Blockchain-Driven Healthcare Systems: Future Trends and Implications

Sampada Bhatt [1], Prof. Ranjan Thakur [2], Prof. Sachin Mahajan[3]

[1]MTECH Researcher, JIT Borawan
[2,3] Computer Science & Engg. Department, JIT Borawan

---***---

Abstract - This Paper focuses on developing blockchain technology into healthcare presents a transformative solution to some of the industry's most critical challenges, including data security, privacy, interoperability, and transparency. This thesis explores the potential of blockchain as a decentralized, tamper-proof system to securely manage sensitive patient information, streamline healthcare processes, and enhance trust among stakeholders. By analyzing blockchain's foundational principles—distributed ledger systems, cryptographic security, and consensus mechanisms—the research highlights its capacity to address systemic inefficiencies and improve data management in healthcare. The focus is on creating secure, immutable records that empower patients and reduce administrative overhead.
A proposed system architecture utilizing blockchain technology is outlined, featuring components like a Blockchain Handshaker, smart contracts, and a public blockchain network to ensure data integrity. The operational workflow demonstrates how transactions are securely validated, recorded, and shared in a decentralized ecosystem, offering a robust alternative to traditional data management systems.

***Key Words*:** Blockchain Technology ,Healthcare System, Data Security, Electronic Health Records (EHRs), Decentralized Systems, Smart Contracts, Data Interoperability,Privacy Protection, Scalability in Blockchain

1.INTRODUCTION

This Blockchain is a decentralised and public digital ledger that records transactions on many computers so that no record involved can be altered retroactively without altering any blocks afterwards. Blockchain is verified and linked to the preceding 'block,' forming a long chain. After all, Blockchain is the name of the record. As any transaction is registered and checked publicly, Blockchain provides a good deal of accountability. When entered, no one can modify all the information written in the Blockchain. It serves to demonstrate that the data is actual and unchanged. In Blockchain, data are maintained on networks instead of a central database, improving stability and showing its proneness to be hacked. Blockchain offers a fantastic forum to develop and compete with traditional companies for modern and creative business models.

Blockchain helps marketers to maintain an overview of the products used in medicine. Health and pharmaceuticals will get rid of counterfeit medications using Blockchain technologies, enabling tracing of all these medicines. It helps discover the cause of falsification. Blockchain can guarantee the confidentiality of patient records; when medical history is developed, Blockchain can also store it, and this record cannot be modified. This decentralised network is used with all commodity hardware in the hospital. Researchers allow computing estimates for therapies, medicines, and remedies of diverse illnesses and disorders using the resources saved by these devices [4,5].

Blockchain is a distributed ledger network that adds and never deletes or modifies records without a common consensus. A Blockchain hash's value depends on a cryptographic hash that connects newly added information block records with each data block. The distributed Blockchain ledger architecture ensures that data is not processed in any centralised venue, making it accessible and accountable to all network users. This decentralised system avoids a single attack, strengthening and securing the system. It facilitates better control of health records and patient care by minimising twice the amount of medical practice and monitoring, saving both practitioners and patients time and resources. The patient will watch where their information goes and achieve it by keeping health records on a blockchain.

1.1 Need of Blockchain in Healthcare?

Blockchain is a distributed ledger system that keeps track of transactions in a database consisting of blocks that are connected by their hash value to resemble a chain. Blockchain technology is a suitable fit for the healthcare systems because of its multiple features:

- **Secure:.** A blockchain is a network of securely connected blocks. Any changes to the data in a block must be approved by the majority of other nodes in the network in order for it to be added to the blockchain.
- **Decentralized:.** A node in the blockchain network is not required to know or trust any other node in the network. Every node in the network has an identical copy of the data as every other node. The majority of the network's member nodes will reject any changes performed to a member's ledger.
- **Self-correcting:.** When information in one of the network's blocks is altered, the other nodes examine their own blocks and cross-reference one another to identify the errors.
- **Distributed:.** Independent computers record, share, and synchronise transactions in their individual electronic ledgers through the use of blockchain, a distributed ledger[6].

1.2 Blockchain's Advantages for the Healthcare

1. **Securing Patient Data:.** The most important aspect of the healthcare industry is safeguarding patient data.

Inaccurately altering patient data might make it difficult for physicians and hospitals to diagnose a condition or issue with a patient. A hack of more than 176 million medical records occurred between 2009 and 2017. The bank and credit card details were taken by the hackers, who then utilised them for illegal activities. Blockchain makes it considerably simpler and more safe to access patient data since it is distributed, unchangeable, and tamper-proof.

2. **Supply Chain Management for Medical Drugs:.** Hospitals do not manufacture pharmaceuticals or medicines. Worldwide, pharmaceutical businesses and labs manufacture them. Depending on each nation's demands, these medications are further delivered. What would happen if someone tampers with the medications when they are being transported across the nation? Therefore, the medical supply chain needs to be visible to importers and exporters and impenetrable to tampering. This issue is mitigated by blockchain thanks to its tamper-proof, decentralised, and transparent properties. Every point of transit for the medicine, from point of origin to destination, will be recorded into the blockchain once a distributed ledger has been established, ensuring transparency throughout the whole transportation process.

3. **Single Longitudinal Patient Records:** All patient records will be added to the blockchain ledger as the technology is essentially a chain of blocks. Machine learning and artificial intelligence may be used to anticipate the disease depending on the patient's next visit by analysing records such as lab test results, treatment costs, and disease history. By evaluating these precompiled records, hospitals are able to provide their clients with savings. Additionally, it can help in learning patient indices, meticulously streamlining documents, and avoiding expensive errors.

4. **Optimizing the supply chain:** Ensuring the genuine origin of medical supplies is a major problem in the healthcare industry to guarantee the genuineness of pharmaceuticals. The food products can be tracked from the point of manufacture to each point in the supply chain, thanks to blockchain technology. This makes the products that may be purchased fully visible and transparent. This may help businesses better anticipate demand, optimize supply, and boost consumer confidence all while utilizing artificial intelligence.

5. **Medicine Traceability:** The most trustworthy, secure method for tracking each drug back to its source is blockchain technology. Each block of data with medication-related information will have a hash value associated with it. This hash value guarantees that no tampering has occurred with the contents. Every authorized party may see the transactions on the blockchain. By scanning the QR code, consumers of medicines may verify the legitimacy of the items they have purchased and obtain all the information they want, including the manufacturer's details.

6. **Decentralized medical record storage:** Versioned file data may be stored in decentralized storage settings thanks to the interplanetary file system (IPFS). To make sure that every file version is the same, the filesystem generates a single hash called the base configured IED description. Users may access data on websites using the hash that the IPFS returns, but since blockchain files are immutable and websites change often, DNS would need to be updated after each update. By translating site addresses to DNS, IPFS hence resolves this issue.

7. **Update Drug supply chain management:** Blockchain is a great tool for controlling and tracking the flow of medicine supplies because of its security, dependability, and decentralized storage. It contributes to the development of a reliable vendor network that improves patient safety. Blockchain unifies all the procedures, including manufacturing, packing, shipping, and warehousing data, into a single, securely recorded, unchangeable record.

8. **Better clinical trial recruitment:** A blockchain based on Ethereum has been developed by researchers to replicate the recruiting method. The resultant blockchain-based solution preserves trial participants' privacy while enabling access to trial data by all researchers.

9. **Enhances electronic health record systems:** Digital health records are produced and maintained by various medical establishments. By connecting electronic health records and distributing record ownership across all parties involved, blockchain solves issues with accessibility, interoperability, and verification.

10. **Blockchain systems make secure remote monitoring healthcare IoT devices:** By storing personal data on the blockchain as a unique hash function, blockchain cryptography guarantees that only authorized parties can access it. Any changes made to the source data will result in a new hash function, which can only be decoded into the source data with a specific set of cryptographic keys. Patient data is almost hard to tamper with once it is posted on the blockchain ledger (as a hash function) since doing so would need access to all stored copies.

Because blockchain is decentralized, instead of passing via a centralized server, as most IoT connections do now, devices may communicate directly with one another. This makes DDoS and man-in-the-middle assaults extremely difficult to execute.

2. Blockchain

The Blockchain technology is decentralized; material contributed to the network is not governed by a single body. Rather, the entries that are added to the blockchain are decided upon via a variety of consensus methods in a peer-to-peer network. Persistence is another important aspect of blockchain technology. The distributed ledger, which is kept across several nodes, makes it very hard to remove items after they have been approved for inclusion on the blockchain.

Blockchains provide audit and traceability by creating a chain of blocks that connects each subsequent block to the preceding one by including a copy of the latter's hash. Each leaf value (transaction) in the Merkle tree [7] created by the transactions in the blocks may be validated against the known root. By just keeping the tree's root on the blockchain, this allows the tree structure to confirm the accuracy of the data. Figure 1 gives an illustration of this fundamental structure.

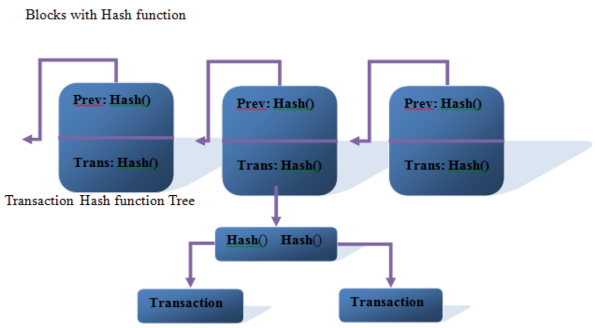

Fig1. Blockchain fundamental

2.1 Blockchain Structure

A lockchain network's transaction records are stored in a series of blocks called a blockchain. Assume the following four transactions: A, B, C, and D, as shown in Figure 2. Each block in the transaction consists of a block header and a block content.

The following is included in the block header [8]:

- Block version: describes validation criteria that are based on a collection of blocks.
- Parent block hash: this holds the hash value corresponding to the block before it.
- Merkle tree root hash: the block-wide hash value of each transaction.
- Timestamp: the current timestamp expressed in seconds.
- N-Bits: a condensed version of the current hashing target.
- Nonce: a 4-byte field that typically has a starting value of 0 and grows with each hash computation.

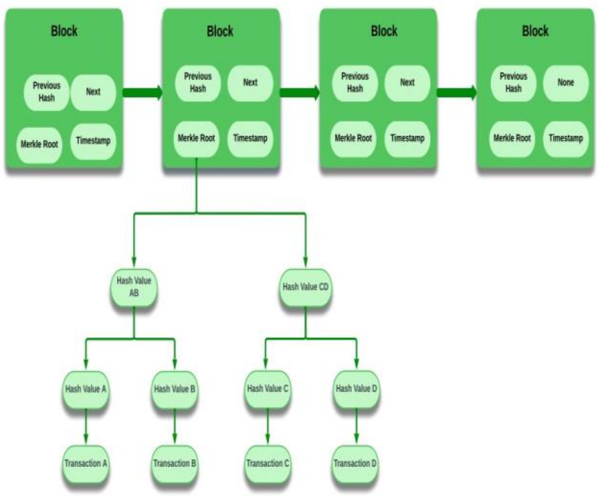

Fig. 2 Blockchain structure and its components

2.3 Smart Contracts

Smart contracts are essentially tiny computer programs that are kept on a blockchain and that, when certain circumstances are met, will carry out a transaction. Consequently, a smart contract is usually expressed as follows: "transfer X to Y if Z occurs." A smart contract is self-executing; that is, once the instructions are written to a blockchain, the transaction will take place automatically when the appropriate conditions are detected, with no further actions required by the parties to the transaction or other third parties. This is in contrast to a regular contract, where parties must execute the agreement after reaching an understanding for it to take effect.

Stated in various ways, smart contracts are computer protocols designed to enable, confirm, or enforce contract execution. Smart contracts are fundamentally similar to a set of if-then expressions that are applied to a transaction's specifics [10]. A smart contract's operation is depicted in Figure 3 [11]. While adopting smart contracts has many advantages, the two main ways to boost digital efficiency by doing away with the need for middlemen are by lowering transaction costs and enhancing transparency.

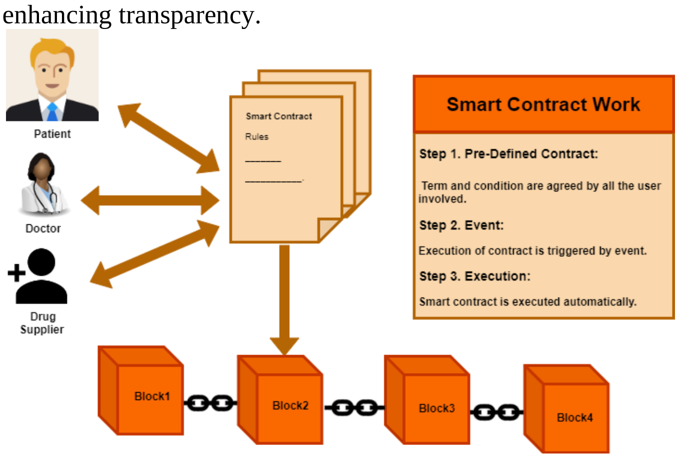

Fig 3 Blockchain Smart Contracts

3. Proposed architecture

This Research proposed architecture for a tamper-proof, Electronic Health Record (EHR) management system utilizing blockchain technology. The architecture is illustrated in Figure 4.1 Our proposed system consists of four main components: the user application, blockchain handshaker, and the public blockchain network. Each of these components is described below:

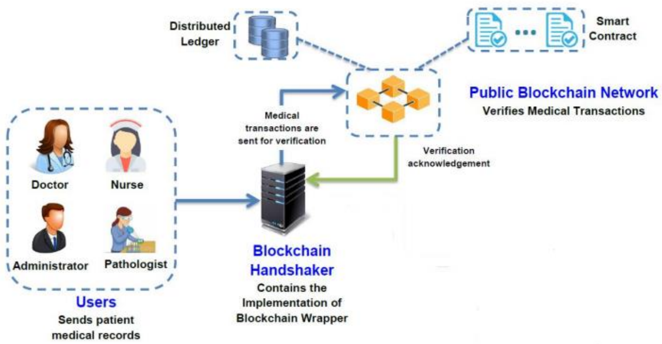

Fig.4 Architecture of Electronic Health Record using Blockchain

1. User application:

The user application is a software module that serves two primary functions. First, it provides user interfaces tailored to different roles within the system. In our design, users such as doctors, nurses, system administrators, and pathologists each have distinct roles, and the user application customizes the interface according to these roles. Second, the user application generates an initial transaction (TI) based on user-inputted data (e.g., patient blood pressure) and system-generated information (e.g., timestamp). This transaction is then sent to the blockchain handshaker for verification. In essence, the user application acts as the intermediary, linking users to the blockchain handshaker for transaction processing.

2. Blockchain Handshaker

The Blockchain Handshaker (BH) is a central component of our proposed architecture. It serves as an intermediary that connects the user application, the EHR system, and the public blockchain network. BH consists of three sub-components:

1. Transaction Template Manager (TTM),
2. Transaction Generator (TG), and
3. Transaction Validator (TV).

Each of these sub-components is described as follows:

• Transaction Template Manager (TTM): This sub-component stores a set of predefined transaction templates designed for the blockchain network. These templates are created by the system administrator based on the specifications of the blockchain platform and the attributes defined in the corresponding smart contracts.

• Transaction Generator (TG): The TG takes an initial transaction (TI) from the user application and builds a blockchain transaction (TC) based on one of the templates from the TTM. It performs the mapping between the initial transaction and the appropriate template in TTM.

• Transaction Validator (TV): The TV is the core of the Blockchain Handshaker, managing interactions between the user application, the blockchain network, and the EHR system. It receives the initial transaction (TI) from the user application, sends it to the TG for processing, and waits for the corresponding blockchain transaction (TC) to be generated. Once the TC is returned by TG, the TV sends it to the blockchain network for validation. If the network validates the transaction, the validated transaction (T'I) is sent back to TV. If the validation is successful, an acknowledgment (ACK) is sent to the database to store the transaction in the database. If validation fails, an ACK indicating an invalid transaction is returned, and the transaction is stored for future audit purposes.

3. Public Blockchain Network

In our proposed architecture, we utilize a public blockchain network (e.g., Ethereum). This network consists of several key components: blockchain nodes, a distributed ledger, and smart contracts.

• Blockchain nodes act as miners within the network and are responsible for maintaining the blockchain in accordance with the consensus mechanism. These nodes receive transactions and validate them based on the rules defined in the smart contracts. Once a transaction is validated, the data is grouped into blocks and added to the distributed ledger. After validation, the public blockchain network sends an acknowledgment to the Transaction Validator (TV) in the blockchain handshaker, indicating whether the transaction is valid (true) or invalid (false).

5. Implementation

A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

I. Smart Contracts :A smart contract is a computer program or a transactional Protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement. The objectives of smart contracts are the reduction of need in trusted intermediators, arbitrations and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions.

II. Ethereum:Ethereum is a decentralized, open-source blockchain with smart-contract functionality. Ether. (ETH) is the native cryptocurrency of the platform. After Bitcoin, it is the second-largest cryptocurrency.

III. Third Party System:This is an off-chain centralised system or server where all the keys can be stored. The Data is encrypted with the help of an encryption algorithm called AES (Advanced Encryption Standard) and the key is generated using an cryptographic hash function called SHA-256 (Secure Hash Algorithm 2).

5.1 Deployment of the Blockchain Network

Ganache acts as a local blockchain emulator, essential for testing and deploying smart contracts. Install Ganache and choose the "Quick Start" option to initialize the local blockchain.

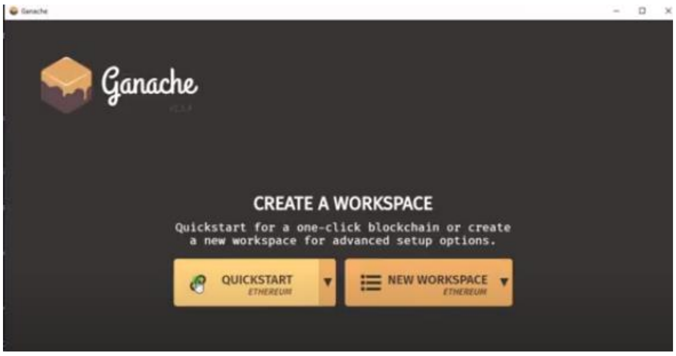

Fig 4. Ganache

MetaMask is a browser extension functioning as an Ethereum wallet. It enables interaction with the blockchain network. After installation, create an account, ensuring it is configured to connect to Ganache's blockchain.

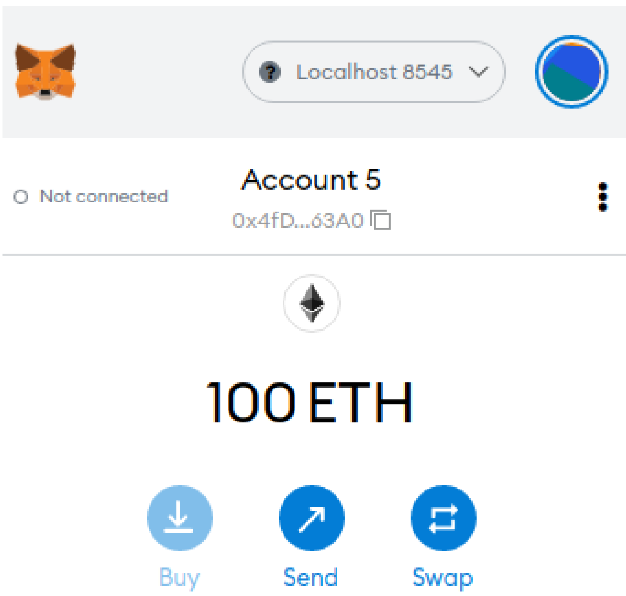

Fig. 5. MetaMask

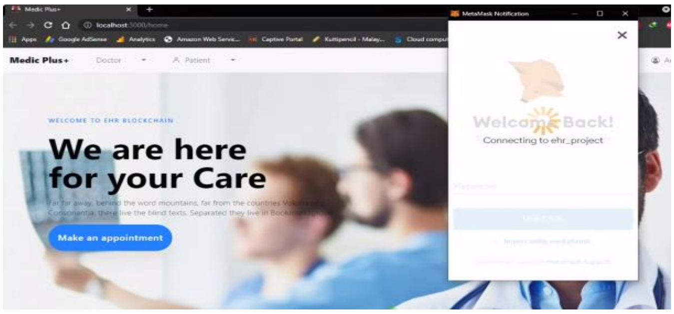

Fig. 6 Snap short

6. CONCLUSIONS

The integration of blockchain technology in healthcare represents a transformative approach to addressing some of the industry's most persistent challenges, including data security, interoperability, transparency, and efficiency. By leveraging the decentralized, immutable, and transparent nature of blockchain, healthcare systems can establish a robust framework for managing sensitive patient data, streamlining administrative processes, and enhancing trust among stakeholders.

This technology enables patients to regain control of their medical information, ensuring privacy while granting selective access to authorized parties. Furthermore, blockchain facilitates secure and traceable transactions in clinical trials, drug supply chains, and insurance claims, reducing fraud and inefficiencies. By adopting smart contracts, healthcare organizations can automate processes, lower administrative burdens, and improve overall operational efficiency.

References

ACKNOWLEDGEMENT

The heading should be treated as a 3rd level heading and should not be assigned a number.

REFERENCES

1. G. Moona, M. Jewriya, R. Sharma, "Relevance of dimensional metrology in manufacturing industries", MAPAN 34 (2019) 97–104.
2. M.H. Kassab, J. DeFrannco, T. Malas, Giuseppe Destefanis , V.V. Neto, "Exploring research in Blockchain for healthcare and a roadmap for the future", IEEE Trans. Emerg. Top. Comput. (2019), 1-1.
3. U. Chelladurai, S. Pandian, "A novel blockchain based electronic health record automation system for healthcare", J. Ambient Intell. Humanized Comput. (2021).
4. Abid Sultan, Muhammad Sheraz Arshad Malik ,Azhar Mushtaq (2018), "Internet of Things Security Issues and their Solutions with Blockchain Technology Characteristics: A Systematic Literature Review". American Journal of Computer Science and Information Technology , 6, 27.
5. Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) An Overview of Blockchain
6. Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data , Honolulu, HI, 25-30 June 2017, 557-564.
7. Timothy, L. (2017) Blockchain for Transportation: Where the Future Starts. White Paper Blockchain for Transportation, a Trimble Company, Sunnyvale, CA.
8. IAB Tech Lab (2018) Blockchain Technology Primer, Version 1.0.
9. Winter Green Research (2018) Blockchain Market Shares, Market Strategies, and Market Forecasts, 2018 to 2024. WinterGreen Research, Inc., Lexington, MA.
10. Grech, A. and Camilleri, F. (2017) Blockchain in Education. Publications Office of the European Union, Luxembourg.
11. PwC (2018) Fourth Industrial Revolution for the Earth Series: Building Block (Chain)s for a Better Planet.
12. Jović, I., Husnjak, S., Forenbacher, I. and Maček, S. (2019) Innovative Application of 5G and Blockchain Technology in Industry 4.0. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems , 6, No. 18.
13. Toshniwal, B., Podili, 1281 P., Reddy, R. J., & Kataoka, K. (2019). Pacex: Patient-centric emr exchange in healthcare systems using blockchain. In 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0954– 0960).
14. Huang, J., Qi, Y. W., Asghar, M. R., Meads, A., & Tu, Y.-C. (2019). Medbloc: A blockchain-based secure ehr system for sharing and accessing medical data. In 2019 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) (pp. 594–601).
15. Rahman, M. S., Khalil, I., Mahawaga Arachchige, P. C., Bouras, A., & Yi, X. (2019). A novel architecture for tamper proof electronic health record management system using blockchain wrapper. In Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure BSCI '19 (p. 97–105). New York, NY, USA:ACM.
16. Daraghmi, E.-Y., Daraghmi, Y.-A., & Yuan, S.-M. (2019). Medchain: A design of blockchain based system for medical records access and permissions management. IEEE Access,164595–164613.
17. Kim, J. W., Lee, A. R., Kim, M. G., Kim, I. K., & Lee, E. J. (2019). Patient-centric medication history recording system using blockchain. In 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM) (pp. 1513–1517).
18. Jabbar., R., Krichen., M., Fetais., N., & Barkaoui., K. (2020). Adopting formal verification and model-based testing techniques for validating a blockchain-based healthcare records sharing system. In Proceedings of the 22nd International Conference on Enterprise Information Systems - Volume 1: ICEIS, (pp. 261–268).
19. Abdul Rahoof, T. P., & Deepthi, V. R. (2020). Healthchain: A secure scalable health care data management system using blockchain. In D. V. Hung, & M. D´Souza (Eds.), Distributed Computing and Internet Technology (pp. 380–391).
20. Tith, D., Lee, J.-S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthcare Informatics Research,
21. Huang, H., Sun, X., Xiao, F., Zhu, P., & Wang, W. (2021). Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. Journal of Parallel and Distributed Computing, 148 , 46–57.
22. Akhter Md Hasib, K. T., Chowdhury, I., Sakib, S., Monirujjaman Khan, M., Alsufyani, N., Alsufyani, A., & Bourouis, S. (2022). Electronic health record monitoring system and data security using blockchain technology. Security and Communication Networks, 2022