International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Blockchain-Based Approach to Ensuring the Security of Electronic Data

[1]Sonali D. Patil, [2]Atul B. Kathole, [3]Savita Kumbhare, [4]Kapil Vhatkar, [5]Vinod V. Kimbahune

Submitted: 05/11/2023 **Revised**: 22/12/2023 **Accepted**: 04/01/2024

Abstract-The digitization of conventional medical data poses substantial difficulties for healthcare organizations in the form of electronic health records (EHRs). Doctors and patients alike are used to spending a lot of time querying EHRs for the information they need; however, the data retrieved isn't necessarily relevant to the sought-after one, and access can be denied if that happens. One of the most important parts of the healthcare system is the sharing and keeping of medical records. In the case of a breach, either the confidentiality of patients' information or the accuracy of their medical records would have disastrous consequences. Consequently, it is a top priority to ensure the security of electronic health records. Data integrity, security, and privacy are three areas where modern healthcare infrastructure is infamously lacking in user-friendliness and efficiency. The security and complexity issues may, however, be mitigated with improved electronic health record monitoring and administration. Thanks to the blockchain's decentralized and trustworthy character, this is now a reality in the healthcare industry. The healthcare delivery system is inherently flawed due to issues with data management and the validation and dissemination of information. The main advantage of using blockchain technology for healthcare data management is the improved access it provides to monitoring medications, hospital assets, drug systems, patient information, and so on. Given the critical nature of access to a patient's medical history for dispensing medication, blockchain technology holds great promise for enhancing the present system of healthcare delivery. Consequently, creating a safeguard for medical records based on blockchain technology is of the utmost importance. Last but not least, the performance evaluation shows that the suggested method is more reliable and resilient than the state-of-the-art designs.

Keywords- *Healthcare, HER,Security, Privacy , blockchain.*

Introduction

Electronic health records are less expensive than older, more inefficient ways of keeping patient information. The idea behind it is to give people more agency over their own health data. Encumbered by a walled garden of limited access, users are unable to access EHRs [9]. One sign of how seriously electronic health records take patient privacy is that users are unable to exchange individual health records with one another. Electronic health records (EHRs) must be encrypted in order to be retrievable [10]. In order to improve communication between the different storage devices and the distributed storage systems, the EHR update was applied. The distributed platforms that store this data are becoming more vulnerable to cyberattacks as the number of these systems increases [11]. Some healthcare pharmaceutical and service support big data apps may solicit assistance from third parties or the public at large for management purposes [12]. Malicious attacks and the risks associated with processes, such as unauthorized access and change, can compromise the medical data of susceptible patients. Consequently, safeguarding private health

1Professor, IT Dept.,
Pimpri Chinchwad College of Engineering
Pune, India
2Associate Professor,
Computer Engineering,
Dr. D. Y. Patil Institute of Technology, Pune
atul.kathole1910@gmail.com
3Assistant Professor,
Computer Engineering,
Dr. D. Y. Patil Institute of Technology, Pune
4Associate Professor,
Computer Engineering,
Dr. D. Y. Patil Institute of Technology, Pune
5Professor, Computer Engineering, Dr. D. Y. Patil Institute of Technology, Pune

information during system design requires resolving this issue [13]. The requirements for safety that healthcare and associated systems must fulfil [14].

To improve patient safety and data privacy, the healthcare industry is considering blockchain technology [15]. Electronic health records are securely kept in encrypted medical blocks on the blockchain, ensuring the utmost confidentiality and data integrity [16]. You may achieve your chosen level of security without depending on a third party by utilizing the blockchain, which is inherently decentralized [17]. Some have attempted to build smart cities and homes by incorporating blockchain technology into the design of IoT systems [18]. There are primarily three types of blockchains: consortium blockchains, private blockchains, and public blockchains [19]. Anyone can access the network's transactions and blocks on a public blockchain, including users and miners. As more parties involved in obtaining prior approval to integrate the blockchain are added to the private blockchain, its flexibility is diminished. Enterprises and big corporations can benefit from the consortium blockchain [20].

Protecting sensitive information and original data from unauthorized access requires the use of privacy-preserving measures [21]. Hiding, distributing, converting, and changing sensitive information like electronic health records is the main objective of these strategies in order to prevent data breaches that occur during processing with third-party systems [22]. When considering the amount of work needed to integrate EHRs into the system, it seems like every job in healthcare is difficult. Providers face numerous obstacles in their pursuit of retaining, safeguarding, and validating patient information due to the enormous volume and diversity of health records. One of the biggest problems in healthcare is getting a high-quality, archived medical record when time is of the essence [23]. Interoperability is frequently mentioned as one of the industry's major challenges, and the exchange of health records among providers is also viewed as a key task. Instead of focusing on efficient storage, safe data exchange among providers, managing patient-provider interactions, and quick retrieval, a new system should be designed to tackle these challenges by considering the constraints of securing EHRs [24]. Protecting patients' privacy is a top priority for healthcare providers. Regrettably, there was a lack of protection for reports regarding scans, drugs, microbiological tests, prescriptions, treatment histories, diseases, and patient identification [25]. But permissioned blockchains are private networks that let only registered users access their data. The conventional blockchain method of obtaining medical records also leaves data owners and data users uneasy. This emphasizes the need for a new blockchain-based data paradigm for healthcare administration.

The following are summaries of the most notable enhancements to the proposed model.

By encrypting the data transmission with the help of optimizations techniques, as in our suggested method, we hope to: In order to prevent the compromise of patient privacy and data integrity, a new permissioned blockchain-based EHR security architecture must be developed.

Convergence, encryption time, and decryption time will be measured to see how well the proposed permissioned blockchain-based EHR security paradigm works.

In this section, we will review the remaining parts. Part II reviews the literature on related EHR security ideas and provides critiques. The paradigm for permissioned blockchain-based EHR security is laid out in Section III. Part IV delves into the algorithm that has been suggested. In Part V, we talk about the outcomes and how we interpreted them. Section VI concludes the model development process.

Literature Survey

A. Related Works

Implementing "unhackable" distributed ledger technology, Zhuang et al. [1] have ensured a practical solution for healthcare data management by 2020 through the unique characteristics of blockchain. The smart contract feature allowed for its implementation on the blockchain as a programmable contract that could execute itself. This was created to give individuals complete control over their own medical records while still protecting the confidentiality of their health information. Simulated in great detail using patient-specific medical records, the model's "feasibility, stability, security, and robustness" were carefully examined [1].

In order to provide data security and access control, Niu et al. [2] utilized the ciphertext for attribute encryption in 2020. In this instance, the utilization of a polynomial equation in conjunction with blockchain technology allowed for the creation of keyword associations at will while simultaneously securing the identity of patients. Compared to the previous tactics, the new strategy also shown better retrieval efficiency, according to the study [3].

In 2019, Rajput et al. [4] utilized Hyperledger composer and Hyperledger fabric to integrate the "Emergency Access Control Management System (EACMS)" into the permissioned blockchain. In order to handle potential emergency situations and the allocated time for patients to access their healthcare data in an emergency, the current system has laid down a set of regulations based on smart contracts. The suggested system was evaluated using Hyperledger Composer for its efficacy in relation to response time, privacy, security, and accessibility.

B. Problem statement

The features and difficulties of existing EHRs using blockchain technologies are summarized in Table 1. The resilience, security, stability, and practicability of a smart contract [1] have been guaranteed. The model's capacity to generalize has proven superior. However, this concept necessitates installation at all healthcare facilities. Superior retrieval efficiency and data validity have been secured by the use of ciphertext-based attribute encryption [2]. The proposed model, however, achieves inferior search efficiency. Patients' personal information is safe with BIoTHR [3], and it's also cheap and widely available. Lightweight Internet of Things devices are not used in this model. When it comes to usability, security, privacy, and reaction time, EACMS [4] provides nothing but the best. When compared to more traditional healthcare systems, this concept has proven to be far more effective. On the other hand, more RAM is required. DBDH [5] optimizes delay and throughput and offers top-notch security.

Process carried out for securing electronic health records based on permissioned blockchain

C. System Model of EHR

The design of the suggested technique on the medical platform is informed by the medical institutions that have exchanged information in certain places. Many hospitals and medical practices use encryption software to protect their patients' electronic health records (EHRs). The server administrator needs to be careful to maintain specific keywords in the permissioned blockchain if they want to achieve electronic health record exchange between hospitals. We dissect the six separate components of the system model below [6].

Information Technology Manager: Before anyone may access the system, including doctors, patients, and data users, they need to enrol with the administrator. These system administrators aid in the generation of public and private keys for data users. Furthermore, system administrators usually delegate and revoke the attribute authority.

Since they are the ones really caring for patients, users of an EHR system are its most valuable component. The majority of healthcare facilities have multiple clients connected to their server. These clients are used to keep track of patients' medical history. The restricted blockchain will be informed of the EHR-related keywords by the server administrator [7]. Typically, the server is the one in charge of adding new patients and doctors to the database. When doctors upload their electronic health records (EHRs), the server needs to make sure the clinician is who they say they are.

A patient is required to complete specific documentation upon first visit to a hospital. A patient's "visit token," given to them upon registration, will act as their "pass" to the doctor's office. The treating physician compiles the patient's EHR and saves it as an encrypted file on the server of the hospital. Secure electronic health record vocabulary can be stored on distributed ledgers using the server manager [12].

The creation and encryption of electronic health records (EHRs) using patients' access codes is the responsibility of practitioners in the healthcare business. Doctors also have an additional responsibility to upload the encrypted EHR to the system. Question Poser: Keyword searching in the blockchain sector requires patient-generated searching trapdoors in cases when data consumers or third-party organizations need access to patient data outside of the patient or hospitals themselves [14].

Only healthcare institutions are allowed to use the permissioned blockchain system, and searchers can only see details on which blockchains are involved in the permissioned system. With the permissioned blockchain's data search feature, users can rest assured that all participating servers have logged and broadcasted their transactions.

D. Permissioned Blockchains

Any user, at any time, can join a public chain—also known as a blockchain—and participate in its data reading, transaction sending, and accounting functions. By employing the cryptography of digital currencies such as Bitcoin and Ethereum, public chains encourage participants to compete to verify the data's authenticity. Decentralization is intrinsic to the concept of public chains [15]. When utilizing a permissioned blockchain, every node in the network

is regarded as a permission node, regardless of whether it is a public, consortium, or private blockchain. A number of permissioned blockchains do not include any digital currency scheme since some nodes are designed to process data independently of the system's requirement for currency encryption [16]. Nodes are utilized by permissioned chains to perform tasks such as reading and writing blocks, adding new blocks to the blockchain, and more. More and more companies are utilizing permissioned blockchain networks as their implementation develops. This network distributes members to certain tasks and enforces relevant limitations so that all applications can be processed. It shows the capacity to store medical data and the process for determining permissioned-chain members.

Security Of Ehr Systems Via Meta-Heuristic Cyphers Based On Policy Attributes

E. Proposed Algorithm

Incorporating the HGHO into the proposed permissioned blockchain-based protected EHR paradigm allows for the creation of extremely secure electronic health records. In order to discover the optimal solution more efficiently and avoid the local optimum problem [18], the constructed model uses GOA. But the search agents get into their grooves quite fast, so there's no convergence at the same spot, and the model can only handle a small subset of optimization problems. The HGHO integrates the DHOA with the GOA to discover the optimal solution to the problem of EHR transmission security.

G. Encryption time analysis

Time spent encrypting medical records was compared between the suggested technique and the standard algorithm, as shown in Fig. 1. The suggested Incorporating the deviation-based technique, the generated HGHO updates the final rank of candidates and finds the best answer. As a first step, we approximate the GOA discrepancy using "the solution in GOA without any computations in it that is represented by." The DHOA deviation is also computed and expressed similarly, except that it does not involve any computation. According to Eq. (1), the last promotion occurs in the following way.

$$Pos = Pos + dv_1 + dv_2 \quad (1)$$

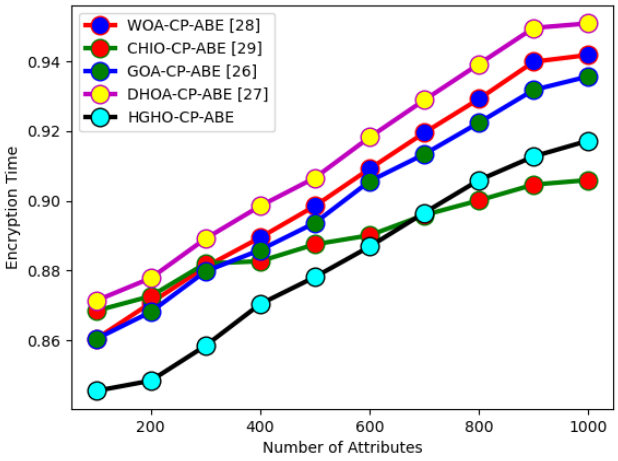
In this illustration, the hunter's role as a potential successor is shown as Xt^{sp}. The fitness of each search agent is then calculated, and the leader and the next in line are updated accordingly until the halting condition is met. The optimal solution has been reached at last.

Results and Discussions

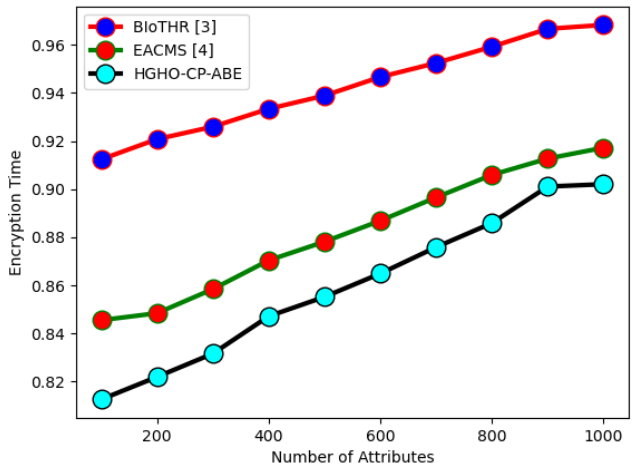
F. Experimental setup

Using Python, we built a permissioned blockchain-based secured EHR model. We ran additional tests to check the system's efficiency, transactional latency, and usage of time. By comparing the developed method to state-of-the-art approaches, an evaluation was carried out to show progress in the blockchain-based EHR transmission model. The built model made use of a 10-person population and an iteration limit of 1000. We compared the proposed approach to some of the most popular ones out there.

HGHO-CP-ABE improves on BIoTHR and EACMS by 12.6% and 13.2%, respectively, indicating that it requires less time for encryption.



(a)

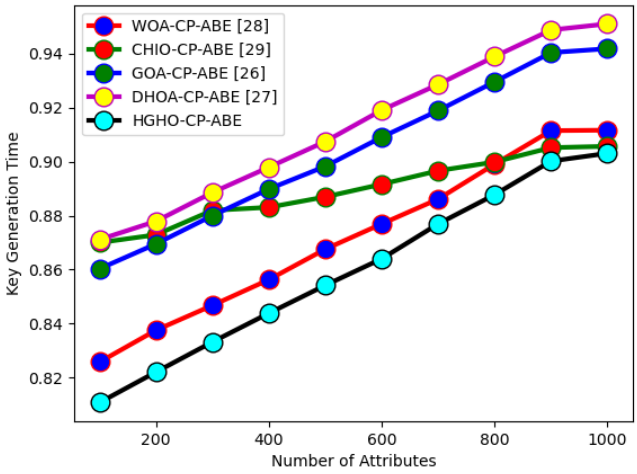


(b)

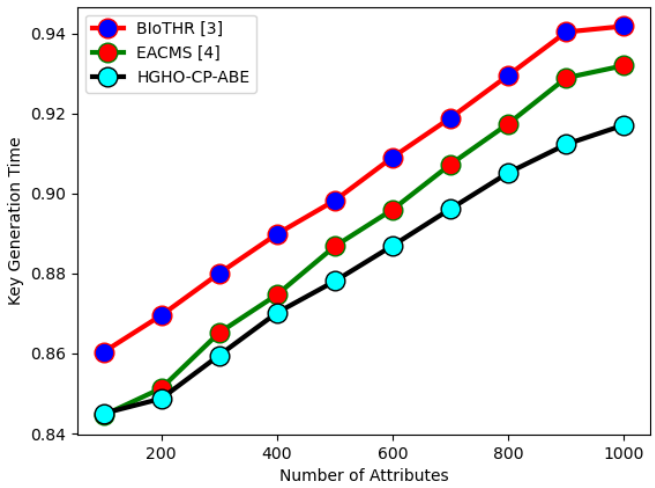
Fig. 1. compares the proposed permissioned blockchain-based secured EHR model to "(a) different heuristic algorithms and (b) existing models" in terms of the amount of time it takes to encrypt and decrypt patient data.

H. Key generation time analysis

The proposed HGHO-CP-ABE-based data encryption method underwent extensive testing using a variety of algorithms and preexisting models, as shown in Fig. 2. The suggested model has increased the security of the EHR system's medical records by 14.5%, 16.7%, 12.3%, and 11.5% compared with existing approaches, respectively, due to the reduced amount of time needed for key generation.



(a)



(b)

Fig. 2. Comparing "(a) alternative heuristic algorithms and (b) existing models with respect to the time required for key generation in the proposed permissioned blockchain-based protected EHR paradigm.

Conclusion

To enhance the security of electronic health records (EHR) kept by hospital patients, this study created a new architecture based on permissioned blockchain technology and an optimization plan. In this case, the created HGHO was used to choose appropriate encryption keys. Thanks to the HGHO-based CP-ABE paradigm, computation, encryption, and cypher text size were all reduced. In terms of encryption efficiency, the results demonstrated that the suggested HGHO-CP-ABE method outperformed BIoTHR and EACMS. This is why the suggested permissioned blockchain-based EHR security

paradigm outshines its predecessors in terms of safety.

Funding: The authors received no funding for this work.

Competing Interests: The authors declare that they have no competing interests.

Data Availability

The following information was supplied regarding data availability: the dataset is available and collected from real life it can be available on demand.

References

[1] Y. Zhuang, L. R. Sheets, Y. -W. Chen, Z. -Y. Shae, J. J. P. Tsai and C. -R. Shyu, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2169-2176, Aug. 2020.

[2] S. Niu, L. Chen, J. Wang and F. Yu, "Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain," IEEE Access, vol. 8, pp. 7195-7204, 2020.

[3] P. P. Ray, B. Chowhan, N. Kumar and A. Almogren, "BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10857-10872, 1 July1, 2021.

[4] A. R. Rajput, Q. Li, M. Taleby Ahvanooey and I. Masood, "EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain," IEEE Access, vol. 7, pp. 84304-84317, 2019.

[5] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei and H. Lu, "Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach," IEEE Transactions on Network Science and Engineering, vol. 9, no. 1, pp. 271-281, 1 Jan.-Feb. 2022.

[6] Usharani Chelladurai & Seethalakshmi Pandian "A novel blockchain based electronic health record automation system for healthcare," Journal of Ambient Intelligence and Humanized Computing, vol. 13, pp. 693–703, 2022.

[7] Gayathri Nagasubramanian, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H. Gandomi, Muthuramalingam Sankayya & Balamurugan Balusamy "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," Neural Computing and Applications, vol. 32, pp. 639–647, 2020.

[8] A. Roehrs, C. A. da Costa, R. da Rosa Righi, S. J. Rigo and M. H. Wichman, "Toward a Model for Personal Health Record Interoperability," IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 2, pp. 867-873, March 2019.

[9] G. Tsang, S. -M. Zhou and X. Xie, "Modeling Large Sparse Data for Feature Selection: Hospital Admission Predictions of the Dementia Patients Using Primary Care Electronic Health Records," IEEE Journal of Translational Engineering in Health and Medicine, vol. 9, pp. 1-13, 2021.

[10] B. Shickel, P. J. Tighe, A. Bihorac and P. Rashidi, "Deep EHR: A Survey of Recent Advances in Deep Learning Techniques for Electronic Health Record (EHR) Analysis," IEEE Journal of Biomedical and Health Informatics, vol. 22, no. 5, pp. 1589-1604, Sept. 2018.

[11] J. Zhang, K. Kowsari, J. H. Harrison, J. M. Lobo and L. E. Barnes, "Patient2Vec: A Personalized Interpretable Deep Representation of the Longitudinal Electronic Health Record," IEEE Access, vol. 6, pp. 65333-65346, 2018.

[12] H. Duan, Z. Sun, W. Dong, K. He and Z. Huang, "On Clinical Event Prediction in Patient Treatment Trajectory Using Longitudinal Electronic Health Records," IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 7, pp. 2053-2063, July 2020.

[13] M. E. Hossain, A. Khan, M. A. Moni and S. Uddin, "Use of Electronic Health Data for Disease Prediction: A Comprehensive Literature Review," IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 18, no. 2, pp. 745-758, 1 March-April 2021.

[14] Atul Kathole , Dinesh Chaudhari “Secure Hybrid Approach for Sharing Data Securely in VANET”, Proceeding of International Conference on Computational Science and Applications pp 217–221, © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[15] Atul Kathole , Dinesh Chaudhari “Securing the Adhoc Network Data Using Hybrid Malicious Node Detection Approach”, Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021) pp 447–457 © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[16] Atul Kathole , Dinesh Chaudhari “Securing the Adhoc Network Data Using Hybrid Malicious Node Detection Approach”, Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021) pp 447–457 © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[17] Atul B Kathole, Dr.Dinesh N.Chaudhari, "Pros & Cons of Machine learning and Security Methods,

"2019.http://gujaratresearchsociety.in/index.php/ JGRS, ISSN: 0374-8588, Volume 21 Issue 4

[18] Atul B Kathole, Dr.Prasad S Halgaonkar, Ashvini Nikhade, " Machine Learning & its Classification Techniques, "International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9S3, July 2019.

[19] Mohammad Moussa Madine, Ammar Ayman Battah, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Yousof, "Blockchain for Giving Patients Control Over Their Medical Records," IEEE Access, vol. 8, pp. 193102-193115, 2020.

[20] X. Liu, Z. Wang, C. Jin, F. Li and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," IEEE Access, vol. 7, pp. 118943-118953, 2019.

[21] Hemant B. Mahajan, Ameer Sardar Rashid, Aparna A. Junnarkar, Nilesh Uke, Sarita D. Deshpande, Pravin R. Futane, Ahmed Alkhayyat & Bilal Alhayani "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," Applied Nanoscience, 2022.

[22] Priti Tagde, Sandeep Tagde, Tanima Bhattacharya, Pooja Tagde, Hitesh Chopra, Rokeya Akter, Deepak Kaushik & Md. Habibur Rahman "Blockchain and artificial intelligence technology in e-Health," Environmental Science and Pollution Research, vol. 28, pp. 52810–52831, 2021.

[23] Arvind Panwar & Vishal Bhatnagar "A cognitive approach for blockchain-based cryptographic curve hash signature (BC-CCHS) technique to secure healthcare data in Data Lake," Soft Computing, 2021.

[24] Azath Mubarakali "Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN (SRHB)Approach," Mobile Networks and Applications, vol. 25, pp. 1330–1337, 2020.

[25] S. Amini, S. Ghasemi, H. Golpira and A. Anvari-Moghaddam, "Coronavirus Herd Immunity Optimizer (CHIO) for Transmission Expansion Planning," IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 2021.