The Original

DIASPORA OF INTERNET OF THINGS, BLOCKCHAIN AND SECURITY IN HEALTHCARE – A SYSTEMATIC REVIEW

Dr John Paul A[1], Dr. Karthik Shunmugavelu[2*]

[1]Assistant Professor, Department of Community Medicine, Saveetha Medical College and Hospital, SIMATS India
[2]Assistant Professor, Department of Dentistry, PSP medical college hospital and research institute Tambaram Kanchipuram main road Oragadam Panruti Kanchipuram district Tamilnadu 631604, Email drkarthiks1981@gmail.com, https://orcid.org/0000-0001-7562-8802

ABSTRACT

Background: The use of IT tools and techniques in the medical field has had a significant impact, opening, a wide range of eHealth service opportunities. The same types of dangers that affect other internet apps also affect these services. One of the important concerns for the successful and efficient deployment of these eHealth services is security. The vast and diverse nature of healthcare data necessitates a high level of availability, confidentiality, and integrity when it is sent to its various stakeholders. The various parties involved in healthcare services, including physicians, patients, nurses, paramedical personnel, and administrative staff, have distinct roles to play, and not all users should have access to all data to protect privacy.

Blockchain technology has made significant advancements in securely sharing data in recent years. Its implementation has greatly benefited various services, particularly in the healthcare sector. Blockchain simplifies the management of medical records and data in a secure environment. When a user creates a record, millions of computers validate the blocks, resulting in a unique record with its own history. If a single record is altered, it disrupts the entire chain, affecting millions of instances.

Many industries are eager to adopt blockchain technology to enhance their data security in today's environment. While protecting data privacy, integration with technologies such as artificial intelligence helps guarantee smooth data sharing between various parties. Additionally, blockchain technology enables real-time interorganizational services or workflows for users both inside and outside of national health systems worldwide. When people are relocating, it is essential to improve and share migrant health data so that analytics can be used to make strategic choices. Blockchain technology has the potential to become a powerful digital tool for enhancing communication and filling in the gaps in the sharing of medical data.

Material and Methods: Major databases such as Medline were explored detailed literature search in resulting in a systematic review pertaining to IoT, blockchain and security.

Results: Five original research scientific articles dated between 2020 – 2024 pertaining to mentioned topic were highlighted.

Conclusions: Blockchain is a powerful technology that has the potential to significantly transform the healthcare industry. However, to achieve widespread acceptance of this technology, substantial research and study are still needed. The integration of blockchain technology with hybrid deep learning offers numerous benefits, including increased scalability, enhanced security, improved interoperability, and better decision-making in healthcare systems.

Nonetheless, for successful implementation, challenges such as computational complexity, regulatory compliance, and ethical considerations must be addressed. Healthcare systems can surpass conventional constraints by utilizing blockchain and hybrid deep learning, which will promote medical research and enable safe and effective data management as well as individualized patient care. Scalability, security, and better patient outcomes are given top priority in the proposed framework, which establishes the groundwork for a future healthcare ecosystem. Detailed information regarding the IoT, blockchain and security is discussed in this systematic review.

KEYWORDS: artificial intelligence; blockchain, Internet of Things; digital; eHealth; machine learning; Security policies; data storage optimization.

INTRODUCTION

Blockchain (BC) technology's decentralized ledger, source provenance, and tamper-proof characteristics have made it a crucial component of numerous applications, such as the Internet of Things (IoT) and healthcare. Thanks to IoT and BC, health systems can now become more stable and scalable on a decentralized platform. The creation of BC-enabled IoT eHealth systems is the outcome of several scientists looking into the potential of BC technology in many eHealthcare domains. Recently, blockchain technology has gained attention because of its potential to increase the security, reliability, and resilience of distributed systems.

Research using this method has benefited several industries, including data analysis, remote sensing, healthcare, and finance. Data immutability, privacy, transparency, decentralization, and distributed ledgers are the main advantages of blockchain technology. The requirement to safeguard the privacy of people whose information is contained in medical

records makes this system even more complicated. "A distributed database that maintains a continuously expanding list of ordered items, called blocks," is one definition of a blockchain. The link between these blocks is encrypted.
Each block in a blockchain includes a timestamp, transaction data, and a cryptographic hash of the previous block. Blockchains are public, decentralized, and distributed digital ledgers used to record transactions across multiple computers. This structure ensures that once a transaction is recorded, it cannot be modified without altering all subsequent blocks and obtaining permission from the network. However, the end-to-end security of IoT devices is compromised by several issues. Security has not always been a top priority for product designers, particularly because networking appliances and other connected devices are still relatively new on the market.
Many designers and manufacturers are more concerned with getting their products to market quickly than with including security from the start because IoT is a relatively new business. IoT security may be jeopardized by hardcoded or default passwords. Even with frequent updates, passwords are often not secure enough to thwart infiltration. The CPU power required to allow adequate security is often lacking in IoT devices. Many devices lack advanced security as a result. Temperature and humidity sensors are unable to handle contemporary security or encryption. IoT devices seldom receive security updates or fixes since many of them are "set it and forget it."

MATERIAL AND METHODS

"IoT" AND "blockchain" AND "security'' were the words used in MEDLINE database using advance search strategy targeting different article categories between 2020 to 2024. The result was 58 articles, out of which we selected 5 articles based in the inclusion criteria. Inclusion criteria was of case studies and scientific literature between 2020-2024. Exclusion criteria was of scientific literature irrelevant to the specific search. This systematic review was conducted to determine importance IoT, blockchain and security in healthcare following the guidelines of the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). PubMed, Lilacs, Embase, Scopus, and Web of Science were the source of electronic databases. The search strategy used Boolean operators (AND and OR): [ALL ("IoT") AND (blockchain OR healthcare OR security OR ehealth OR technology OR AI) AND (erosion)]. The following data were collected: first author, year, country of study, type of study and outcome. The quality of studies was assessed using the STROBE (Strengthening the Reporting of Observational Studies) checklist.

RESULTS

Five articles were included in this systematic review based on the selection criteria. We analyzed and mentioned in the five articles reviewed. This included only relevant research articles and excluded articles pertaining to non-specific search terms.

Table 1 – An overview

Author	Title	Journal	Outcome
Shilpa Srivastava, Millie Pant, Sunil Kumar Jauhar, Atulya K Nagar	Analyzing the Prospects of Blockchain in Healthcare Industry	Srivastava S, Pant M, Jauhar SK, Nagar AK. Analyzing the prospects of blockchain in healthcare industry. Computational and mathematical methods in medicine. 2022;2022(1):3727389. doi: 10.1155/2022/3727389.	suggestions for strengthening the healthcare system by blending machine learning, artificial intelligence, big data, and IoT with blockchain.
Aitizaz Ali, Hashim Ali, Aamir Saeed, Aftab Ahmed Khan, Ting Tin Tin, Muhammad Assam, Yazeed Yasin Ghadi, Heba G Mohamed	Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning	Ali A, Ali H, Saeed A, Ahmed Khan A, Tin TT, Assam M, Ghadi YY, Mohamed HG. Blockchain-powered healthcare systems: enhancing scalability and security with hybrid deep learning. Sensors. 2023 Sep 7;23(18):7740. doi: 10.3390/s23187740.	The proposed framework lays the foundation for a future healthcare ecosystem
Bouthaina Dammak, Mariem Turki, Saoussen Cheikhrouhou, Mouna Baklouti, Rawya Mars, Afef Dhahb	LoRaChainCare: An IoT Architecture Integrating Blockchain and LoRa Network for Personal Health Care Data Monitoring	Dammak B, Turki M, Cheikhrouhou S, Baklouti M, Mars R, Dhahbi A. Lorachaincare: An iot architecture integrating blockchain and lora network for personal health care data monitoring. Sensors. 2022 Feb 15;22(4):1497. doi: 10.3390/s22041497.	This work proposes LoRaChainCare, an architecture model for HCS which combines the technologies Blockchain, Fog/Edge computing, and the LoRa communication protocol.

Hanaa Fatoum, Sam Hanna, John D Halamka, Douglas C Sicker, Peter Spangenberg, Shahrukh K Hashmi	Blockchain Integration With Digital Technology and the Future of Health Care Ecosystems: Systematic Review	Fatoum H, Hanna S, Halamka JD, Sicker DC, Spangenberg P, Hashmi SK. Blockchain integration with digital technology and the future of health care ecosystems: systematic review. Journal of Medical Internet Research. 2021 Nov 2;23(11):e19846. doi: 10.2196/19846.	the potential benefits of blockchains are limitless
Alessandra Rizzardi, Sabrina Sicari, Jesus F. Cevallos M., Alberto Coen-Porisini	IoT-driven blockchain to manage the healthcare supply chain and protect medical records	Rizzardi A, Sicari S, Coen-Porisini A. IoT-driven blockchain to manage the healthcare supply chain and protect medical records. Future Generation Computer Systems. 2024 Dec 1;161:415-31. doi.org/10.1016/j.future.2024.07.039	blockchain may facilitate the resolution of consistency and accuracy problems associated with healthcare data by further enhancing them using AI techniques.

DISCUSSION

Blockchain is a revolutionary decentralized, distributed ledger technology (DLT) that enables secure, transparent, and immutable record-keeping. Think of it as a special kind of database that stores data in "blocks," and these blocks are then linked together in a "chain" using cryptography.1

Blocks: Each "block" in a blockchain contains a batch of validated transactions or data. It also includes a cryptographic hash of the previous block, a timestamp, and other relevant information. Once a block is filled with data, it's closed and added to the chain.2

Chain: Blocks are linked together chronologically using cryptographic hashes. This means each new block contains a unique digital "fingerprint" (hash) of the previous block. This linking creates a secure and immutable record. If someone tries to alter a transaction in an old block, the hash of that block would change, which would then invalidate the hash in the next block, and so on, breaking the chain. This makes it extremely difficult to tamper with data without being detected.3

Decentralization: Unlike traditional databases that are controlled by a single central authority (like a bank or a company server), a blockchain is distributed across a network of computers (called "nodes"). Each node maintains a copy of the entire ledger. This means there is no single point of failure or control, making the system highly resilient to attacks or censorship.4

IoT enables a network of physical entities by embedding sensors, operating software, and other technologies. IoT plays an important role in various fields due to its capability to provide sensor-based information and its ability to enable device-to-device communication.5

Blockchain can be defined as a decentralized storage system that facilitates cryptographically secure storing and sharing of records immutably through a network comprising of distributed peer-to-peer members.6

Simply said, a blockchain is a shared digital record that can be accessed by any computer connected to the internet. Since information is stored digitally, a blockchain may be compared to an online database.7

Blockchains serve an important purpose in cryptocurrency networks like Bitcoin's by providing a secure and decentralized ledger of transactions. Novel blockchain technology guarantees the authenticity of each recorded transaction without the need for a neutral third party.8

One definition of a blockchain is "a distributed database that maintains a continuously expanding list of ordered items, called blocks." The encrypted connection between these blocks. Each block contains transaction data, a timestamp, and a cryptographic hash of the previous block.9

Blockchains are distributed digital ledgers that are public and decentralized, and which are used to record transactions across several computers in a way that precludes modifications to the ledger from being made in the past without also modifying the subsequent blocks and getting network permission.10

History of Blockchain: In the year 1976, a paper was released on "New Directions in Cryptography" discussed the concept of distributed ledger. With the advancement in the field of Cryptography, another paper entitled as "Hot to Time-Stamp a Digital Document" by Stuart Haber and Scott Stornetta which laid out the concept to timestamp the data instead of the medium.11

Another important concept called as "Electronic cash" or "Digital Currency" which came into existence based on a model proposed by David Chaum also contributed towards the development of the concept of Blockchain which was followed by Protocols such as e-cash schemes that introduced double spending detection.12

In 1997, Adam Back introduced another concept called "hashcash" which offered a solution to control spam emails. This led to the concept of creating money called as "b-money" by Wei Dai based on peer-to-peer network. Satoshi Nakamoto is considered as the inventor of blockchain technology when he published a paper on bitcoin in 2008 as "Bitcoin: A Peer-to-Peer Electronic Cash System,".13

Blockchain technology works on the concept of decentralized database where these databases exist in multiple computers and every copy of these databases are identical. Organizations maintain their data in centralized database which makes them an easy target for the hackers whereas due to decentralized structure of blockchain, it has made the blockchain as a temper proof technology.14
Blockchain can be considered as a peer-to-peer network that run on the top of the internet. Blockchain architecture can be mainly divided in three layers which are Applications, Decentralized Ledger, and Peer-to-Peer Network. Applications is the top layer pf the network which is followed by the Decentralized Ledger and the bottom layer is the Peer-to-Peer Network.15

Features Of Blockchain: Information on a blockchain, which is a sort of distributed database, is stored in blocks that are cryptographically linked to one another. When new information is received, it is stored in a new block. Once a block is filled, it is connected to the one before it, producing a chain that stores information in chronological order.

- Blockchains may be used to record other sorts of data, although thus far they have mostly been used as a distributed ledger for recording financial transactions.16
- Blockchain is employed in a decentralized fashion in Bitcoin, meaning that no central authority or group of people has control over the system and instead all Bitcoin users have equal voting rights.
- By its very nature, the data placed into a decentralized blockchain cannot be changed after it has been recorded. For Bitcoin, this implies that all trades are publicly accessible and forever recorded.17

The term “blockchain” is used to refer to the digital ledger used to keep track of information. It is organized as a series of blocks, and the cryptographic principle is built into the whole thing. Data and conversational exchanges can be protected using cryptography.18
Supported by mathematical ideas and a collection of rule-based calculations, it alters communications in a way that is difficult to decode. Blockchain technology is decentralized, thus it may be used by anybody. In other words, no one can claim ownership. The level of transparency is too high and protects individual privacy.19
Because information saved on a blockchain cannot be altered after it has been recorded, it is considered immutable. Blockchain technology’s core purpose is to keep sensitive information safe from prying eyes while making it available to a select, pre-approved audience.20
Blocks Numerous blocks make up each chain, with the following three providing the bulk of its functionality: Information alone constitutes the building component. Each time a new block is formed, an encrypted one is generated using a random 32-bit nonce. And so, a block header hash is born. Connected to the nonce, the hash is a 256-bit integer. The first digits should be a bunch of zeroes. In addition, the nonce will be used to produce the cryptographic hash whenever a new block is created.21
The Internet of Medical Things (IoMT) is a framing structure for smart medical devices, as these devices are linked to health services, applications, and systems via the Internet. Many challenges associated with IoT must be considered regarding health data privacy and security, availability, ease of data access, and scalability.22
IoMT devices are wearable devices that collect private and sensitive data about the human body, which enables healthcare service providers to make appropriate decisions at the right time. Because of the sensitivity and confidentiality of data, they must be treated securely and confidentially so that users can be assured of their safety.23
Blockchain is a technology that stores data in a ledger so that the data are saved in blocks. Each block is linked to others so that a blockchain is formed, and the data are transferred through a peer-to-peer network. Finance and banking were considered the first fields to use blockchain technology, and today, blockchain is used in energy, industry, insurance, healthcare, and others.24
Many features of blockchain make it useful in all fields, as it is distributed, decentralized, and secured, so there is no need for a central authority, as a consensus algorithm is used to archive data and reach agreement between nodes, where the ledger is distributed and maintained by agreement among all nodes within the network.25
Integrating Blockchain with the healthcare IoT will bring about significant transformations. This integration will create new paradigms and force us to reevaluate current systems and processes. In addition to securing user data and protecting privacy, blockchains can boost IoT adoption by improving security and privacy. Blockchain has revolutionized the sharing of medical and e-health information through secure applications.26
Healthcare IoT applications are an industry that will be revolutionized using blockchain technology. This integration has emerged as a cutting-edge technology for the decentralized sharing of medical records, ensuring the privacy of patient records, and monitoring of patients. In general, blockchains can be utilized for data management, specifically to improve data security, which includes data integrity, access control, and privacy preservation.27
Blockchain is divided into two types permission and permissionless. Blockchain types such as Bitcoin and Ethereum do not require approval to join and participate in the consensus process. Permission blockchain types such as Hyper-ledger and Quorum need prior authorization to join the network and participate in the consensus process.28
Permission is helpful when we need to restrict participation and access to data, especially when dealing with sensitive information, as is the case in the medical and healthcare industries. A permissionless blockchain is public, meaning that anyone can participate in the data validation and access processes. By contrast, a permission blockchain is a private or consortium, meaning that only permission entities can participate in data validation and access.29

Public Blockchain: Anyone can join and participate in the consensus process on a public blockchain, such as Bitcoin or Ethereum, without permission.

Private Blockchain: Because it is entirely under the control of one entity, this type of blockchain is considered a centralized network. A regulatory body certifies the addition of new members and provides write-and-read permission in a private blockchain. This power may be exercised solely or collaboratively by all the participants.30

Consortium Blockchain: The consortium blockchain is private, and a group, rather than a single organization, is responsible. A consortium between known businesses is formed to select those who have access to the blockchain ledger, whose transactions may remain public, and who must be restricted to a smaller group of members.31
Health data are stored both on- and off-chains. On-chain data means On-chain data are data with identity features and with the hash of all health data, but off-chain data means data stored in the form of document-oriented databases. The following is a collection of authors who used blockchain types in their research.32
The application type is the security of medical records and remote patient monitoring by using a consortium blockchain. While the authors presented the application type of medical record deposits using only a private blockchain, the authors presented the application type of medical record security and remote patient monitoring using a private blockchain.33
On the other hand, the application type in the security of medical records using a public blockchain, the application type in is medical image retrieval with privacy protection using a public blockchain, and the application type in is remote patient monitoring and diabetic disease prediction using a public blockchain.34

Blockchain Technology: With the creation of Bitcoin in 2008, blockchain technology has become increasingly popular. The system enables transaction transmission and storage by relying on a peer-to-peer network. Without centralized authority, transactions are organized into blocks and kept in a distributed ledger.35
Technically stated, blockchain is a system that incorporates many other concepts and technologies, including Ethereum, a Distributed Ledger system, Hyperledger Fabric, Immutability, Transparency, Cryptography, Consensus Algorithm, and Smart Contract.

Ethereum: To provide generalized blockchain technology in which all transaction-based state-machine concepts may be constructed, the project Ethereum was released as a platform in 2013. The goal is to provide end developers with access to a tightly integrated end-to-end system.36

Distributed Ledger: The ledger is shared among all blockchain participants in a distributed ledger blockchain, which can span numerous businesses. Records are kept in a distributed ledger continuously rather than in sorted blocks, and can be either private or public.37

Hyperledger Fabric: Developed by consensus, the Hyperledger is a distributed peer-to-peer ledger. A new generation of transactional applications that establish trust, accountability, and transparency at their core while streamlining business processes and legal restraints can be built using Hyperledger, a blockchain combined with a system for ‘‘smart contracts’’ and other supporting technologies.38
Immutability: Blockchain immutability occurs because their transaction data are tamper-proof, which means they cannot be altered or withdrawn.39

Transparency: The primary benefit of blockchain is transparency, which allows the creation of an unchangeable public record of transactions and the ability to trace them from their origin to their destination. Additionally, transparency provides financiers, policymakers, and investors with the knowledge they need to be sustainability of supply chains.40

Cryptography: The conversion of data and files from a well-known formula to other types of files is a component of encryption in terms of information technology. There are various encryption algorithms with different characteristics. Depending on the application, the correct algorithm can be selected. Finding new cryptographic strategies to enhance blockchain solutions is always possible because cryptography is a large area of study.41

Consensus Algorithm: Owing to its decentralized nature, the blockchain has scattered nodes throughout the network. The Byzantine Generals (BG) problem is analogous to the problem in which all network nodes establish consensus (i.e., general agreement). The BG dilemma arises when the generals in charge of the Byzantine army disagree with one another during the assault.42
Owing to the absence of a central node that maintains the ledger of all nodes, it is difficult for nodes in a dispersed network to reach a consensus. Blockchain can use different methods to reach consensus; further, consensus algorithms are classified as proof-based and voting-based consensus algorithms.43

Smart Contract: A set of computer programs, called smart contracts, is used to simplify the exchange of money, assets, or data. It becomes autonomous and impossible for a third party to stop or interfere with it once it is connected to the blockchain. In healthcare, smart contracts and blockchain technology are regarded as a secure way to transfer data from remote patient monitoring devices or to share the patient’s record electronically.44
There has been a growing interest in healthcare issues recently due to the search for safer and faster ways to serve patients and monitor patients remotely using Internet of Things technology. As follows,

Remote Patient MONITORING (RPM): A subtype of telemedicine called remote patient monitoring (RPM) enables people to use portable medical equipment to gather and transmit patient-generated health data (PGHD) to healthcare professionals. These devices include typical physiological data that can be gathered utilizing a remote patient monitoring system, such as weight, blood pressure, and heart rate.45

Patient Tracking: Inside a hospital or healthcare facility, a system for keeping track of patients is an integrated system with a base station, tracking routers, sensor pendants for patients and caregiver units, and other peripheral devices.46

Disease Prediction: The system used to Predict Disease Prediction utilizing machine learning models is a method that uses symptoms provided by patients or other users to forecast diseases.47

Fighting Covid-19 Pandemic: An IoT and AI-based method for remotely detecting the COVID-19 disease so that it can be stopped early.48

Image Retrieval For Medical Iot Systems: The variety and quantity of medical images have greatly expanded with the introduction of IoT devices for the medical industry. Medical image retrieval facilitates disease diagnosis and enhances medical image processing.49

Security Of Medical Records: Healthcare is one of the most sensitive industries since it deals with sensitive data, and privacy, security, access control, and the accessibility of medical records are significant concerns. Transmission, storage, and manipulation are three main stages where security in this industry must be guaranteed.50

Smart Telemedicine: Modern telemedicine technology uses communication to help doctors virtually visit their patients by using recorded video, email, or live video and obtaining patient information about their illnesses.51

Secure The Internet Of Medical Things: Beyond 50 billion devices across a wide range of application domains are expected to be connected through the Internet of Things. However, user security and privacy remain significant IoMT concerns.52

Healthcare And Big Data Generating enormous amounts of medical big data by intelligent Internet of Things (IoT) devices makes this another massive industry to investigate.53

Sensors And Blockchain: A sensor are a piece of equipment that receives a signal or stimulus and reacts to it by producing an electrical signal. The output signals represent various electrical signals, such as current or voltage. A sensor is a tool that receives multiple signals, such as physical, chemical, or biological signals and transforms them into an electric signal.54

Accurate Medical Decision: Non-communicable illness diagnoses are sometimes incomplete, undesired, or unnecessary. Therefore, we need accurate medical decisions to lessen the burden of sickness, promote public health, and effectively treat any disease. health information exchange (HIE) has yet to be able to solve will be resolved by accurate medical decisions.55

Healthcare Monitoring: A system for monitoring healthcare that would deliver the greatest possible medical care to everyone, everywhere, always. Many contemporary technologies are combined to address the growing need for solutions to health-related issues. There are numerous current studies in this area.56

Advantages: The main advantage of Blockchain is it’s decentralized property, this means there is no such centralized node to make decisions in a network. The decisions are solely based on each node in a distributed network. The databases are more vulnerable to attacks in a centralized network when the systems are working with third-party organization.57

Blockchain provides security by having it’s own proof of validity and authorization to process the transaction independently by each node. The immutable nature of Blockchain makes it harder to change the records or transaction, unless as explained by S. Nakamoto, the attacker should possess the computing power to redo the proof-of-work of the block and all the blocks in the chain.58

Each record is available to each participant in the network. This gives the transparency and trust among the participants who are aware of all the transactions that happens in the network. The transactions between peer to peer takes place by digitally signing a hash of previous transaction and public key of next peer or block in the network.59

Issues of Blockchain: Blockchain require more computing power when the number of transactions increases. Whenever a new transaction happens in the network, the nodes should verify whether the transaction contains the correct hashing details and takes care about double spending problem. It is said that miners involve in transaction process prefer to high transaction fee while transaction with low fee are delayed.60

The proof-of-work is said to cost more resources because when a node gets added, all the other node should calculate the hashing value out of which one value gets selected. If the attacker possess more than 51% of computing power in a chain then it can result in calculating Nonce value quicker and decide to change transaction details, which can also cause double spending attack.61

The IoT is growing exponentially year by year with its aim in 5G technologies, like Smart Homes and Cities, e-Health, distributed intelligence etc. but it has challenges in security and privacy. The IoT devices are connected in a decentralized approach. So, it is very complex to use the standard existing security techniques in the communication among IoT nodes.62
The BC is a technology they provide the security in transactions among the IoT devices. It provides a decentralize, distribute and publicly available shared ledger to store the data of the blocks that are processed and verified in an IoT network. The data stored in the public ledger is managed automatically by using the Peer-to-peer topology.63
The BC is a technology where transactions fired in the form of a block in the BC among IoT nodes. The blocks are linked with each other and every device has its previous device address. The blockchain and IoT together work in the framework of IoT and Cloud integration. In the future, the BC would revolutionize the IoT communication.64
The goals of BC and IoT integration could be summarized as follows.
Decentralized framework: This approach is similar in IoT and BC. It is removed the centralized system and provide the facility of a decentralized system. It improves the failure probability and performance of the overall system.

Security: In the BC, the transactions among nodes are secured. It is a very novel approach for secure communication. BC allows IoT devices to communicate with each other in a secure way.65

Identification: In IoT, all the connected devices are uniquely identified with a unique ID. Every block in BC is also uniquely identified. So, BC is a trusted technology that provides uniquely identified data stored in public ledger.

Reliability: IoT nodes in BC have the capabilities to authenticate the information passed in the network. The data is reliable because it is verified by the miners before entering in BC. Only verified blocks can enter in the BC.66

Autonomous: In BC, all IoT nodes are free to communicate with any node in the network without the centralized system.

Scalability: In BC, the IoT devices will communicate in high-available, a distributed intelligence network that connects with destination device in a real-time and exchange information.67

The Role of BC In IoT: The IoT enables the connected physical things to exchange their information in the heterogeneous network. The IoT could be divided into the following sections.
1. Physical Things: The IoT provide the unique id for each connected thing in the network. The physical things can exchange data with other IoT nodes.
2. Gateways: The gateways are the devices work among physical things and the cloud to ensure that the connection is established and security provided to the network.68
3. Networking: it is used to control the flow of data and establish the shortest route among the IoT nodes.
4. Cloud: It is used to store and compute the data. The BC is a chain of verified and cryptographic blocks of transactions held by the device connected in a network. The blocks data are stored in the digital ledger that is publicly shared and distributed.69

The following table represents the differentiation among all kind of blockchains. The database in blockchains has the properties such as decentralized trust model, high security, highly publicly accessed, privacy is low to high and the transferable identities while in a centralized database, the properties are centralized trust model, low in security, low publicly accessed, privacy is high and non-transferable identities. From the above properties, the blockchain is more advanced than the centralized storage.70
While blockchain technology offers a robust foundation for secure healthcare systems, its potential can be further augmented by integrating it with deep learning techniques. Deep learning, a subset of artificial intelligence, enables the analysis and extraction of complex patterns and insights from large-scale healthcare data.71
Traditional machine learning models often struggle with the inherent complexity and heterogeneity of healthcare data, limiting their effectiveness. In contrast, deep learning models, such as convolutional neural networks and recurrent neural networks, excel at recognizing patterns in unstructured data like medical images, sensor data, and natural language.72
However, deep learning models also come with computational challenges, particularly in resource-constrained environments. Hybrid deep learning approaches aim to overcome these limitations by combining the strengths of deep learning algorithms with traditional machine learning techniques, striking a balance between accuracy and computational efficiency.73

CONCLUSION

Blockchain is a groundbreaking idea that has revolutionized the way numerous businesses operate, effectively increasing user transparency. By eliminating corruption, dismantling bureaucratic barriers, and establishing the ownership of the common mass, blockchain promotes entrepreneurship. Peer-to-peer technology has created a personal platform for economic empowerment and offered up new opportunities. Although it is too soon to predict the future, blockchain technology appears to have a bright future and is therefore here to stay.
The confidentiality and uniqueness of medical records highlight the importance of having a robust security framework for their access and preservation. This framework is crucial for the advancement of digital healthcare. This study examines how blockchain technology can enhance the management and transfer of medical records by making them transparent,

traceable, and secure. It explores the evolution of medical record preservation, from digital certificates to the latest advancements with 5G and innovative blockchain technology.

Additionally, the study addresses the challenges and complexities of integrating blockchain technology into existing healthcare systems, aiming to support the fourth industrial revolution and improve digital healthcare. This evolution represents a shift away from simple automation toward intelligent solutions, personalized care, and interconnected systems, with the ultimate objective of delivering not only functional healthcare but also a patient-centered approach.

REFERENCES

1. ElRahman SA, Alluhaidan AS. Blockchain technology and IoT-edge framework for sharing healthcare services. Soft Computing. 2021 Nov;25(21):13753-77. https://doi.org/10.1007/s00500-021-06041-4'
2. Xu X, Wang X, Li Z, Yu H, Sun G, Maharjan S, Zhang Y. Mitigating conflicting transactions in hyperledger fabric-permissioned blockchain for delay-sensitive iot applications. IEEE Internet of Things Journal. 2021 Jan 8;8(13):10596-607. DOI: 10.1109/JIOT.2021.3050244
3. Khezr S, Moniruzzaman M, Yassine A, Benlamri R. Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences. 2019 Apr 26;9(9):1736. https://doi.org/10.3390/app9091736
4. Kumar T, Ramani V, Ahmad I, Braeken A, Harjula E, Ylianttila M. Blockchain utilization in healthcare: Key requirements and challenges. In2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom) 2018 Sep 17 (pp. 1-7). IEEE. DOI: 10.1109/HealthCom.2018.8531136
5. Moona G, Jewariya M, Sharma R. Relevance of dimensional metrology in manufacturing industries. Mapan. 2019 Mar 7;34(1):97-104. https://doi.org/10.1007/s12647-018-0291-3
6. Sivasankari B, Varalakshmi P. Blockchain and IoT technology in healthcare: a review. Challenges of Trustable AI and Added-Value on Health. 2022:277-8. doi: 10.3233/SHTI220455.
7. Wong MC, Yee KC, Nøhr C. Socio-technical considerations for the use of blockchain technology in healthcare. InBuilding continents of knowledge in oceans of data: The future of co-created ehealth 2018 (pp. 636-640). IOS Press. PMID: 29678038
8. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography. 2019 Jan 2;3(1):3. https://doi.org/10.3390/cryptography3010003
9. Dash S, Gantayat PK, Das RK. Blockchain technology in healthcare: opportunities and challenges. Blockchain Technology: Applications and Challenges. 2021 May 1:97-111. https://doi.org/10.1007/978-3-030-69395-4_6
10. Angraal S, Krumholz HM, Schulz WL. Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes. 2017 Sep;10(9):e003800. doi: 10.1161/CIRCOUTCOMES.117.003800.
11. Pilkington M. Blockchain technology: principles and applications. InResearch handbook on digital transformations 2016 Sep 30 (pp. 225-253). Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781784717766.00019
12. Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond bitcoin. Applied innovation. 2016 Jun;2(6-10):71.(doi: not available)
13. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In2017 IEEE international congress on big data (BigData congress) 2017 Jun 25 (pp. 557-564). Ieee. DOI: 10.1109/BigDataCongress.2017.85
14. Malinova K, Park A. Market design with blockchain technology. Available at SSRN 2785626. 2017 Jul 26.http://dx.doi.org/10.2139/ssrn.2785626
15. Nguyen QK. Blockchain-a financial technology for future sustainable development. In2016 3rd International conference on green technology and sustainable development (GTSD) 2016 Nov 24 (pp. 51-54). IEEE. DOI: 10.1109/GTSD.2016.22
16. Saeed H, Malik H, Bashir U, Ahmad A, Riaz S, Ilyas M, Bukhari WA, Khan MI. Blockchain technology in healthcare: A systematic review. Plos one. 2022 Apr 11;17(4):e0266462. doi: 10.1371/journal.pone.0266462
17. Radanović I, Likić R. Opportunities for use of blockchain technology in medicine. Applied health economics and health policy. 2018 Oct;16(5):583-90. doi: 10.1007/s40258-018-0412-8.
18. Leeming G, Cunningham J, Ainsworth J. A ledger of me: personalizing healthcare using blockchain technology. Frontiers in medicine. 2019 Jul 24;6:171. doi: 10.3389/fmed.2019.00171
19. Chakraborty S, Aich S, Kim HC. A secure healthcare system design framework using blockchain technology. In2019 21st international conference on advanced communication technology (ICACT) 2019 Feb 17 (pp. 260-264). IEEE. DOI: 10.23919/ICACT.2019.8701983
20. Yaeger K, Martini M, Rasouli J, Costa A. Emerging blockchain technology solutions for modern healthcare infrastructure. Journal of Scientific Innovation in Medicine. 2019 Jan 24;2(1). DOI: 10.29024/jsim.7
21. Azogu I, Norta A, Papper I, Longo J, Draheim D. A framework for the adoption of blockchain technology in healthcare information management systems: A case study of Nigeria. InProceedings of the 12th International Conference on Theory and Practice of Electronic Governance 2019 Apr 3 (pp. 310-316). https://doi.org/10.1145/3326365.3326405
22. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and ubiquitous computing. 2024 Feb;28(1):59-72. https://doi.org/10.1007/s00779-021-01583-8
23. Seliem M, Elgazzar K. BIoMT: Blockchain for the internet of medical things. In2019 IEEE international black sea conference on communications and networking (BlackSeaCom) 2019 Jun 3 (pp. 1-4). IEEE.

DOI: 10.1109/BlackSeaCom.2019.8812784
24. Azbeg K, Ouchetto O, Andaloussi SJ. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. Egyptian informatics journal. 2022 Jul 1;23(2):329-43. https://doi.org/10.1016/j.eij.2022.02.004
25. Johari R, Kumar V, Gupta K, Vidyarthi DP. BLOSOM: BLOckchain technology for Security of Medical records. Ict Express. 2022 Mar 1;8(1):56-60. https://doi.org/10.1016/j.icte.2021.06.002
26. Azbeg K, Ouchetto O, Andaloussi SJ, Fetjah L. A taxonomic review of the use of IoT and blockchain in healthcare applications. Irbm. 2022 Oct 1;43(5):511-9. https://doi.org/10.1016/j.irbm.2021.05.003
27. Ktari J, Frikha T, Ben Amor N, Louraidh L, Elmannai H, Hamdi M. IoMT-based platform for E-health monitoring based on the blockchain. Electronics. 2022 Jul 25;11(15):2314. DOI:10.3390/electronics11152314
28. Attia O, Khoufi I, Laouiti A, Adjih C. An IoT-blockchain architecture based on hyperledger framework for health care monitoring application. InNTMS 2019-10th IFIP international conference on new technologies, mobility and security 2019 Jun 24 (pp. 1-5). IEEE Computer Society. DOI : 10.1109/NTMS.2019.8763849
29. Mohammed R, Alubady R, Sherbaz A. Utilizing blockchain technology for IoT-based healthcare systems. InJournal of Physics: Conference Series 2021 Mar 1 (Vol. 1818, No. 1, p. 012111). IOP Publishing. DOI:10.1088/1742-6596/1818/1/012111
30. Faruk MJ, Shahriar H, Valero M, Sneha S, Ahamed SI, Rahman M. Towards blockchain-based secure data management for remote patient monitoring. In2021 IEEE international conference on digital health (ICDH) 2021 Sep 5 (pp. 299-308). IEEE. DOI: 10.1109/ICDH52753.2021.00054
31. Reegu FA, Abas H, Gulzar Y, Xin Q, Alwan AA, Jabbari A, Sonkamble RG, Dziyauddin RA. Blockchain-based framework for interoperable electronic health records for an improved healthcare system. Sustainability. 2023 Apr 7;15(8):6337. DOI:10.3390/su15086337
32. Kazmi HS, Nazeer F, Mubarak S, Hameed S, Basharat A, Javaid N. Trusted remote patient monitoring using blockchain-based smart contracts. InInternational Conference on Broadband and Wireless Computing, Communication and Applications 2019 Oct 18 (pp. 765-776). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-33506-9_70
33. Sabu S, Ramalingam HM, Vishaka M, Swapna HR, Hegde S. Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain. Global Transitions Proceedings. 2021 Nov 1;2(2):429-33. https://doi.org/10.1016/j.gltp.2021.08.033
34. Chinaei MH, Gharakheili HH, Sivaraman V. Optimal witnessing of healthcare IoT data using blockchain logging contract. IEEE Internet of Things Journal. 2021 Jan 13;8(12):10117-30. DOI: 10.1109/JIOT.2021.3051433
35. Elgendy MA, Aborizka M, Allam AM. A blockchain-based model for securing IoT transactions in a healthcare environment. International Journal of Advanced Computer Science and Applications. 2022;13(9). DOI:10.14569/IJACSA.2022.0130908
36. Sarmah SS. Understanding blockchain technology. Computer science and engineering. 2018 Aug;8(2):23-9. DOI: 10.5923/j.computer.20180802.02
37. Al-Nbhany WA, Zahary AT, Al-Shargabi AA. Blockchain-IoT healthcare applications and trends: a review. IEEE Access. 2024 Jan 2;12:4178-212. DOI: 10.1109/ACCESS.2023.3349187
38. Politou E, Casino F, Alepis E, Patsakis C. Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing. 2019 Oct 25;9(4):1972-86. DOI: 10.1109/TETC.2019.2949510
39. Andrade J, Voora V. 'Traceability systems a powerful tool for agricultural voluntary sustainability standards. SSI, Tech Rep, Dec; 2016 Dec.(doi: not available)
40. [1]Wafaa AA, Zahary A. A Comparative Study among Cryptographic Algorithms: Blowfish, AES and RSA.(doi: not available)
41. Raikwar M, Gligoroski D, Kralevska K. SoK of used cryptography in blockchain. Ieee Access. 2019 Oct 11;7:148550-75. DOI: 10.1109/ACCESS.2019.2946983
42. Rama RK. Overview of blockchain technology: consensus algorithms, applications [Internet]. 2021doi: 10.13140/RG.2.2.17450.75205
43. Dai HN, Wu Y, Wang H, Imran M, Haider N. Blockchain-empowered edge intelligence for internet of medical things against COVID-19. IEEE Internet of Things Magazine. 2021 Jul 21;4(2):34-9. DOI: 10.1109/IOTM.0011.2100030
44. Wang M, Zhang H, Wu H, Li G, Gai K. Blockchain-based secure medical data management and disease prediction. InProceedings of the fourth ACM international symposium on blockchain and secure critical infrastructure 2022 May 30 (pp. 71-82). https://doi.org/10.1145/3494106.3528678
45. Vyas S, Shabaz M, Pandit P, Parvathy LR, Ofori I. [Retracted] Integration of Artificial Intelligence and Blockchain Technology in Healthcare and Agriculture. Journal of Food Quality. 2022;2022(1):4228448. DOI 10.1155/2022/4228448
46. Gamboa H, Silva F, Silva H. Patient tracking system. In2010 4th international conference on pervasive computing technologies for healthcare 2010 Mar 22 (pp. 1-2). IEEE. DOI: 10.4108/ICST.PERVASIVEHEALTH2010.8916
47. Kulkarni V, Surwase S, Pingale K, Sarage S, Karve A. 'Prediction of disease using machine learning. Irjet. 2020 May;7(5):56-72.(doi: not available)
48. Onik MM, Aich S, Yang J, Kim CS, Kim HC. Blockchain in healthcare: Challenges and solutions. InBig data analytics for intelligent healthcare management 2019 Jan 1 (pp. 197-226). Academic Press. https://doi.org/10.1016/B978-0-12-818146-1.00008-8
49. Mudarri T, Al-Rabeei S, Abdo S. Security fundamentals: access control models. Interdisciplinarity in theory and practice. 2015 Aug;8.(doi: not available)

50. Godly CJ, Balasubramanian V, Jinila BY. Blockchain adaptation of remote patient monitoring with Internet of Medical Things. In2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS) 2022 Jun 23 (pp. 1-7). IEEE. DOI: 10.1109/IC3SIS54991.2022.9885298
51. Hameed K, Bajwa IS, Sarwar N, Anwar W, Mushtaq Z, Rashid T. Integration of 5G and block-chain technologies in smart telemedicine using IoT. Journal of Healthcare Engineering. 2021;2021(1):8814364. doi: 10.1155/2021/8814364
52. Quasim MT, Algarni F, Radwan AA, Alshmrani GM. A blockchain based secured healthcare framework. In2020 International Conference on Computational Performance Evaluation (ComPE) 2020 Jul 2 (pp. 386-391). IEEE. DOI: 10.1109/ComPE49325.2020.9200024
53. Altay A, Learney R, Güder F, Dincer C. Sensors in blockchain. Trends in Biotechnology. 2022 Feb 1;40(2):141-4. https://doi.org/10.1016/j.tibtech.2021.04.011
54. Ntayagabiri JP, Bentaleb Y, Ndikumagenge J, EL H. AThorough STUDY OF THE INTERNET OF THINGS: FROM CORE COMPONENTS TO SECURITY AND APPLICATIONS. DOI: 10.5121/ijnsa.2024.16603
55. Khabya R, Goel S, Singh M. ‘Solar energy based blockchainenabled healthcare monitoring using IoT. Int. Res. J. Eng. Technol.. 2022 Jun;9(06):1-7. (doi: not available)
56. Somani S, Choure N, Jadhav S, Gurav S. ‘Blockchain based soldier health monitoring $ tracking system. Int. J. Advance Sci. Res. Eng. Trends.;4(8):1-6. (doi: not available)
57. Bach LM, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms. In2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO) 2018 May 21 (pp. 1545-1550). Ieee. DOI: 10.23919/MIPRO.2018.8400278
58. Alsunaidi SJ, Alhaidari FA. A survey of consensus algorithms for blockchain technology. In2019 International Conference on Computer and Information Sciences (ICCIS) 2019 Apr 3 (pp. 1-6). IEEE. DOI: 10.1109/ICCISci.2019.8716424
59. Golosova J, Romanovs A. The advantages and disadvantages of the blockchain technology. In2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE) 2018 Nov 8 (pp. 1-6). IEEE. DOI: 10.1109/AIEEE.2018.8592253
60. Lin IC, Liao TC. A survey of blockchain security issues and challenges. Int. J. Netw. Secur.. 2017 Sep 1;19(5):653-9. (DOI: 10.6633/IJNS.201709.19(5).01)
61. Han M, Li Z, He J, Wu D, Xie Y, Baba A. A novel blockchain-based education records verification solution. InProceedings of the 19th annual SIG conference on information technology education 2018 Sep 14 (pp. 178-183). https://doi.org/10.1145/3241815.3241870
62. Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems. 2018 Nov 1;88:173-90. https://doi.org/10.1016/j.future.2018.05.046
63. Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: A survey. International journal of web and grid services. 2018;14(4):352-75. https://doi.org/10.1504/IJWGS.2018.095647
64. Haber S, Stornetta WS. How to time-stamp a digital document. InConference on the Theory and Application of Cryptography 1990 Aug 11 (pp. 437-455). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-38424-3_32
65. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system.(doi: not available)
66. Alphand O, Amoretti M, Claeys T, Dall'Asta S, Duda A, Ferrari G, Rousseau F, Tourancheau B, Veltri L, Zanichelli F. IoTChain: A blockchain security architecture for the Internet of Things. In2018 IEEE wireless communications and networking conference (WCNC) 2018 Apr 15 (pp. 1-6). IEEE. DOI: 10.1109/WCNC.2018.8377385
67. Alam T, Benaida M. The role of cloud-MANET framework in the internet of things (IoT). arXiv preprint arXiv:1902.09436. 2019 Feb 25.https://doi.org/10.3991/ijoe.v14i12.8338
68. Alam T. Middleware implementation in cloud-MANET mobility model for internet of smart devices. arXiv preprint arXiv:1902.09744. 2019 Feb 26.https://doi.org/10.48550/arXiv.1902.09744
69. Singh P, Kumar P, Alam T. Generating different mobility scenarios in ad hoc networks. International Journal of Electronics Communication and Computer Technology. 2014;4(2):582-91. .(doi: not available)
70. Sharma A, Alam T, Srivastava D. Ad hoc network architecture based on mobile Ipv6 development. Advances in Computer Vision and Information Technology. 2008 Jan 10;224. .(doi: not available)
71. Ali A, Ejaz A, Jabbar M, Hameed K, Mushtaq Z, Akhter T, Haider A. Performance analysis of AF, DF and DtF relaying techniques for enhanced cooperative communication. In2016 Sixth International Conference on Innovative Computing Technology (INTECH) 2016 Aug 24 (pp. 594-599). IEEE. DOI: 10.1109/INTECH.2016.7845056
72. Mushtaq Z, Sani SS, Hamed K, Ali A, Ali A, Belal SM, Naqvi AA. Automatic agricultural land irrigation system by fuzzy logic. In2016 3rd International Conference on Information Science and Control Engineering (ICISCE) 2016 Jul 8 (pp. 871-875). IEEE. DOI: 10.1109/ICISCE.2016.190