JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Secure Privacy Preserve EHR Framework Using Proof of Work Algorithm of Blockchain Technology

[1]Vanita Ganpatrao Sonkamble, [1]Dr. Vilas Kamble, [1]Suvarna D. Pingle

M.Tech. Research Scholar, Associate Professor, Assistant Professor
[1]P.E.S. College of Engineering Nagsenvan, Aurangabad, India

Abstract: Conventional healthcare systems involve patient registration, medical record production, appointment scheduling, invoicing, and traditional forms of communication. They also rely on manual processes and paper-based record-keeping. Interoperability problems, data silos, and security flaws are some of the difficulties these systems must overcome. These systems are at serious risk from identity theft, data breaches, and cyberattacks. Furthermore, the necessity for upgrades is highlighted by maintenance difficulties, security issues, and inefficiencies in information transmission. Although the adoption of Electronic Health Records (EHR) is a revolutionary change, there are drawbacks. As a remedy, blockchain technology shows up, providing data interoperability, smart contracts, immutability, and decentralized security. Access controls are automated by smart contracts, and security risks are reduced by the decentralized architecture of blockchain technology. Immutability guarantees data integrity, while standardized data formats and a decentralized network improve data interchange. IPFS is used for distributed file storage, Ethereum is used for decentralized apps, and On-chain transactions are used for blockchain updates in the suggested methodology. An authorized agreement between parties is what the smart contract does. This thorough analysis offers a sophisticated grasp of the problems facing traditional healthcare, blockchain-based solutions, and the changing EHR management landscape.

Keywords: Healthcare, EHR, Blockchain, Privacy

I. INTRODUCTION

Centralized databases and paper-based records are the mainstays of traditional healthcare systems [1]. Healthcare organizations maintain digital databases or physical files containing patient data, such as diagnosis, treatments, and medical histories [2]. These systems frequently lack standardized data formats, which leads to data silos and makes it difficult to communicate information seamlessly. Since most healthcare providers implement their own EHR systems, patient data is dispersed across various platforms, creating a fragmented environment. In conventional healthcare systems, patient data is usually managed using manual procedures and paper-based record-keeping. Several essential elements are included in the workflow of these systems [3]:

1. Patient Registration: A patient must go through the registration process to receive healthcare services. Administrative personnel compile demographic and personal data to create a patient file. These days, centralized computer databases or physical files are frequently used to store this data.
2. Medical Record Creation: Medical records are created and kept up to date for every patient by healthcare practitioners. Information like test results, prescriptions, diagnoses, treatment plans, and medications are all included in these records. This data is manually recorded in traditional systems or input into digital systems.
3. Appointment Scheduling: The scheduling of appointments is done by administrative staff, who also oversee the availability of medical specialists and plan appointments according to patient requirements. Phone calls, real appointment books, or simple digital scheduling tools may all be used in this procedure.

4. Billing and Insurance: Manual billing and insurance process management is a feature of traditional healthcare systems. Employees create paper bills, deal with insurance claims, and keep track of finances. This frequently results in mistakes, inefficiencies, and delays in the financial elements of managing healthcare.
5. Communication: Conventional means of communication such as phone calls, faxes, or physical mail are frequently used in the healthcare system, notably when coordinating between various departments or healthcare professionals. This may cause delays and make it more difficult to make decisions quickly.
6. Prescription and Medication Management: Patients write prescriptions on paper and deliver them in person to pharmacies to be filled. Medication administration is dependent on patients' manual record-keeping or recollection.
7. Data Storage: Either physical files or centralized databases are used to keep patient data. To protect privacy and confidentiality, access to these records is usually limited to authorized persons only.

Although these conventional systems have been in use by the healthcare sector for a long time, they have certain inherent drawbacks, such as the possibility of mistakes, inefficiencies in the flow of information, and possible security flaws.

1.1.Traditional Healthcare Systems Working

The main components of traditional healthcare systems are centralized databases and paper-based records. Healthcare organizations maintain digital databases or physical files including patient data, such as diagnosis, treatments, and medical histories. These systems frequently lack standardized data formats, which leads to data silos and makes it difficult to communicate information seamlessly. Since most healthcare providers implement their own EHR systems, patient data is dispersed across various platforms, creating a fragmented environment.

Attacks on Traditional Healthcare Systems

1. **Cyber Threats:** Cyberattacks, such as ransomware, malware, and phishing efforts, can target traditional healthcare systems [4].
2. **Data Breaches:** Because these systems have centralized storage, hackers find them appealing, which increases the risk of unauthorized access and data breaches [5].
3. **Identity Theft:** Identity theft can be committed using patient data, and thieves may use the information they obtain to commit fraud [6].

Other Disadvantages of Traditional Healthcare Systems

1. **Interoperability Issues:** Ineffective data interchange between various healthcare organizations is hampered by the absence of defined data formats and communication methods [7].
2. **Maintenance Challenges:** It can be costly, time-consuming, and complex to upgrade or migrate to new systems [8].
3. **Security Concerns:** Because databases are centralized, there is a greater chance of security lapses that could jeopardize patient privacy and undermine public confidence in the healthcare system [9].

Improvements Required for Traditional Healthcare Systems

1. **Enhanced Interoperability:** standardized communication protocols and data formats to enable smooth data transfer [10].
2. **Improved Security Measures:** Strong cybersecurity protocols to guard against data breaches and illegal access.
3. **Technological Upgrades:** adoption of cutting-edge techniques to facilitate easier system maintenance and scalability.

In order to overcome these obstacles and improve the general effectiveness and security of healthcare administration, a trend toward digitization and the integration of technologies such as blockchain are being implemented. The transition from conventional paper-based health records to Electronic Health Records (EHR) represents a significant change in the administration of healthcare information. Electronic Health Records (EHRs) serve as all-inclusive digital archives that safely store a patient's complete medical history in digital form. There are issues with data security, integrity, and interoperability with the traditional EHR administration architecture, which is based on centralized databases that are managed by healthcare organizations.

The need for safe, open, and interoperable data management systems has increased dramatically as healthcare systems develop. Blockchain is a distributed, decentralized ledger system that eliminates the need for middlemen and guarantees safe, open, and unchangeable transactions. It is made up of a series of blocks, each of which has a list of transactions on it. The data's integrity and immutability are guaranteed by the cryptographic methods used to link and secure these blocks. Because blockchain is decentralized, there is no need for a central authority, which promotes trust among users. Originally designed for decentralized finance, blockchain technology shows promise as a game-changer in the field of healthcare data management [11]. Blockchain's decentralized design, cryptographic security, and trust-building qualities offer a viable remedy for the problems inherent in conventional EHR systems.

Blockchain Usage for the Benefits of Traditional Healthcare Systems

1. **Decentralized Security:** By removing a single point of control, blockchain's decentralized architecture lowers the danger of data breaches and unauthorized access [12].
2. **Smart Contracts:** Self-executing contracts ensure that only authorized parties, such as patients and healthcare professionals, can view and alter particular sections of a patient's medical history by automating and enforcing access constraints [13].
3. **Data Interoperability:** A decentralized network and standardized data formats make it easier and safer for various healthcare providers to exchange data, enhancing patient care continuity and lowering the risk of mistakes.
4. **Immutability:** Because of its immutability, blockchain protects patient records from unwanted changes and tampering, ensuring data integrity.

This thorough material offers insights into the difficulties and weaknesses of conventional healthcare systems as well as possible enhancements. It also highlights the revolutionary role that blockchain technology may play in resolving these problems and presenting a host of benefits for healthcare administration.

II. LITERATURE SURVEY

This careful study evaluates the difficulties associated with the adoption of Electronic Health Records (EHRs), carrying out a comprehensive analysis of tools and resources available to the healthcare industry. It examines the complex process of converting paper-based records to digital formats and highlights the necessity of effective mechanisms. The study examines adoption hurdles for EHRs critically and provides insights on areas that need improvement and targeted attention. It makes a major contribution to the current discussion about improving healthcare data management [14].

The work establishes a new paradigm by strengthening Electronic Health Records (EHR) with the integration of blockchain technology and the Internet of Medical Things (IoMT). It looks at creative solutions with the goal of strengthening data security and resilience in healthcare data management. The report provides a forward-looking perspective on enhancing the reliability and efficiency of electronic health record systems by employing cutting-edge technologies. It provides insightful information about how blockchain-IoMT integration may be used to secure medical data [15]. This study presents a blockchain-based EHR sharing system with an emphasis on the chaincode notion, introducing a permission-based method. It seeks to offer a secure architecture by tackling important problems with access control and data integrity. This research explores new uses of blockchain in healthcare and adds to the continuing efforts to protect and optimize EHR management. It clarifies how permission-based approaches might be used to guarantee safe data exchange [16]. The study explores how various blockchain topologies might improve data security and secrecy while providing a detailed knowledge of the trade-offs. It makes a major contribution to the investigation of various blockchain systems for protecting private medical data, opening the door for well-informed choices [17]. This thorough manual examines issues and fixes related to the implementation of Electronic Health Records (EHR). By navigating the complexities of data management and patient information, it suggests a blockchain-based framework to enhance system efficiency and interoperability. The study adds to the continuing conversation on healthcare data practices by offering insightful information about how EHR deployment techniques are changing [18].

The study places blockchain at the forefront of the change of healthcare and offers a comprehensive analysis of the possible advantages and difficulties of applying blockchain to EHR management. It helps to comprehend how blockchain technology is changing the way that traditional healthcare data procedures are carried out, promoting a more open and safer environment for patient information management. The study considers how blockchain technology could revolutionize healthcare data procedures [19]. This paper presents a secure decentralized healthcare system based on smart contracts within the field of decentralized healthcare systems. It investigates how smart contracts might improve automation and security in the handling of medical data. Through exploring the possibilities of decentralized systems, the study adds to the continuous endeavors to enhance trust and effectiveness in healthcare procedures. It provides information on how smart contracts can be used to secure medical data [20].

The study conducts a thorough survey on interoperability in the management of Electronic Health Records (EHRs) and suggests a blockchain-based framework to overcome current issues. It offers a thorough examination of the obstacles to full interoperability and an assessment of current solutions. The study contributes to the creation of reliable and effective healthcare data management solutions by providing insightful information on methods for enhancing interoperability in healthcare data systems [21]. Specifically addressing interoperability issues with sharing Electronic Health Records (EHR), this study highlights the importance of standardization. It attempts to support the creation of strategies for improving interoperability in healthcare data systems by navigating the challenges of smooth data transmission between various healthcare entities. The study clarifies the significance of standards for effective interchange of healthcare data [22].

The study investigates how blockchain technology can be integrated with Electronic Health Records (EHRs), providing important insights into the possible advantages and difficulties of doing so. The research adds to the continuing conversation about how blockchain technology can revolutionize healthcare data practices by examining the implications of blockchain in this domain. It considers the possible benefits and difficulties of putting blockchain technology to use for safe healthcare data administration [23].

This study offers solutions to help healthcare companies make the shift from paper-based records to digital systems more smoothly by identifying and removing obstacles to Electronic Medical Record (EMR) systems. The paper provides useful ideas to improve the adoption of electronic record-keeping in healthcare while critically analyzing the difficulties encountered throughout this transition. It offers perceptions into methods for getting across obstacles to the implementation of digital health records [24]. This study looks into privacy and security issues with EHRs, offering a thorough examination of the difficulties in protecting private medical data. The study contributes to current efforts to improve the security of electronic health data by offering technology and tactics to resolve privacy issues. It highlights how crucial it is to protect the integrity and security of medical data [25]. Examining Electronic Health Record (EHR) security strategies, this study offers thorough understandings of the methods and tools used to protect medical records in electronic systems. By investigating novel strategies to reduce potential hazards, the study makes a substantial contribution to our understanding of the dynamics involved in improving the security of healthcare information. It highlights how crucial it is to use strong security measures to safeguard private medical information [26]. The landscape of Electronic Health Records (EHR) systems is examined in this article, along with potential and problems related to the digitization of medical records. Through an examination of the challenges associated with switching from conventional paper-based systems to electronic health records, the study offers important new perspectives on the dynamic changes in healthcare information management. It considers the difficulties and possibilities brought about by the digitization of medical records [27].

This research highlights the significance of standardized techniques by identifying and analyzing difficulties associated to achieving total interoperability in sharing Electronic Health Records (EHR). The study intends to contribute to the creation of methods for enhancing interoperability in healthcare data systems by navigating through the difficulties of seamless data sharing among various healthcare entities. It provides information on how crucial standardization is to accomplishing effective healthcare data interchange [28].

This study investigates the use of smart contracts to improve automation and security in the handling of medical data. The study explores the possibilities of smart contracts to enhance security and efficiency in healthcare procedures by aiding in the creation of decentralized healthcare systems. It considers how smart contracts can be used to secure medical data and promote a climate in the healthcare industry that is more open and responsible [29]. This study surveys the state of interoperability in the management of Electronic Health Records (EHRs) and suggests a blockchain-based architecture to overcome obstacles. The research intends to contribute to the development of strategies for enhancing interoperability in healthcare data systems by providing an extensive survey of current options. It provides information about the difficulties in reaching total interoperability in the interchange of medical data [30].

An overview of blockchain's potential applications for protecting the privacy and security of electronic health record systems is given in this study. Through its contribution to the developing field of blockchain applications in healthcare data security, the study sheds light on both possible opportunities and obstacles. It provides a sophisticated perspective on how blockchain technology could revolutionize the protection of private medical information [31]. Decentralized patient-controlled data management using blockchain technology is the main topic of this study. The goal of the project is to improve data ownership and privacy in healthcare information management by highlighting the transfer of authority over health data to individual patients. It considers how blockchain technology could revolutionize current healthcare data procedures and promote a patient-centered approach to data [32]. This study classifies possible areas of exploration and development and provides a thorough review and future research direction for blockchain-based Electronic Health Records (EHR) administration. By pointing scholars and practitioners toward new trends and difficulties, it advances knowledge of the future directions for blockchain-based EHR systems. The study establishes the foundation for continuing conversations about how blockchain technology is developing in the field of healthcare data management [33].

All this work is summarized in Table 1.

Table 1: Research work done on blockchain based EHR Management

Paper	Blockchain Platform Used	Implementation Details	Advantages	Limitations
[14]	Not specified	Enhanced data security, robustness in healthcare data management	Improved data security, resilience	Lack of specific blockchain platform details
[15]	Integrates with IoMT	Strengthening data security in EHR	Forward-looking perspective, potential of blockchain-IoMT integration	Limited information on specific implementation
[16]	Permission-based system with chaincode	Secure EHR sharing system	Improved data integrity, access control	Emphasis on permission-based model, potential scalability concerns
[17]	Ethereum (permissionless) and Hyperledger (permissioned)	Privacy and security preservation	Enhanced confidentiality, data protection	Trade-offs between permissionless and permissioned blockchains not extensively discussed
[18]	Not specified	Framework for interoperable EHR	Improved interoperability, system efficiency	Limited details on specific blockchain platform and implementation
[19]	Not specified	Overall benefits and challenges	Potential transformative role of blockchain in healthcare	Lack of specific implementation details
[20]	Smart contract-based decentralized system	Application of smart contracts for security	Enhanced security, automation in healthcare data management	Focus on decentralized systems and smart contracts
[21]	Proposes a blockchain-based framework	Addressing interoperability challenges	Insights into hurdles, survey of existing solutions	Emphasis on achieving complete interoperability
[22]	Advocates for standardized approaches	Improving interoperability in sharing EHR	Importance of standardization for efficient data exchange	Focus on standardized approaches
[23]	Not specified	Benefits and challenges of blockchain in EHR	Potential advantages and challenges	Lack of specific blockchain platform and implementation details
[24]	Not specified	Strategies for overcoming barriers	Practical strategies for electronic record-keeping	Limited details on specific blockchain platform and implementation
[25]	Not specified	Strategies and technologies for privacy	Enhanced security measures for healthcare data	Comprehensive exploration of security techniques

Paper	Blockchain Platform Used	Implementation Details	Advantages	Limitations
[26]	Not specified	Challenges and opportunities	Insights into digitalization of healthcare records	Lack of specific implementation details
[27]	Advocates standardized approaches	Improving interoperability in sharing EHR	Importance of standardization for efficient data exchange	Emphasis on achieving complete interoperability
[28]	Implementation of smart contracts	Enhancing security and automation	Application of smart contracts for securing healthcare data	Focus on decentralized systems and smart contracts
[29]	Advocates for standardized approaches	Challenges in sharing EHR	Importance of standardization for efficient data exchange	Focus on standardized approaches
[30]	Not specified	Applications of blockchain in EHR security	Insights into blockchain applications in healthcare	Lack of specific blockchain platform and implementation details
[31]	Emphasizes blockchain for decentralized data control	Shifting control to individual patients	Enhanced data ownership and privacy	Focus on patient-centric approach
[32]	Not specified	Categorizes potential areas of exploration	Future research directions in blockchain-based EHR systems	Lack of specific implementation details

III. PROPOSED APPROACH

A Turing-complete programming language is integrated into the Ethereum [34] blockchain network, which may be used to create a variety of decentralized applications, or Dapps. The "ether" coin is what powers the Ethereum network. IPFS (Interplanetary File System) [11] is essentially a file system that functions similarly to BitTorrent [35], allowing you to store files and track versions across time. It is similar to Git in that it keeps track of data over a distributed network. These are blockchain-based transactions that happen. Anyone with a copy of the decentralized ledger can view them since they are stored there. Every time an On-chain transaction takes place, the blockchain network is updated. On-chain transactions can proceed quickly when there is little transaction volume. The agreed-upon, verified contract, complete with all required details, is represented by the smart contract. Its logic draws implications for any situation that might occur under a contract.

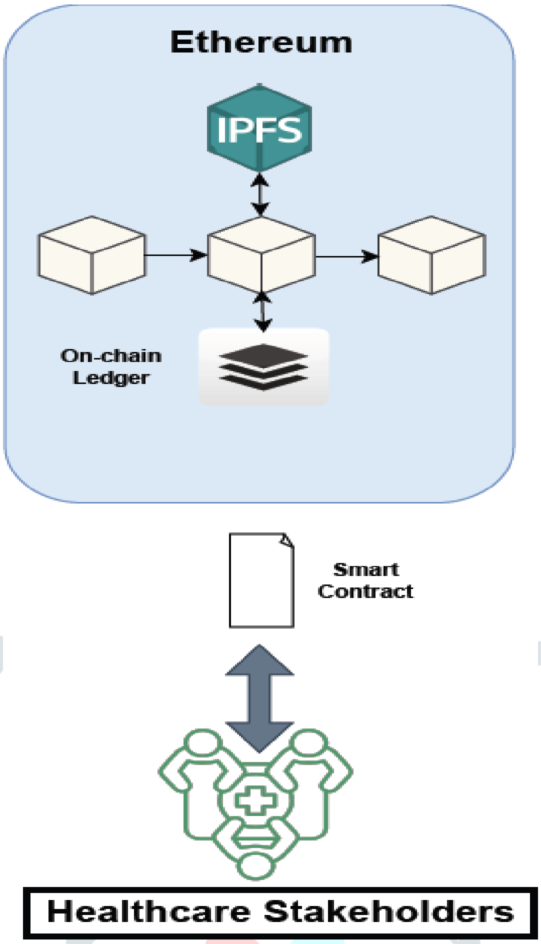

Fig 1. Proposed Architecture

IV. Conclusion

The difficulties that conventional methods confront are revealed by a thorough examination of established healthcare systems and the incorporation of blockchain technology for the management of Electronic Health Records (EHRs). Vulnerabilities in traditional healthcare systems include cyber threats, data breaches, and interoperability problems since they rely on paper-based records and centralized databases. These flaws call for advancements in technology generally as well as in interoperability and security protocols. Blockchain appears to be a game-changing technology that can improve established healthcare systems since it is decentralized and impervious to manipulation. A more safe and effective healthcare data management system is made possible by its immutability, decentralized security, smart contracts for automatic access controls, and data interoperability. A review of the literature dives deeper into the state of the field, showcasing research that combines blockchain with the Internet of Medical Things (IoMT), suggests permission-based systems for exchanging electronic health records, and investigates blockchain architectures that operate on two platforms. These studies offer insightful information about the possible advantages and difficulties of implementing blockchain technology in the healthcare industry. The suggested method makes use of IPFS for decentralized file storage, Ethereum for blockchain implementation, and on-chain transactions for blockchain ledger updates. In order to create legally binding agreements between parties, smart contracts are essential. To sum up, the integration of blockchain technology into healthcare systems provides improved security, transparency, and efficiency in the management of patient data while addressing current issues. The suggested method lays the groundwork for patient-centered, decentralized data management, opening up new possibilities for the development of healthcare information systems.

V. REFERENCES

[1] J. Bajwa, U. Munir, A. V. Nori and B. Williams. "Artificial intelligence in healthcare: transforming the practice of medicine". Future healthcare journal. vol. 8. no. 2. pp. e188-e194. Jul. 2021. 10.7861/fhj.2021-0095.

[2] R. Raziansyah, M. N. Ifansyah, M. R. Pertiwi and K. P. Reviagana. "PENGUATAN PENGISIAN DOKUMEN REKAM MEDIK SECARA ELEKTRONIK PADA PETUGAS KESEHATAN DI RSD IDAMAN BANJARBARU". Selaparang. vol. 7. no. 2. pp. 1089-1089. Jun. 2023. 10.31764/jpmb.v7i2.15134.

[3] B. A. Aufa, I. S. Renindra, J. S. Putri and M. I. Nurmansyah, "An application of the Unified Theory of Acceptance and Use of Technology (UTAUT) model for understanding patient perceptions on using hospital mobile application.".

[4] S. Thakral and A. Vaish. "CYBER SMART: PROTECT THE PATIENT; PROTECT THE DATA ON ELECTRONIC MEDICAL RECORD". International journal of technical research & science. pp. 13-17. Jan. 2022. 10.30780/ijtrs.v07.i01.004.

[5] A. H. Seh et al.. "Healthcare Data Breaches: Insights and Implications". Healthcare. vol. 8. no. 2. pp. 133-133. May. 2020. 10.3390/healthcare8020133.
[6] Judson, T., Haas, M., & Lagu, T. (2014). Medical identity theft: prevention and reconciliation initiatives at Massachusetts General Hospital. *The Joint Commission Journal on Quality and Patient Safety*, *40*(7), 291-AP1.
[7] R. Sonkamble, S. Phansalkar, V. Potdar and A. M. Bongale. "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR". Institute of Electrical and Electronics Engineers. vol. 9. pp. 158367-158401. Jan. 2021. 10.1109/access.2021.3129284.
[8] C. S. Kruse, C. Kristof, B. F. Jones, E. L. Mitchell and A. Martínez. "Barriers to Electronic Health Record Adoption: a Systematic Literature Review". Journal of Medical Systems. vol. 40. no. 12. Oct. 2016. 10.1007/s10916-016-0628-9.
[9] D. Freeze, "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021".
[10] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere and S. P. Mohanty. "Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems". IEEE Transactions on Engineering Management. vol. 67. no. 4. pp. 1363-1376. Nov. 2020. 10.1109/tem.2020.2989779.
[11] D. Dimitrov. "Blockchain Applications for Healthcare Data Management". Healthcare Informatics Research. vol. 25. no. 1. pp. 51-51. Jan. 2019. 10.4258/hir.2019.25.1.51.
[12] W. J. Gordon and C. Catalini. "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability". Computational and Structural Biotechnology Journal. vol. 16. pp. 224-230. Jan. 2018. 10.1016/j.csbj.2018.06.003.
[13] M. Sookhak, M. R. Jabbarpour, N. S. Safa and F. R. Yu. "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues". Journal of Network and Computer Applications. vol. 178. pp. 102950-102950. Mar. 2021. 10.1016/j.jnca.2020.102950.
[14] Aguirre, R. R., Suarez, O., Fuentes, M., & Sanchez-Gonzalez, M. A. (2019). "Electronic Health Record Implementation: A Review of Resources and Tools." Cureus. DOI: 10.7759/cureus.5649
[15] Han, Y., et al. (2022). "Blockchain Technology for Electronic Health Records." PMC. DOI: 10.1016/j.jbi.2021.103992
[16] Tanwar, S., et al. (2020). "Blockchain-based electronic healthcare record system for..." ScienceDirect. DOI: 10.1016/j.jksuci.2021.02.033
[17] Kiania, K., et al. (2023). "Blockchain-based privacy and security preserving in..." Springer. DOI: 10.1007/s11042-023-14488-w
[18] Reegu, F. A., et al. (2023). "Blockchain-Based Framework for Interoperable Electronic..." MDPI. DOI: 10.3390/su15086337
[19] Onik, M. M. H., et al. (2019). "Blockchain in Healthcare: Challenges and Solutions." ScienceDirect. DOI: 10.1016/j.future.2019.11.048
[20] Raj, A., & Prakash, S. (2022). "Smart Contract-Based Secure Decentralized Smart Healthcare System." IJSI. DOI: 10.4018/ijsi.315742
[21] Sonkamble, R., et al. (2021). "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain-Based Framework." IEEE Access. DOI: 10.1109/access.2021.3129284
[22] Bhartiya, S., Mehrotra, D., & Girdhar, A. (2016). "Issues in Achieving Complete Interoperability while Sharing Electronic Health Records." Procedia Computer Science. DOI: 10.1016/j.procs.2016.02.033
[23] Shahnaz, A., Qamar, U., & Khalid, A. (2019). "Using Blockchain for Electronic Health Records." IEEE Access. DOI: 10.1109/access.2019.2946373
[24] McDonald, C. J. (1997). "The Barriers to Electronic Medical Record Systems and How to Overcome Them." JAMIA. DOI: 10.1136/jamia.1997.0040213
[25] Keshta, I., & Odeh, A. (2021). "Security and privacy of electronic health records: Concerns and challenges." Egyptian Informatics Journal. DOI: 10.1016/j.eij.2020.07.003
[26] Kruse, C. S., Smith, B., Vanderlinden, H., &Nealand, A. (2017). "Security Techniques for the Electronic Health Records." Journal of Medical Systems. DOI: 10.1007/s10916-017-0778-4
[27] McDermott, D. S., Kamerer, J. L., & Birk, A. T. (2019). "Electronic Health Records." International Journal of Cyber Research and Education. DOI: 10.4018/ijcre.2019070104
[28] Toledo, P. D., et al. (2006). "Interoperability of a Mobile Health Care Solution with Electronic Healthcare Record Systems." DOI: 10.1109/iembs.2006.259339
[29] Shi, S., et al. (2020). "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey." Computers & Security. DOI: 10.1016/j.cose.2020.101966
[30] Bhartiya, S., Mehrotra, D., & Girdhar, A. (2016). "Issues in Achieving Complete Interoperability while Sharing Electronic Health Records." Procedia Computer Science. DOI: 10.1016/j.procs.2016.02.033
[31] Toledo, P. D., et al. (2006). "Interoperability of a Mobile Health Care Solution with Electronic Healthcare Record Systems." DOI: 10.1109/iembs.2006.259339
[32] Makhdoom, I., et al. (2022). "Enabling Decentralized Patient-Controlled Data Management through Blockchain Technology." Sensors. DOI: 10.3390/s22052050
[33] Zekri, A., et al. (2023). "Blockchain-based Electronic Health Records Management: A Comprehensive Review and Future Research Direction." ResearchGate. DOI: 10.13140/RG.2.2.10358.72642
[34] Available Online: https://ethereum.by/en/what-is-ethereum/ (Accessed on 25th February 2024)
[35] L. Guo, S. Chen, Z. Xiao, E. Tan, X. Ding and X. Zhang. "A performance study of BitTorrent-like peer-to-peer systems". IEEE Journal on Selected Areas in Communications. vol. 25. no. 1. pp. 155-169. Jan. 2007. 10.1109/jsac.2007.070116.