Medical Records Management Using Distributed Ledger and Storage

Samia Anjum(✉), R. Ramaguru(✉), and M. Sethumadhavan

TIFAC-CORE in Cyber Security, Amrita School of Engineering,
Amrita Vishwa Vidyapeetham, Coimbatore, India
cb.en.p2cys19014@cb.students.amrita.edu,
{r_ramaguru,m_sethu}@cb.amrita.edu

Abstract. In the last decade, blockchain technology has seen adoption to infinite domains, health care sector is one of the major domains where there are a greater opportunity and advantage to leverage the benefits of distributed ledgers in storing and securing patient medical records. The Government of India (GoI) is also very keen on digitization in addition to their wider adoption of blockchain technology to serve the citizens by ensuring their privacy and security of personally sensitive . In this paper, we propose a framework for the secure management of patient medical records (PMR) based on the Ethereum blockchain. The PMR is tokenized using the ERC-721 standard which is a Non-Fungible Token (NFT) that can be uniquely mapped to the individual patient. To ensure a higher level of security and non-redundancy, the medical records are stored and maintained in distributed storage like InterPlanetary File System (IPFS); to ensure privacy, the patient's sensitive information is anonymized through a privacy-preserving scheme. To provide complete control of the medical record to individual patients, we have employed a secret sharing scheme with essential share that is owned by the patient. The proposed framework aims to provide correctness and consistency in managing the PMR over its life cycle.

Keywords: Patient medical record · Electronic health record · IPFS · ERC-721 · PACS

1 Introduction

A Patient Medical Record (PMR) is the historical document that maintains the patient's health details like patient's health history, clinical findings, diagnostic test results, pre-and post-operative care, patient's health progress, and prescribed medication, etc. [1]. The medical practitioner can use the information provided in a medical record to understand the patient's present condition and to provide informed care. These records are created, updated, and maintained either by the medical practitioners or by the health care providers. It is the most important part of dispensing medical care to the patient. The need

M. Singh et al. (Eds.): ICACDS 2021, CCIS 1441, pp. 52–62, 2021.
https://doi.org/10.1007/978-3-030-88244-0_6

for maintaining a good medical record includes monitoring the patient, medical research and audit, statistical study, and insurance cases, criminal cases. PMR is important to understand the health condition of the patient at the same time it contains a lot of personal sensitive information that needs to be kept secure and confidential.

The challenges in managing medical records are storage, access permissions, privacy, and security. Hospitals with manual and paper-based medical record systems face numerous challenges like the revision of forms, management of active and inactive records, destruction of records [1]. The Digital India initiative of the MeitY has developed the e-hospital, the e-blood bank, and Online Registration System (ORS) which is a cloud-based application to provide healthcare services to all the citizens across the country [2]. This outlines the importance and the need for digitizing medical records & health care services and the absence of such a system among healthcare providers. Generally, the record is the responsibility of the health care provider, but a copy of the record should be given to the patient when requested. Ownership and maintenance of PMR vary from country to country. The U.S. Federal Law, to protect sensitive patient health information called Health Insurance Portability and Accountability Act (HIPAA) of 1996 outlines that the data within the medical record owned by the patient and the physical form belongs to the organization responsible for maintaining the record. If a patient finds any error in the record, the patient can petition the health care provider to update the correct data. According to Indian Medical Council (IMC) Regulations, 2002, the medical records of the patients should be maintained by medical practitioners for at least a period of three years. Also, they are supposed to keep the patient's data confidential even the details about the patient's personal and domestic life. If the patient or authorized legal personnel make any request for medical records, the medical practitioner is supposed to make such records available within 72 h. If the medical practitioner is found guilty of performing professional fraud, dismissal of the name from the record of the licensed practitioner entirely or for a specified time. Under European Union law, the General Data Protection Regulation (GDPR) is a data protection and privacy regulation. There is a right for patients to access their health records through a subject access request (SAR) according to the GDPR and Data Processing Agreement (DPA), 2018, which can be submitted by the patient or patient-authorized third party. It should be made mandatory to secure the medical record of every patient so that it can't be misused in any manner. If any third party can get the medical records of patients, it's a breach of patient's confidentiality and privacy. The lack of interoperability among various systems, i.e. the patient data held in the systems of different hospitals, is probably the biggest issue with Electronic Health Records. Different systems must be able to interact with each other to provide a clear and complete understanding of the medical history of the patient.

Blockchain Ledger is a data structure similar to a linked list, every block is a container linked to each other cryptographically. Blockchain Technology is a decentralized computation and distributed ledger platform to immutably store

transactions in a verifiable manner efficiently, through a rational decision-making process among multiple parties in an open and public system [3]. Blockchain which is the major technology underlying cryptocurrencies has found its effective use in various domains like Digital Rights Management (DRM) [4], IoT [5], Supply Chain Management, Identity Management, including the health care sector for insurance coverage and securely storing medical records. By adopting blockchain to healthcare record maintenance could help the PMR information be distributed, and prevents intentional and unintentional alteration to the PMR. As in distributed healthcare blockchain network, the PMR can be accessed and updated in real-time with the patient's consent and knowledge.

The rest of the paper is divided as follows. Section 2 outlines the related works of blockchain in health care. In Sect. 3, we have detailed our proposed work with the system architecture and its use-cases. We have concluded and discussed the scope for future work in Sect. 4.

2 Related Works

In this section, we refer and provide an outline to the related works on electronic health records or medical records maintenance through blockchain technology.

Most of the work defines the accessibility of patient's data and interoperability of medical records among hospitals. An electronic medical record storage system using Ethereum blockchain, named MedRec [6] which gives the patient and medical practitioner easy access to the patient's medical records. It incentivizes medical researchers and health care providers by releasing access to aggregate and anonymized medical data. Medchain [7] proposed a similar incentive model based on Proof of Authority (PoA) which incentivizes health care providers to create, validate, and append new blocks with timed-based smart contracts to govern transactions and to control access to the medical records. OmniPHR, a publish-subscribe model using a chord algorithm ensures the balanced, scalable, and elastic service for integrating Personal Health Records (PHRs). OpenEHR standard connects with other health data standards, such as HL7, LOINC, SNOMED-CT, and DICOM, which is the prescribed standard for this model. [8].

Anclie [9], an Ethereum-based solution for privacy-preserving and interoperable healthcare records uses smart contracts along with proxy re-encryption to provide improved access control, data obfuscation, and advanced security. Similarly, a work based on smart contract to provide an access control mechanism and use a privacy-preserving scheme framework called MedBloc [10] using permissioned blockchain. Madine et al. [11] proposed a system to give patients control on the PHR through Ethereum blockchain-based smart contracts. Additionally, it employs InterPlanetary File Systems (IPFS) to securely store and share patients' medical records through trusted reputation-based re-encryption oracles.

3 Proposed Solution

In this section, we present our proposed blockchain-based framework for patient medical records maintenance.

3.1 System Architecture

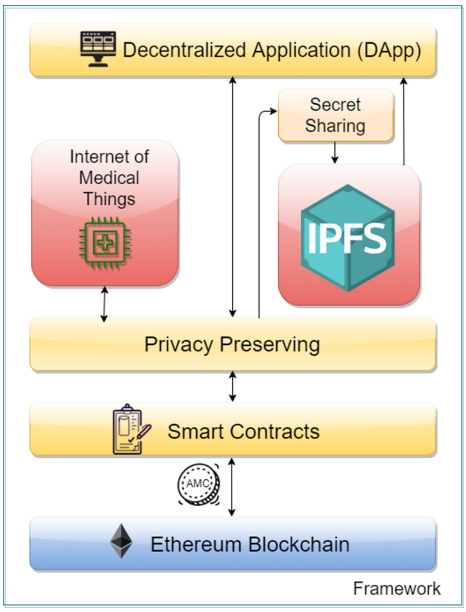

Fig. 1. System architecture

The proposed framework uses the below components as seen in Fig. 1.

Decentralized Application (DApp) is an application that integrates the front-end with smart contracts[12]. The hospital staff and the doctors would use this to register patients and record their medical conditions, and the patients can use them to view their health reports. DApp is created using Ethereum JavaScript API called Web3.js.

Internet of Medical Things (IoMT) also known as Healthcare IoT, consists of medical devices and applications that generate and collect medical information and uploads the data to the healthcare provider's network. Examples of IoMT devices are wearable devices, smart pills with a sensor, etc. [13]. The data from IoMT devices of the patient can be stored in the blockchain using smart contracts by referring to the unique Patient-ID.

InterPlanetary File System (IPFS) is a content-addressing distributed file system for storing and sharing data. It uniquely identifies each file stored by a cryptographic hash value [14]. The medical records that are large like lab and diagnostic reports are securely stored in private IPFS and referenced in the blockchain using their hash value.

Privacy Preserving Module helps in maintaining the privacy of the PMR details that are stored in the private IPFS. We are using the anonymization method in addition to the NLSS Scheme.

Secret Sharing Module splits each medical record (X-Ray, Scan reports, etc.,) that is stored in private IPFS into multiple shares. We are using a Non-Linear Secret Sharing (NLSS) scheme (1,t,n) which splits the given medical record into 'n' shares where 't' shares are required to get back the record with one essential share (secret) held by the patient [15].

ERC-721 Token is an Ethereum standard for Non-Fungible Token (NFT), used to represent unique assets that are not interchangeable [16]. We have used the ERC-721 standard to tokenize the Patient's Medical Record (PMR).

Smart Contracts is a self-executing code deployed and executed on top of blockchain which is agreed upon between two or more parties. They execute automatically when the predetermined conditions are met. We have used solidity programming language for writing smart contracts [12]. Each stakeholder is represented and their operations are handled through a dedicated smart contract.

Ethereum is the second-generation blockchain technology that provides smart contracts functionality which uses a special Virtual Machine called EVM for the execution of the transactions in the blockchain. Ether (ETH) is the native cryptocurrency of the ethereum blockchain. The execution of every operation requires a cost that is measured in terms of Gas [17]. We have used Ethereum-Ropsten Testnet for the development and deployment of our proposed framework.

3.2 Usecases

Hospital and Doctor Registration play an important role in ensuring the authenticity and verification of service of the medical service provider and the medical practitioner. The hospital needs to register itself by providing information regarding their *Government Registration ID, Name, Location, and their Specialization, and Contact Details* as shown in Fig. 2. These details are stored in the blockchain after verification by regulatory bodies like medical associations, which generates a unique *Hospital-ID*.

Once the hospital is registered on the blockchain, the medical practitioners can be on-boarded to the blockchain by the hospital by providing the details like *Registration Number, Name, Specialization, and Contact Details*. The *Doctor-ID* is generated by the smart contract which is then used to uniquely identify the medical practitioner and the actions taken by the corresponding stakeholder. Both these IDs are in turn referenced in the Patient Medical Record.

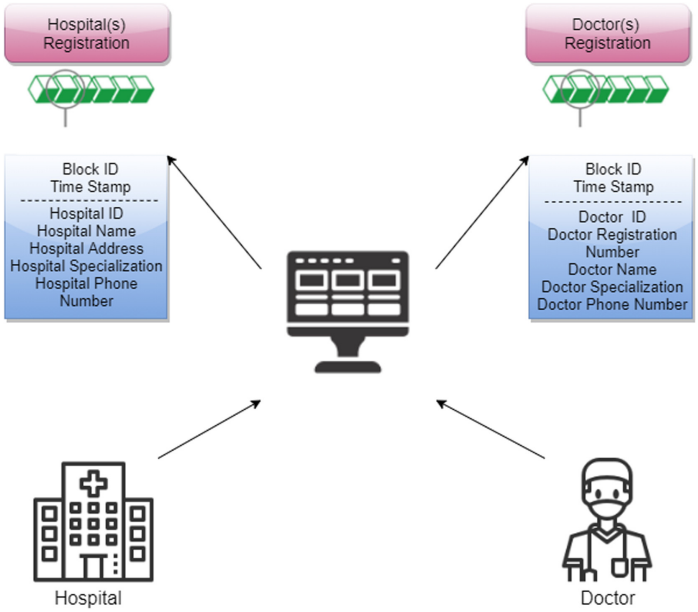

Fig. 2. Hospital and doctor registration

Patient Registration is required the first time when a patient visits the hospital, and for further consultancy, the same *Patient-ID* could be referred. The patient gets registered by the hospital's registration desk. The details captured does not only contains the patient's information but also the attendant's information which would be helpful in case of medical fraud or negligence. The details requested from the patient could include *Name, Age, Gender, Weight, Height, Contact Details* are stored in blockchain along with the details of the attendant (if any).

The attendant details requested to store could include the *Attendant's Name, Phone Number, and Relationship with the patient* as shown in Fig. 3. The smart contract generates a *Patient-ID* that uniquely identifies the patient and is referenced in the Patient Medical Record.

Patient Consulting Medical Practitioner. The patient along with the attendant can visit the medical practitioner for detailed diagnosis and consultancy as shown in Fig. 4. The medical practitioner creates the PMR of the patient based on the information received from the patient's past illness & diagnosis performed and this PMR is mapped to the *Patient-ID*. The PMR of the patient is created based on the date-of-visit and is identified by a unique *PMR-ID* which is the *Patient-ID* appended with the date in the format DDMMYYYY. (Say, a Patient with *Patient-ID* 85437 visits the medical practitioner on 26th January 2021, then the *PMR-ID* generated will be 8543726012021).

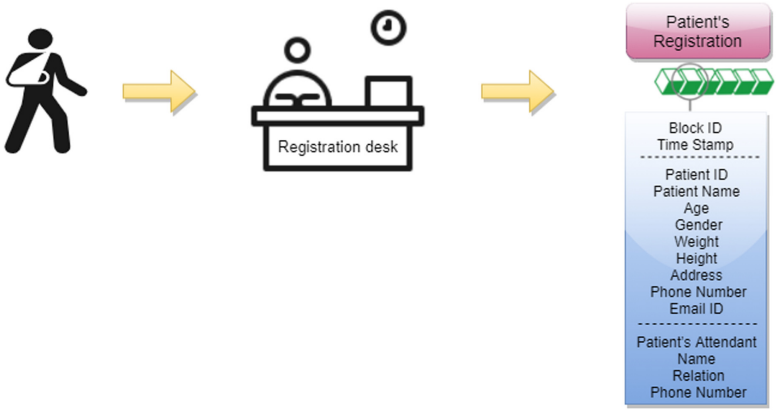

Fig. 3. Patient's registration

The PMR includes details like *Present Illness Details, Past Illness Details, Provisional Diagnosis Details, Treatment Summary, Lab Diagnostics Report, IOMT Device Data, and Insurance Details*. The PMR details are anonymized through the privacy-preserving scheme to ensure the privacy of sensitive information. These details are tokenized using the ERC-721 standard which creates a unique, non-fungible token with *PMR-ID* as *TOKEN-ID*.

Lab Diagnostics is recommended by the medical practitioner for a patient based on the preliminary diagnosis. The diagnosis can be X-Ray Imaging, MRI Scan, CT Scan, Ultrasound, Mammography, etc. As shown in Fig. 5, let us say a patient is advised to go for a digital X-Ray. In general, most health care providers use advanced PACS Systems (Picture Archiving and Communication System) which provide economical storage, retrieval, management, distribution, and presentation of medical images [18]. These medical images are normally stored and transferred in DICOM (Digital Imaging and Communications in Medicine) format. To improve the storage efficiency and to provide additional security, these lab reports are anonymized through our privacy-preserving module and securely split into multiple shares with one essential share that is given to the patient. These shares are stored into private IPFS which is uniquely identified by a *hash-value*, which in turn is referenced in the PMR. The details of the Lab report like *Patient-ID, Date of Capture, Reason, and Observations, IPFS-Hash* are stored in the blockchain.

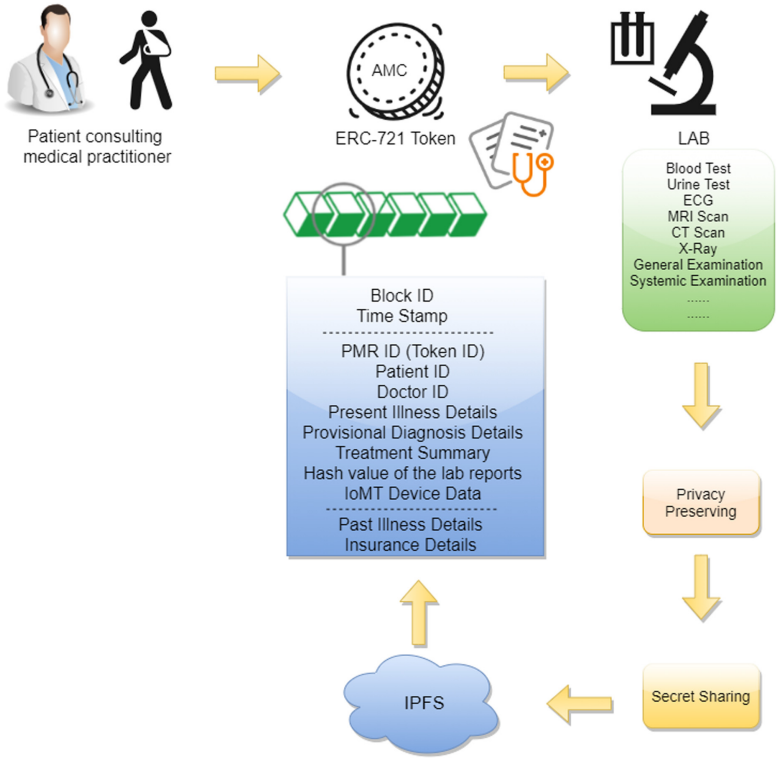

Fig. 4. Patient consulting medical practitioner

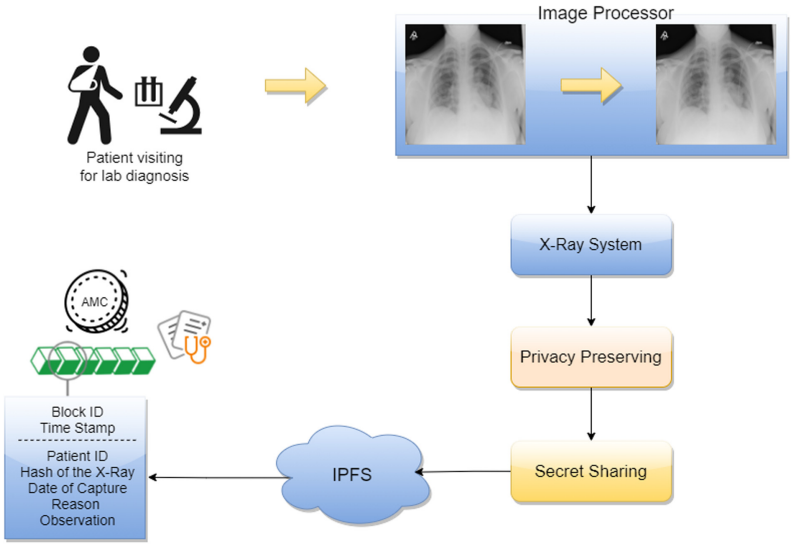

Fig. 5. Lab diagnostics

Patient Visits Different Practitioner. There are situations when a patient would require to take a second opinion from a different medical practitioner or due to the relocation can visit a new practitioner. The medical practitioner, if registered on the blockchain could access the PMR with the consent and the knowledge of the patient. The patient can share the *Patient-ID* and the essential share of the PMR to the medical practitioner to provide access. This essential share is provided in such a manner that it will only be available to the medical practitioner for a specific duration of time and post the duration, the access is revoked automatically. This new medical practitioner can also create a PMR with the findings, observations, and recommendations on the blockchain by referring to the *Patient-ID*.

The project is hosted in GitHub under the name "Patient-Medical-Records" [19].

Discussion. In this section, we draw attention to briefly describe the advantages and limitations of the proposed blockchain framework. Proxy Re-encryption and its variants like Threshold and Time-based proxy re-encryption are used in the existing systems. The key generation and management can incur additional overhead to the system's cost and its operations. We have addressed this through the implementation of a non-linear secret sharing scheme. Besides, we have secured the individual patient's data through isolation of personally sensitive information via private IPFS after preserving the privacy through anonymization. The PMR is considered to be highly sensitive and personal, tokenizing these real-world non-fungible digital assets would enable for easy, efficient, and effective management which is new and unique in our framework. Data Privacy and related laws govern how the data is stored and managed by the data providers, through the usage of private IPFS, and with minimal modification, the proposed work can be made 100% GDPR compliant. As a standalone system, the proposed work may suffer from interoperability issues but if implemented or mandated by suitable authorities and regulations, the system could largely become highly interoperable.

4 Conclusion and Future Work

We have discussed the need for secure Electronic Health Record management and the blockchain technology that could help in addressing the challenges faced. We have also analyzed the existing frameworks and solutions based on blockchain technology. We have proposed a framework based on Ethereum Blockchain to tokenize the PMR using ERC-721 standard, thus enabling the patient to have ownership & control over their medical records through secret sharing, efficient storage through distributed storage IPFS with the privacy-preserving scheme in place. We believe with the proposed framework the PMR information is complete, consistent, correct, and non-redundant over its life cycle.

The proposed blockchain-based Medical Records Management could be extended to a Hospital Management System. The proposed system currently

uses the ERC-721 standard to tokenize the medical records, for efficient usage, this can be replaced with the new Multi-token standard ERC-1155. Additionally, the Machine Learning layer could be added to the proposed framework to perform real-time analysis of the patient record and provide useful insights and can even help in the early detection of abnormal conditions [20]. The new policy proposed by the Medical Council of India to issue a Unique Permanent Registration Number (UPRN) to medical practitioners to maintain one record for one doctor can be implemented in our proposed framework.

References

1. Bali, A., Bali, D., Iyer, N., et al.: Management of medical records: facts and figures for surgeons. J. Maxillofac. Oral Surg. **10**(3), 199–202 (2011). https://doi.org/10.1007/s12663-011-0219-8
2. Digital India Initiative - e-hospital. Available. https://ehospital.gov.in/ehospitalsso/. Accessed on 25 Dec 2020
3. Ramaguru, R., Minu, M.: Blockchain terminologies. NamChain Open Initiative Research Lab, (2021). https://github.com/NamChain-Open-Initiative-Research-Lab/Blockchain-Terminologies. Accessed 25 Dec 2020
4. Kripa, M., Nidhin Mahesh, A., Ramaguru, R., Amritha, P.P.: Blockchain framework for social media DRM based on secret sharing. In: Senjyu, T., Mahalle, P.N., Perumal, T., Joshi, A. (eds.) Information and Communication Technology for Intelligent Systems (ICTIS 2020). Smart Innovation, Systems and Technologies, vol 195. pp. 451–458. Springer (2020). https://doi.org/10.1007/978-981-15-7078-0_43
5. Samal, D., Arul, R.: A novel privacy preservation scheme for internet of things using blockchain strategy. In: Bindhu, V., Chen, J., Tavares, J. (eds.) International Conference on Communication, Computing and Electronics Systems, vol 637, pp. 695–705. Springer, Singapore (2020) . https://doi.org/10.1007/978-981-15-2612-1_66
6. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25–30 (2016). https://doi.org/10.1109/OBD.2016.11
7. Daraghmi, E., Daraghmi, Y., Yuan, S.: MedChain: a design of blockchain-based system for medical records access and permissions management. IEEE Access **7**, 164595–164613 (2019). https://doi.org/10.1109/ACCESS.2019.2952942
8. Roehrs, A., André da Costa, C., da Rosa Righi, R.: OmniPHR: a distributed architecture model to integrate personal health records. J. Biomed. Inform. vol. 71, pp. 70–81 (2017). https://doi.org/10.1016/j.jbi.2017.05.012
9. Dagher, C.G., Mohler, J., Milojkovic, M., Babu, A., Marella, A.: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. **39**, 283–297 (2018). https://doi.org/10.1016/j.scs.2018.02.014
10. Huang, J., Qi, Y.W., Asghar, M.R., Meads, A., Tu, Y.: MedBloc: a blockchain-based secure EHR system for sharing and accessing medical data. In:18th IEEE International Conference On Trust, Security And Privacy in Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand,, pp. 594–601 (2019). https://doi.org/10.1109/TrustCom/BigDataSE.2019.00085

11. Madine, M.M., Battah, A.A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., Ellahham, S.: Blockchain for giving patients control over their medical records. IEEE Access **8**, 193102–193115 (2020). https://doi.org/10.1109/ACCESS.2020.3032553
12. Vitalik. B.: A next-generation smart contract and decentralized application platform. White paper 3.37(2014). https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf
13. Internet of Medical Things: https://healthtechmagazine.net/article/2020/01/how-internet-medical-things-impacting-healthcare-perfcon. Accessed 25 Dec 2020
14. IPFS - Content Addressed, Versioned, P2P File System. https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf. Accessed 08 Dec 2020
15. Aishwarya Nandakumar, P.P. Amritha, K.V. Lakshmy, V.S.T.: Non linear secret sharing for gray scale images. Procedia Eng. **30**, 945–952 (2012). https://doi.org/10.1016/j.proeng.2012.01.949
16. ERC-721 Token Standard. http://erc721.org/. Accessed 08 Dec 2020
17. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum project Yellow Paper. 151.2014 (2014). https://ethereum.github.io/yellowpaper/paper.pdf
18. PACS Systems: Everything You Need to Know About them. https://blog.peekmed.com/pacs-systems/. Accessed 08 Dec 2020
19. Patient Medical Records GitHub Page. https://amrita-tifac-cyber-blockchain.github.io/Patient-Medical-Records/
20. Misha Abraham, A.M., Vyshnavi, H., Srinivasan, C., P.K. Namboori, K.: Healthcare security using blockchain for pharmacogenomics. J. Int. Pharm. Res. **46**(1), 529–533 (2019)