A Review on Blockchain-Based Electronic Health Record (EHR) System for Secure Data Storage

Vandani Verma and Garima Thakran

1 Introduction

Cryptography is the underlying foundation of the blockchain. The upsurge of blockchain technology as a trustworthy and transparent mechanism for storing and distributing data is opening up new possibilities for addressing serious private information, safety, and data breaches in a variety of fields, including healthcare. Messages were written in codes thousands of years ago to protect them from enemies, and this is where cryptography comes in. Numerous research papers were published in the 1980s and 1990s that theorized the use of cryptography in accordance with secure data chains for the creation of digital currencies. In 1982, David Chaum [1] proposed the digital cash and blind signatures that allow someone to sign a document and prove their ownership while at the same hiding the information in the document. In 1990, David founded DigiCash which created an untraceable digital currency [2] using cryptography, private and public keys, and signatures. Later, DigiCash was declared bankrupt in 1998. In 1997, Adam Back developed hash cash, a proof-of-work algorithm for reducing email spam. Before sending an email, the sender had to prove they had solved a computer puzzle. This consumed computing power and resources, increasing the cost of sending bulk spam emails. He described it more formally in a 2002 paper [3]. In 1998, Nick Szabo [4] proposed a decentralized digital currency called "bit gold." This included proof-of-work blended with a network of computers that recognized the proof-of-work as legitimate and incorporated it with a time and date into the next puzzle. Bit gold was never a real currency; it existed only in theory. In 1998, Another paper published by Wei Dai [5] illustrated the groundwork for cryptocurrencies, together with Bitcoin, and it is cited in Satoshi Nakamoto's Bitcoin paper. It was the work during the 1980s to 2000s that laid the groundwork for Bitcoin and the blockchain. In 2008, Satoshi Nakamoto [6] in his paper outlined

V. Verma (✉) · G. Thakran
Department of Mathematics, Amity Institute of Applied Sciences, Amity University, Noida, India
e-mail: vandaniverma@yahoo.com

B. K. Roy et al. (eds.), *Cryptology and Network Security with Machine Learning*,
Algorithms for Intelligent Systems, https://doi.org/10.1007/978-981-99-2229-1_2

the creation of Bitcoin and blocks of transactions linked in chains. In 2009, When Satoshi Nakamoto developed the Bitcoin network and the initial blockchain, Bitcoin became a lot more than an idea. This first blockchain was a key aspect of Bitcoin, restricting double spending and serving as a distributed public ledger for all Bitcoin network transactions. Nakamoto also mined the first block on the Bitcoin network known as the "genesis block."

In a blockchain, all the records (transaction record or a medical record) are stored in blocks. When a block is filled with data, it is added to the chain of previous blocks, and a new block is created for the data entry. Hence, blocks added to the blockchain cannot be altered as they are permanently added to the blockchain and any change in the block is to be notified to each of the previous user. Blockchain technology's scalability and decentralized implementation make it a valuable tool for enhancing record-keeping processes. Many studies [7–9], proposed changes and developed new approaches to improve and apply a variety of use cases, including smart contracts, supply chain management, and healthcare.

2 Characteristics of Blockchain

- Immutability: It's an essential feature of the blockchain that ensures the integrity of the digital ledger by creating immutable ledgers. Previously, in money transfer, the transaction details can be easily altered, and it also needed a trusted third party to guarantee the integrity of information. In, blockchain, each block relates to the previous block. Thus, minimizing any possibility of block alteration.
- Decentralization: The blockchain network is decentralized, i.e., it doesn't need any trusted third party or governing authority to look after all the transactions. Thus, decentralized distributed ledger solves the issue of single point failure and need of third party to maintain the integrity of transactions.
- Enhanced Security: Every information in the blockchain is hash based which is irreversible, so once the can transaction details are hashed and added to the block and published, it becomes impossible to tamper with the transaction details without changing the hash value. So, is someone wants to alter data, he must corrupt every block in the network.
- Distributed Ledgers: Every information about a transaction and the participant are shared among all the participants involved in that transaction. Thus, any malicious change in transaction can be easily discovered and makes it transparent/temper proof.

3 Motivations for Blockchain-Based EHR System

EHRs typically include a patient's medical history, personal data like weight and age, results of lab tests, and other things. Verifying the confidentiality and privacy of patient information is crucial. The implementation of healthcare systems in practice is fraught with significant difficulties. The risk of insiders disclosing patient personal information to another organization exists. The key goals for the implementation of secure blockchain-based EHR system are as privacy, security, confidentiality, integrity, availability, auditability, accountability, authenticity, and anonymity. Existing blockchain-based research in the healthcare industry focuses on the primary components listed below to achieve the objectives: Data storage, Data sharing, Data audit, and Identity manager.

3.1 Data Storage

Using blockchain technology is one option to increase security in the EHR system. However, given that blockchain may be public information, there may also be possible privacy concerns for all the encrypted data contained in the public ledger. Personal information is encrypted using public key cryptography within the MediBchain blockchain, which is supported by a healthcare platform. The use of cryptography is not entirely secure. For a select few limited devices, cryptography has a high machine cost. The public ledger's stored encryption text could be cracked by malicious attackers. The loss of a personal key renders data control impossible for the bearer. The EHR systems will use the blockchain to transport medical data. If the data is stored directly in the blockchain, the computational cost and storage load are raised due to the fixed and constrained block size. To solve the storage problem, we use an off-chain store design, where huge volumes of original, encrypted data are stored using reliable third party systems. It can ease the strain on the blockchain's storage system and increase data confidentiality and privacy.

3.2 Data Sharing

The healthcare industry depends on a wide variety of knowledge sources that are documented in various systems including hospitals, clinics, labs, etc. To be used for medical purposes, healthcare information must be stored, retrieved, and altered by various healthcare providers. Interoperability of EHR is the degree to that EHR is known and employed by totally different suppliers as the browse every other's information. It can be classified into three levels: Syntactic interoperability, symmetric interoperability, cross-domain interoperability. One of the main obstacles is the absence of standardized interoperability standards for data sharing between completely unrelated companies. The risk of a single point attack and data leakage exists with centralized systems. Patients also cannot keep their own personal information in their hands to communicate with a trusted third party. It ought to result in unauthorized use of personal information by some businesses. Additionally, different organizations that lack trust in their collaborations do not appear to be willing to exchange information, which could affect the event of knowledge sharing. Protection of users' data and privacy must be ensured, and ownership of knowledge must be returned to them. Secure access control will promote data sharing. One of the typical strategies to promote data sharing is for secure access control mechanisms that only authorized entities may access. The act of granting authorization to legitimate users so they can access the protected resources is known as share data authorization. This mechanism's access policies are focused on who is doing what action, on what data item, and for what reason.

3.3 Data Audit

Healthcare systems rely on audit log management as a security measure. Since there are some outliers that happened as a result of third parties abusing their power or acting dishonestly. When conflicts emerge, the audit log can be used as evidence to hold users responsible for their transactions with patient records. The blockchain's ledger and smart contracts can offer immutable control for all access requests to establish accountability and traceability. The lack of or manipulation of clinical trials, medical research, and pharmaceutical data severely undermines patient and healthcare provider trust. Blockchain's transparency and accountability can monitor past trial logs and prevent the storage of only the positive results of clinical studies. Audit log offers trustworthy proof of criminal behavior to improve the security of access control models. By obtaining knowledge about interpersonal relationships and hospital work processes, it also helps to improve healthcare services.

3.4 Identity Manager

Membership verification is the initial stage in ensuring the security and privacy of any system before gaining access to any resource. To ensure that certain permissions are granted to data requesters with valid identities, identity authentication is always carried out in the beginning. Users have undergone authentication, biometric authentication, and identity verification before sharing any data. Public key infrastructure, which relies on dependable third parties, is frequently utilized and is based on public key cryptography methods. To manage individual data in the EHR system and to guarantee identification, integrity, and correctly connected individual information, a central master patient index is used. Identity registration is carried out through smart contracts that use public key cryptography to link a legitimate form of identity information to a specific ETHEREUM address. Member identification with anonymity is in a permissioned blockchain was also designed. Finding and relying on a reliable third party that authenticates user identity and completes authentication honestly without running the danger of actual identity leaking is challenging. Most systems use various authentication techniques. Some of them might not be appropriate for an IoT setting. The trend for enhancing the efficiency of blockchain-based EHR systems, particularly in the IoT environment, is the lightweight authentication protocol. Privacy-preserving membership verification through appropriate cryptographic methods and transaction privacy of blockchains without disclosing real identities should be given attention.

4 Blockchain-Based Electronic Health Record (EHR) System

The term "electronic health record" (EHR) refers to the collection of a patient's health data in the form of digital medical records storing personal health-related information. However, the challenge is to maintain privacy and security of data in such systems. Digitalization is increasing day by day in every field. People are intrigued by digitalizing the healthcare sector furthermore. An electronic health record (EHR) is an electronic version of a patient's history that is managed over time and will embody all the vital information related to patient's personal and medical history.

A decentralized management system is required for the health system, which has numerous stakeholders. Blockchain technology has the potential to be that decentralized health management system in which all parties involved would have controlled access to the same health records without any central authority. Since the information cannot be corrupted once it has been saved to the blockchain, the blockchain's unchangeable nature considerably enhances the security and privacy of the health information contained on it. Every piece of health information on the blockchain is properly ordered and key-encrypted. Additionally, medical records are stored on blockchains utilizing cryptographic keys that help protect patients' identities. Patients must have access to their information and maintain awareness. Patients would like the assurance that their health information don't seemed to be misused by other stakeholders and should have a method to detect when such misuse happens. Blockchain helps to fulfill these requirements.

Decentralized blockchain [10] helps in implementing distributed healthcare applications that do not place confidence in a centralized authority. Besides this, the fact that the information in the blockchain is mirrored across all nodes in the network generates an atmosphere of transparency and openness, enabling all stakeholders, and thus patients, to comprehend how their data is used, by whom, when, and how. Furthermore, because information is recorded in the public Ledger and all nodes in the blockchain network have Ledger backups, blockchain-based systems can resolve the restriction of a single point of failure. User can also prevent their real identities in the sense of pseudo-anonymity. The importance of EHR can also be seen by the latest coronavirus pandemic where distant patient monitoring is increasingly utilized to handle the situation.

There are currently two types of blockchain-based eHealth systems [11]: permissioned blockchain-based eHealth systems and public blockchain-based eHealth systems. To manage EMR storage and sharing, permissioned blockchain-based eHealth systems rely on a modest number of super nodes. Despite its elevated capacity, permissioned blockchain is by no means ideal for secure medical data sharing because it relies on centralized authority (a group of corporations with a common interest that will oversee the entire system). As a result, the data integrity of data in permissioned blockchain is undermined, raising the possibility of a central authority reversing blockchain records. On the other hand, designs based on public blockchain offer greater security and openness but at the cost of scalability. Since the public blockchain is powered by cryptocurrencies, a particular number of coins must be exchanged to include transactions and participate in block mining. Such methods work well for keeping clean organizations like banks, but they offer no incentive for medical facilities. The low efficiency of data retrieval is another barrier to the development of public blockchain-based eHealth solutions. We can perform a direct search on the information kept in the main database. On the blockchain, however, we must first search the block before searching the necessary transactions that are contained in the block. These systems use blockchain technology to trade medical data between medical institutions using smart contracts and scripting language. The medical data is dispersed in blockchain systems because of the data exchange and storage mechanism. It is ineffective in this situation to search through a sea of block data to find patient medical records. Additionally, it takes a long time to access a patient's complete medical records in such systems. Even worse, public blockchain-based eHealth systems struggle to complete transactions quickly. Some Chameleon hash function [10] create new block structures that detail each patient's complete medical history and use the local databases of medical institutions' EMRs to protect them via proxy re-encryption methods. Only accredited healthcare organizations are permitted access to patient EMRs. The proxy re-encryption was presented to ensure the security of data sharing. In these schemes, one party wants a trusted third party to transform the cipher text encrypted with its public key into cipher text encrypted with the other party's public key. Then, other one could decrypt the cipher text with its own private key, i.e., the data is being shared. During the process, the key is not disclosed. Therefore, the data encrypted is private and secure. The specific steps of this process are as follows:

- Party 1 encrypts the text with own public key, i.e., $C_1 = E_1(M)$, where M is the message party 1 wants to share with party 2, and E is an asymmetric encryption algorithm.
- Party 2 sends the request to party 1, and then party 1 generates one conversion key K.
- Party 1 sends C_1 and conversion key K to the agent.

- The agent converts the cipher text C_1 into C_2 using encryption key K. Here, C_2 is the cipher text of M encrypted with party 2's public key.
- The agent sends the cipher text C_2 to party 2.
- Party 2 decrypts C_2 with its own private key to get the plaintext M.

5 Review of Blockchain-Based EHR Systems

In this section, we will discuss the model proposed by Liu et al. [12] that is a medical data sharing and protection scheme based on the private blockchain of the hospital. The two-way proxy re-encryption technology is utilized in the scheme. Also, it has provided a symptoms-matching mechanism for patients with the same disease symptoms. The scheme makes use of two-way proxy re-encryption technology and also established a system for identifying patients with the same disease symptoms. The network's three participants are the system manager (S1), the hospital (H1), and the user (U1). The health management department functions as a trusted third party, creating the master key and system parameters. Hospital (H1) registers with S1 first, and then develops its private and public keys. If a user (U1) sees a doctor in a hospital (H1), he or she must first register with H1 and establish a private key. When the treatment is completed, the doctor will release the outcomes in the blockchain. If they pass the server's verification, the medical results of U1 will be saved in the H1 block chain. If a doctor in any hospital wishes to inquire about the patient U1's medical history, both the doctor and the patient should apply to the S1. SM will compute the conversion key and generate the cipher text of the medical history records, which will have been re-encrypted with the doctor's public key. The encrypted message is then sent to the doctor by S1. Finally, any two patients, US-1 and US-2, could perform mutual authentication and establish a passcode for their subsequent session. This scheme includes six phases: setup, hospital join phase, user join phase, data join blockchain phase, data search and sharing step, and patients' session process (Fig. 1).

This section also explores the studies about the blockchain-based EHR and precisely discusses the contribution of different scientists along with their limitations in the EHR system. We also discuss the various attacks and requirements of blockchain that these schemes can withstand and fulfill in Table 1. We analyze these schemes based on Security (A1), Anonymity (A2), Privacy (A3), Integrity (A4), Authentication (A5), Controllability (A6), Auditability (A7), and Accountability (A8) in Table 2.

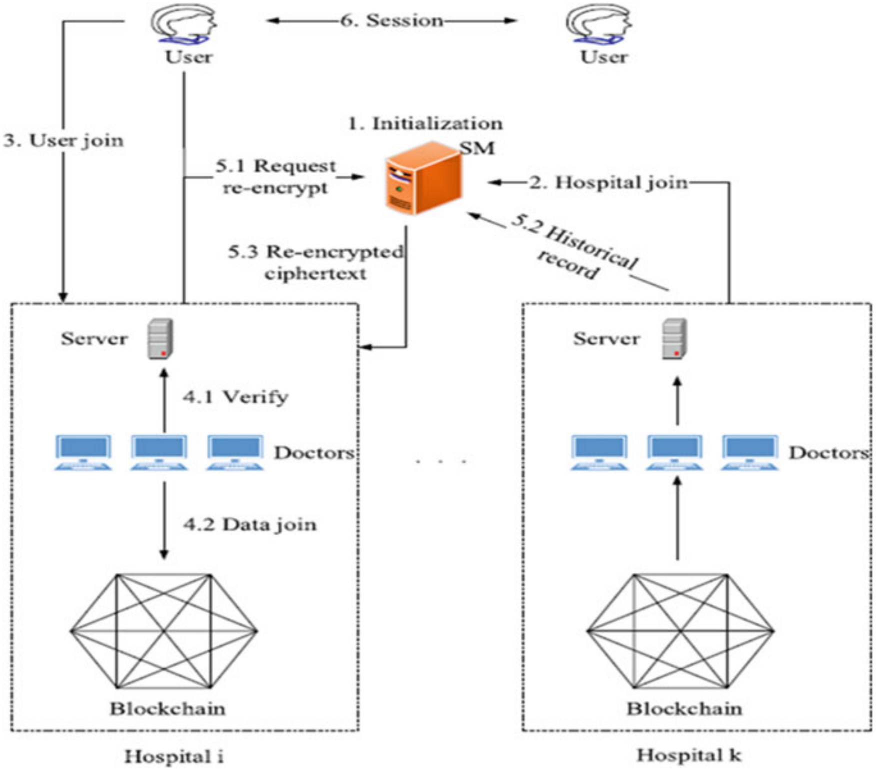

Fig. 1 Medical data sharing and protection scheme architecture Liu et al. [12]

6 Benefits of Blockchain to Healthcare Applications

- **Decentralization**: The stakeholders in the healthcare system are dispersed. They require a decentralized management system. With no centralized authority over the global health information, blockchain will become that redistributed health information management system where all stakeholders will have controlled access to the medical records.
- **Increased data security and privacy**: The blockchain significantly increases the security and privacy of the medical data stored there. Since data saved in a blockchain cannot be edited or corrupted. Every piece of health data on the blockchain is encrypted, time-stamped, and added following a formal account sequence [21–25]. The privacy and identity of patients are protected by utilizing cryptographic keys to store health information on a blockchain.
- **Ownership of health data**: Patients must be required to own their information and must be aware of how it is being used. Patients must be forced to guarantee that other stakeholders are not abusing their health information. Every patient should have a way to know when their information is being used. Through the use of

Table 1 Main contributions and limitations of blockchain-based EHR systems

Ref.#	Contribution	Limitations
[13]	– Healthcare Clara is versatile and simple to incorporate utilizing an indicator-centric storage model, and it is protected from confidentiality and integrity attacks by being kept in a private block chain cloud – MPC may be used to compute on encrypted data without leaking any data – It makes it possible for patients to safely control their own data	– High-cost PKE computation – Complexity of key management – Possibility of user's password and data leakage
[14]	– Maintain the integrity and accountability of sensitive healthcare data – Data on patients can be protected via cryptographic techniques – Give patients their old control over private data – The patient's true identity can be safeguarded through the use of pseudo-anonymity	– High-cost MPC computation – Data leaking without the owner's consent may result from the replication of data for requestors
[15]	– Significantly lessen the amount of encryption keys stored in the blockchain – Use different keys to significantly improve the privacy of the data in the block – Why Without matching symmetric keys, the chances of the attackers successfully decrypting cipher messages are reduced	– Once the corresponding symmetric key is lost all of data will be exposed or corrupted
[16]	– The information contained in nail image data can be utilized to identify individuals and aid in future studies of health and disease – For quick and precise biometric authentication, use the SVM and random forest tree method – Use blockchains to safeguard the confidentiality and integrity of sensitive data	– Bottlenecks may appear in the resource-limited 1oT devices – The potential for nail image data to be exposed in the public ledger of a blockchain
[17]	– Utilizing machine learning approaches, wearable device data quality can be enhanced – Large datasets are stored in an off-chain storage database – Improve data security and privacy – Users have the authority to regulate and share their private health information	– Data leakage caused intentionally or unintentionally by users who decrypted the desired information
[18]	– Permit patients to only exchange certain signed medical records – To protect a user's true identity, use multiple public keys for various transactions – Patient transactions that are voluntary and anonymous – Tracking of malicious requestors is possible	– Affect transaction processing directly because it takes time to construct a new block
[12]	– Easy to use and low cost – Cloud computing marked the rise of EHR – Attribute-based encryption is used to protect data	– Data leakage risk

(continued)

Table 1 (continued)

Ref.#	Contribution	Limitations
[19]	– No express assertion of the patient's identity for privacy in the signature – Remove the ability to forge the verifier – Block attempts at collusion	– High-cost computation
[20]	– Papers with both clinical and technical designs – Medical SCM and drug traceability	– Non-peer-reviewed literature included by the authors as mentioned in [20] – It can affect robustness of the data

Table 2 Security comparison of blockchain-based EHR systems

Ref.#	A1	A2	A3	A4	A5	A6	A7	A8
[13]	Yes	Yes	Yes	Yes	No	Yes	Yes	No
[14]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[15]	Yes	Yes	Yes	Yes	No	Yes	No	No
[16]	Yes	Yes	Yes	Yes	Yes	No	Yes	No
[17]	Yes	Yes	Yes	Yes	Yes	Yes	No	No
[18]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[12]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[19]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[20]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

smart contracts and robust cryptographic keys, blockchain enables the fulfillment of these criteria [26–30].

- **Availability**: Blockchain records are distributed among several nodes. Being protected from information loss and information corruption, the storage of health data on a blockchain is warranted.
- **Transparency and trust**: The open and transparent nature of the blockchain fosters a culture of trust surrounding distributed healthcare apps. This results in the care stakeholders accepting blockchain apps.
- **Data verifiability**: It is possible to check the accuracy and reliability of these records without having access to the blockchain records themselves. This capability is extremely beneficial in healthcare settings where record verification is required, such as in the management of the pharmaceutical supply chain and the filing of insurance claims.

7 Conclusion

Service providers, patients, and other stakeholders must all have access to unified secure information sharing technologies in order to make informed healthcare decisions. In this study, we share insights on blockchain-based technologies and their potential applications in the healthcare sectors. As previously stated, the digitization of records opens up fresh possibilities for investigating medical trends and assessing quality. There are various benefits of blockchain for support services. The use of blockchain technology improves connection while enhancing security and privacy and lowering costs. Blockchain-based medical records will improve diagnostic accuracy, allow for more informed treatment decisions, and provide a more cost-effective solution. It is critical to bring attention to the obstacles impeding the growth of blockchain implementations in healthcare. Our thorough review of the literature revealed both the benefits and drawbacks of blockchain technology for the healthcare sector.

References

1. Chaum D (1982) Blind Signatures for Untraceable Payments. In: Advances in Cryptology: Proceedings of CRYPTO ’82, Santa Barbara, California, USA, August 23–25, 1982, pp. 199–203. doi: https://doi.org/10.1007/978-1-4757-0602-4_18
2. Chaum D, Roijakkers S (1990) Unconditionally secure digital signatures. In: Advances in Cryptology—CRYPTO ’90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11–15, 1990, Proceedings, vol. 537, pp. 206–214. doi: https://doi.org/10.1007/3-540-38424-3_15
3. Back A (2002) Hashcash-A Denial of Service Counter-Measure. [Online]. Available: https://www.researchgate.net/publication/2482110
4. Szabo N (2022) Bit gold: towards trust-independent digital money. Accessed Oct. 28, 2022. [Online]. Available: https://nakamotoinstitute.org/bit-gold/
5. Dai W (2022) B-Money, an anonymous, distributed electronic cash system. Accessed: Oct. 28, 2022. [Online]. Available: http://www.weidai.com/bmoney.txt
6. Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf
7. Uddin M, Salah K, Jayaraman R, Pesic S, Ellahham S (2021) Blockchain for drug traceability: Architectures and open challenges. Health Inform J 27(2). doi: https://doi.org/10.1177/14604582211011228
8. Dwivedi SK, Amin R, Vollala S (2020) Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. J Inform Security Appl 54. doi: https://doi.org/10.1016/j.jisa.2020.102554
9. Khezr S, Moniruzzaman M, Yassine A, Benlamri R (2019) Blockchain technology in healthcare: A comprehensive review and directions for future research. Appl Sci 9(9). doi: https://doi.org/10.3390/app9091736
10. Zou R, Lv X, Zhao J (2021) SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Inf Process Manag 58(4):102604. https://doi.org/10.1016/j.ipm.2021.102604
11. Jin H, Luo Y, Li P, Mathew J (2019) A review of secure and privacy-preserving medical data sharing. IEEE Access 7:61656–61669. https://doi.org/10.1109/ACCESS.2019.2916503

12. Liu X, Wang Z, Jin C, Li F, Li G (2019) A blockchain-based medical data sharing and protection scheme. IEEE Access 7:118943–118953. https://doi.org/10.1109/ACCESS.2019.2937685
13. Yue XH, Wang D, Jin L, Jiang W (2016) Healthcare data gateways: found healthcare intelligence on Blockchain with novel privacy risk control. J Med Syst 40(10). doi: https://doi.org/10.1007/s10916-016-0574-6
14. M. S., B. A., K. S., al Omar Abdullah, Rahman (2017) MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. In: Security, Privacy, and Anonymity in Computation, Communication, and Storage, pp. 534–543
15. Liang X, Zhao J, Shetty SS, Liu J, Li D (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5
16. Lee SH, Yang CS (2018) Fingernail analysis management system using microscopy sensor and blockchain technology. Spec Collect Artic Int J Distrib Sens Netw 14(3):2018. https://doi.org/10.1177/1550147718767044
17. Zheng X, Mukkamala RR, Vatrapu R, Ordieres-Mere J (2018) Blockchain-based personal health data sharing system using cloud storage. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1–6. doi: https://doi.org/10.1109/HealthCom.2018.8531125
18. Liu J, Li X, Ye L, Zhang H, Du X, Guizani M (2018) BPDS: a blockchain based privacy-preserving data sharing for electronic medical records. IEEE Global Communications Conference (GLOBECOM) 2018:1–6. https://doi.org/10.1109/GLOCOM.2018.8647713
19. Shi S, He D, Li L, Kumar N, Khan MK, Choo KKR (20202) Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Comput Security 97. Elsevier Ltd, Oct. 01, 2020. doi: https://doi.org/10.1016/j.cose.2020.101966.
20. Ng WY et al. (2021) Blockchain applications in health care for COVID-19 and beyond: a systematic review. The Lancet Digital Health, vol. 3, no. 12. Elsevier Ltd, pp. e819–e829, Dec. 01, 2021. doi: https://doi.org/10.1016/S2589-7500(21)00210-7
21. Shukla V, Chaturvedi A, Srivastava N (2019) Nanotechnology and cryptographic protocols: issues and possible solutions. Nanomater Energy 8(1):1–6. https://doi.org/10.1680/jnaen.18.00006
22. Misra MK, Chaturvedi A, Tripathi SP, Shukla V (2019) A unique key sharing protocol among three users using non-commutative group for electronic health record system. J Discret Math Sci Cryptogr 22(8):1435–1451. https://doi.org/10.1080/09720529.2019.1692450
23. Shukla V, Chaturvedi A, Misra MK (2021) On authentication schemes using polynomials over non commutative rings. Wireless Pers Commun 118(1):1–9. https://doi.org/10.1007/s11277-020-08008-4
24. Chaturvedi A, Shukla V, Misra MK (2018) Three party key sharing protocol using polynomial rings. 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1–5. DOI: https://doi.org/10.1109/UPCON.2018.8596905
25. Shukla V, Misra MK, Chaturvedi A (2022) Journey of cryptocurrency in India in view of financial budget 2022–23. Cornell university arxiv, 2022, 1–6, DOI: https://doi.org/10.48550/arXiv.2203.12606
26. Shukla V, Srivastava N, Chaturvedi A (2016) A bit commitment signcryption protocol for wireless transport layer security (wtls). In: IEEE international conference on electrical, computer and electronics engineering, pp. 83–86. DOI: https://doi.org/10.1109/UPCON.2016.7894629
27. Shukla V, Chaturvedi A, Srivastava N (2019) A secure stop and wait communication protocol for disturbed networks. Wireless Pers Commun 110:861–872. https://doi.org/10.1007/s11277-019-06760-w
28. Chaturvedi A, Shukla V, Misra MK (2021) A random encoding method for secure data communication: an extension of sequential coding. J Discret Math Sci Cryptogr 24(5):1189–1204. https://doi.org/10.1080/09720529.2021.1932902

29. Shukla V, Chaturvedi A, Srivastava N (2019) A new one time password mechanism for client-server applications. J Discret Math Sci Cryptogr 22:1393–1406. https://doi.org/10.1080/09720529.2019.1692447
30. Shukla V, Misra MK, Chaturvedi A (2021) A new authentication procedure for client-server applications using HMAC. J Discret Math Sci Cryptogr 24(5):1241–1256. https://doi.org/10.1080/09720529.2021.1932908