DOI: https://doi.org/10.51846/vol5iss4pp21-28

Pakistan Journal of Engineering and Technology, PakJET
ISSN (p): 2664-2042, ISSN (e): 2664-2050
Volume: 5, Number: 4, Pages: 21- 28, Year: 2022

E-Healthcare Using Block Chain Technology and Cryptographic Techniques: A Review

Hafiz Burhan Ul Haq[1], Akifa Abbas[1], Rabia Aslam Khan[1], Ahmed Naeem Akhtar[1], Waseem Akram[2], Sabreena Nawaz[1], Faraz Imllak Mayo[1] and Ahmad Iftikhar Bhatti[1]

[1]Department of Information Technology, Faculty of Computer Sciences, Lahore Garrison University, Lahore 54000, Pakistan
[2]Department of Computer Sciences, Faculty of Computer Sciences, Lahore Garrison University, Lahore 54000, Pakistan

Corresponding author: Hafiz Burhan Ul Haq (e-mail: burhanhashmi64@lgu.edu.pk).

Received: 15/09/2022, Revised: 20/11/2022, Accepted: 22/12/2022

***Abstract*- The potential of information technology has influenced the efficiency and quality of healthcare worldwide. Currently, several republics are incorporating electronic health records (EHRs). Due to reluctance of technological adaptation & implementational complexities, electronic health record systems are not in practice. Due to the emphasis on achieving general compatibility, users may perceive systems as being imposed and providing insufficient customizability, which may exacerbate issues in a setting of national implementation. EHS improves patient safety and confidentiality and ensures operative, effective, well-timed, reasonable, and patient-centred care, all of which substantially impact healthcare quality. Blockchain technology has been used by the EHS system, which supports web-based accessibility and availability. The difficulties of exchanging medical data can now be overcome by consumers using an infrastructure based on cloud computing. A variety of cryptographic approaches have been employed to encrypt and safeguard the data. This review paper aims to highlight the role and impact of blockchain in EHR. The proposed research describes cryptography methods, their classifications, and the challenges associated with EHR to identify gaps and countermeasures.**

***Index Terms*—Blockchain, Electronic health record (EHR), Electronic medical records system, healthcare.**

I. INTRODUCTION

Nowadays, engineering and manufacturing sectors, including those in the automotive, computer and electronics, aerospace, and defence sectors, have been significantly altered by smart technologies like the Internet of Things, artificial intelligence, machine learning, virtual reality, and augmented reality. There is no exception regarding how healthcare providers like hospitals and general practitioners build healthcare systems. They have become more significant and useful over time. [1]. Smart technologies have improved their ability to handle big data volumes in real time, allowing for disease diagnosis and identification. Patients and healthcare professionals can be more organized via blockchain (BC) technology [2]. BC is a shared and immutable digital ledger data system. It's a distributed database that keeps track of transactions in chronological order as they happen. Digital transactions, data records, and executables can all be part of this framework [3]. The benefits of BC technology include increased speed, traceability, cargo security, billing, and payment procedures, and the areas of use are now greatly broadened. The BC can improve health care services for patients and the system. It helps you design and operates a large distributed database that can handle transactions over several network nodes. As a result, this technology is now being used in the biological and healthcare fields [4]. IoT can use BC to deliver reliable data [5]. Security and privacy should be considered while integrating IoT with BC [6–7]. There is still a lot of misinformation about BC, and users may favour standard apps over decentralized ones [8]. Even still, accumulating, keeping, and analyzing personal data related to healthcare without enhancing privacy breaches remains a major problem for healthcare data systems [9]. There is a novel way to deal with electronic medical records (EMR). A complete log can enable perceptibility, interoperability, and approachability [10]. As a result, challenges with interoperability across multiple EHR systems via nationally recognized standards and issues with affordability, privacy, security, and consumer adoption of electronic personal health records (ePHRs) must be addressed. In contrast to electronic health records, which are kept by healthcare professionals, electronic patient health records, or ePHRs, are managed by the patient [11]. Healthcare providers compile the data in an EHR, which medical experts can only access. Furthermore, an EHR can only receive information from one healthcare provider. On the other hand, a single person can maintain control over ePHR, which includes health information from diverse sources, for example, the patient or health care providers [12]. Despite the many benefits of electronic health records, consumer adoption is modest. Technical, individual, environmental, societal, and legal concerns must all be addressed to enhance ePHR adoption [13]. Figure 1 depicts a healthcare system based on BC.

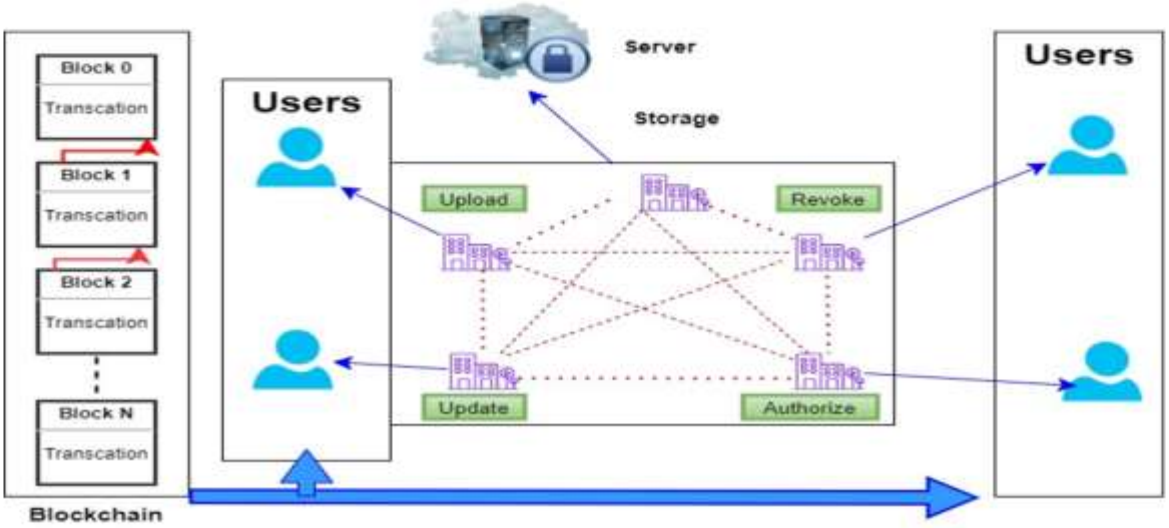

FIGURE 1. BC-based Healthcare System.

II. ELECTRONIC HEALTH RECORDS

EHRs are digital data that compile a patient's medical history. A hospital or clinician will keep electronic medical records in digital format for the rest of their lives [14]. The computerized medical records include information on magnetic resonance imaging (MRI) reports, previous physical exams, vaccination records, test results, and any allergies the patient may have [15]. Only authorized users have access to these real-time, patient-specific records, which are easily available to patients and doctors. It is an improvement over the old paper-based ways of keeping patient medical records, which are vulnerable to risks like theft, conflict, natural disasters, and illicit manipulation. EHRs allow for the automatic retrieval of data, which might make practitioners more productive. Through several interfaces, it can also help with other care-related tasks, either directly or indirectly. EHR improved the quality and clarity of health information by reducing the number of errors in records. Patients can gain from EHRs by accessing their health information at any time and location, eliminating the need for repeat testing, hastening the course of treatment, and receiving education to help them make wiser choices [16]. EHRs have allowed doctors and patients to communicate instantly whenever necessary, fostering a stronger bond. However, as information technology advances, these electronic data become more vulnerable to attacks from unauthorized users. Using sophisticated software or hacking tools, these illicit users gain access to patients' sensitive information, alter their records, and utilize the data for harm or financial gain. As a result, protecting patients' private information and medical records from hackers has become urgently necessary [17]. Today's cloud-based EHR storage method is unsafe and open to attack from skilled hackers. Electronic health records (EHRs) are kept in the cloud and secured using easily crackable passwords [18]. Since then, there has been a compelling need to safeguard patient records and their privacy from unauthorized users.

III. BLOCKCHAIN

This distributed ledger system effectively records transactions among two parties [19]. Every transaction is documented on a block, then connected to other blocks via encryption to create a list, or BC [20]. Because it is decentralized, it can also help with data management. The blocks of a BC network include transaction information, a cryptographic hash, the hash of the preceding block, and a timestamp. The architecture of the BC makes it impossible to change [21]. Any data can't be modified later without impacting all following blocks since the BC is a decentralized, distributed ledger system capable of maintaining transactions across several computers. As a result, users of the BC may independently and cheaply authenticate transactions. An autonomous BC database is built via a peer-to-peer network. The vast bulk of the network's consensus confirms them. A BC with this kind of design may enable a reliable workflow. Using a BC also eliminates the need for double spending [22]. BC technology is used by most cryptocurrencies, including bitcoin, to store transaction data.

Additionally, BC-based smart contracts may be developed that can be partially or wholly executed or enforced without the involvement of a human. The same programmers that constructed the BC network also produce smart contracts [23]. BC is also used in banking, where distributed ledgers are used in the financial industry. BC technology is being used in both supply chain materials and supply chain management [24]. BC technology has security, decentralization, and transparency, among other things. This makes it stand out as a cutting-edge technology for efficiently and safely performing transaction processes. A consensus process involving every other node in the network is used for every new block in the BC to guarantee that the node being added is one that has been given permission. This procedure is finished with a consensus algorithm [25]. BC uses cryptography to offer network security [26]. The individual blocks in a BC are connected to the blocks before and after them. This makes it challenging for hackers to alter any data since they would need to change the records or blocks associated with the record they want to access or edit; this is extremely hard to accomplish in a big network with numerous blocks on a BC, as indicated in Fig. 2.

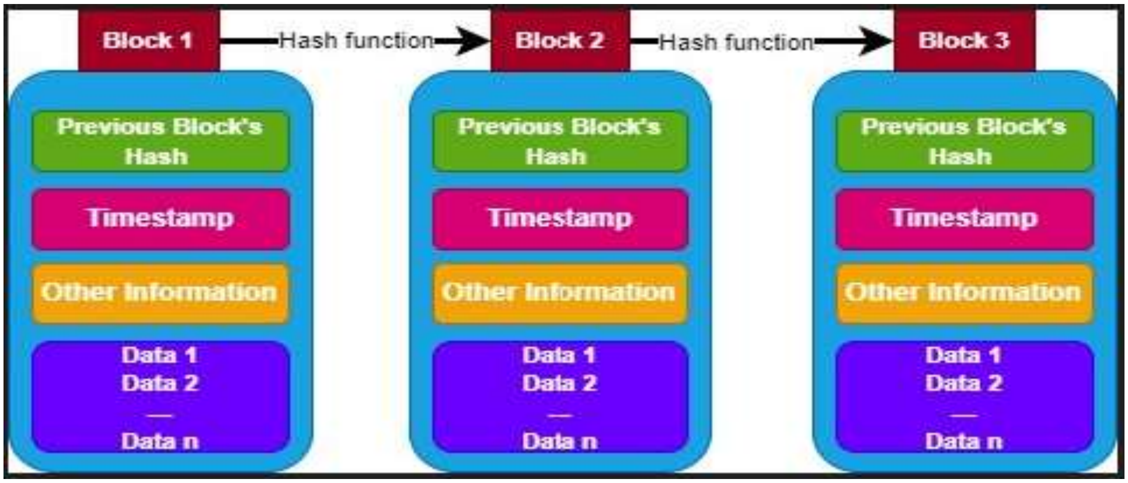

FIGURE 2. BC Structure

The genesis block is the first block in any BC and the foundation for all succeeding blocks. A BC's blocks each include transaction information, a timestamp, a nonce, and the block's hash before it. Cryptographic methods are utilized to produce the hash for that specific block. The hash of a BC block acts as a unique identifier. By storing a previous block's hash, these hash pointers also link each block to its predecessor. The BC is immutable because each block in the chain is linked to the one before. A BC uses cryptography to safeguard its blocks. Each participant in the network has a unique set of private keys connected to the transactions they carry out. These private keys are used to establish a personal digital signature. The person who created the block or did the transaction uses their private key to encrypt the transaction's contents. Anyone impacted by the transaction or wants access to it can decrypt the transaction's contents using the sender's public key. The signature becomes invalid if the record is altered, alerting the peer network that something has been tampered with. Early warning is essential for greater system security and to limit any harm. The BC network becomes more egalitarian than conventional systems since it lacks a central authority. The idea of decentralization makes BC more dependable and secure. BC are decentralized networks, meaning no one person or organization can control the system. A centralized organization does not manage the BC network. BC depends on the peer-to-peer paradigm to enable communication between two network users without the aid of a middleman. It uses a peer-to-peer (P2P) protocol to ensure that every network user has an identical copy of all transactions, enabling consensus-based sanctions [27].

IV. CRYPTOGRAPHY

Cryptography is a technique for securing data and communications that uses codes to guarantee that only those who can interpret and process the information may do so. As a result, unwanted data cannot be accessible. The term "cryptography" is derived from the terms "writing" and "hidden." The cornerstone for the methods used in cryptography to protect data is a set of rule-based calculations known as algorithms that modify signals in ways that make them difficult to decipher. Cryptography is a technique for securing data and communications that uses codes to guarantee that only those who can interpret and process the information may do so. As a result, unwanted data cannot be accessible. The fundamental workings of the encryption and decryption operations are shown in Fig. 3.

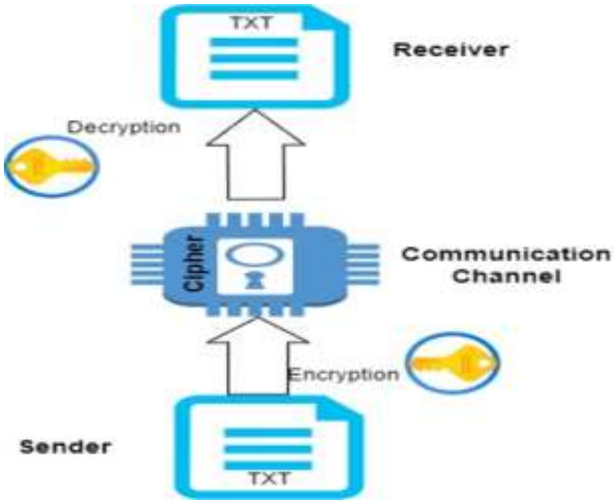

FIGURE 3. Working of encryption and decryption

Symmetric and asymmetric cryptography are frequently used methods of encryption. Asymmetric cryptography secures communication by employing public and private keys, whereas symmetric cryptography focuses on providing secure communication between sender and recipient using the same secret key. Due to its general character, a private key is kept by an individual in communication, whereas everyone knows a public key. Symmetric and asymmetric cryptography are depicted in Fig. 4 and 5, respectively. The most significant criterion for securing communication in symmetric and asymmetric cryptography is key size. Symmetric cryptography's key size is smaller than asymmetric cryptography, making it less safe for sensitive data.

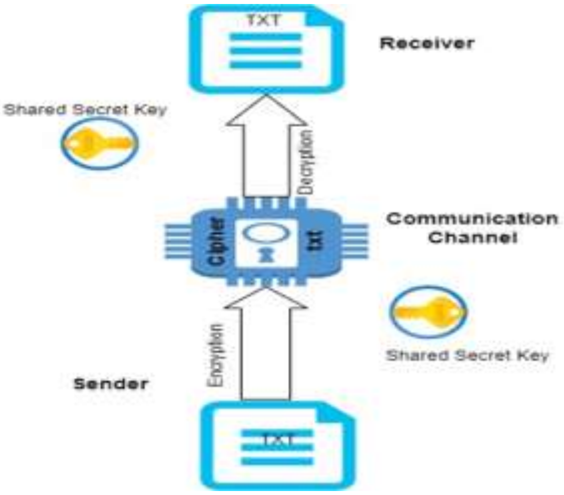

FIGURE 4. Symmetric Cryptography

Large-scale data encryption and decryption are more challenging with asymmetric cryptography since it takes longer to compute than symmetric cryptography. Public key cryptography is solely used for key exchange. In contrast, symmetric key cryptography is used for additional encryption and decryption since asymmetric cryptography has a smaller key size and is faster to compute. Encryption and decryption times, key generation times, and key exchange times are all components of the computational time of cryptography algorithms. Converting plaintext into cypher text is how encryption and decryption times are calculated. The time it takes to produce the key depends on its length, which differs for symmetric and asymmetric cryptography. The sender-receiver communication route dictates how long it takes to exchange a key. Numerous cryptographic algorithms are used to carry out encryption and decryption. There are two different categories of encryption systems: symmetric and asymmetric algorithms.

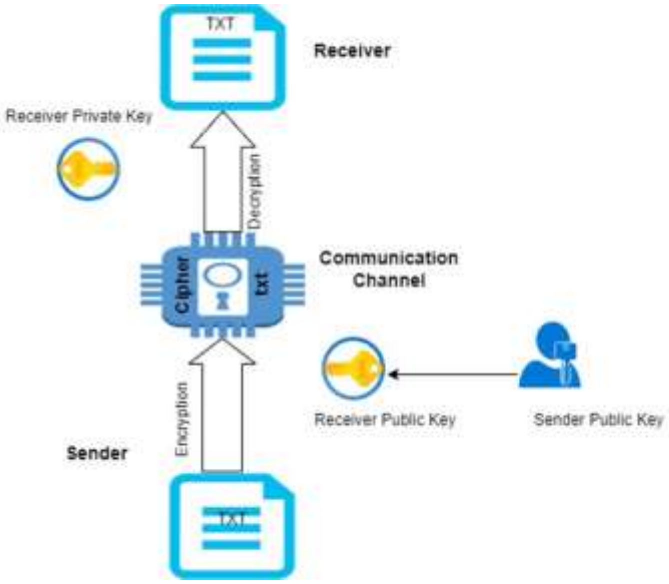

FIGURE 5: Asymmetric Cryptography

Symmetric techniques include Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). Asymmetric algorithms include Rivest, Shamir, and Adleman (RSA), Elgamal, and Elliptic Curve Cryptography (ECC). Figure 6 depicts a taxonomy of cryptographic methods, while Table I and II key generation times and encryption/decryption times.

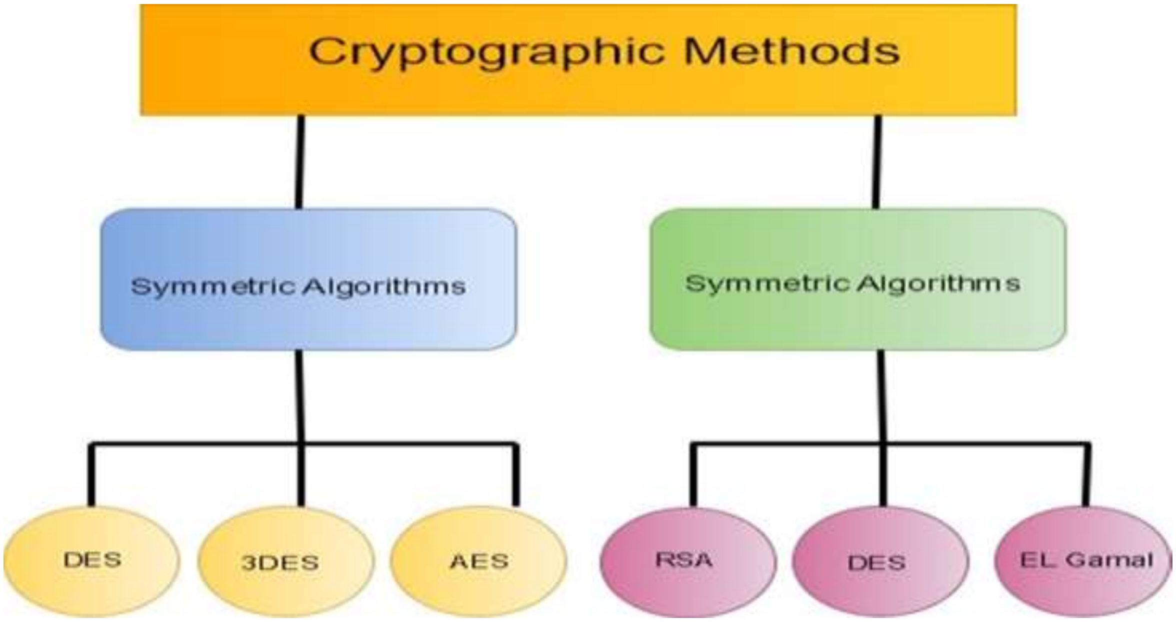

FIGURE 6. Taxonomy of Cryptography Technique.

TABLE I
SIZES OF THE KEYS AND THEIR GENERATION TIMES

Cryptography Algorithms		Key size (bits)	Generation Time (milliseconds)
Symmetric	DES	56	29 ms
	AES	128	75 ms
Asymmetric	RSA	1024	287 ms
	ElGamal	160	86 ms

TABLE II
TIMES FOR ENCRYPTION AND DECRYPTION FOR FILE SIZE

Cryptography Algorithms	**File Size (kilo bytes)**	**Encryption Time(in seconds)**	**Decryption Time(in seconds)**
DES	32	0.27	0.44
	126	0.83	0.65
	200	1.19	0.85
	246	1.44	1.23
	280	1.67	1.45
AES	32	0.15	0.15
	126	0.46	0.44
	200	0.72	0.63
	246	0.95	0.83
	280	1.12	1.10
RSA	32	0.13	0.15
	126	0.52	0.43
	200	0.74	0.66
	246	1.11	0.93
	280	1.39	1.23
ElGamal	32	0.45	0.43
	126	1.03	0.85
	200	1.41	1.13
	246	1.75	1.30
	280	1.83	1.64

V. ELECTRONIC HEALTH RECORDS USING BLOCKCHAIN

Cloud computing's popularity continues to rise, as does its use in various industries and businesses. Users benefit from inexpensive storage costs, space availability, and scalability by storing their data on the cloud. Furthermore, there is no need to worry about maintaining the storage infrastructure, upgrading the program, or performing periodic maintenance. Security and privacy issues remain a barrier to cloud computing technologies. Many firms are concerned about a lack of storage space and centralized data; thus, [28] suggests creating a cloud space that enables secure and trustworthy data sharing using a cryptographic framework is a must. Standard security levels can be met by executing crucial information encryption [29]. The encryption process aids in predicting and thwarting attempts by unauthorized personnel to break the security and obtain the required information. The two trustworthy correspondence hubs can share a secret key to perform symmetric information encryption using the technique mentioned above in the three frameworks (AES, XTEA, and IDEA).

Unusual encryption, such as RSA, scrambles data with open keys and unscrambles it in frames. As a result, cryptographic systems must effectively meet such stringent requirements while also demonstrating their ability to work with forced devices. Zhang et al. [30] described replacing the original signature in the BC with the ABS approach, which provides fine-grained access control. Because the cloud is prone to leaking user data or ensuring insecure user privacy, advocates have advocated for a privacy-preserving and user-controlled data-sharing architecture and fine-grained access control based on the BC model and an attribute-based cryptosystem. Shi et al. [31] discussed the HDG (Healthcare Data Gateway), a BC-based PC app design. The proposed reason-driven admission control model is split into crude and measured information based on access purposes. Various sharing approaches are used to carry out any exchange to achieve multiple goals.

As a result, patients may easily monitor and review their shared medical information. Some frameworks use smart contracts, which include pre-defined access strategies depending on requestors' goals and benefits based on job/reason. Attending such impromptu or dynamic events might be difficult and can appear to pose a security risk. Manoj et al. [32] developed a crossover solution for exchanging EHRs in a hybrid cloud environment, taking into account security and protection characteristics. The two ABE (attribute-based encryption) methodologies for encoding the EHR record of each patient have been merged to achieve fine-grained admission control for EHRs. Despite significant benefits and administrations, obtaining clinical information or overall security for administration providers continues to be difficult. On the other hand, the Advanced

Encryption Standards (AES) technique has proven to be sufficiently resilient in preserving important information while revealing insurance competence. However, it has a drawback regarding security assurance and preparation time.

VI. REAL-TIME APPLICATIONS

Nowadays, various types of applications are developed related to HER. Some of the applications are discussed below:

A. PRESERVING A PATIENT'S SPECIFIC DATA

Before and throughout the different clinical study phases, a significant amount of patient information and health data are generated. Numerous blood tests, quality evaluations, estimates, and wellness surveys are offered. It may offer information demonstrating the existence of a document or record. Healthcare professionals will go through the data that has been captured and question its validity, which they will confirm by comparing it to the original data stored on the BC system. Current cryptographic methods, including one suited for data sharing, provide the basis for constructing BC. When entering patient details, the healthcare provider records the patient's name, date of birth, diagnosis, treatments, and ambulatory history in EHR format; this data is stored in a local database and the cloud [33-34].

B. SECURITY AND TRANSPARENCY

BC might be the perfect instrument for maintaining medical records. It may be used for things like the transfer of medical data, the maintenance of electronic health records, the control of insurance, and the execution of administrative tasks. Patients may connect a BC network with their health data through an app. Digital BC contracts make it easier for sensors and intelligent devices to work together. The majority of the time, various care facilities share electronic health records. All information will be combined through BC, giving patients access to past data. We will gain new insights into a patient's health status due to the consolidation of all data in one location. Thus, the BC paradigm will ensure the legitimacy and authenticity of the information while preserving user privacy [35].

C. FALSE CONTENT IDENTIFICATION

BC will increase information transparency and help identify false information. Medical research for patients and consumers should continue to be easily verifiable. An intelligent contract is useful for obtaining consent and maintaining the transparency of protocol outcomes and documentation. Initially, the technology allowed members of the public to see what was going on in clinical research closely. Its main objectives are this technology's user-friendliness and safe, real-time access to patients' health and insurance information [36].

D. PRESERVING A PATIENT'S SPECIFIC DATA

Medical professionals can ensure patients have access to medical equipment when needed because of the trust built into BC technology. Additionally, doctors could spend more time observing their patients and remotely responding to health-related issues. BC technology may help enhance bed use, supply availability, and monitoring of patient room temperatures. Combining BC and IoT technologies to increase supply chain responsiveness and traceability and make healthcare logistics extremely transparent for efficient patient monitoring, a BC healthcare system was created to give healthcare organizations and providers a solid digital identity [37].

E. FINANCIAL RECORD MAINTENANCE

It is essential to have an accurate record of the financial statements throughout the accounting process. The clinical trials are ideal for smooth operation and assessment. BC businesses have created solutions for enhancing accounting and reporting procedures. Anyone can utilize this service to arrange a visit with a healthcare professional in advance and complete the required papers. Customers will save time since they won't have to stand in line. However, via its real-world implementations and the problems, it resolves in the healthcare system, we may learn about the risks and benefits of BC [38].

VII. CHALLENGES OF BLOCKCHAIN IN HEALTHCARE

The benefits of BC in healthcare are numerous and have the potential to alter the entire industry. Certain challenges are impeding its widespread adoption. For the entire healthcare system to improve, mass adoption is essential. Table III describes the challenges related to BC in healthcare.

TABLE III
UNITS FOR MAGNETIC PROPERTIES

Symbol	Quantity
1	Slow in terms of speed
2	Inadequate awareness
3	Consumption of energy in a huge manner
4	Problems with interoperability
5	Authentication problems due to the absence of a central point
6	Data replication
7	Integration Issue
8	Costly

VIII. CONCLUSION

A literature review of electronic health record systems was carried out in this study. The study looks at various solutions to the security and privacy challenges of using EHRs. According to the literature, electronic health records allow for the easy sharing of organized health information across certified healthcare professionals, thereby significantly improving the quality of healthcare provided to patients. The use of e-health helps users think more broadly, and healthcare professionals network more proficiently. Health data can be easily accessed among providers, and patient data can be retrieved and modified as a patient receives medication, thanks to electronic health records. However, with such systems, security and privacy considerations are critical because if confidential data is shared with a foreign entity, the patient may face catastrophic consequences. Diverse rules and norms linked to security and privacy are evident in electronic health records, as evidenced by the papers studied and the security areas examined. Therefore, these systems must be harmonized to overcome potential standard conflicts and inefficiencies. Numerous articles have proposed a variety of encryption techniques. Based on the most recent EHR data, it is strongly advised to employ a strong encryption system that can be used effectively by both health professionals and patients. BC technology is the most widely used encryption mechanism in electronic health record systems. BC uses cryptography, hashing, and decentralization to ensure EHRs and protect patient privacy. This can facilitate healthcare research and innovation in the coming years. Furthermore, the application and challenges are discussed, demonstrating BC's weakness or gap in healthcare.

FUNDING STATEMENT

The authors declare they have no conflicts of interest to report regarding the present study.

CONFLICT OF INTEREST

The Authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] A. Kumari, S. Tanwar, S., Tyagi, and N. Kumar. "Fog computing for Healthcare 4.0 environment: Opportunities and challenges." *Computers & Electrical Engineering* vol. 72, pp1-13, 2018. https://doi.org/10.1016/j.compele ceng.2018.08.015

[2] S. Tanwar, K. Parekh and R., Evans. "Blockchain-based electronic healthcare record system for healthcare 4.0 applications." *Journal of Information Security and Applications*, 2020. https://doi.org/10.1016/j.jisa.2019.102407

[3] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacoc. "Blockchain technology in the energy sector: A systematic review of challenges and opportunities." *Renewable and Sustainable Energy Reviews*, pp.143–174. https://doi.org/10.1016/j.rser.2018. 10.014

[4] T.T. Kuo, H.E, Kim, L. Ohno-Machado. "Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association' vol. 24, pp. 1211–1220, 2017. https://doi.org/10.1093/jamia/ocx068

[5] T.M. Fernández-Caramés, P. Fraga-Lamas. "A Review on the Use of Blockchain for the Internet of Things." *IEEE Access, vol.*6, pp.32979–33001, 2018. https://doi.org/10.1109/ACCESS.2018.2842685

[6] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz. "On blockchain and its integration with IoT. Challenges and opportunities." *Future Generation Computer Systems*, vol. 88, pp. 173–190. 2018 https://doi.org/10.1016/j.future.2018.05.046

[7] I.C. Lin, T.C. Liao. "A survey of blockchain security issues and challenges." *International Journal of Network Security*, vol. 19, pp. 653–659. 2017. https://doi.org/10.6633/IJNS.201709.19(5).01

[8] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaría. "Blockchain and smart contracts for insurance: Is the technology mature enough?" *Future Internet*, vol. 10, 2018 https://doi.org/10.3390/fi10020020

[9] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang. "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control." *J Med Syst*, vol. 40, pp. 218. 2016 https://doi.org/10.1007/s10916-016-0574- 6

[10] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman. "MedRec: Using Blockchain for Medical Data Access and Permission Management", *in: 2016 2nd International Conference on Open and Big Data (OBD). Presented at the 2016 2nd International Conference on Open and Big Data (OBD), IEEE*, Vienna, Austria, pp. 25–30. 2016, https://doi.org/10.1109/OBD.2016.11

[11] N. Archer, U. Fevrier-Thomas, C. Lokker, K.A McKibbon, S.E. Straus. "Personal health records: A scoping review." *Journal of the American Medical Informatics Association*, vol. 18, pp. 515–522. https://doi.org/10.1136/amiajnl-2011-000105

[12] A. Roehrs, C.A. Da Costa, R. Da Rosa Righi, K.S.F. De Oliveira. "Personal health records: A systematic literature review." *Journal of Medical Internet Research*, vol. 19. 2017, https://doi.org/10.2196/jmir.5876

[13] A.Y.A. Alsahafi, B.V. Gay. "An overview of electronic personal health records. Health Policy and Technology" vol. 7, pp. 427–432. 2018. https://doi.org/10.1016/j.hlpt.2018.10.004

[14] T. Gunter and N. Terry, "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions", *Journal of Medical Internet Research*, vol. 7, no. 1, pp. e3, 2005. Available: 10.2196/jmir.7 1.e3.

[15] S. Hufnagel, "National Electronic Health Record Interoperability Chronology", *Military Medicine*, vol. 174, no. 5, pp. 35-42, 2009. Available: 10.7205/milmed-d-03-9708.

[16] R. Evans, "Electronic Health Records: Then, Now, and in the Future", *Yearbook of Medical Informatics*, vol. 25, no. 01, pp. S48-S61, 2016. Available: 10.15265/iys 2016-s006.

[17] E. Bertino, R. Deng, X. Huang and J. Zhou, "Security and privacy of electronic health information systems", International *Journal of Information Security*, vol. 14, no. 6, pp. 485-486, 2015. Available: 10.1007/s10207- 015-0303-z.

[18] J. Fernández-Alemán, I. Señor, P. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541-562, 2013. Available: 10.1016/j.jbi.2012.12.003.

[19] "The great chain of being sure about things", The Economist, 2019. [Online]. Available: *https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things*.

[20] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaram, "Blockchain Technology." 2019.

[21] G. Karame and S. Capkun, "Blockchain Security and Privacy", *IEEE Security & Privacy*, vol. 16, no. 4, pp. 11-12, 2018. Available: 10.1109/msp.2018.3111241.

[22] J. Aoyagi and D. Adachi, "Fundamental Values of Cryptocurrencies and Blockchain Technology", *SSRN Electronic Journal*, 2018. Available: 10.2139/ssrn.3132235.

[23] "Smart contract", En.wikipedia.org, 2019. [Online]. Available: *https://en.wikipedia.org/wiki/Smart_contract*. [Accessed: 30- Nov- 2019].

[24] Y. Tribis, A. E.L. Bouchti and H. Bouayad, "Supply Chain Management based on Blockchain: A Systematic Mapping Study", *MATEC Web of Conferences*, vol. 200, p. 00020, 2018. Available: 10.1051/matecconf/201820000020.

[25] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks", *IEEE Access*, vol. 7, pp. 22328-22370, 2019. Available: 10.1109/access.2019 .2896108.

[26] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security Services Using Blockchains: A State- of-the-Art Survey", *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858-880, 2019. Available: 10.1109/comst.2018.2863956.

[27] "Peer-to-Peer Insurance: How Blockchain is challenging the traditional insurance model", *Medium*, 2019. [Online]. Available: *https://medium.com/@fidentiaX/peer-to-peer-insurance-how-blockchain-is challenging- the-traditional-insurance-model-fd63f6130c4*. [Accessed: 30- Nov- 2019].

[28] N. Eltayieb, R. Elhabob, A. Hassan and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud", *Journal of Systems Architecture*, 102, p.101653, 2020, Elsevier.

[29] L. Malina, J. Hajny, R. Fujdiak and J. Hosek, "on perspective of security and privacy preserving solutions in the internet of things", *Computer Networks*, vol. 102, 2016, pp.83-95, Elsevier.

[30] Y. Zhang, D. He and K.K.R Choo, "BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT", Wireless Communications and Mobile Computing, 2018.

[31] S. Shi ,D. He ,L. Li, N. Kumar, M.K. Khan, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey", *Computers & Security*, 2020, pp.101966, Elsevier.

[32] R.. Manoj, A. Alsadoon, P.C. Prasad, N. Costadopoulos, and S. Ali, "Hybrid secure and scalable electronic health record sharing in hybrid cloud", *In 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2017, pp. 185-190. IEEE.

[33] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, E. Harjula,. "Health-BlockEdge: blockchain-edge framework for reliable low-latency digital healthcare applications",*Sensors*, vol. 21 no. 7, 2021, pp. 2502.

[34] S. Aggarwal, N. Kumar, M. Alhussein, G. Muhammad. "Blockchain-based UAV path planning for healthcare 4.0: current challenges and the way ahead", *IEEE Network*, vol. 35, no. 1, 2021, pp. 20-29.

[35] J. Hathaliya, P. Sharma, S. Tanwar, R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0", *In 2019 IEEE 9th International Conference on Advanced Computing (IACC)*, IEEE, 2019, pp. 87-91.

[36] A. Haleem, M. Javaid, R.P. Singh, R. Suman and S. Rab. "Blockchain technology applications in healthcare: An overview". *International Journal of Intelligent Networks*, 2, 2021, pp. 130-139.

[37] P.P. Ray, D. Dash, K. Salah, N. Kumar, "Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases", *IEEE Syst. J.*, 15 (1) (2020 Jan 21), pp. 85-94.

[38] R.W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, M. Omar, "The role of blockchain technology in telehealth and telemedicine", *Int. J. Med. Inf*, 2021, pp. 104399.

[39] S. Srivastava, M. Pant, S.K. Jauhar and A.K. Nagar. "Analyzing the Prospects of Blockchain in Healthcare Industry. *Computational and Mathematical Methods in Medicine*", 2022.