforms; at the initiative of the federal executive bodies, an all-Russian e-learning platform has been created, the content of which is maintained and replenished by leading higher educational institutions in the country. It should be noted that it is supposed to fix at the legislative level the possibility of setting off disciplines taught in this educational environment in all educational institutions of the country. Thus, educational institutions support the implementation and use of e-learning platforms in various courses of study, e-assessment and passing an electronic exam. Evaluation of students' educational achievements, especially e-evaluation, is the most serious problem when using an e-learning environment [1].

Electronic assessments are based on the use of the Internet-based infrastructure of e-learning and distance learning, which often becomes the site of unlawful actions by intruders. As a result, the e-learning platform itself is subject to various types of threats. It should be noted that some e-learning platforms are applied without taking into account the ever-increasing requirements for ensuring information security. Fulfillment of these requirements should ensure confidentiality, integrity, accuracy, and availability of information in e-learning systems. Issues of ensuring the security of these systems were discussed by stakeholders of the educational process [2], but its provision encounters opposition from intruders who exploit weaknesses in e-learning systems using interception, modification, and interruption [3].

Based on the above reasons, users of e-learning and distance learning systems argue that the existing platforms do not have reliable authentication mechanisms that could be used for reliable e-grading and an electronic exam. Thus, one of the key problems in the deployment of electronic and distance learning platforms remains the problem of user authentication to identify and terminate the actions of unauthorized persons compromising information security policies [4, 5], as well as identifying the learner during knowledge testing. Therefore, many remote programs involve only a full-time exam session. In part, this problem is solved by installing cameras on the side of the subject; however, given the modern development of communication tools, even such a measure cannot guarantee the “honesty” of the examination [4].

In this work, the term “identification” is understood to mean both the process of identification itself (user’s representations, the student being trained when trying to access system resources, guaranteeing the person who has access to which resources) and the authentication process (authentication). It should also be emphasized that many teachers are concerned about the errors in authentication and the security of exams using the electronic environment, as well as the unethical behavior of students in e-learning [6, 7].

In the works of domestic and foreign researchers, the problem of trainee identification was repeatedly discussed, for example, in [8] a combined e-learning organization model with the ability to monitor attendance was proposed. This model uses two behavioral biometric characteristics (mouse movements and dynamics of keystrokes) and physical (facial features). However, this model can be used to track the continuous attendance of user’s only at the most sensitive stages of the e-learning process since it requires the use of rather expensive additional equipment and significant computing power used by computers.

The authors from Canada [9] analyzed publications, reports, and websites in order to identify the characteristics of personal profiles in order to prepare the development of a personalized learning environment. It has been shown that confidentiality problems may arise when working with personal profiles and measures should be taken to ensure compliance with the policies and legislation of the country in which the training takes place.

A report by researchers from Australia [10] concluded that using a strong authentication mechanism would help remove restrictions on the use of e-learning systems. Biometrics is one such authentication method that provides a unique and universal identification for any system. Several different biometric frameworks have been developed for e-learning systems, but there are still gaps that need to be taken into account in actual learning systems.

It is known that a number of works were devoted to the introduction of authentication mechanisms to ensure the security of the e-learning platform in the process of assessing students' knowledge. In [11, 12], the authors noted that a more active use of new learning technologies leads to an increase in unethical behavior of students, which is expressed in fraud during the electronic exam through the use of electronic devices (smartphones, tablets), collaboration through the use of chat rooms and forums, registration with another student's username and password. It is noted that the development of new technologies leads to the fact that students began to use such fraudulent methods, that obtaining reliable results in assessing student knowledge becomes unattainable [13].

Not enough attention is paid to the development of student identification and authentication solutions, which contributes to deception during the electronic exams. The same procedures are necessary to confirm the student’s access to a particular training course [14]. In [15], the authors focused on protecting the technological structure of the e-learning system from unauthorized persons. It is noted that modern security methods in electronic and distance learning systems are based primarily on the use of password authentication mechanisms.

The approaches discussed above make a significant contribution to the problem under consideration, but they do not address the issues of continuous monitoring of a specific student during the electronic exam or require a large amount of additional expensive equipment for reliable user authentication, which does not allow using the approaches proposed by the authors on a large scale.

We also note that as a result of the analysis of publications on the issue under consideration, a group of countries conducting the most intensive research in this area can be distinguished (Fig. 1). India, Spain, Italy, and China were in the lead, in which distance learning and e-learning are rapidly developing.

In this paper, we explore a new approach to student authentication, based on a number of biometric features that are the most reliable and do not require the use of a large number of additional expensive equipment [16, 17].

2 Analysis of modern approaches to student biometric identification

Biometric methods, according to [18-20], include various methods that can be divided into two subgroups:

1. Static methods [21, 22] are based on the physiological (static) characteristics of a person, that is, a unique property given to him from birth and inherent in him. Static forms include palms, fingerprints, iris, retina, face shape, vein position on the hand, etc.;
2. Dynamic methods [23] are based on the behavioral (dynamic) characteristics of a person, the features characteristic of subconscious movements in the process of reproducing an action (signature, speech, acoustic properties of the heart, keyboard-typing dynamics).

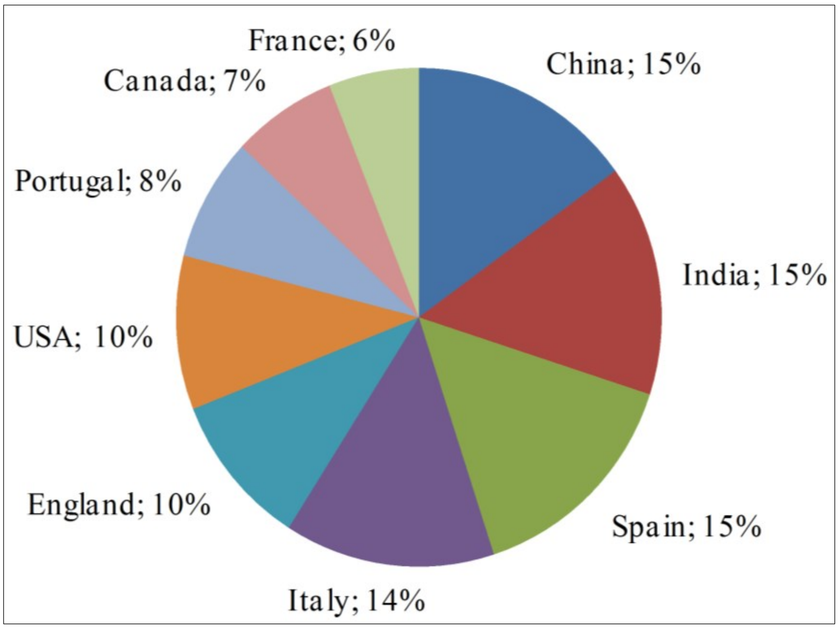

Fig. 1. Rating of countries conducting research in the field of security systems, distance, and e-learning

The advantages and disadvantages of biometric authentication methods are presented in Table 1.

Thus, after analyzing the positive and negative sides of various authentication methods, it can be concluded that the quality of the authentication procedure using various methods will directly depend on the following indicators: collection rate, uniqueness, stability, universality. The rational authentication characteristic of the student should be consistent with the above indicators.

Table 1. Biometric methods Characteristics

Authentication type	Description	Advantage	Limitations
Biometric authentication.	Based on the uniqueness of a number of human characteristics.	1. Ease of use; 2. The difficulty of deceiving the system, since each user has individual indicators (there is a link to the subject); 3. The ability to use not only as a process when entering from the OS, but also to monitor user actions at the computer network.	1. For a timely response, the need to integrate other means of authentication; 2. Low stability.

The general scheme of the functioning of biometric authentication methods in the distance learning system is shown in Fig. 2.

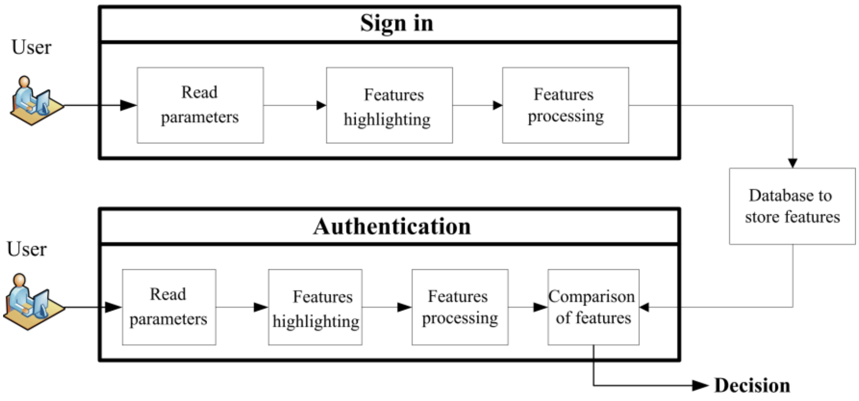

Fig. 2. Generalized scheme of functioning of biometric authentication methods

The presented scheme illustrates the existence of two phases of the functioning of a biometric system: registration and authentication (recognition, authentication).

In the registration phase, the following actions are performed sequentially:

- reading the user name (login) and his personal data;
- reading biometric parameter of the user;
- processing of a biometric parameter and the selection of stable features for this parameter;
- processing of signs - the creation of a biometric standard based on the selected signs for the user;
- saving the received standard in the system database for the registered user.

At the registration stage, rights for access to information resources may be additionally determined for the user.

In the authentication phase, the following actions are performed:

- the authenticated user declares that he is identical to some user from the database, presenting his login to the system, as well as, possibly, additional personal data and a biometric parameter;
- the system reads the biometric parameter;
- the biometric parameter is processed and its stable features are highlighted;
- a comparison of the received features with the features downloaded from the database is made, and a decision is made about the identity of the user.

It should be noted that when adding new users, the system should be transferred to the registration phase.

The analysis of existing methods of biometric authentication showed that the most appropriate for distance and e-learning systems are [1, 5, 11, and 12]:

- static user fingerprint recognition method;
- dynamic recognition method by handwriting.

A generalized description of these user authentication methods (student, student) is given in table 2.

Table 2. Characterization of authentication methods

Types of biometric authentication	Description	Advantages	Disadvantages
Fingerprint recognition	A fingerprint image obtained using a special scanner is converted into a digital code (convolution) and compared with a previously entered pattern (reference) or a set of templates (in the case of authentication).	High uniqueness rates	1. The complexity of the implementation. 2. The need for additional special equipment.
Keyboard handwriting recognition	The method is similar to that described above, but the signature in it is replaced by a certain code word.	1. No additional hardware required (only a keyboard is needed). 2. High stability. 3. High coefficient of equal probability of errors of the first and second kind.	It takes some time to collect statistics and form a reference sample.

3 Content of the proposed student identification methods

Based on the analysis of existing world achievements in the field of effective identification of users of e-learning systems, as well as based on their own experience of operating and supporting the distance learning system of the Computer Technologies and Information Security Department of the Kuban State Technological University, the authors concluded that the use of an identification model is optimal based on keyboard writing, which has a high degree of uniqueness for each person, which was shown by the experiments conducted by the authors with a group of students in 125 people.

In the case of particularly responsible events (tests, exams), it is advisable to use two-factor identification, which in our case allows us to control both the initial phase of the process and the course of the control measure itself, which does not allow for the replacement of the examinee during the control measure.

The trainee's authentication model developed by the authors based on the keyboard handwriting is shown in Fig. 3.

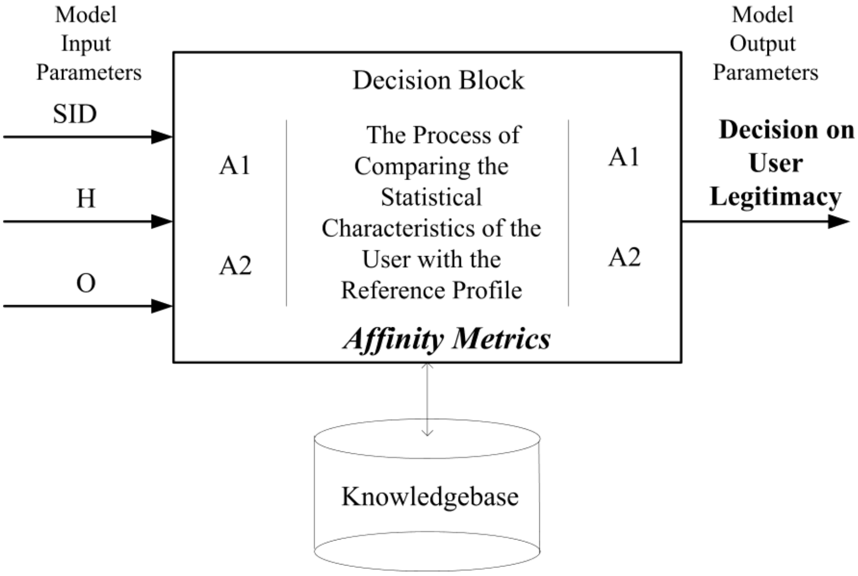
Model Input Parameters
SID
H
O
Decision Block
A1
A2
The Process of Comparing the Statistical Characteristics of the User with the Reference Profile
A1
A2
Affinity Metrics
Model Output Parameters
Decision on User Legitimacy
Knowledgebase

Fig. 3. Trainee authentication model based on keyboard handwriting

The biometric user profile is calculated using the mathematical apparatus for determining the affinity of monitored parameters. When processing data obtained from a training set, it is very important to exclude from it uncharacteristic values of parameters or anomalous emissions. These emissions can be the time before and after pressing the spacebar, punctuation marks, numbers, and control keys.

To reduce the uncertainty of the source data and analysis results it is proposed to use the mathematical apparatus of fuzzy sets.

To identify the user's image, the Euclidean distance and quadratic fuzziness index between the vectors of the membership functions of the sets of input and stored characteristics were chosen as metrics for determining the affinity between the quantitative characteristics of the statistical characteristics of the user and the reference profile [6].

It is proposed to use a performance indicator based on the calculation of the first and second kind errors for assessing the quality of the user authentication model based on keyboard handwriting, which will be defined for authentication tasks as follows: taking a legitimate user as unregistered - first kind errors; the adoption of an unregistered user in the system for a legal one - errors of the second kind.

For biometric authentication systems, the errors of the first and second kind determine the quality of the functioning of the system. The chosen authentication algorithm, the decision-making method, the amount of the training sample, directly influences the number of errors of the first and second kind and the number of statistical characteristics of the subject in the knowledge base, as well as the error and metric used to determine the affinity of the signs.

The effectiveness of the developed user authentication model based on keyboard handwriting refers to the ratio of error indicators of the first and second kind when using biometric authentication based on keyboard handwriting and using other types of biometric authentication.

The solution, based on the student's fingerprint, is implemented in the form of a mouse manipulator with an ultrasound scanner. The difference from the well-known similar approaches to authentication is that the trainee's fingerprint scan and crypto storage are embedded in the case of a computer mouse device, which has improved the security settings and authentication reliability.

4 Conclusion

The purpose of writing this article is to promote ideas and implement the methodology of distance and e-learning in the realities of the national education system. In recent years, significant steps have been made in this area. In the Law of the Russian Federation “On Education”, reference was made to the technology of distance and e-learning, the Ministry of Education and Science of the Russian Federation issued an order legalizing the specified educational technologies. Active work is underway in Russia and other leading countries of the global educational market, aimed at improving these learning technologies, in particular, aimed at improving the reliability of trainee identification methods, which will significantly change the current understanding of the effectiveness of various student-learning technologies in the coming years.

In this article, we turned to the problem of identifying students, because existing models do not provide a sufficient level of reliability in electronic assessment and in the electronic exam. To achieve this goal, a new security scheme has been proposed, which is based on biometric features (the main one is the user's keyboard type, an additional one is a fingerprint), which does not require additional expensive equipment. No additional hardware is required for keyboard handwriting authentication, only software developed by the authors; for the second fingerprint authentication stage, a mouse with a sensor and crypto storage is needed, which do not significantly increase the cost of a mouse.

In this work:

1. A student's authentication model has been developed and formalized based on behavioral biometrics - keyboard handwriting. The metrics for determining the affinity of the statistical characteristics of the user's keyboard handwriting to study the effectiveness of the model are selected. The architecture of the software model prototype has been developed;
2. It is proposed to use a mouse “mouse” with an ultrasound scanner for authentication of the student, which differs from those known in that the fingerprints of the students and the crypto storage are embedded in the body of the computer mouse device.
3. The results of modeling and real experiments have shown that the proposed approach can significantly improve the authentication process and ensure high reliability of the electronic knowledge assessment of students.
4. The results of this study can provide such an authentication model that can be used for reliable authentication of students in an electronic environment that will positively affect the quality of the educational process and the possibility of widespread use of electronic and distance learning systems.

Acknowledgment

This work was supported by the Grant of the Russian Foundation for Basic Research and the Administration of the Krasnodar Region No. 18-410-230024.

References

1. Hillier, M., Fluck, A.: Arguing again for e-exams in high stakes examinations, 30th ascilite Conference 2013 Proceedings, Macquarie University, Sydney, - PP 385-389. (2013)
2. Gathuri, J. W., Luvanda, A., Matende, S., Kumundi, S.: Impersonation Challenges Associated with E-Assessment of University Students, Journal of Information Engineering and Applications, 4 (7). (2014)
3. Neila, R., Rabai, L.: Deploying Suitable Countermeasures to Solve the Security Problems within an E-learning Environment, Proceedings of the 7th International Conference on Security of Information and Networks, NY; USA, Association for Computing Machinery. (2013) DOI: 10.1145/2659651.2659721
4. Timirgaleeva, R.R., Grishin, I.Yu.: Issues and prospects for the development of distance learning in the education system of the Republic of Crimea, III International Scientific and Practical Conference "Problems of Theory and Practice of Distance and Electronic Education (PDEO-2014)". Collection of scientific papers (on the reports of the plenary session). - 2014. - P. 7-10. (2014)
5. Levy, Y. & Ramim, M.: A Theoretical Approach for Biometrics Authentication of e-Exams, Nova Southeastern University. (2007)
6. Kennedy, K., Nowak, S., Raghuraman, R., Thomas, J., & Dacis, S.: Academic dishonesty and distance learning: student and faculty views, College Student Journal, 34(2), - PP 309-315. (2000)

7. Pillsbury, C.: Reflections on academic misconduct: An investigating officer’s experiences and ethics supplements, Journal of American Academy of Business, 5(1/2), - PP 446-454. (2004)
8. Dehnavi, M.K., Fard, N.P.: Presenting a multimodal biometric model for tracking the students in virtual classes, Procedia - Social and Behavioral Sciences Volume 15, – PP. 3456-3462. (2011) DOI: https://doi.org/10.1007/978-3-319-07593-8_22
9. Lapointe, J.-F., Kondratova, I., Molyneaux, H., Shaikh, K.: Vinson N.G. A review of personal profile features in personalized learning systems, Advances in Intelligent Systems and Computing, 596, – PP. 46-55. (2018) DOI: https://doi.org/10.1007/978-3-319-60018-5_5
10. Kaur, N., Prasad, P.W.C., Alsadoon, A., Pham, L., Elchouemi, A.: An enhanced model of biometric authentication in E-Learning: Using a combination of biometric features to access E-Learning environments, 2016 International Conference on Advances in Electrical, Electronic and Systems Engineering, ICAEES – 2016, – PP. 138-143. (2017) DOI: 10.1109/ICAEES.2016.7888025
11. McLafferty, C. L., Foust, K. M.: Electronic plagiarism as a college instructor’s nightmare prevention and detection: Cyber dimensions, Journal of Education for Business, 79(3), - PP 186-190. (2004)
12. Sarita & Dahiya, R.: Academic cheating among students: pressure of parents and teachers, International Journal of Applied Research, 1(10), - PP 793-797. (2015)
13. Levy, Y., Ramim, M.: Initial Development of a Learners’ Ratified Acceptance of Multibiometrics Intentions Model (RAMIM), Interdisciplinary Journal of E-Learning and Learning Objects, (5), - PP 380-396. (2009)
14. Sung, Y.T., Chang, K. E., Yu, W. C.: Evaluating the reliability and impact of a quality assurance system for E-learning courseware, Computers & Education, 57 (2), - PP 1615-1627. (2011) DOI: http://dx.doi.org/10.1016/j.compedu.2011.01.020
15. Rashad, M., Kandil, M., Hassan, A., Zaher, M.: An Arabic Web-Based Exam Management System, International Journal of Electrical & Computer Sciences IJECS-IJENS, 10 (1), - PP 48-55. (2010)
16. Grishin, I.Yu., Timirgaleeva, R.R.: Remote educational technologies in providing training for modern specialists, Information technologies: science, technology, technology, education, health. Abstracts of the XXIIV International Scientific and Practical Conference. - P. 177. (2016)
17. Mironov, M.V.: User authentication in a computer system based on behavioral biometrics, Problems of informatics and modeling. Abstracts of the sixteenth International Scientific and Technical Conference. NTU "KPI". - P. 28. (2016)
18. Bodnar, A.A., Ahmetov, B.S.: Information technologies - the efficient management basis of high educational institution, Bulletin of the Taras Shevchenko Kiev National University. Philosophy and Political science. # 94-96. - PP. 44-50. (2010)
19. Grishin, I.Yu.: Analysis of promising approaches to the design of security systems of distributed computer networks, Herald of the Russian New University. #10. - PP. 36-40. (2015)
20. Ryabov, A.M., Skidan, R.A.: Models of provision, types and main problems of information security of cloud computing, Quality Strategy in Industry and Education-2016. Proceedings of the XII International Conference (Varna, Bulgaria). - PP. 534-537. (2016)
21. Timirgaleeva, R.R., Grishin, I.Yu.: Formation of professional competences of students of the direction “Applied Informatics” based on the use of technologies of the EMC corporation, Academic Forum of the EMC Corporation. Collection of theses of the reports of the participants of the EMC Academic Forum Russia & CIS 2014 conference. Faculty of Computational Mathematics and Cybernetics of Moscow State University. - PP. 71-75. (2014)

22. Shostak, M.A.: Information and logistics systems in the activities of universities, Information technologies: science, technology, technology, education, health. Abstracts of the XX International Scientific and Practical Conference. NTU "KPI". - P. 199. (2012)
23. Kazak, A.N.: The student learning process mathematical model, Information technologies: science, technology, technology, education, health. Abstracts of the XXX International Scientific Practical Conference. NTU "KPI". - P. 34. (2015)