Documents

Haddad, A.[a] , Habaebi, M.H.[a] , Elsheikh, E.A.A.[b] , Islam, M.R.[a] , Zabidi, S.A.[a] , Suliman, F.E.M.[b]

E2EE enhanced patient-centric blockchainbased system for EHR management

(2024) *PLoS ONE*, 19 (4 APRIL), art. no. e0301371, .

DOI: 10.1371/journal.pone.0301371

[a] Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[b] Department of Electrical Engineering, College of Engineering, King Khalid University, Abha, Saudi Arabia

Abstract
To secure sensitive medical records in the healthcare clouds, this paper proposes an Endto- End Encryption (E2EE) to enhance a patient-centric blockchain-based system for electronic health record (EHR) management. The suggested system with a focus on the patient enables individuals to oversee their medical records within various involved parties by authorizing or withdrawing permission for access to their records. Utilizing the inter-planetary file system (IPFS) for record storage is chosen due to its decentralized nature and its ability to guarantee the unchangeability of records. Then an E2EE enhancement maintains the medical data integrity using dual level-Hybrid encryption: symmetric Advanced Encryption Standard (AES) and asymmetric Elliptic Curve Cryptography (ECC) cryptographic techniques. The proposed system is implemented using the Ethereum blockchain system for EHR data sharing and integration utilizing a web-based interface for the patient and all users to initiate the EHR sharing transactions over the IPFS cloud. The proposed system performance is evaluated in a working system prototype. For different file sizes between 512 KB to 100 MB, the performance metrics used to evaluate the proposed system were the time consumed for generating key, encryption, and decryption. The results demonstrate the proposed system's superiority over other cutting-edge systems and its practical ability to share secure health data in cloud environments.

Index Keywords
article, data integrity, diagnosis, electronic health record, encryption, health data, human, medical record, open access publishing, blockchain, computer security, electronic health record, health care delivery, patient care; Blockchain, Computer Security, Delivery of Health Care, Electronic Health Records, Humans, Patient-Centered Care

References

- Low, C, Hsueh Chen, Y.
  Criteria for the evaluation of a cloud-based hospital information system outsourcing provider
  (2012) *Journal of medical systems*, 36, pp. 3543-3553.
  Dec; PMID: 22366976

- Poulymenopoulou, M, Malamateniou, F, Vassilacopoulos, G.
  Emergency healthcare process automation using mobile computing and cloud services
  (2012) *Journal of medical systems*, 36, pp. 3233-3241.
  Oct; PMID: 22205383

- Shakeel, T, Habib, S, Boulila, W, Koubaa, A, Javed, AR, Rizwan, M, Gadekallu, TR, Sufiyan, M.
  A survey on COVID-19 impact in the healthcare domain: worldwide market implementation, applications, security and privacy issues, challenges and future prospects
  (2023) *Complex & intelligent systems*, 9 (1), pp. 1027-1058.
  Feb

- Al-Issa, Y, Ottom, MA, Tamrawi, A.
  eHealth cloud security challenges: a survey
  (2019) *Journal of healthcare engineering*, 2019.
  Sep 3; PMID: 31565209

- Xiao, J., Liu, X., Zeng, J., Cao, Y., Feng, Z.
  Recommendation of Healthcare Services Based on an Embedded User Profile Model
  (2022) *International Journal on Semantic Web and Information Systems (IJSWIS)*, 18 (1), pp. 1-21.

- Nguyen, G. N., Le Viet, N. H., Elhoseny, M., Shankar, K., Gupta, B. B., Abd El-Latif, A. A.
  Secure blockchain enabled Cyber-physical systems in healthcare using deep belief network with ResNet model
  (2021) *Journal of parallel and distributed computing*, 153, pp. 150-160.

- Boumezbur, I, Zarour, K.
  Privacy-Preserving and Access Control for Sharing Electronic Health Record using Blockchain Technology
  (2022) *Acta Informatica Pragensia*, 11 (1), pp. 105-122.
  Feb 17

- Pugazhenthi, A, Chitra, D.
  Data access control and secured data sharing approach for health care data in cloud environment
  (2019) *Journal of medical systems*, 43 (8), p. 258.
  Aug; PMID: 31264005

- Rajakumar, MP, Ramya, J, Sonia, R.
  A novel scheme for encryption and decryption of 3D point and mesh cloud data in cloud computing
  (2021) *Journal of Control Engineering and Applied Informatics*, 23 (1), pp. 93-102.
  Mar 26

- Singh, N, Singh, AK.
  Data privacy protection mechanisms in cloud
  (2018) *Data Science and Engineering*, 3 (1), pp. 24-39.
  Mar

- Suresh, D, Florence, ML.
  Securing personal health record system in cloud using user usage based encryption
  (2019) *Journal of medical systems*, 43 (6), p. 171.
  Jun; PMID: 31065802

- Lu, J., Shen, J., Vijayakumar, P., Gupta, B. B.
  Blockchain-based secure data storage protocol for sensors in the industrial internet of things
  (2021) *IEEE Transactions on Industrial Informatics*, 18 (8), pp. 5422-5431.

- Ali, M, Dhamotharan, R, Khan, E, Khan, SU, Vasilakos, AV, Li, K, Zomaya, AY.
  SeDaSC: secure data sharing in clouds
  (2015) *IEEE Systems Journal*, 11 (2), pp. 395-404.
  Jan 13

- Jana, B, Poray, J, Mandal, T, Kule, M.
  A multilevel encryption technique in cloud security
  (2017) *In2017 7th International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 220-224.
  Nov 11 IEEE

- Vinoth, R., Deborah, L. J., Vijayakumar, P., Gupta, B. B.
  An anonymous pre-authentication and post-authentication scheme assisted by cloud for medical IoT environments
  (2022) *IEEE Transactions on Network Science and Engineering*, 9 (5), pp. 3633-3642.

- Sri Vigna Hema, V, Kesavan, R.
  ECC based secure sharing of healthcare data in the health cloud environment
  (2019) *Wireless Personal Communications*, 108, pp. 1021-1035.
  Sep

- Bentajer, A, Hedabou, M, Abouelmehdi, K, Igarramen, Z, El Fezazi, S.
  An IBE-based design for assured deletion in cloud storage
  (2019) *Cryptologia*, 43 (3), pp. 254-265.
  May 4

- de Oliveira, MT, Dang, HV, Reis, LH, Marquering, HA, Olabarriaga, SD.
  AC-AC: dynamic revocable access control for acute care teams to access medical records
  (2021) *Smart Health*, 20, p. 100190.
  Apr 1

- Chen, L, Lee, WK, Chang, CC, Choo, KK, Zhang, N.
  Blockchain based searchable encryption for electronic health record sharing
  (2019) *Future generation computer systems*, 95, pp. 420-429.
  Jun 1

- Michalas, A, Bakas, A, Dang, HV, Zalitko, A.
  MicroSCOPE: enabling access control in searchable encryption with the use of attribute-based encryption and SGX
  InSecure IT Systems: 24th Nordic Conference, NordSec 2019, Aalborg, Denmark, November 18-20, 2019, Proceedings 24 2019, pp. 254-270.
  Springer International Publishing

- Egala, B. S., Pradhan, A. K., Badarla, V., Mohanty, S. P.
  Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control
  (2021) *IEEE Internet of Things Journal*, 8 (14), pp. 11717-11731.

- Mendonca, SN.
  Data security in cloud using AES
  (2018) *Int. J. Eng. Res. Technol*, 7.
  Jan

- Feldman, J, Misenar, S, Conrad, E.
  (2016) *Eleventh Hour CISSP: Study Guide*,
  Syngress; Sep 3

- Azad, TB.
  Understanding XenApp Security
  (2008) *Securing Citrix Presentation Server in the Enterprise*, pp. 259-316.
  Jan

- Thin, TT, Vaspongayya, S.
  Blockchain-based access control model to preserve privacy for personal health record systems
  (2019) *Security and Communication Networks*,
  Jun 25; 2019

Correspondence Address
Habaebi M.H.; Department of Electrical and Computer Engineering, Malaysia; email: habaebi@iium.edu.my

Publisher: Public Library of Science

ISSN: 19326203
CODEN: POLNC
PubMed ID: 38557695
Language of Original Document: English
Abbreviated Source Title: PLoS ONE

2-s2.0-85189174900
Document Type: Article
Publication Stage: Final
Source: Scopus