The European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.10.03.126

ICEST 2020

International Conference on Economic and Social Trends for Sustainability of Modern Society

CONFIDENTIALITY, INTEGRITY AND ACCESSIBILITY IN THE DISTANCE EDUCATION SYSTEM

Julia Antokhina (a), Anatoly Ovodenko (b), Oksana Novikova (c), Sergey Bezzateev (d)*
*Corresponding author

(a) Saint Petersburg State University of Aerospace Instrumentation, Bolshaya Morskaya st., 67, Saint Petersburg, Russia
(b) Saint Petersburg State University of Aerospace Instrumentation, Bolshaya Morskaya st., 67, Saint Petersburg, Russia
(c) Saint Petersburg State University of Aerospace Instrumentation, Bolshaya Morskaya st., 67, Saint Petersburg, Russia
(d) Saint Petersburg State University of Aerospace Instrumentation, Bolshaya Morskaya st., 67, Saint Petersburg, Russia, bsv@aanet.ru

Abstract

At the present time, there is no doubt and practically confirmed that distance education is presently topical and top-requested mode of study in completely unexpected situations. The necessity to establish a self-isolation regime has led to the need for a large number of training sessions in the distance learning mode. The experience of distance training application revealed critical moments and challenges in the system of organization and management of the distance education process. In particular, problems appeared in the field of security of distance education in the broad sense of the term. In this work, we will consider the main problems and possible solutions to the main aspects of the distance education security. In particular, the possibilities of cryptographic transformations and protocols application to ensure reliable students' authentication as well as integrity and accessibility of educational and test materials and blockchain technology use to provide the safety of assignments, presence at lecture courses, participation in practical exercises information are considered.

Keywords: Distance education, management, security.

https://doi.org/10.15405/epsbs.2020.10.03.126
Corresponding Author: Sergey Bezzateev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The distance learning system contains two fundamentally different types of training:

1. The so-called on-line education when teacher plays an active role throughout the lesson, lecture, practical training, laboratory workshop, etc. This type of training implies, for the most part, an active teacher-student, student-student dialogue, and in this sense it turns out to be the closest to ordinary face-to-face education. Such education is characterized by a maximum teaching load on the one hand and the ability to control the audience and educational material from the teacher side on the other.

2. Particularly electronic education when student is provided with some pre-prepared training material and a set of complex and adaptable to the student's knowledge trajectory tests that student must pass through. Then demonstrate the knowledge gained while listening pre-prepared material that also could be issued to him in accordance with the level of student's knowledge. Using this type of distance learning, education process can be controlled by the teacher in accordance with the tests results demonstrated by student. At the same time teacher cannot control the learning process (and in some cases simply does not have such an opportunity).

When creating and implementing distance education systems (DES), the following components are used:

- external interface, for example, web application designed to provide remote access for teachers and students to the training course components. These components can be presentations, multimedia materials, tests and systems for active interaction with the teacher and between students. Moreover, in many cases, it implies the possibility of confidential communication between teacher-student and student-student;
- information database with training courses content, multimedia demonstration materials, additional educational materials (books electronic copies, textbooks and articles suitably matched to the course material);
- test materials database for providing students' knowledge evaluation;
- electronic journals (statements) with academic performance;
- server of distance education system, which is the core of the system and provides its basic functionality;
- devices (stationary and mobile) of various configurations and performance used by students in the process of educational material mastering.

The main users of distance education system are:

- teachers of educational institution (school, university);
- specialists of Curriculum & Instruction Departments;
- system administrators, programmers, web designers, information security specialists of the educational institution;
- students.

https://doi.org/10.15405/epsbs.2020.10.03.126
Corresponding Author: Sergey Bezzateev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

2. Problem Statement

In accordance with the above mentioned elements and participants of the distance education system, the standard process of information processing can be represented as follows:

1) user's connection to the website of the distance education system by his personal electronic device (currently it is more often mobile device, such as a tablet or smartphone) using an open communication channel;

2) identification and authentication procedure (Belk et al., 2017; Takamizawa & Kaijiri, 2006; Walters, 2016) to enter student's personal account or to use the distance learning resource. At the same time, the user is required to provide personal registration data (in many cases - multifactor authentication (Ometov et al., 2018; Ometov et al., 2017; Ometov et al., 2019), that may contains even biometric characteristics (Bandara et al., 2015; Bartlett et al., 2012; Biometrics and Authentication in Elearning wiki, 2007);

3) distance education server user's authorization. At the same time, depending on the user' status or/and group affiliation the rights to the appropriate level access issue.

4) request to the DES server for providing information, courses resources access and subsystems of DES. Such request fulfillment or non-fulfillment depends on the level of user's access;

5) input, modification or output of information of open and / or limited access;

6) user's disconnection from the DES resources.

Certainly, all the listed work stages in the distance education system are fragile from the information security point of view, and, therefore, require appropriate protection measures (Report Positive Research, 2016). Such measures should be specified already at the stage of DES development and be constantly improved in the process of its use. Let us further consider how the information security triad could be implemented in this case.

3. Research Questions

3.1. Confidentiality in distance education

Information confidentiality in DES is a necessary and essential requirement while developing a database of test assignments and test cases for students. Indeed, premature disclosure of questions and correct answers is unacceptable. Thus, students should not be able to "snoop" this information until testing begins. At the same time, such participants of the system application as administrators and teachers should have access in order to verify, correct and update information. All these requirements can be met using standard means of access control and critical information encryption (Merkle, 1980). Since, obviously, the system has a multi-level access structure, it becomes necessary to use hierarchical or multi-level systems of key distribution among users (Bezzateev, 2010). In addition, authentication in the system is necessary when student connects to the distance learning system from his personal device. Currently, this problem is being solved using various methods of user's multi-factor authentication (Ometov et al., 2018; Ometov et al., 2017; Ometov et al., 2019) using various authentication information:

https://doi.org/10.15405/epsbs.2020.10.03.126
Corresponding Author: Sergey Bezzateev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

- password - standard version of a characters' set with sufficient length from various groups (large and small letters, signs and numbers);
- key – RF tag, QR code, etc.;
- biometric information (Jain & Nandakumar, 2012; O'Neal et al., 2016; Voice Biometrics Group. Authenticating the Identity of Distance Learning Students, 2012) - fingerprint, vein pattern, face oval, etc.;
- behavioral features - dynamics of handwriting, features of work on a computer, etc.

Such authentication becomes especially topical in the case when it is necessary to conduct permanent ongoing monitoring, ensuring verification of participation in the educational process or during testing of a particular student (Levey & Jeff Maynard, 2011; Oladko et al., 2017). Of course, in addition to authentication, the system should keep an audit trail, entries which should be protected from possible intentional distortions, additions or deletions. Currently, blockchain technology (Dorri et al., 2017; Gorbunova et al., 2020) can be effectively used for these purposes. Taking distance education as a case. blockchain technology (Ponikarova et al., 2018; Raval, 2017; Stukova, 2019) is seen as especially effective due to the distributed nature of DES, its high dynamism and large number of users connecting and leaving the system at random times (Haberand & Stornetta, 1990).

3.2. Integrity in distance education

The integrity of the teaching materials used in the distance learning process is important for both student and teacher. Any change to these materials may occur only with the consent of teacher and author-developer. Digital signature can be used to prevent unauthorized changes in the content. Both individual (specific author-developer) and coalition (ring), confirming the authorship or responsibility of some team. In this case, it is also possible to use various threshold schemes (Kaya & Selçuk, 2007) that allow authorized change of information content in the training course with the consent of the author or/and part of the team responsible for this course.

In addition, in many cases, preservation and protection of authorship of course developers is important factor in distance education. Various text analysis systems (type "anti-plagiarism") use has proven itself to prevent the theft of original text materials, but unfortunately for now, graphic and illustrative material cannot be protected in this way. It is necessary to use special digital watermark systems to protect media information and prevent the unauthorized use of someone's illustrations. In addition, the digital watermark method allows you to detect illegally changes on copyright illustrations.

3.3. Accessibility in distance education

Accessibility in the distance education system implies:

- Students' ability to connect to training course at any time or in accordance with predetermined timetable;
- teachers, methodologists of the educational institution ability to access the material of the educational course to for making changes, additions and adjustments;

https://doi.org/10.15405/epsbs.2020.10.03.126
Corresponding Author: Sergey Bezzateev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

- students and teachers ability to access test tasks, giving access to the correct answers only to teachers;
- teacher or system administrator ability to disconnect a particular student from the distance learning system (in case of incorrect behavior) at any time.

Obviously, to provide DES protection against unauthorized access, various authentication systems listed above can be used.

4. Purpose of the Study

The purpose of the study was to determine the main cryptographic algorithms and protocols that are necessary and possible to use in distance education systems to ensure an acceptable level of security for the main components of such systems:

- database of test materials;
- electronic journal (statements);
- distance education system servers;
- devices (stationary and mobile) used by students in the process of mastering educational material.

And also directly participants of distance education systems themselves:

- teachers of educational institutions (schools, universities);
- students.

5. Research Methods

The main research method in this work is an analytical review of existing cryptographic methods and possibility of its use consideration for solving the triad of information security tasks in distance education. At the same time, we considered both long-known and well-established methods of protection against unauthorized access (encryption and authentication), integrity (hash functions and digital signatures) and new, relatively recently appeared and actively used in various applications cryptographic protocols (blockchain technologies) (Ponikarova et al., 2018; Raval, 2017; Report Positive Research, 2016).

At the same time, blockchain technologies use in distance education systems not only ensures the integrity of information, which can certainly be achieved with the help of traditional and well-proven digital signature technologies, but also make integrity protection open and transparent for all users of the system, which certainly significantly increases students' trust to the distance learning system.

6. Findings

The general approaches proposed in this paper for information security problems solution certainly do not determine all possible solutions, but can be used as a kind of "skeleton" to create a more complete,

https://doi.org/10.15405/epsbs.2020.10.03.126
Corresponding Author: Sergey Bezzateev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

comprehensive information protection system in open education structures. In this work, we have listed the main cryptographic functions and protocols that have proven themselves in information security systems and some new algorithms that can significantly improve the quality and effectiveness of distance education security and make it more attractive for all user groups.

7. Conclusion

The paper considers various security problems of distance education systems. Methods are proposed for most frequently arising information protection tasks solution. The possibilities and necessity of using modern cryptographic methods and protocols to ensure reliable and safe operation of distance education systems are identified.

References

Bandara, H., De Silva, S. R. P., & Weerasinghe, P. D. (2015). The universal biometric system. In *Proceedings of the International Conference on Advances in ICT for Emerging Regions* (pp. 1–6). Colombo, Sri Lanka.

Bartlett, M. S., Movellan, J. R., & Sejnowski, T. J. (2012). Face recognition by independent component analysis. *IEEE Trans. Neural Netw*, *13*, 1450–1464.

Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2017). The interplay between humans, technology and user authentication: A cognitive processing perspective. *Comput. Hum. Behav*, *76*, 184–200.

Bezzateev, S. V. (2010). Mnogourovnevaya systema razgranicheniya dostupa po sheme Mak Elisa [Multilevel access control system based on the Mac Eliece scheme] *Information Security Issues. Computer systems*, *3*, 42-44.

Biometrics and Authentication in Elearning wiki (2007). http://biometrics.pbworks.com

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: Adistributed solution to automotive security and privacy. *IEEE Communications Magazine, 55*(12), 119–125.

Gorbunova, M. V., Ometov, A. Y., Komarov, M. M., & Bezzateev, S. V. (2020) Obzor problem vnedreniya technologiy raspredelennogo reestra [Problems overview on distributed registry technology implementation] *Information control systems*, *2*, 10-19.

Haberand, S., & Stornetta, W. S. (1990) How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437–455). Springer.

Jain, A. K., & Nandakumar, K. (2012). Biometric Authentication: System Security and User Privacy. *IEEE Comput, 45*, 87–92.

Kaya, K., & Selçuk, A. A. (2007). Threshold cryptography based on Asmuth–Bloom secret sharing. *Inf. Sci., 177*, 4148–4160.

Levey, S., & Jeff Maynard, B. (2011). *Identity Proofing for Online Student ID Verification: Report of Pilot with Houston Community College.* Huston.

Merkle, R. C. (1980). Protocols for Public Key Cryptosystems. *IEEE Symposium on Security and Privacy*, 122–122.

Oladko, V. S., Babenko, A. A., & Aleksina, A. A. (2017). Otsenka zaschischennosti sistemy distantsionnogo obrazovaniya vuza [Security evaluation of the university distance education system] *Scientific Result. Information Technologies*, *2*(1).

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, N., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography, 1*(5).

Ometov A., Bezzateev, S., & Koucheryavy, Y. (2017). Authenticating electronic devices for temporary use: access rights management protocol. *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunications and Control Systems*, *10*(4) 29–40.

Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y., & Gerla, M. (2019) Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications *IEEE Network*, *33*(2), 82-88.

O'Neal, M., Balagani, K., Phoha, V., Rosenberg, A., Serwadda, A., & Karim, M.E. (2016) Context-Aware Active authentication using touch gestures, typing patterns and body movement. *Technical Report.* Louisiana Technical University.

Ponikarova, A., Zotov, M., & Dolgov, P. (2018). Nekotorie aspekti realizatsii technologii blokchein v sovremennikh usloviyakh [Some aspects of blockchain technology realization in modern conditions. Sustainable development management], *4*(17), 33-37.

Raval, S. (2017). *Detsentralizovannie priloheniya. Technologiya blokchein v deistvii* [Decentralized applications. Blockchain technology in action]. Piter.

Report Positive Research (2016). *Analytics of Positive Technologies Company 2016.* http://www.ptsecurity.ru/upload/ptru/analytics/Positive-Research-2016-rus.pdf

Stukova, E. N. (2019). Primenenie technologii blockhein v organizatsii I upravlenii naukoemkimi proizvodstvami [Application of block chain technologies in knowledge-intensive industries organization and management]. *Innovative economy: prospects for development and improvement*, *6*(40).

Takamizawa, H., & Kaijiri, K. (2006). *Reliable Authentication Method by Using Cellular Phones in WBT.* Faculty of Engineering, Shinshu University.

Voice Biometrics Group. Authenticating the Identity of Distance Learning Students (2012). *Voice Biometrics Group (VBG) Vocal-ID™ Service Assures Identity*. www.voicebiogroup.com

Walters, R. (2016). Continuous Authentication: The Future of Identity and Access Management (IAM). https://www.networkworld.com/article/3121240/security/continuous-authenticationthefuture-of-identity-and-access-management-iam.html