The 12th International Conference on Business Information Security

(BISEC-2021), 3rd December 2021, Belgrade, Serbia

SECURING ONLINE ASSESSMENTS IN ONLINE EDUCATIONAL SYSTEMS USING BLOCKCHAIN

JOVANA JOVIĆ

Belgrade Metropolitan University, Faculty of Information Technologies, jovana.jovic@metropolitan.ac.rs

VIJAYAKUMAR PONNUSAMY

Department of ECE, SRM Institute of Science and Technology, Kattankulathur, India, vijayakp@srmist.edu.in

VLADIMIR MILIĆEVIĆ

Belgrade Metropolitan University, Faculty of Information Technologies, vladimir.milicevic@metropolitan.ac.rs

NEMANJA ZDRAVKOVIĆ

Belgrade Metropolitan University, Faculty of Information Technologies, nemanja.zdravkovic@metropolitan.ac.rs

Abstract: *The ongoing COVID-19 pandemic has led to more and more universities adopting an online-only option for studying. As a result, students often take course assessment through an online form within the Learning Management System (LMS), and hence the need for secure LMSs become more evident. Commercially available LMS solutions may not be secure in every aspect, especially when it comes to online assessments and their grading, either automatic or manual. In this paper, we present a blockchain-based add-on for the purposes of securing online assessments. We show that with our proposed solution, secure assessment and grading can be achieved with the innate security properties of blockchain.*

Keywords: *blockchain, learning management system, online assessments, secure eLearning.*

1. INTRODUCTION

The ongoing global COVID-19 pandemic has forced education institutions on all levels of study (primary, secondary, and higher education) to consider a switch from traditional „face-to-face“ learning methodologies to blended learning, or completely online learning [1]. Indeed, this switch presented a challenge to all parties involved – students, but also teaching staff, and their mutual communication. As most teacher-to-student communication is now being conducted exclusively online, several security issues arise [2, 3].

One of the main security issues regards communication channels. Namely, commercial video conferencing platforms such as Skype, Microsoft Teams, or Zoom are being implemented ever more in virtual classrooms offer limited security options without purchasing or subscribing to the service.

In some cases, the use of these platforms has shown more efficient student engagement [4], topics which include writing on the blackboard, such as mathematics and similar subjects, still face difficulties in presentation [5].

Another security issue regards online exams in which, without a complex e-monitoring system, cheating is possible [6-8]. The authors of [6] pointed out that security requirements for such a system would account for accessibility, monitoring, management, authenticity, integrity, secrecy and copy prevention and detection. It should be noted that most final exams in Higher Education Institutions (HEIs), unlike from Massive Open Online Courses (MOOCs), are conducted on-campus.

The third security issue, which is the topic of this paper, are online assessments which are conducted in online and blended methods in HEIs, as well as in MOOCs. The COVID-19 pandemic showed that not all HEIs were completely prepared for the completely online or blended learning, especially regarding conducting exam obligations such as individual assessments, tests, homework etc. [9]. Most HEIs employ some sort of Learning Management

System (LMS); however, these systems are often expensive, or lack specific functionalities such as assessment submission. Some HEIs, especially Science, Technology, Engineering, and Mathematics (STEM) universities choose to develop an in-house solution regarding these functionalities, and security issues are often overlooked due to time constraints. Most LMSs and similar learning platforms do not provide Virtual Private Networks (VPNs) when a student or teaching staff member connects to the LMS platform, and data transfer is often conducted using Hypertext Transfer Protocol (HTTP) which is prone to security vulnerabilities [10, 11].

Continuing from our previous work done in [12, 13], in this paper we provide a solution to securely monitor and access student's assessment by implementing Blockchain Technology (BCT). The rest of the paper is organized as follows. Section 2 presents our motivation, broken into two subsections: identified use-cases for the proposed platform, and a short introduction to the security properties of BCT, highlighting its advantages in these use-cases. Section 3 presents our solution with appropriate discussion, while Section 4 concludes the paper.

2. MOTIVATION

Our main motivation comes from the fact that communication between student and teaching staff regarding pre-exam obligations, upon switching to a completely online learning and teaching model, is at the same time simplified, and yet more complicated. Students which complete their assignments online within an in-house developed LMS can have difficulties if that LMS does not natively support fully online assignment submission.

Use-cases with security issues in online learning

We have identified multiple use-cases in which students' assignments may be prone to security issues. Namely, the first case, presented in Image 1, shows an unsecure channel between the student and the server-side LMS app. As stated in [10, 11], if no security measurements have been applied, a third party can potentially monitor local network traffic and obtain information about the assessment and about the student's submitted answers. This issue is even more important if the make-shift online assessment in developed with no encryption.

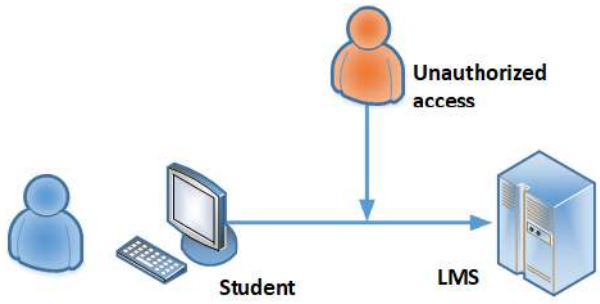

Image 1: Use-case #1: Unsecure traffic between the learner and the LMS.

The second use-case is any type of student's answer correction without authorization. This can be achieved either by the student, or by the teaching staff. The motivation behind this use-case is to remove any teaching staff bias. Finally, the third use-case is in regards to presenting the students their complete results upon their or teaching staff's request. If not implemented correctly, the student and/or teacher can only see, for instance, the number of correct or incorrect answers in a multiple-choice test, but not which ones were correct or not, which can be an issue of lack of complete information. The second and third use-case are presented in Images 2 and 3, respectively.

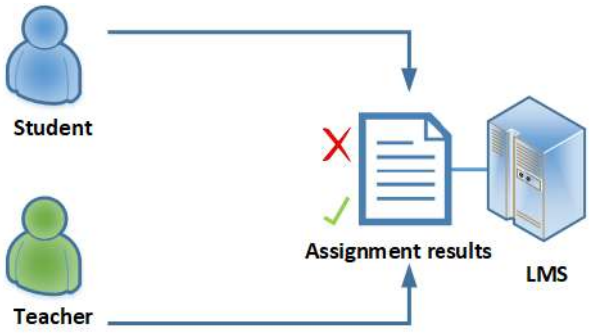

Image 2: Use-case #2: Unauthorized assignment result correction.

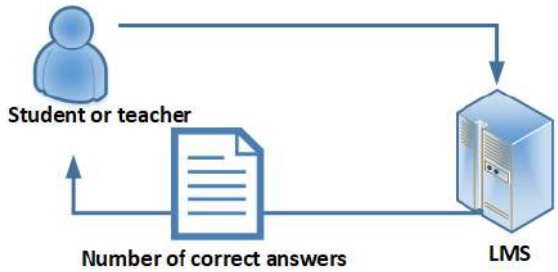

Image 3: Use-case #3: Incomplete access to assignment results.

We note that in most commercially available LMSs these security issues will not happen often, and that these use cases are more in line with in-house developed LMSs. In addition, in-house developed LMSs are, in general, open to modification and upgrades, which corresponds with our BCT extension regarding issues with online assessments.

Security properties of Blockchain technology

A Blockchain is a shared, append-only distributed ledger, in which all events, which are usually denoted as transactions, are stored in linked blocks [14]. Every event contains data regarding the event itself, as well as a unique cryptographic signature, which ensures that the blockchain ledger is resilient to modifications. A block can be viewed as a data structure consisting of a list of events, coupled

with a header. This header connects the block to the previous one, forming a chain all the way to the genesis block. The combination of peer-to-peer networks, public-key cryptography, and distributed consensus is what secures blockchain transactions. Unlike a centralized system, no single entity within the blockchain should be able to adding a block to the chain: all nodes in the chain share equal rights. This type of decentralized storage is managed with a distributed consensus mechanism. Depending on the consensus algorithm, nodes can either compete for correct transaction validation, be chosen randomly, or apply a different algorithm altogether. One significant advantage of using BCT is that it can provide a decentralized management and access to all types of databases, providing only authorized access when needed.

3. SYSTEM MODEL AND DISCUSSION

In this Section, we provide a model for in-house developed LMSs which can connect to a blockchain running on the HEI's computers. It is important to note here that this type of blockchain would be a private blockchain, as all the nodes are in the ownership of the HEI. Multiple nodes running the blockchain can be deployed within an HEI's servers or multiple computers on campus, needed to run the consensus. This approach may seem redundant; however, this system still has an advantage compared to a traditional database, as any type of access to the blockchain will be recorded and verified by multiple nodes with the consensus mechanism, leaving a traceable timestamp on all the machines running the blockchain.

Our system is designed in such a manner that an endpoint from the LMS's regarding assessment is connected to the HEI's private blockchain. Each time a user, be it student or teaching staff, is accessing anything related to pre-exam assignments, an event is triggered and a new transaction is formed. This transaction is broadcast to all noted within the blockchain network, and is verified. This type of blockchain may need not have a processor-heavy consensus mechanism such as proof-of-work, used in Bitcoin [15]; it can use one of the mechanisms found in the Hyperledger family of BCTs [16]. The types of transactions can be categorized into deploying assessments, submitting assessment answers, and result view. These categories correspond with the requests sent from the user to the LMS, and replies sent from the LMS to the user, respectively. The overall system diagram is shown in Image 4.

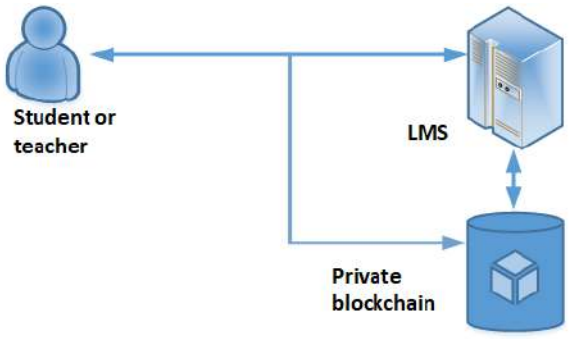

Image 4: Connecting a private blockchain to the user-LMS communication.

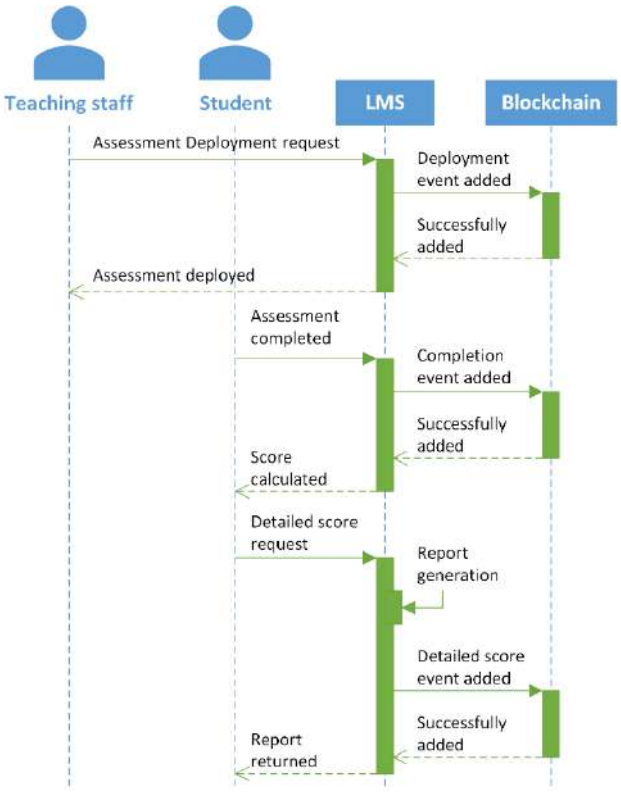

Image 5: Sequence diagram of assessment report with blockchain events.

Image 5 shows a sequence diagram where teaching staff is deploying an assessment, and a student is submitting assessments results, with a detailed result view afterwards. The blockchain will be triggered to make an event every time a request or response is made regarding assessments. This type of system ensures that no modification made to scores are made without being traceable. Furthermore, use case #1 can be addressed with the data in the events themselves. For instance, if assessments are made up of randomly chosen questions, each combination for each student will be written in a separate event. If an unauthorized party is monitoring unsecure traffic, the information they obtained may be traced back to the exact combination of questions.

5. CONCLUSION

In this paper, we have identified several security issues regarding in-house developed LMSs and pre-exam assessment submission and modification. By applying a private blockchain extension to this type of LMS, an additional layer of security can be achieved. Furthermore, this blockchain extension can be easily deployed on several on-campus computers, and with the correct choice of consensus mechanism, the extension may not be processor-heavy. Currently, we are exploring the possibilities of adding BCT in e-Learning systems, as they will most definitely be a crucial part of future learning methodologies in all levels of studies. Our future work will focus on an overall blockchain-supported LMS, which may expand to multiple campuses or even multiple universities.

ACKNOWLEDGMENT

This paper was supported in part by the Blockchain Technology Laboratory at Belgrade Metropolitan University, Belgrade, Serbia, and in part by the Ministry of Education, Science and Technological Development, Republic of Serbia (Project III44006).

REFERENCES

[1] J. Davis, „Traditional vs. Online learning: It's not an either/or proposition," Employment Relations Today, vol. 27, no. 1, 2000, pp. 47-60.

[2] J. B. Earp, F. C. and Payton, "Data protection in the university setting: Employee perceptions of student privacy," in Proc. of the 34th IEEE Annual Hawaii International Conference on System Sciences, 2001, pp. 6.

[3] N. H. M. Alwi, and I. S. Fan, "E-learning and information security management," International Journal of Digital Society, vol. 1, no. 2, pp.148-156., 2010.

[4] J. Alameri, R. Masadeh, E. Hamadallah, H. B. Ismail, H.B. and H. N. Fakhouri, 2020. "Students' Perceptions of E-learning platforms (Moodle, Microsoft Teams and Zoom platforms) in The University of Jordan Education and its Relation to self-study and Academic Achievement During COVID-19 pandemic," Advanced Research & Studies Journal, vol. 11, no. 5, pp. 21-33, 2020.

[5] M. Irfan, B. Kusumaningrum, Y. Yulia, and S. A. Widodo, "Challenges during the pandemic: use of e-learning in mathematics learning in higher education," Infinity Journal, vol. 9, no. 2, pp.147-158, 2020.

[6] I. Y. Jung, and H. Y. Yeom, "Enhanced security for online exams using group cryptography," IEEE transactions on Education, vol. 52, no.3, pp. 340-349, 2009.

[7] Y. Atoum, L. Chen, A.X. Liu, S. D. Hsuand X. Liu, "Automated online exam proctoring. IEEE Transactions on Multimedia, " vol. 19, no. 7, pp. 1609–1624, 2017.

[8] H. Ilgaz, and G. A. Adanır, G.A., "Providing online exams for online learners: Does it really matter for them?," Education and Information Technologies, vol. 25, no. 2, pp. 1255-1269, 2020.

[9] E. Edelhauser, L. Lupu-Dima, "Is Romania Prepared for eLearning during the COVID-19 Pandemic?," Sustainability, vol. 12, pp. 5438, 2020.

[10] G. D. Bissias, M. Liberatore, D. Jensen, and B. N. Levine, "Privacy vulnerabilities in encrypted HTTP streams," in Proc. Workshop on Privacy Enhancing Technologies, pp. 1-11, 2005.

[11] M. Vieira, N. Antunes and H. Madeira, "Using web security scanners to detect vulnerabilities in web services," in Proc. IEEE/IFIP, pp. 566-571, 2009.

[12] M. Damnjanović, V. Grković, and N. Zdravković, „Towards Secure online studies: Applying Blockchain to e-Learning, " in Proc. Of the 11th international conference on eLearning, 2020.

[13] N. O. Vesić, N. Zdravković, and D. J. Simjanović, „Securing Online Assessments using Christoffel Symbols," in Proc. Of the 11th international conference on eLearning, 2020.

[14] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, „An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. of the IEEE international congress on big data (BigData congress), pp. 557–564, 2017.

[15] S. Nakamoto, „Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, pp. 21260, 2008.

[16] V. Milićević, J. Jović, and N. Zdravković, „An overview of Hyperledger blockchain technologies and their uses," in Proc. Of the 11th International Conference on Information Society and Technology (ICIST 2021), pp. 62-65, 2021.