Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, June 2021: 813- 816

A Study of Block Chain Based Security Architecture for Online Education

Dr. Shaji N Raj

Assistant Professor SAS SNDP Yogam College, Mahatma Gandhi University Kerala, India
ammashajinraj@gmail.com,

Abstract

A prototype model named Online Education Protection is introduced, that enables to link online education technologies with blockchain technology. In this technology students details are put in the Blockchain. Blockchain technology is commonly used in crypto currencies but the innovative use of this technology can boost cyber security and protect online education more effectively. A model has been explored with a combination of online education platform and blockchain technology to construct new security for the online learning system. These models allow direct access to online classes, which requires restricted access to data and protected from intruders and provides trust and security.

Keywords: Security, Online education, Hashing, Blockchain

1. Introduction

On the month of may 2020 the epidemic caused by Covid-19 broke out in India. Due to this epidemic all the schools and colleges were shutdown. Therefore they had to adapted online learning and teaching methods. First try to understand about the concept block chain. A blockchain is a continuously growing list of records, secured using cryptography [21]. As of now, centralized databases play a major role in online education system, while a trade-off between blockchain and conventional databases is a good choice for online education system. Other than trust, secure and robustness, blockchain can do nothing more than a centralized database[22]. Blockchains are also considered slower in performance than regular databases. Furthermore, as long as the blocks are stored in the memory and hard disk of computer or nodes, it can also be vulnerable. Considering the above scenario, this paper concentrates on a trade-off between online education platfom and blockchain databases.

The paper is structured as follows: After introducing the background information on Blockchain and related concepts, literature review follows. Section 3 presents the proposed methodology and the new algorithm. The section 4 presents the results and evaluations. The paper concludes in Section 5, with future work.

2 Background Literature

Ali Alammary, article specifies a systematic review of research investigating blockchain-based educational applications. It focuses on three main themes such as educational applications developed with blockchain technology. [1]

Yumna et. al. on their paper explained all the features of blockchain and provide appropriate solutions for problems encountered in education system.[2]

Researchers developed various techniques for privacy using the blockchain technique. David Shrier, Weige Wu, Alex Pentland, of Connection Science & Engineering, Massachusetts Institute of Technology published a paper entitled “Blockchain & Infrastructure” describing the need for blockchain based identity authentication. Using blockchain, a global identity was created for each user[3].

Loi et al. discovered that among the 19,366 existing Ethereum contracts, 8,833 are vulnerable [4]. The researches show the new blockchain technology had a number of security and privacy issues. In June 2016, the smart contract DAO (Decentralized Autonomous Organization) was attacked [5] and the attacker exploited a recursive calling vulnerability, resulting in DAO losing about 60 million dollars.

There is a number of security models for databases available, but 100% protection is still a daunting problem for researchers. The proposed Online Education Protection[OEP) for different platform is novel, maintaining a centralized and decentralized databases together. Therefore, OEP benefits both the advantages, wherein blockchains are suited for the record of certain functions, while a centralized database is entirely appropriate for other functions.

3 Online Education Protection(OEP)

The unauthorized use of digital content and participants details and examination is the main threat of digital education. OEP model provide a block chain based a safer personal learning environment which provides a solution for authentication, assures the security of online assessments, and personal security.

The blockchain technologies are widely used in cryptocurrencies but due to its decentralization and immutability properties, it is now used in many applications of information technology. Since many of the existing applications are in centralized databases, and considering blockchain's trust, robustness and distributed over existing databases, a fusion of both provides a better scenario. . They are defined as two trade-offs, given as:

Trade-off 1: Online Education with blockchain technology
Trade-off 2: Examination with blockchain technology
Figure 1 illustrates the proposed scenario named OEP combining centralized database system with and block chain technology to ensure the security of data and prevents the different types of attacks

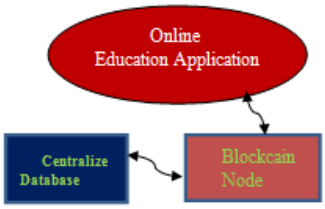

Figure 1. Online Education Protection Model

3.1 Ameliorate Security Algorithm (ASA)

An Ameliorate Security Algorithm is proposed for OEP, in which two trade-offs have been implemented with certain customization for each one.

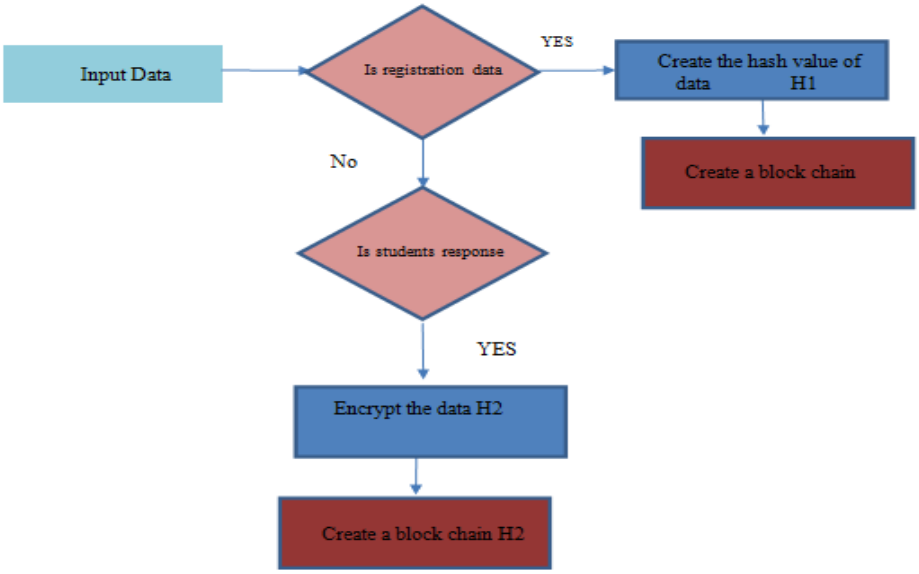

Figure 2. Block diagram of Ameliorate Security Algorithm

In this method, registration inputs are hashed and stored in a database and students response data are stored in an encrypted form and the hash value of the data is stored in the blockchain. The flow of Ameliorate Security Algorithm is depicted in Figure 2.

3.2 Online Education with blockchain technology

In the midst of the corona virus pandemic, many higher education institution were forced to online education. Student have different ideas some time these ideas are controversy and teachers share some critical ideas to the students thus need a secure place for online learning. Some time intruders are login into the online classroom and record the classes. Creating a strictly controlled environment enables institutions to manage privacy and security more effectively. This protection is done by using the password. But the password protection is not secure because a member of the online class may steel the data.

One of the challenges facing now by developers is the privacy of online teaching. The centralized database still has some advantages over blockchain technology, especially in its confidentiality and performance. Blockchain is distributed, shared across boundaries of trust in different nodes, which is viewable to anyone. Therefore, the confidentiality of any data stored is essentially zero, though it has its own proof of validity and its own proof of authorization. Since, in many cases, data needs confidentiality, the public blockchain may not be very useful in many business applications.

The proposed model has two phases named

1. Hashing phase 2. Linking Phase

Hashing phase: In the hashing phase, the hash value of the registration data is taken and permanent input data are hashed together stored in blockchain

Linking phase: The second phase named linking phase is an efficient phase, which is used for creating a block chain. The block chain contains encrypted response.

4 Evaluation

Blockchain technology is one of the promising technologies to protect data from hackers. When an intruder try to access the online class it is not possible due to hashing and encryption and data is stored in a block chain. Also in real time monitoring techniques, this algorithm prevents all types of attacks.

The experiment results showed this system provide high security. The advantage of these systems is more resilient against many security threats.

5 Conclusion

This paper proposes a models with blockchain technology to provide high security for online teaching. While keeping the confidentiality and integrity of centralized databases, blockchain's trust and robustness benefited to it. The Ameliorate Security Algorithm proposed is tuned for different trade-offs . In security analysis of our experiment, it is found that online education platform with blockchain and show better results for confidentiality..

References

[1] Ali Alammary,Blockchain-Based Applications in Education: A Systematic Review 2019 , https://www.researchgate. net/deref/http%3A% 2F%2Fdx.doi .org%2F10.3991%2Fijet.v13i10.9455

[2] Yumna, Hafiza & Khan, Muhammad Murad & Ikram, Maria & Ilyas, Sabahat. (2019). Use of Blockchain in Education: A Systematic Literature Review. 10.1007/978-3-030-14802-7_17.

[3] Getsmarter.com, 2018. [Online]. Available: https:// www.getsmarter. com/career-advice/wp-content /uploads /2017 /07/ mit_ blockchain_ transactions_report.pdf. [Accessed: 05- Jan- 2018].

[4] "The Daily Beast", The Daily Beast, 2018. [Online]. Available: http://www.thedailybeast.com. [Accessed: 05- Feb- 2018].

[5] E.Foundation," Critical updateRe: DAOVulnerability" , Blog .ethereum .org,2018.[Online].Available:https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/. [Accessed: 07- Jan- 2018].

[6] [6]X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, "A survey on the security of blockchain systems", 2018.

[7] "Blockchain Architecture| Pluralsight", Pluralsight.com, 2018. [Online]. Available:https://www.pluralsight.com/guides/blockchain-architecture. [Accessed: 03- Feb- 2018].

[8] 2018. [Online].Available: https://www.quora.com/How-can-blockchain-be-used-as-a-database-to-store-data. [Accessed: 07- Feb- 2018].

[9] H. Vranken, "Sustainability of bitcoin and blockchains", 2018.

[10] "Blockchain: A Technical Overview - IEEE Internet Initiative", Internetinitiative.ieee.org, 2018. [Online]. Available: https:// internetinitiative.ieee.org/newsletter/march-2018/blockchain-a-technical-review. [Accessed: 03- Jan- 2018].

[11] Jamie Paul, "Integrated Innate and Adaptive Artificial Immune Systems for Anomaly Detection", University of Nottingham, 2007.

[12] Muhammad Awais Shibli, "MagicNET: The Human Immune System and Network Security System", Paper.ijcsns.org, 2009. [Online]. Available: http://paper.ijcsns.org/07_book/200901/20090113.pdf. [Accessed: 16- Jun- 2018].

[13] Doyen Sahoo, Steven C.H. Hoi and Chenghao Liu, "Malicious URL Detection using Machine Learning: A Survey", https:/ /arxiv.org /abs/ 1701.07179, 2017.

[14] Y. Fan, Y. Ye and L. Chen, "Malicious sequential pattern mining for automatic malware detection", Expert Systems with Applications, vol. 52, pp. 16-25, 2016.

[15] Anjali B. Sayamber and Arati M. Dixit, "On URL Classification", Ijcttjournal.org, 2018. [Online]. Available: http:// www. ijcttjournal. org/Volume12/number-5/IJCTT-V12P148.pdf. [Accessed: 16- Mar- 2018].

[16] [16]Feroz Zahid, "Network Optimization for High-Performance Cloud Computing", University of Oslo, 2017.

[17] W. Halfond and A. Orso, "Combining static analysis and runtime monitoring to counter SQL-injection attacks", ACM SIGSOFT Software Engineering Notes, vol. 30, no. 4, p. 1, 2005.

[18] Gaurav S. Kc et al., "Countering Code-Injection Attacks With Instruction-Set. Randomization", Proceedings of the 10th ACM conference on Computer and communications security, pp. 272-280, 2003.

[19] Pankaj Deep Kaur and Kanwal Preet Kour, "SQL injection: Study and augmentation", in Conference: Conference: 2015 International Conference on Signal Processing, Computing and Control (ISPCC), Waknaghat, India, 2015.

[20] Gary Wassermann and Zhendong Su, "An Analysis Framework for Security in Web Applications", http:// web.cs. ucdavis.edu /~su /publications /savcbs. pdf 2014.

[21] "Bitcoin", En.wikipedia.org, 2018. [Online]. Available: https: //en. wikipedia. org/wiki/Bitcoin. [Accessed: 01- Mar- 2018].

[22] G. Greenspan, "Blockchains vs centralized databases | MultiChain", Multichain.com,2018.[Online].Available: https:// www.multichain.com/blog/ 2016/ 03/blockchains-vs-centralized-databases/. [Accessed: 03- Mar- 2018]