IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Security with Blockchain for Electronic Health Records Management System (Decoy- Cloud System)

Dr. K. Velmurugan[1], R. S. Iswarya[2], R. Jayaprithvi[3]
Head, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *The global electronic health record (EHR) industry is predicted to develop at a rapid pace, reaching $39.7 billion by 2022. Access control is a critical tool for managing EHR data to ensure its security and privacy. This study offers a hybrid architecture that uses both blockchain and edge nodes to facilitate access control of EHR data. A blockchain-based controller controls identity and access control regulations and acts as a tamper-proof log of access events inside the architecture. In addition, in combination with the blockchain-based access control logs, off-chain edge nodes store EHR data and apply policies provided in the Abbreviated Language For Authorization (ALFA) to impose attribute-based access control on EHR data. We test the proposed hybrid architecture by measuring the performance of executing smart contracts and ACL policies in terms of transaction processing time and response time against unauthorized data retrieval using the Hyperledger Composer Fabric blockchain.*

Keywords: Attribute-based Access Control, Access Control List, Blockchain, Edge Computing, Hyperledger, Smart Contract.

REFERENCES

[1]. Hao Guo, Wanxin Li, Mark Nejad, Chien-Chung Shen.” Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture” in 2019 IEEE International Conference on Blockchain (Blockchain) Electronic ISBN:978-1-7281-4693-5 Print on Demand (PoD) ISBN:978-1-7281-4694-2 DOI: 10.1109/Blockchain.2019.00015

[2]. M. Aguilera and S. Toueg. “Failure Detection and Randomization: Hybrid Approach to Solve Consensus”. In: SIAM Journal on Computing 28.3 (Jan. 1998), pp. 890–903. ISSN: 0097-5397. DOI: 10.1137/S0097539796312915. URL: https://epubs.siam.org/doi/abs/10.1137/S0097539796312915(visited on 06/20/2018).

[3]. Elli Androulaki et al. “Hyperledger fabric: a distributed operating system for permissioned blockchains”. en. In: ACM Press, 2018, pp. 1–15. ISBN: 978-1-4503-5584-1. DOI: 10.1145/3190508.3190538. URL: http://dl.acm.org/citation.cfm?doid=3190508.3190538 (visited on 05/23/2018).

[4]. Asaph Azaria et al. “MedRec: Using Blockchain for Medical Data Access and Permission Management”. In: IEEE, Aug. 2016, pp. 2530. ISBN: 978-1-5090-4054-4. DOI: 10.1109/OBD.2016.11. URL:http://ieeexplore.ieee.org/document/7573685/ (visited on 05/23/2018).

[5]. Alysson Bessani, Joao Sousa, and Eduardo E.P. Alchieri. “State Machine Replication for the Masses with BFT-SMART”. In: IEEE, June 2014, pp. 355–362. ISBN: 978-1-4799-2233-8.DOI: 10.1109/DSN.2014.43. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6903593 (visited on 05/31/2018).

[6]. Vitalik Buterin. Proof of Stake FAQ. 2016. URL: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ(visited on 05/25/2018).

[7]. Christian Cachin and Marko Vukolic. “Blockchain Consensus Protocols in the Wild”. In: CoRR abs/1707.01873 (2017). arXiv: 1707.01873. URL: http://arxiv.org/abs/1707.01873.

[8]. Calliper: A blockchain benchmark framework to measure performance of multiple blockchain solutions. original-date: 2018-03-20T01:46:34Z. June 2018. URL: https://github.com/hyperledger/caliper (visited on 06/13/2018).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

[9]. Miguel Castro and Barbara Liskov. "Practical byzantine fault tolerance and proactive recovery". In: ACM Transactions on Computer Systems 20.4 (Nov. 2002), pp. 398–461. ISSN: 07342071. DOI: 10.1145/571637.571640. URL: http://portal.acm.org/citation.cfm?doid=571637.571640 (visited on 05/31/2018).

[10]. 111th Congress. "American Recovery and Reinvestment Act of 2009". In: (2009). URL: https://www.gpo.gov/fdsys/pkg/PLAW111publ5/html/PLAW-111publ5.htm (visited on 03/20/2018).

[11]. George F Coulouris, Jean Dollimore, and Tim Kindberg. Distributed Systems - Concepts and Design (5th Edition). Pearson Eduction, May 2011. ISBN: 978-0132143011.

[12]. Centers for Disease Control, Prevention, et al. "HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services". In: MMWR: Morbidity and mortality weekly report 52.Suppl. 1 (2003), pp. 1–17.

[13]. Alevtina Dubovitskaya et al. "Secure and Trustable Electronic Medical Records Sharing using Blockchain". In: arXiv preprint arXiv:1709.06528 (2017).

[14]. European Commission. Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services. Final report and recommendations. 2014. URL: https://ec.europa.eu/health/ehealth/projects/nationallaws_ electronichealthrecords_en (visited on 05/13/2018).

[15]. Ittay Eyal and Emin Gun Sirer. "Majority is not Enough: Bitcoin Mining is Vulnerable". In: arXiv:1311.0243 [cs] (Nov. 2013). arXiv: 1311.0243. URL: http://arxiv.org/abs/1311.0243 (visited on 09/17/2018).

[16]. Juan Garay, Aggelos Kiayias, and Nikos Leonardos. "The Bitcoin Backbone Protocol: Analysis and Applications". In: Advances in Cryptology - EUROCRYPT 2015. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9057. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 281–310. ISBN: 978-3-662-46802-9 978-3-662-46803-6.

[17]. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of Medical Systems, vol. 40, no. 10, p. 218 (8 pages), 2016.

[18]. A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:medrec prototype for electronic health records and medical research data," in Proceedings of IEEE Open & Big Data Conference, vol. 13, 2016, p.13.

[19]. R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, pp. 11 676–11 686, 2018.

[20]. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

[21]. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops. IEEE, 2015, pp. 180–184.

[22]. S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, vol. 6, pp. 38 437–38 450, 2018.

[23]. H. Guo, E. Meamari, and C.-C. Shen, "Multi-authority attribute-based access control with smart contract," In Proceedings of 2019 International Conference on Blockchain Technology (ICBCT 2019). ACM, 6 pages. https://doi.org/10.1145/3320154. 3320164.

[24]. A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2016.

[25]. D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in IFIP International Conference on Distributed Applications and Interoperable Systems. Springer, 2017, pp. 206–220.