Securing Educational Data Using Agent-Based Blockchain Technology

Millicent Ubaka-Okoye, Ambrose A. Azeta, Aderonke A. Oni, Hilary I. Okagbue, Olanike S. Nicholas-Omoregbe

Abstract: Educational data security especially examination, results and certificate management systems should be upheld with the utmost integrity. Blockchain has a prospective that possibly will offer a system with considerable sincerity and secure database in educational systems. Existing large databases of students' external examinations, results and certificate management data are subject to manipulation and lack security in terms of confidentiality, integrity and availability. These cases are peculiar to external examinations conducted in tertiary institutions. Unfortunately, there is an abuse by system administrators/IT personnel in exercising their access privileges as a superuser. Hence, this work explored an agent based Blockchain-technology in securing educational data against insider threats focusing on Ethereum's Proof of Authority (PoA) consensus algorithm to implement an agent-based blockchain model system. The work was able to discover a foundation for advancing current understanding of blockchain systems, development of models for blockchain using the immutable features of the technology and incorporation of intelligent agents

Index Terms: Blockchain technology, Educational data, Intelligent agent, Data security, insider threats, POA.

———————————— ◆ ————————————

1 INTRODUCTION

Educational institutions among others such as healthcare and finance are tremendously tormented by insider attacks, from copying and selling personal information to an insider, trading to data leaks by mistake [1-3]. In December 2016 Lynda.com, the online learning platform owned by LinkedIn was hit by a Hack where an authorized external party accessed students' data with 9.5 million user accounts affected [4]. In 2015, University servers were hacked and some grades were changed. In 2015, A New Jersey university student network system was compromised, of course, a ransom of bitcoin was being asked. These instances among many others show the vulnerabilities in our current systems [5]. In 2015, two database administrators (DBA) in the data center in a Nigerian university colluded and altered students' examination scores to the advantage of the students, after they were bribed. In 2009, a male data operator in the result processing room, in a higher institution manipulated the final year results of a female student that was about to graduate to move from 3rd class to second class lower [6]. The investigation revealed that the data operator and female students were in a relationship [6]. In 2016, a Head of IT responsible for processing results in a public Nigerian university changed the scores of his relative for the student to cross the cumulative grade point average (CGPA) bother line to first class. The case was reported and the HOD claimed that it was an entering error [6]. Lastly, existing challenges faced by bodies involved in external examinations such as West African Examination Council (WAEC) is basically on exam malpractices and conducting exams for all the various secondary schools throughout the regions covered by WAEC, verification of certificate online irrespective of location and time also over-centralization of candidate's data is an issue. More so, a centralized network requires a system administrator with superuser privileges to manage the server resources, however, these roles have been misused.

————————————————————

• *Millicent Ubaka-Okoye is of the Department of Computer Science and IT, Bells University of Technology, Ota, Nigeria.*
• *Ambrose A. Azeta is of the Department of Computer & Information Sciences, Covenant University, Ota, Nigeria*
• *Aderonke A. Oni is of the Department of Computer & Information Sciences, Covenant University, Ota, Nigeria*
• *Hilary I. Okagbue is of the Department of Mathematics, Covenant University, Ota, Nigeria*
• *Olanike S. Nicholas-Omoregbe is of the Department of Sociology, Covenant University, Ota, Nigeria*

IT personnel also play a major role in managing the examination, results, and certificate [7-8]. Insider threats are the prime security leakages in every organization, and they are exceedingly expensive to correct. According to Gogan [9] insider threat report, 53 percent of companies calculated approximately $100,000 and 12 percent approximately more than $1 million. The same report discovered that 74 percent of companies' experiences were open to insider threats, in the midst of seven percent reporting excessive exposure. Subsequently, insider threats are expensive to correct, hence hard to deal with? There are quite a lot of reasons insider threats can go unnoticed for years. When a security breach or a leakage exceedingly goes undetected, the more the correction cost goes up. Insider threats can be hard to detect, that is why they are the most expensive to correct. It is hard to differentiate destructive procedures from usual work. This is subsequently the reason insider threats are tough to detect. Once a member of staff is operational with sensitive information, it is unfeasible to identify whether they are doing something malevolent or not. It is simple for workers to envelop their procedures at the same time as it's tough to detect malevolent procedures as they occur, it can be impracticable to detect them instantly. Insider threats disguised as System Administrators or Information Technology personnel identify malevolent programs by editing or deleting logs to hide actions. Often when these insider threats are detected the offenders will claim system error or mistake. Blockchain technology is an innovating new generation internet that is immutable, decentralized, transparent, auditable, persistent and secured [10]. The blockchain is a distributed database that multiple parties share and everyone can trust. Each party participating in the transactions of the network maintains a personal copy of the database. This database has automatic trust, tamper-proof, shared data, transparent and resilient. Blockchain technology is one of the most impactful inventions of the last decade [11]. This paper focuses on securing educational data using agent-based blockchain that will create a widely accessible and secure data distribution services that connect to existing educational data. Institutions can easily aggregate their data history without requesting a copy from central servers. Connections to personal smart devices are also possible as blockchains remove trust concerns amongst users or between third-party institution tracking applications and services. Educational data security especially examination, results and certificate management systems should be upheld with the utmost integrity. Blockchain has a prospective that

possibly will offer a system with considerable sincerity and secure database in educational systems [12]. Blockchain enhances data security and removes trust concerns amongst users.   Applying an agent-based blockchain technology structure to educational institutions will secure and enhance data security by preventing insider threats.

2 AIM AND PROBLEM STATEMENT

A safety measure is a prime prerequisite to sustain confidence and authenticity of data. The investigation from different literature reveals that there are still security issues about existing information systems, particularly as it relates to confidentiality, integrity and availability of data stored in the system. A large organization such as national examination bodies and similar organizations have been a victim of insider threats. Also security issues in national examinations such as insider threats has remained a critical concern that is yet to be fully addressed [11], [13-16]. In a specific scenario, there have been reported cases where officials of these organizations gain legal access into the complex information system or database only to carry out illegal activities such as fraudulent change (tampering) of information stored in a database. (In these cases, students' results and the status of their certificates) [7].

3 PROPOSED SECURITY FRAMEWORK

3.1 Blockchain Technology

This is an innovating new generation internet technology. It is immutable, decentralized, transparent, auditable, persistent and secured. The blockchain is a distributed database that multiple parties share and everyone can trust. Each party participating in the transactions of the network maintains a personal copy of the database. This database has automatic trust, tamper-proof, shared data, transparent and resilient. Looking at figure 1: an agent-based blockchain architectural framework for educational data security, which is an extension of the incorporated data security layer on the blue dotted line that comprises intelligent agent and blockchain technology, will help to enhance security and prevent insider threats on educational database.

3.2 Intelligent Agent

Intelligent Agent (IA) is software unit that carries out some operations on behalf of a user or another program with some scale of autonomy. In so doing, employs some information of the user's goals or desires while an agent is a computer system situated in a certain kind of environment and hence, capable of autonomous transaction to meet its designed objectives [17]. Agent Based approach is all-purpose and authoritative because it enhances capturing of difficult structures and dynamics [18]. The intelligent agent will be implemented with Java programming language. This work will use intelligent agent-based blockchain as a tracking autonomous system that will monitor what anyone on the network is doing. If it detects an insider threats, it will send an alert to all the users on the network.

3.3 Description of the Security Framework

The Database Layer: contains the student, examination, results and certificate database where the educational database of the institutions or organization is being stored. The database will be linked to the data security layer. Data

Security Layer: The layer with dotted blue lines was the additional architectural security framework we added to secure the database against insider threats. We have an intelligent agent that will aid as a gossip protocol to blockchain in order to improve data security against access-privileged users from tampering with the data or malicious users or attacker from gaining access to educational database. From the reviewed literature, we can see that there are still issues with the existing blockchain security framework models being used to secure information or database. Blockchain technology alone cannot guarantee 100% security on our data that was the reason we introduced these data security layer to facilitate the process. Logic Layer: We have the student, registration, examination, results and certificate Menu. The layer contains menu application which collaborate to make effective processing or facilitates processing of any data or information. For example, all the list of options function can provide location information to the system during processing. However, the applications should be integrated carefully since vulnerabilities in one application may give intruders access to other dependent processes. Presentation Layer: It is also known as the communication layer where the processed and safe information or data is communicated to the users. In this presentation layer, networks use different communication tools such as Web, Mobile, Bluetooth, WiFi, Ethernet, 3G, and 4G to exchange
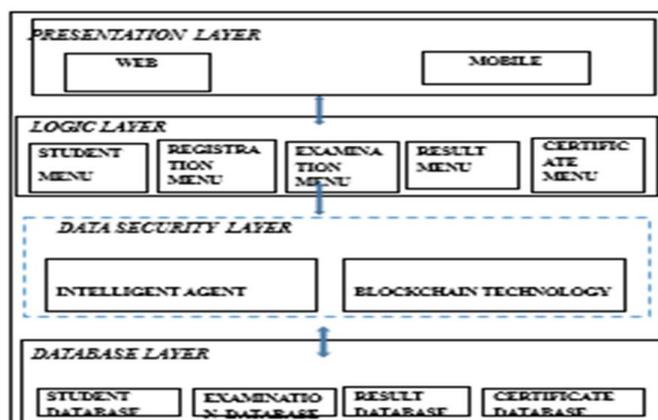
Figure 1: *An Agent-Based Blockchain Architectural Framework for Educational Data Security*

information among different systems. The blockchain protocols need to be blended with this layer to provide security and privacy of transmitted data. For example, the transaction records can be converted into blocks using telehash which can be broadcast in the network. Protocols like BitTorrent can be used for peer to peer communication whereas Ethereum can provide smart contract functionalities.

4 IMPLEMENTATION

The architectural design, we implement a decentralized private network by using the following hardware and software as summarized in Table 1.

TABLE 1: *SPECIFICATIONS FOR SYSTEM HARDWARE AND SOFTWARE*

Hardware	CPU: Intel® Core Tm i8-880CPU @4.60GHz; RAM: 8.00GB
Software (including tool and standards)	OS: Microsoft windows 10 Enterprise; Open SSL V1.02 Win64; Java compiler; Node.js v8.9.3; Microsoft Visual Studio Professional 2015; Solidity Compiler; Remix Web Browser IDE.

5 CONCLUSION

In education, there is requirement to be trusted beyond the technology. Blockchain has prospective that possibly will offer a system with considerable sincerity and secure database in educational systems. Hence, blockchain can play a part here, as one could picture a variety of teachers and learners that deploys blockchain technology to cut across institutions. This, in our view, will enhance educational data security and reduce insider threats and the research corroborates or improves on the ones earlier done by [19].

6 ACKNOWLEDGMENT

7 REFERENCES

[1] JPonemon Institute LLC (2016). Research Department 2308 US 31 North Traverse City, Michigan 49686 USA 1.800.887.3118 research@ponemon.org Complete copies of all country reports are available at www.ibm.com/security/data-breach.

[2] Eweoya, I., Ayodele, A., Azeta, A. & Olatunji, O. (2019). Fraud prediction in bank credit administration: A systematic literature review. J. Theo. Appl. Info. Tech., 97(11), 3135-3157.

[3] Oladimeji, T.O., Ayo, C.K. & Adewumi, S.E. (2019). Review on Insider Threat Detection Techniques. Journal of Physics: Conference Series, 1299(1), 012046.

[4] Lynda.com (2015): Available at https: // www.toronto publiclibrary .ca/detail.jsp?R=EDB0187.

[5] Diamond, R., & Persson, P. (2016). The long-term consequences of teacher discretion in grading of high-stakes tests (No. w22207). National Bureau of Economic Research.

[6] PC Data &Society Magazine, (2017). Blockchain: The Invisible Technology That's Changing the World. http: // www.pcmag.com/article/351486/ blockchain-the-invisible-technology-thats-changing-the world.

[7] Haber, S. & Stornetta, W.S. (2017). How to time-stamp a digital document. J. Cryptol., 3(2), 99-111.

[8] Turkanovic, M., Holbl, M., Kosic, K., Hericko, M., & Kamisalic, A. (2018). EduCTX: A Blockchain-Based Higher Education Credit Platform. IEEE Access, 6, 5112–5127.

[9] Gogan, M. (2017). Insider Threats as the main Security Threat in 2017," 11 April 2017.

[10] Tschorsch, F. Scheurman, A. Grech, A. & Camilleri, F. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutorials, 18(3), 2084-2123.

[11] Chen, L. Xu, B. Lu, M. and Chen, N. (2018) Exploring Blockchain Technology and its potential Applications for Education. Smart Learning Environment 5:1.

[12] Schneck, P. Tumasjan, A. & Welpe, I. (2018). Disrupting the disruptors: An in-depth analysis of the implications of blockchain technology for today's sharing economy.

Industry Mag. 24(2), 29-32.

[13] Ali, J. (2016). Conceptualizing Intelligent Agents for Educational Institutions: the main provider of smart agents for e-learning ecosystems, Educause Quarterly, 78(4), 200-210.

[14] Kraft, D. (2016). Difficulty Control for blockchain- based consensus systems. Peer-to-Peer Network. Appl. 9(2), 397-413.

[15] Kirill-Kuvshinov, I. Nikiforov, I. Mostovoy, J. Mukhutdinov, D. & Andreev, V. (2018). Disciplina: Blockchain for Education, retrieved from https/bitcoin.org/bitcoinpdf.

[16] Elisa, N. Yang, L. Chao, F. & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving E-government system. Springer, 203–214.

[17] Ahmed, K. Andrew, M. Elaine, S. Wen, Z. & Charalampos, P. (2017). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. University of Maryland and Cornell University Conference Proceedings, 6 (31) 1-31.

[18] Kavak, H., Padilla, J.J., Lynch, C.J. & Diallo, S.Y. (2018). Big data, agents, and machine learning: Towards a data-driven agent-based modeling approach. Simulation Series, 50(2), 125-136.

[19] Yli-Huumo, J., Ko, S., Choi, S., Park, K. & Smolander, K. (2016). Where is current research on blockchain technology? – A systematic review. PloS One, 11(10), 1–2.