"BLOCK CHAIN IN PRIVACYPRESERVATION OF RECORDS IN EDUCATION -A CURRENT RESEARCH TREND"

Meenu Jain[1], Dr. Manisha Jalia[2]

[1]Research Scholar, *Information Technology*, *Banasthali Vidyapeeth* Rajasthan, India, meenu16jain@gmail.com
[2]Associate Professor, Department of Mathematics Applications, *Banasthali Vidyapith*, Rajasthan manishajalia@yahoo.o.in

ABSTRACT:

Nowadays, Block chain is one of the most promising application areas in the field of privacy protection where its scope of applications can almost be limited. The use of the Block series in the field of education is currently of great interest to researchers and scientists, and is the focus of our study. In the age of data security and strict compliance: it has become crucial for education Institutes to store and share their information with other institutes. The main objective of this research is to highlight the existing privacy issues in educational data and use block chain as a solution to resolve these issues. This paper identifies and analyzes relevant books, research papers and articles to determine their classification in the field of education, to find the best ways to use the Block chain in education, and to determine its current and future use.. We have adopted a systematic literature review approach. This survey paper describes various techniques for privacy preservation and block chain as a solution to share data securely.

Keywords

Crpto currency, block chain,,privacy preserving hyper ledger ,privacy preservation ,Nonce, ,distributed, ethereum

Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

INTRODUCTION

Block chain is a type of link list in which every node is connected through cryptographic hash functions. Block chain is a distributed database that stores a growing list of ordered records called blocks.. Each block contains a time stamp to previous block. There is no need of trust all users in the network. It is suitable for theuntrusted environment. Record Keeping and searching is a complete task. It is also called trust machines. All transactions in block chain are immutable. Types of Block chain Public block chain is the block chain with no restrictions. Anybody can access this type of block chain. In private block chain user can do with permission. In this a single organization has a control. Consortium block chain is also permissioned block chain only difference is that in consortium block chain much organization has control the access of block chain. Hybrid block chain is combination of public and private block chain.

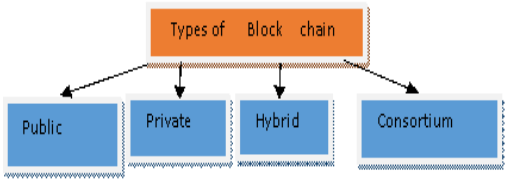

Figure 1

Structure of a Block

There are various fields of header of a block in block chain.

Previous Hash-Each block except the first block contains the hash of previous block.

Timestamp-Each block contains the time when the block was added in the transaction.

Markle Root-It is the root hash of markle tree.

Nonce-Nonce is total iteration before we find a valid transaction.

The contributions of this paper are manifold:

- First, this paper identifies and categorizes the main privacy challenges of shared data.
- It performs a systematic review of the main privacy-preserving techniques used for privacy preservation of educational data.
- In addition, the paper provides a survey of the privacy-preserving model using block chain, comparing them and analyzing the current trends per scenario.

The rest of the paper is organized as follows. Section III overviews main concepts about privacy and block chain, and oversees the privacy preserving. Section IV surveys the main research papers and Privacy solutions finally, the conclusions are drawn in Section V.

I. Challenges in Current Educational Record Storage for sharing data

The challenges confronted by the conventional strategies based on privacy preservation using education data is illustrated below:

- Precise and whole educational data are the precious benefit for individuals. In recent days, the educational data are digitized. However, there exist issues which are not addressed. First one was to attain safe and privacy-preserving storage in educational data and other is regarding educational records sharing to facilitate security in sharing process [1].
- Testing and educational examinations includes huge data shared for dealing with answer sheets, question papers, aptitude tests and quizzes for new admissions. It is important part in e-learning models for evaluating the grades of student. However, the suspicious students may engage themselves in deceptive activities for illegally subverting the examination materials considering answer sheets and question papers [2].
- In [3], locality-sensitive hashing (LSH) technique is adapted for attaining the goal of privacy preservation. However, the classical LSH-based recommendation method suffered from less accuracy wherein the quality of service varies in big range.
- Even though educational data principle persist, usually trader offering education technology has no enticement, while most keep hold of primary data ownership produced with usage of the products. As an issue, it is complex to manage what trader accumulates and how it utilizes the data of student, while many have indistinguishable policies and terms in privacy of data [4].

II Privacy and Block chain

Block chain provides a better solution for privacy preservation.

- There are various consensus algorithm to insure consistency and updating of transaction.
- There are various authentication Protocols to ensure that every valid transaction belongs to a particular node.
- Security: Block chain provides security of the data because all data cannot be tempered.
- Block chain allows users to manage their data and exclude third parties, some [believers] believe in certain features of the technology that violate user privacy. Because block chains are geographically segmented and allow any node to access transactions, user events and actions are transparent.

LITERATURE REVIEW RESEARCH METHODOLOGY

Li, H. and Han, D [1] developed block chain-based storage and sharing method, storage and sharing method, The method integrated storage servers, cryptography and block chain methods for creating consistent ,the block chain technology was utilized for facilitating reliability and security in data storage wherein smart contracts on block chain were utilized for regulating the process of sharing and storage. In precise, the storage servers accumulate obtained educational data in an encrypted format which poses hash information and stored on block chain. The off-chain records using hash information facilitate security in storing data. Furthermore, the Cryptography methods were used in handling messages digital signatures and the records encryption. Hillman, V. and Ganesh, V [4] devised an immutable and publicly verifiable data management system, namely Kratos which facilitated LA and EDM to maintain the privacy of data and empower students with user interface contribution in school. The goal of model was to attain interoperability in data which utilizes LA and EDM to prioritize student agencies with data. The model provides schools and students with irreversible log for inclusive data access that are speckled amongst systems and vendors. The fundamental rules set are described with a group of smart contract amidst education technology and schools. Here, the smart contracts are deployed in public block chain like Bitcoin or Ethereum for time-stamping and notarizing different interactions. Third parties request entrée to data has an exclusive virtual token allocated, which assisted to remain trail of data adjustment, usage and access.

Toapanta, S.M.T *et al.*[6] devised an evaluation of Blockchain to adapt in the process of National Public Data System for Ecuador. The investigative - research and deductive method were employed for analyzing the information from research editorials. The technique employed Security Algorithm, Conceptual Model of National Data System and Mixed Architecture. The method devised that the adaption of Blockchain system was beneficial for public entities to offer improved data security and improved efficiency in the processes demanded by citizens and other public entities.

Amo, D *et al.*[7] devised Blockchain as a technique considering security faults by devising which turns into untrustworthy protocol based on the privacy of data. The Smart contracts automated the agreements of data privacy between the entities like educational institutions and students. Here, other solution was devised in Block chain which utilize smart contracts and cloud that facilitates automation of laws and ensures security to student data. The agreements of privacy, namely Personal Data Broker (PDB), facilitated students for controlling and managing their own data for performing certain operations. However, the method failed to execute PDB in Moodle for saving logs in real-time.

Liu, J *et al.*[19] devised block chain based privacy preserving data sharing (BPDS) for privacy preservation in educational data. The method employed EMRs which was accumulated in cloud and index were retained. The technique helps to reduce the risk of leakage in medical data and simultaneously the index of block chain facilitate EMRs modification. Here, the secure sharing of data can be accumulated automatically based on the specified permissions to access patient records using smart contracts. In addition, the joint-design of CPABE-based access control method and the content extraction signature scheme offered privacy in sharing data. The analysis of security proved that the BPDS were securing for realizing sharing of data in EMR.

Al Omar *et al.*[20] devised privacy preserving mechanism method for healthcare data. The method used the potency of this platform for analysis. The goal of the method was to devise a distributed model for diverting the web platform. In addition, issue over the anonymity was effectively solved using the method, but this method was not applicable with other data.

Wang, Y *et al.* [21] devised blockchain based secure and privacy-preserving EHR sharing

protocol to attain privacy preservation in medical data. The requester of data searched the required keyword via data provider to detect the pertinent EHRs with EHR consortium blockchain and acquire the re-encryption ciphertext using cloud server and acquire authorization of owner. The method utilized conditional proxy re-encryption and searchable encryption for realizing the security of data, access control and privacy preservation. In addition, the authorization was devised with the consensus mechanism for guaranteeing the availability of system. The analysis of security was devised for attaining effective security goals. Moreover, the method was modelled on Ethereum platform, but it acquired high computational complexity.

Baza, M *et al.*[10] devised a method named B-Ride for attaining privacy preservation. Here, the BRide facilitated drivers to provide services related to sharing ride without depending on trusted third party. Here, drivers and riders can discover if it could distribute rides by protecting data. The suspicious users exchange the anonymity offered with blockchain to transmit different requests of ride to detect the best recommend. The B-Ride addresses the issue by of privacy, namely Personal Data Broker (PDB), facilitated students for controlling and managing their own data for performing certain operations. However, the method failed to execute PDB in Moodle for saving logs in real-time.

Liu, J *et al.*[19] devised block chain based privacy preserving data sharing (BPDS) for privacy preservation in educational data. The method employed EMRs which was accumulated in cloud

guaranteeing the availability of system. The analysis of security was devised for attaining effective security goals. Moreover, the method was modelled on Ethereum platform, but it acquired high computational complexity.

Baza, M *et al.*[10] devised a method named B-Ride for attaining privacy preservation. Here, the BRide facilitated drivers to provide services related to sharing ride without depending on trusted third party. Here, drivers and riders can discover if it could distribute rides by protecting data. The suspicious users exchange the anonymity offered with blockchain to transmit different requests of ride to detect the best recommend. The B-Ride addresses the issue by devising a time-locked deposit protocol to share rides by addressing smart contract. Employed EMRs which was accumulated in cloud guaranteeing the availability of system. The analysis of security was devised for attaining effective security goals. Moreover, the method was modelled on Ethereum platform, but it acquired high computational complexity.

Authors	Reference No.	Methods	Advantages	Disadvantages
HONGZHI LI AND DEZHI HAN (2019)	[1]	EduRSS, a block chain-based storage and sharing scheme	Yields high security, effectiveness, and reliability.	Failed to utilize decentralized storage technologies.
Liu, J., Li, X., Ye, L., Zhang, H., Du, X. and Guizani	[19]	Block chain based privacy preserving data sharing for EMRs, called BPDS	Offers strong privacy preservation while sharing data.	More overhead in communication.
Al Omar *et al*	[20]	Block chain Based Privacy Preserving Platform	Preserve patient's data with cryptographic functions	Not compatible with privacy laws.
Hillman, V. and Ganesh, V	[4]	Kratos: an immutable and publicly verifiable data management system	Can facilitate sharing of data in an irretrievable and transparent manner.	The Kratos prototype is not applicable to other data.
Wang, Y *et al.*	[21]	Block chain based secure and privacy-preserving EHR sharing protocol	Can attain the devised goals of security.	Not applicable on Hyper ledger Fabric to run algorithms of data sharing.

Table 1 Summarized Literature Review

CONCLUSION

Block chain can be used to store educational record in trustful manner due to its temper proof and authentication without third party involvement. In this survey various research method for storing and sharing educational records has been discussed and we highlight the major challenges to store educational records and how block chain provides solution for sharing educational records. Finally the future applications, opportunities and challenges of block chains in future and design and develop some pf architecture in area educational record storage.

REFERENCES

[1] Li,an, H and Han. D,"EduRSS:ABlockchain based Educational Records secure storage and sharing scheme,"IEEE Access Vol. 7,pp 179273-179289,2019.

[2] Yan, C., Chen, X. and Kong, Q., "LSH-based private data protection for service quality with big range in distributed educational service recommendations," EURASIP Journal on Wireless Communications and Networking, vol.1, pp.1-9, 2019.

[3] Hillman, V. and Ganesh, V., "A secure, authenticated and publicly verifiable system for educational data using the blockchain," In proceedings of IEEE International Conference on Big Data (Big Data), pp. 5754-5762, 2019.

[4] Chen, X., Liu, H., Xu, Y. and Yan, C., "Robust and Privacy-Preserving Service Recommendation over Sparse Data in Education," Wireless Communications and Mobile Computing, 2019.

[5] Topanga, S.M.T., Gallegos, L.E.M., Baldeon, P.O. and Triviño, F.D.T., "Blockchain Analysis Applied to a Process for the National Public Data System for Ecuador,"2020.

[6] Amo, D., Fonseca, D., Alier, M., GarcíaPeñalvo, F.J. and Casañ, M.J., "Personal data broker instead of blockchain for students' data privacy assurance,"

[7] Information Systems and Technologies, Springer, pp. 371-380, 2019.

[8] Bahaa, A., Sayed, A. and Elfangary, L., "A Secured Interoperable Data Exchange Model," International Journal of Advanced Computer Science and Applications, vol.9, no.1, pp.253-260, 2018.

[9] W. Gong et al., "Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment," Wirel. Commun.Mob. Comp, vol.8, no.3075849, 2018.

[10] Baza, M., Lasla, N., Mahmoud, M., Srivastava, G. and Abdallah, M., "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," IEEE Transactions on Network Science and Engineering, 2019.

[11] Militello, M., Bass, L., Jackson, T. K., and Wang, Y, "How data are used and misused in schools: Perceptions from teachers and principals," Education Sciences, vol.3, pp.98-120, 2013.

[12] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," IEEE Access, vol. 7, pp. 58241-58254, 2019.

[13] Gursoy, M.E., Inan, A., Nergiz, M.E. and Saygin, Y., "Privacy-preserving learning analytics: challenges and techniques," IEEE Transactions on Learning technologies, vol.10, no.1, pp.68-81, 2016.

[14] S. SobithaAhila et al., "Role of agent technology in web usage mining: homomorphic encryption based recommendation for Ecommerce applications," Wirel. Pers. Commun, vol.87, no.2, pp.499–512, 2016.

[15] J. Zhu et al., "A privacy-preserving QoS prediction framework for web service recommendation," in proceedings of 2015 IEEE International Conference on Web Services (ICWS), pp. 241–248, 2015,

[16] L. Kuang et al., "A privacy protection model of data publication based on game theory," Secur. CommunNetw, vol.3486529, no.13, 2018.

Memon, "Authentication user's privacy: an integrating location privacy protection algorithm for secure moving objects in location based services," Wirel. Pers. Commun, vol.82, no.3, pp.1585–1600, 2015.