IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 15, May 2023

Document Verification and Validation using Blockchain

Prof. A. D. Londhe, Dipali Sanjay Chavan, Radhika Natwarlal Dayama, Pratik Prashant Joshi, Prajyot Pradip Pawar
Department of Information Technology,
Smt. Kashibai Navale College of Engineering, Vadgaon (Bk.), Pune, India

Abstract: *The Indian Ministry of Education's data indicate that there are about one million graduates per year. Some of them will continue their education in colleges or high schools, while others will get ready for the workforce. When the students have finished their studies, their numerous stellar performance records, grade transcripts, certificates, etc., will be an essential source of reference for entrance to other schools or positions. When schools produce various awards or certificates, just the names of the schools and the students are mentioned. Due to the lack of an anti-forge mechanism, events that lead to the graduation document being forged are regularly identified. A suggestion for a solution to the problem of document forgery would be the blockchain-based digital document system. The process for issuing digital documents under this system is outlined below. An electronic counterpart of a paper document should be created and added to the database along with any pertinent information. Find the hash value of the electronic file in the interim. The block in the chain system should then have the hash value appended to it. The technology will produce a linked QR-code and an inquiry string code to be attached to the printed document. It will allow the demand unit to use online searches or mobile phone scans to verify the legitimacy of the printed document. Due to the dynamic nature of the blockchain, the technology not only boosts the legality of various paper-based documents but also considerably reduces the likelihood of document loss.*

Keywords: Data Mining, RBAC, Multi cloud data security, Proxy Key generation

REFERENCES

[1] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchainin internet of things: Challenges and Solutions,"arXiv:1608.05187 [cs], 2016. [Online]. Available:http://arxiv.org/abs/1608.05187%5Cnhttp://www.arxiv.org/pdf/1608.05187.pd
[2] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian.IEEE, 2018.
[3] Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Healthcare Data."Proceedings of the Norwegian Information Security Conference. 2017.
[4] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security.Acm, 2006.
[5] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.
[6] Michalevsky Y, Joye M. Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy.
[7] Wu, Axin, et al. "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.
[8] Khan S, Khan R. Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions. Energies. 2018 May;11(5):1154.
[9] Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 15, May 2023

[10] Ouaddah, Aafaf, AnasAbouElkalam, and AbdellahAitOuahman. "FairAccess: a new Blockchain-based access control framework for the Internet of Things." Security and Communication Networks 9.18 (2016): 5943-5964.
[11] Kiviharju, Mikko. "Enforcing Role-Based Access Control with Attribute-Based Cryptography in MLS Environments."
[12] He, Qingsu, et al. "A privacy-preserving Internet of Things device management scheme based on blockchain." International Journal of Distributed Sensor Networks 14.11 (2018): 1550147718808750.
[13] Rahulamathavan, Yogachandran, et al. "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption." 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS).IEEE, 2017.
[14] Wu, Axin, et al. "Efficient and privacy-preserving traceable attribute-based encryption in blockchain." Annals of Telecommunications (2019): 1-11.
[15] Sui, Zhimei, et al. "An Encrypted Database with Enforced Access Control and Blockchain Validation."