IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Systematic Review on AI-Blockchain based E-Healthcare Records Management Systems

Alaa Haddad[1], Mohamed Hadi Habaebi[1], *Senior Member*, IEEE, Mohd Rafiqul Islam[1], *Senior Member*, IEEE, Nurul Fadzlin Hasbullah[1*], *Member*, IEEE, and Suriza Ahmad Zabidi[1]

[1] Department of Electrical and Computer Engineering, International Islamic University Malaysia (IIUM), Jalan Gombak, KL 53100, W.P., Malaysia

Corresponding author: *Nurul Fadzlin Hasbullah (nfadzlinh@iium.edu.my)

This material is based upon work supported by the Air Force Office of Scientific Research under award number FA2386-21-1-4025. The research work was conducted at the IoT & wireless communication protocols laboratory, International Islamic University Malaysia (IIUM).

ABSTRACT Electronic health records (EHRs) are digitally saved health records that provide information about a person's health. EHRs are generally shared among healthcare stakeholders, and thus are susceptible to power failures, data misuse, a lack of privacy, security, and an audit trail, among other problems. Blockchain, on the other hand, is a groundbreaking technology that provides a distributed and decentralized environment in which nodes in a list of networks can connect to each other without the need for a central authority. It has the potential to overcome the limits of EHR management and create a more secure, decentralized, and safer environment for exchanging EHR data. Further, blockchain is a distributed ledger on which data can be stored and shared in a cryptographically secure, validated, and mutually agreed-upon manner across all mining nodes. The blockchain stores data with a high level of integrity and robustness, and it cannot be altered. When smart contracts are used to make decisions and conduct analytics with machine-learning algorithms, the results may be trusted and unquestioned. However, Blockchain is not always indestructible and suffers from scalability and complexity issues that might render it inefficient. Combining AI and blockchain technology can handled some of the drawbacks of these two technical ecosystems effectively. AI algorithms rely on data or information to learn, analyze, and reach conclusions. The performance of AI algorithms is enhanced through the data obtained from a data repository or a reliable, secure, trustworthy, and credible platform.

Researchers have identified three categories of blockchain-based potential solutions for the management of electronic health records: conceptual, prototype, and implemented. The purpose of this research work is to conduct a Systematic Literature Review (SLR) to identify and assess research articles that were either conceptual or implemented to manage EHRs using blockchain technology. The study conducts a comprehensive evaluation of the literature on blockchain technology and enhanced health record management systems utilizing artificial intelligence technologies. The study examined 189 research papers collected from various publication categories. The in-depth analysis focuses on the privacy, security, accessibility, and scalability of publications. The SLR has illustrated that blockchain technology has the potential to deliver decentralization, security, and privacy that are frequently lacking in traditional EHRs. Additionally, the outcomes of the extensive analysis inform future researchers about the type of blockchain to use in their research. Additionally, methods used in healthcare are summarized per application area while their pros and cons are highlighted. Finally, the emphasized taxonomy combines blockchain and artificial intelligence, which enables us to analyze possible blockchain and artificial intelligence applications in health records management systems. The article ends with a discussion on open issues for research and future directions.

INDEX TERMS Blockchain, artificial intelligence, healthcare, management, EHR

I. INTRODUCTION

Medical and healthcare researchers emphasize the importance of their ability to collect and analyze multi-source data in order to identify potential community health hazards, provide case-specific therapies, and deliver focused medicine [1], which could promote informed clinical decision making

and lead to improved patient care quality. This information can help to improve personal health information systems such as patient health records (PHR) and patient portals. Patients frequently do not have easy access to their historical data, while clinicians retain primary ownership.

Incorporating blockchain, AI, and other readily available technologies into a business's DNA is the key to success [3]. To enhance medical research and attain patient-centricity, the industry needs to use technology to produce user- and customer-centric interfaces and data-driven decisions for creative ways to data processing and improved outcomes [2,16]. For example, artificial intelligence (AI) could assist in identifying and prioritizing patients for drug monitoring and development, which is essential for regulated drug production and accelerated timeframes [3]. Using numerical drug design methodologies and AI, clinical trial data was evaluated for repurposing marketed pharmaceuticals, exploring the efficacy of medication formulations, and dose measurement [6]. Blockchain facilitates the development of a system that creates and manages content blocks known as ledgers, incorporating secure and automated data analysis. All health-related information will be recorded and analyzed securely, allowing physicians, healthcare providers, and payers to receive rapid updates. However, storing massive records on the blockchain, such as complete electronic medical records or genetic data records, would be expensively inefficient due to the large computational resources required. This is a major drawback of blockchain technology, as it makes data queries within a blockchain difficult. Implementing AI algorithms into the blockchain, however, can help overcome this drawback [6]. To comprehend health trends and patterns, artificial intelligence began to learn and reason like a clinician. It collects unstructured data from a variety of sources, including the patient, the radiologist, and the pictures. AI is also capable of conducting complex computational processes and evaluating enormous quantities of patient information fast. However, some doctors are still hesitant to use AI in healthcare, particularly in positions that may affect a patient's health, due to the significant capabilities that AI may bring, which have proved that it can execute numerous dynamic and cognitive processes faster than a person. The automobile sector has already demonstrated its capacity to utilize AI to produce autonomous automobiles. However, some businesses have already identified machine learning-based methods for detecting fraud and identifying financial dangers and demonstrating AI's maturity level [17].

The following section discusses the main terms and principles of intelligent technology in healthcare. We look at how intelligent technologies evolve and the security criteria for their implementation in the healthcare industry sector. In addition, the advent of modular IT systems has been observed since the implementation of healthcare provisions in the 1970s.

Healthcare 1.0 is the name given to this period. Because of a lack of funding, healthcare services were limited and not coordinated with digital systems during this period. On the other hand, bio-medical machines had not yet been built and did not integrate with networked electronic devices. Paper-based medications and reports were commonly used in healthcare institutions during this period, resulting in increased costs and time.

From 1991 to 2005, the Healthcare 2.0 period was observed. During this time, health and information technology were merged to form the foundations of today's healthcare systems. This process saw the introduction of automated monitoring, which provided doctors with imaging systems for assessing patients' health. Simultaneously, new user-enabled innovations in the healthcare sector started to evolve, coinciding with the advent of social media. Healthcare services began to build online communities to exchange information and expertise, store data on cloud servers, and provide mobile access to documentation and patient records, allowing both the provider and the patient to have constant access. During this time, critics shared their dissatisfaction with the misleading facts and the invasion of patients' privacy. Healthcare systems used networked electronic health management practices combined with clinical imaging systems to help doctors get more reliable, accurate, and timely access to patient's data.

Healthcare 3.0 debuted simultaneously as Web, allowing users to customize how patient healthcare records were distributed. User interfaces became simpler and more tailored, allowing for more customized and optimized experiences. Electronic Healthcare Records (EHRs) and wearable and implantable devices were also introduced, allowing for real-time, ubiquitous monitoring of patients' healthcare. Similarly, EHR systems [7] emerged that incorporated stand-alone non-networked systems, such as social media networks, to store patient's data.

Finally, the care period proliferated, inspired by the idea of Industry 4.0, in which Hi-tech and Hi-touch systems are implemented, using cloud computing, fog, and edge computing, big data analytics, AI, and machine learning to create blockchains that allow for real-time access to patient's clinical data [8]. The fundamental goal of this period is to improve virtualization, allowing for real-time personalized healthcare. The emphasis is now on teamwork, coherence, and integration, using AI technology to make healthcare more predictive and personalized.

By considering the above scenario, this paper aims to identify the potentiality of AI-blockchain to manage EHRs and show the challenges and future scopes. This systematic review explores research that offers conceptual solutions, experimental results, prototypes, and blockchain implementations for managing EHRs.

It is also important to note that the purpose of this review is not only to identify the use cases or examples of blockchain-based applications in healthcare, but also to understand the limitations and challenges of blockchain-based healthcare applications as well as the technical approaches, and how to

overcome these blockchain limitation by employing AI technologies, methodologies, and concepts in developing AI-blockchain applications. The implementation of blockchain technology in healthcare is a relatively new paradigm that is expanding rapidly; thus, there are numerous new publications on the subject.

Existing literature lacks a unified and systematic view of blockchain applications in the healthcare area; these gaps necessitated this study. This work focuses mostly on the following issues:

- A progressive evolution of blockchain technology over time.
- Recognizing the technological limits of blockchain architecture that impact various healthcare processes
- The evolution of artificial intelligence in the health records management system over time.
- Evaluating the extent to which the consequences of managing EHR using ai and blockchain are appropriate.

The rest of the paper is outlined as follows. section 2 shows the contribution of the paper, in addition, section 3 illustrates the motivation of AI-blockchain in EHR systems. Sections 4, 5 and 6 discuss the background of AI-Blockchain technologies and their applications in the healthcare system scope.

Research methodology, research questions, and discussion are detailed in Section 7. Then, the taxonomy of the AI blockchain is discussed next in section 8. Thoughts on open challenges and future work are presented in Section 9. Section 10 concludes the paper.

II. CONTRIBUTION

In this paper, the main contributions are summarized as follows:

1) A detailed discussion on the benefits of applying Blockchain to the problem of health record management.
2) An expanded discussion on the benefits of applying AI to the problem of health record management.
3) An updated discussion on privacy and security issues related to EHR management.
4) A taxonomy of proposed AI-Blockchain solutions to the problem of EHR.
5) A discussion on open challenges and future research directions to pave the way for an efficient and trusted AI-Blockchain EHR ecosystems that improves on current centralized models and enable a patient-centric data-sharing platform by giving the patients complete control over their data.

III. MOTIVATION

A. MOTIVATION FOR BLOCKCHAIN-BASED IMPLEMENTATION ON EHR SYSTEM

EHRs typically contain information like a patient's medical history, personal statistics (such as age and weight), laboratory test results, and other information. As a result, these data must be kept secure and private. Furthermore, hospitals are subject to strict governmental scrutiny in some countries like the United States [13]. Deploying and implementing healthcare systems in practice also presents several problems. As previously mentioned, centralized server models are prone to single-point attack constraints and malevolent insider assaults. Users (for example, patients) who have their data outsourced or stored in these EHR systems lose ownership of their data. They have no means of knowing who is accessing it and for what purposes (i.e., violation of personal privacy). Such information may also be in danger of being leaked to another organization by malicious insiders; for example, an insurance company may reject coverage to a patient based on leaked medical records. In the meantime, data exchange is becoming more important, especially as our society and population become more mobile. Shared data can improve medical service delivery, for example, by exploiting the interconnectedness between different healthcare organizations. It will be difficult to overcome the "Information and Resource Island" (information silo), for example, due to privacy concerns and restrictions. In addition, the information silo contributes to unnecessary data redundancy and bureaucracy.

In this situation, the United States Congress passed and signed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 [190]. It established standards to protect the privacy and security of personal health information, as well as many programs to combat fraud and abuse in the healthcare system, including the following five rules:

- The privacy rule. Regulations governing the use and dissemination of patient health information in the treatment and operations of healthcare organizations.
- The rule of Transactions and Code Sets. All health plans must uniformly engage in healthcare transactions.
- The rule of security. The security rule supplements privacy by limiting access to computer systems and preventing interception of communications via open networks.
- The Rule of Unique Identifiers. To secure patient personal information, only the National Provider Identifier (NPI) is used to identify covered entities in standard transactions.
- The Rule of Enforcement. For breaking HIPAA rules, there will be an investigation and fines.

ISO 27789 [9] is another typical audit trail for EHRs that keeps personal health information auditable across systems and domains. A secure audit record must be created every time an operation is triggered by a system that complies with ISO 27789. As a result, a collaborative and open data-sharing system is essential, as it simplifies auditing and post-incident

inquiry or forensics in the event of alleged misbehavior (e.g., data leakage). Forensic scholars also do highlight this concept (forensic-by-design) [9,10].

When the next generation of secure EHR systems has been generated, we should follow the next requirements based on the relevant standards listed above:

- Data accuracy and integrity: e.g., unauthorized data modification is not allowed and can be detected.
- Data security and privacy.
- Efficient data sharing mechanism [11].
- The patient control mechanism allows the patient control mechanism of EHRs (e.g., the patients will have control over their records and can get a notification if there is unauthorized access or loss of their data).
- Data auditing and accountability (e.g., forensic by design [9,10].
- The decentralization of power. In contrast to the centralized approach, blockchain does not require a semi-trusted third party.
- Safety and security. The blockchain-based decentralized system is resistant to a single point of failure and insider attacks.
- The use of a pseudonym. Each node is assigned a pseudonymous public address to safeguard its true identity.
- Impermanence. using the cryptographic hash function in one way, it will make the computationally hard to delete or change any records of any record of any block included in the chain.
- Independence. Patients have control over their data and can share it in a variety of ways thanks to the settings of special items in the smart contract
- Mechanism of motivation. Blockchain's incentive structure can encourage competitive institutions to collaborate and share information to advance medical services and research.
- Transparency. Can track every operation in the blockchain because every previous transaction is recorded in the chain.

Based on the following explanation, blockchain technology can be used to achieve the previously mentioned requirements.

B. BENEFITS OF USING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE.

The coronavirus epidemic can be dealt with in a variety of ways using blockchain and AI. There are many real-world applications for the blockchain that can be put to good use in the fight against the coronavirus outbreak. Blockchain could be used to monitor the spread of coronavirus infections around the world by installing blockchain network client software on users' mobile devices. One of the most important aspects of blockchain is its ability to protect user privacy, allowing early identification of epidemics while prohibiting the publication of user information. It also helps with epidemic and treatment management by making vaccine trials more efficient and transparent, as well as keeping track of all fundraising activities and donations. When it comes to combating the Coronavirus, AI has a range of approaches to help. AI may be used to identify viruses and anticipate how they will spread by analyzing the accumulated knowledge of environmental factors [5], healthcare access, and the transmission method. By classifying coronavirus inside localized outbreaks of sickness, AI can help determine whether or not it is indeed there. Pneumonia, severe acute respiratory syndrome, and renal failure are all possible outcomes of coronary virus infections. For example, a genome-based neural network that has already been developed for personalized care can be very useful in managing these adverse events or symptoms caused by a coronavirus, particularly when virus impact is dependent on individual immunity and genome structure and no single treatment can effectively treat all symptoms at this time. AI may also be useful in speeding up the development of a new vaccination for novel coronaviruses [6]. As a final application of AI, it may be possible to develop an automated model or correlation between medical records and results. Clinical protocols for coronavirus-like outbreaks could benefit from these models' quick identification of diagnostic and therapeutic options. A recent White House request to deploy AI to assist the US government in responding to the coronavirus pandemic [7] is based on these prospective advantages.

Disintermediation is defined as the absence of a centralized authority that collects, processes, and validates data & models designed and shared. It enables a reduction in the time, error, and cost of process performance aimed at building and updating a predictive model that supports clinical practice and risk management. Transactions certified by the blockchain, and the data included within them are irreversible, in the sense that they cannot be changed or erased, ensuring their legitimacy while also strengthening the security of the system in which the activities take place [9]. Furthermore, the cryptographic system, the immutability of the data communicated across the network, and the lack of a centralized authority foster greater trust in the system, as the need to maintain this confidence among the parties involved in the process fades [10].

C. THE HEALTHCARE SYSTEMS' SHORTCOMINGS

In the wake of the COVID-19 pandemic, current healthcare systems have come under scrutiny. Currently some existing healthcare systems may be overburdened by the COVID-19 outbreak. As of right now, there is no trustworthy data monitoring system in place [18] to give key healthcare organizations the information they require about potential epidemics in real-time. In fact, most of the current coronavirus information comes from separate sources such as the public,

hospitals, clinical labs with a large amount of inaccurate data without being monitored thoroughly. The use of unreliable information makes it challenging for potential outbreak identification and quarantine. Another limitation is the current time-consuming and in-accuracy coronavirus detection procedure that often takes several hours to complete the virus tests. This is unacceptable in light of the rapid spread of the coronavirus. It is critical to learn how to swiftly and accurately identify coronaviruses. Coronavirus data processing utilizing human-dependent medicinal software is exceedingly tough, especially when dealing with complex patterns and enormous volumes. Blockchain technology offers promising security solutions to aid in the fight against pandemics. Indeed, the blockchain creates immutable transaction ledgers for medical data sharing systems. More importantly, the combination of blockchain and smart contract technology eliminates the need for central servers to ensure fairness among transaction parties. Traceability and decentralization are two key characteristics of blockchain that are not found in other traditional security techniques. Furthermore, blockchain can provide reliable data analytics. Data collection is an important step in disease analytics. How to ensure the reliability of collected data during data collection is important for ensuring the high quality of disease data analytics [66]. The use of incorrect data or untrustworthy database sources can lead to biased analytical results, which can have fatal consequences, such as incorrect diagnosis. Furthermore, in an emergency epidemic situation, many sources of contagious disease data are collected without protection from hospitals, the public, or the media, which can result in data modifications. These issues would undoubtedly affect the accuracy of the collected data, reducing the reliability of the analysis process. Because of its security, blockchain is in high demand in such contexts to ensure the reliability of collected data. Due to consensus mechanisms, blockchain also ensures the correct ordering of data records from data sources to destinations (e.g., hospitals or clinical labs), ensuring the high quality of data collection. These blockchain features would ensure accurate data collection and thus reliable disease analysis.

As the last point, there are privacy issues over the mass monitoring of the population to monitor the coronavirus. Healthcare organizations can monitor individuals' cell phones without a court order to prevent the spread of the COVID-19 coronavirus, for example [4]. However, human rights and privacy advocates have objected to the plan since it might potentially disclose citizens' private information, which could lead to major civil liberties abuses. To combat the spread of the coronavirus, real-time monitoring systems that protect user privacy are needed. As privacy become more of a concern, secret blockchain networks, that uses Privacy by Blockchain Design (PbBD) technologies to customize the level of privacy, are now gaining attention.

IV. Background of Blockchain in Health Records Management System

We briefly outline blockchain technology to assist readers in comprehending the remainder of the article. In the following subsections, we will cover the fundamental structure of blockchain technology to facilitate better grasping of the survey and the notion of blockchain.

A. BLOCKCHAIN

A blockchain may be thought of as a decentralized public ledger that is accessible to all peers in a network where all committed, valid, and completed transactions are stored in a list or chain of blocks. The chain grows as new blocks are appended to it continuously. Blockchain technology employs a combination of two technologies: asymmetric cryptography and P2P distributed consensus to guarantee ledger consistency and user security. Hence, these time stamped blocks are linked together by a cryptographic hash [11]. Typically, each block contains transaction records that have been verified by peers, often known as miners. The chain is continually lengthened, with each new block being added to the end. Each new block, on the other hand, contains a reference to the preceding block's header, which is essentially a cryptographic hash (e.g., SHA-256). the creation of each block has been with pseudonymity, transparency, and immutability [12,13].

A block is made up of the block header and the block body, defined below, as seen in Figure 1.

- Version: the cryptocurrency version number that indicates which set of block validation rules should be followed.
- Previous block hash: the hash value of the block before it.
- Time stamp: the current block's creation time is the timestamp.
- Nonce: to solve a PoW problem, miners alter a four-byte random field each time they hash the code.
- Hash target: new block's hash value must fall within a certain range before it is considered valid. Target hash is used in determining the difficulty of the input and can be adjusted in order to ensure that blocks are processed efficiently.
- Merkel Root: transactions in the block's body generate the Merkle tree root's hash value.

Transactions regularly are included in the block's body. Each leaf node of the Merkle tree represents a transaction, and every nonleafy node represents the hash value of the two concatenated child nodes that make up the leaf node. To validate the presence and integrity of a transaction, every node only needs to check the hash value of the two concatenated child nodes that make up the leaf node rather than the entire Merkle tree. There will be a new hash value generated in the top layer for any changes made to a transaction, which will result in one root hash. In addition to the block size, the maximum number of transactions per block is determined by the size of each transaction. Once the

hash function is used, all blocks will be linked. Because data that has been validated cannot be modified or deleted in the blockchain, as new data comes in, it will be added to the linked blocks. Every change to the block will result in a new hash value (a new block) and a new link relationship based on this state. Immutability and security are fundamental features of blockchain technology.

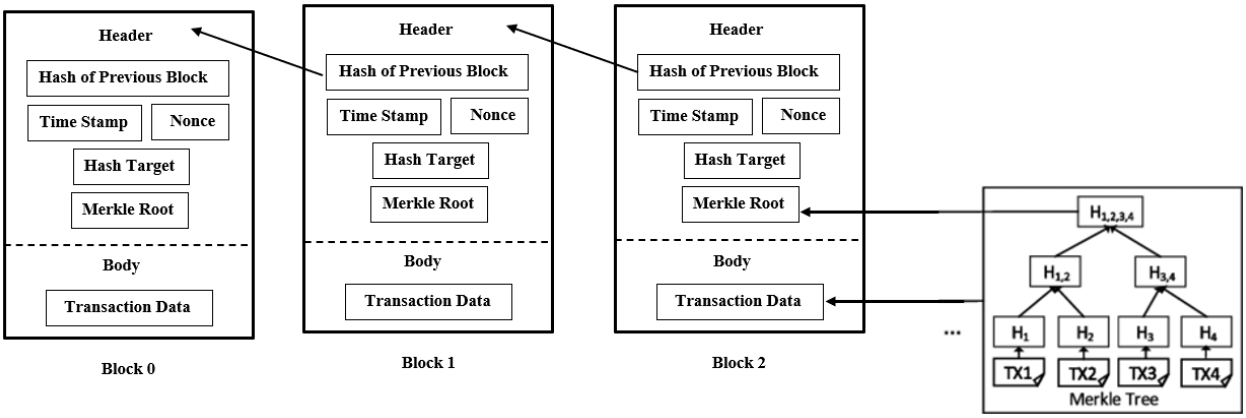

FIGURE 1. Standard Block Structure

B. DIGITAL SIGNATURE

For transaction authentication in an untrustworthy environment, asymmetric cryptography is often utilized [11]. To send and verify the legitimacy of transactions, asymmetric cryptography is a key component of the Blockchain. In a P2P network, transactions are signed with the transaction initiator's private key before they are received. Most current blockchains use the elliptic curve digital signature technique (ECDSA) [15].

When a transaction is requested or initiated, a block representing that transaction is generated and broadcasted to all adjacent nodes via the peer-to-peer (P2P) network, in which peers have equal Privileges. This block will be received by other nodes. The sender's public key is used to validate the legitimacy of the received block using specified block validation rules. If the block is genuine, it will be transmitted to other nodes until they have all verified it. If not, it will be discarded during the procedure. Only valid blocks can be added and stored in the blockchain network.

Figure 2 illustrates the process using coins, where Bob receives from Alice a specific number of coins. She initiates a transaction using her private key, which is then confirmed by the network. Anyone with access to Alice's public key can easily verify the transaction. In the second step, the P2P network disseminates the transaction to other nodes. In the third step, the transaction is verified by each node according to predetermined rules. Each validated transaction will be grouped chronologically and added to a new block in step 4 after the miner solves the problem. Then, each node will update and back up the new block.

C. ALGORITHMS FOR BUILDING CONSENSUS

There is no one point of authority in the blockchain network. As a result, a fundamental issue is the Byzantine Generals Problem [14], a variant of which was created in the context of distributed networks in 1982. A gang of Byzantine generals is surrounding the city, and they have little chance to win the fight unless they all attack at the same time, the Byzantine Generals claims. There is a question as to whether or not there will be any traitors in a dispersed context. So they must make a choice: attack or retreat. It is the same challenge for the blockchain network.

To obtain a consensus protocol among all the distributed nodes before a new block can be attached to the blockchain, different protocols have been developed [15].

• PoW (Proof of Work): PoW is the name of Bitcoin's consensus algorithm (Proof of Work). Before receiving any rewards, a miner node with a certain level of computing (hashing) power must perform laborious task of mining to prove that he is not malicious [99,100]. To find an eligible nonce value that is smaller than (or equal to) the target hash value, the node must continually perform hash calculations. It is difficult to generate a nonce, yet it is trivial for other nodes to check its validity. The task is costly as a result of the numerous computations required (computational resources). If the blockchain network were to be attacked by a 51 percent attack [191], this would be an extreme case. A miner or a group of miners having more than 51% of the processing power can delay the generation of new blocks and create fraudulent records of transactions that benefit the attackers.

• Proof of Stake (PoS) Compared to PoW, PoS uses less power. It is widely believed that nodes with the highest stakes (such as cash) are less likely to attack the network [105]. It's unfair to decide based on account balance because the wealthiest node is more likely to take over the network, making it a centralized one.

• Delegated Proof of Stake (DPoS) Similar to PoS, DPoS can also be used. The key distinction between DPoS and PoS is that the DPoS is democratically representative [192], whereas the PoS selection is based on all nodes. Stakeholders can elect delegates to decide who generates and validates new blocks. The fewer nodes that validate a block, the faster the transactions are confirmed by other nodes. In addition, dishonest representatives could be easily removed from office, making network maintenance simpler.

• Proof of Authority (PoA) is an efficient algorithm for achieving consensus [105]. Nodes with the ability to build new blocks are permitted. Each node must first undergo a pre-authentication process. On the other hand, this method produces a design that is centered by nature.

• Proof of Capacity (PoC) is a consensus mechanism that achieves consensus by utilizing available hard disc space rather than computational resources [107]. With additional storage capacity, you may store more solutions, increasing the likelihood that a new block will be generated.

Rather than depending on a single consensus algorithm, an increasing trend is to combine many consensus algorithms to improve performance in a variety of applications.

D. SMART CONTRACT

Smart contracts are self-executing programs that are implemented on the blockchain. They have been employed in a variety of areas, including finance, healthcare, and government.

Such a system can achieve complex programmable functionality by delivering a contract-invoking transaction to the appropriate contract address. The smart contract will execute the secure container's predefined terms automatically. Ethereum is the first open-source blockchain platform that includes Turing-complete smart contract languages, enabling developers to create any decentralized application (Dapps) they desire. Dapps are programs developed on the blockchain, also known as decentralized applications, that allow communication between patients and doctors to take place without the need for a third-party intermediary other than the Ethereum network. This will allow patients to have greater control over their records [137].

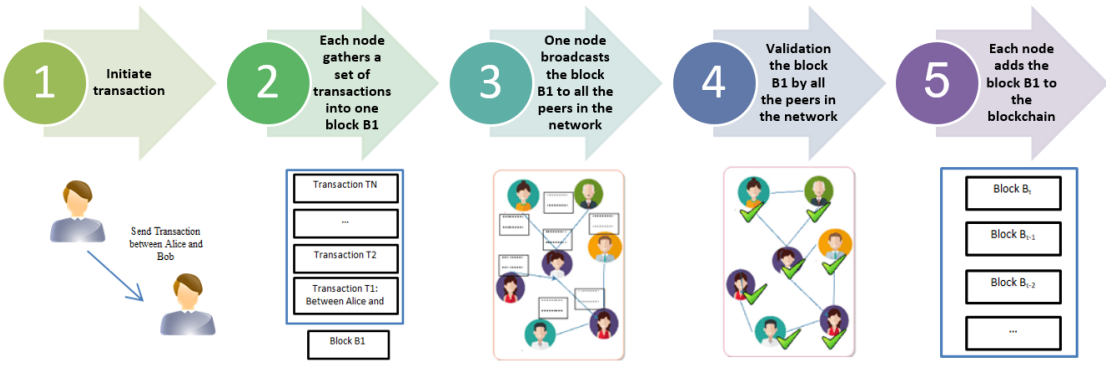

FIGURE 2. Diagram of the transaction flow in the blockchain.

V. BLOCKCHAIN APPLICATIONS IN HEALTH RECORDS SYSTEM

A. DATA MANAGEMENT IN ELECTRONIC MEDICAL RECORDS

Pilot programs around the world have begun to study the application of blockchain technology in hospitals, and some of these projects are now underway. After developing and launching a blockchain-based pilot platform in the United States last year, Booz Allen Hamilton Consulting was tasked with advising the Food and Drug Administration's Office of Translational Sciences on how to apply the technology in healthcare data management (Figure 3). The pilot project, which is presently being implemented at four large hospitals and which makes use of Ethereum to regulate data access via virtual private networks, is being run by the Ethereum Foundation. As a result of its use of IPFS, the project can employ encryption and decrease data replication by utilizing off-chain cloud components and cryptographic techniques to facilitate user sharing [19].

B. BLOCKCHAIN AND DATA PROTECTION IN HEALTHCARE

A connection exists between blockchain technology, and the General Data Protection Regulation (GDPR) implemented in

the European Union. GDPR, on the other hand, places a high value on the inclusion of blockchain technology (when the data can be portable, for data traceability, legal access auditing). Based on the information previously provided, a variety of issues can be experienced (the actual control may be weakened when the technical implementation of the smart contract over data). Dynamic consent management [20] is one such solution, which is completely compatible with the GDPR consent clause. Aside from the "private blockchains," Enterprise Blockchain are thought to be particularly well-suited for complying with GDPR directives because transactions involving digital records of stored information can be changed and deleted by private individuals or authorities who own and manage the network, using a specific type of consensus algorithm [21]. These private blockchains are operated by a single corporation or organization, and access to them is restricted to individuals, usually companies, who meet specific pre-determined credentials or restrictions [22].

The way a firm handles its private web apps will be comparable to the way it handles its public web applications. Government departments, proprietors of public health data, and healthcare reimbursement corporations are all examples of use cases that might be addressed by their technology. Specifically, these private blockchains are expected to have the most significant impact on the future of healthcare policy and management. Additionally, the European Commission's Research & Innovation Program IMI (Innovative Medicine Initiative) Pilot project "Blockchain-Enabled Healthcare," headed by Novartis, is looking into the possibilities of blockchains. It hopes to capitalize on established standards like Ethereum while simultaneously developing supplementary standards as needed. The emphasis is on those who can facilitate programs that would directly benefit patients [23].

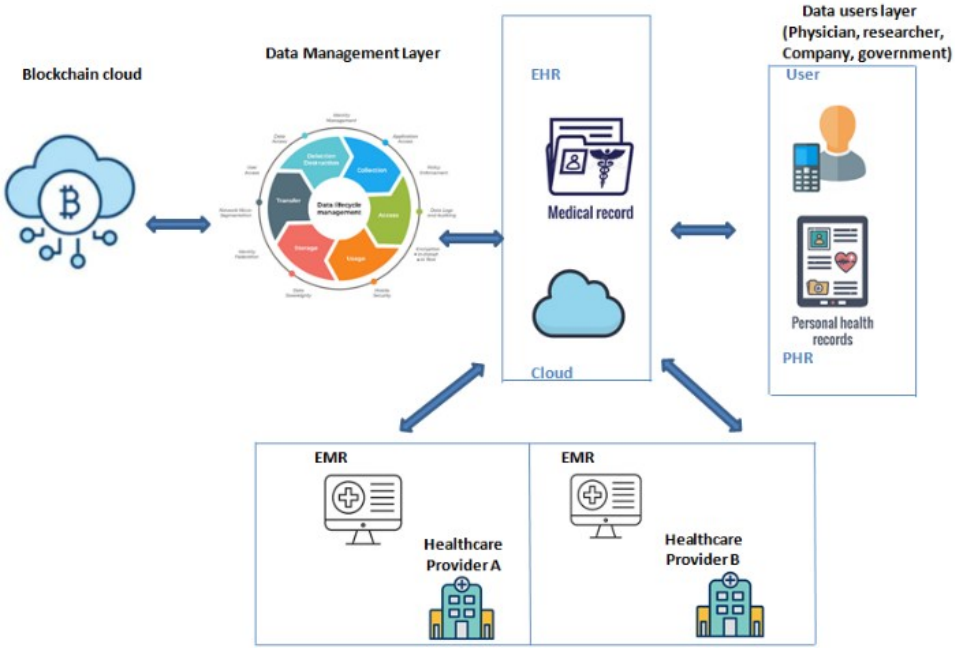

FIGURE 3. Structure of blockchain technology for hospitals.

C. PERSONAL HEALTH RECORD (PHR) DATA MANAGEMENT ON THE BLOCKCHAIN

Personal health records (PHR) have lately begun to be built utilizing data from sensors, which can be wearable or medical Internet of Things devices. A variety of stakeholders, including patients, doctors, pharmaceutical specialists, and payers will benefit from real-time AI-powered healthcare analytics [24, 25]. A key data source for blockchain service providers is the complete PHR service trajectory, which is becoming increasingly important. (See Figure 4).

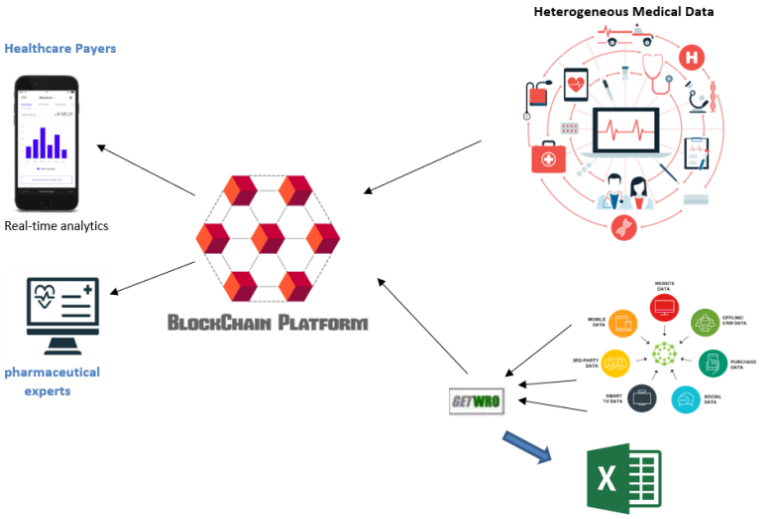

FIGURE 4. Blockchain service for PHR data.

Blockchain technology is also a feasible solution for managing personal electronic health records. Patients may be reimbursed with tokens for providing health data with physicians and research collaborators through the use of so-called "smart contracts," which are electronic contracts that exchange data between parties. Using blockchains to tokenize data, Health Wizz, for example, is experimenting with a blockchain- and Fast Healthcare Interoperability Resources (FHIR)-enabled EHR aggregator mobile app that will allow patient groups to aggregate and organize their medical records in a safe manner, as well as exchange, donate and/or swap their medical records [24]. To facilitate improved coordination between healthcare institutions and caregivers for a higher level of care, the goal is to make it as simple as managing online bank accounts to manage one's health information.

In the context of an EHR blockchain business [24], medical chain allows a variety of healthcare agents to apply for and obtain authorization to view and communicate with patients' medical records. These agents include physicians, hospitals, laboratories, pharmacies, and insurers. In the medical chain's distributed ledger, each interaction is recorded as a transaction, and the ledger is auditable, open, and stable at all times.

VI. OVERVIEW OF ARTIFICIAL INTELLIGENCE IN HEALTH RECORDS MANAGEMENT SYSTEM

AI systems in health care are often built upon supervised or unsupervised methods. In supervised learning, labeled data with regard to output or reaction of interest is used to train machines to predict these classifications using a set of predictors or inputs [26]. The unsupervised method, on the contrary, does not use labeled data nor does it anticipate a result or reaction. Instead, it finds patterns and correlations in the data to classify variables or observations into related categories [26]. The majority of existing machine learning structures in the health care industry, some of which build electronic phenotyping algorithms, employ supervised learning methods [27]. In this part, we provide a quick review of a few machine learning approaches widely utilized to categorize clinical results from electronic health records, including random forests and support vector machines, as well as supervised and unsupervised models for deep learning and neural networks [27–29].

Support vector machines determine the optimum disconnected hyperplane in the covariate space between observations of different outcome groups for the identification of variables [27]. The best hyperplane is defined as the one with the greatest margin or distance separation from the closest observation to either of its sides from distinct outcome groups, which essentially is referred to as ‘support vectors’ [20]. On the other hand, random forests are regulation-based batch classifiers that identify inputs by averaging estimates through a group of decision trees models [23].

Every tree in the random forest classifier would be trained with a sample of bootstrap data points, with the sample split at each node on the most descriptive among a randomized subset of the potential predictors [27]. In recent years, deep learning models, as well as neural networks have grown in popularity, particularly for their application in diagnostic imaging and forecasting activities [27]. When they are used for the supervised learning approach, the models may be regarded as progressively complicated extensions of the classic regression paradigm [27]. A conventional logistic regression model consists of an output and input layer, with a node in the input layer for every parameter and a collection of relation weights linking the input nodes to the coefficients or the output node. To generate the final output of the model, the output node undertakes the total from each parameter multiplied by the matching relation weight, which is known as input nodes' weighted sum, and runs it through the activation function, or

the logistic function in this example. Neural networks extend this structure by including a concealed layer between the output and input layers, in which the nodes would allow the neural network to simulate more complicated and non-linear relationships between the response and predictor factors [26]. Following that, deep learning models improve this approach by incorporating several hidden layers between the output and input layers to detect even more subtleties in the data [29].

All of these algorithms are designed in such a way that they can autonomously simulate sophisticated interactions and relationships in datapoints with priori constraints from the investigator and with little assumptions. These algorithms, however, can be harder to decipher, are prone to overfitting, and frequently need a large quantity of training data to provide appropriate results [31]. To both justify and optimize the application of machine learning for the categorization of health responses from EHR data, researchers ought to consider when these techniques are most appropriate and for which tasks, they should be employed [30].

A. THE CHALLENGES OF USING AI IN HEALTH RECORDS SYSTEM

In this section, we discuss the issues surrounding the use of AI for health record systems such as the portability and transparency of these algorithms, as well as the requirement of the training sizes necessary for satisfactory productivity.

1) TRANSPARENCY

The issue of inadequate transparency related to elaborate algorithms of machine learning such as deep learning creates hurdles to their application in phenotyping tasks, especially when the stakes are significant and end-user confidence is essential. Clinicians, for example, would prefer the algorithms to supplement or enhance their expertise as opposed to merely dictating their decision-making process [140]. Regulatory authorities, on the other hand, require algorithms to be decipherable for transparency reasons because their classification system may have substantial legal or financial ramifications [32]. As a result, improving the interpretability of such "black box" models is crucial.

The results from previous research that employed a recently established approach in interpreting deep learning model predictions were outstanding [32, 33]. Researchers in [32] applied a modified variant of saliency, which is dubbed ‘saliency’ [34], to classify the most appropriate terms from clinical material and were subsequently utilized for prediction purposes by convolutional neural networks. Based on the authors, clinicians would assess these terminologies as more descriptive and applicable to the desired trait than the most crucial characteristics determined using a more standard definition of extraction-based NLP method. [33] created heatmaps by using mappings of class activation in agreement with radiologists' assessments, representing the most significant portions of chest X-ray images applied by their deep neural network for the prediction of chest diseases [35]. Such initiatives to improve the transparency and interpretability of complicated machine learning models strengthen the trust and confidence of physicians and other end users in these technologies, hence encouraging the number of uses.

2) TRANSPORTABILITY

Due to privacy concerns and administrative constraints, a lot of electronic phenotyping research was conducted in a single-site environment [36 – 38]. It was worth noting that there is a rising interest in exchanging the algorithms among researchers and healthcare bodies to improve their versatility, provided ample time and resources for the development of phenotyping algorithms were given [39]. Initiatives such as the Phenotype Knowledgebase (PheKB), an online platform meant to help researchers build, share, and validate electronic phenotyping algorithms, demonstrate that progress is being made in this area [39]. However, few phenotyping algorithms also have been customized for applications in various settings, especially those involving machine learning [15]. To build scalable phenotyping algorithms, they should be externally verified to determine their portability, and then modified, if needed, to account for idiosyncrasies of site-specific. This "validation-adaptation" strategy is especially useful for phenotyping algorithms that use NLP systems even though it could be extremely laborious and work-intensive [38]. Since these versatile methods are vulnerable to overfitting, it is especially essential to validate phenotyping algorithms that implement machine learning externally before implementing them in different settings [40]. If additional fine-tuning is required, for example, to model relationships differently or to detect new acronyms in clinical documentation, machine learning algorithms may take up less human work to be retrained than manual-engineered algorithms. In another instance, deep learning NLP systems would seldomly utilize manually supplied feedback and maybe quickly retrained to new datasets [32]. Deep learning models that are usually employed to classify health responses from imaging procedures might theoretically be considerably more portable than those utilized for NLP tasks because of the smaller degree of between-site heterogeneity in medical images compared to clinical narratives.

3) TRAINING SIZE

To achieve optimal efficiency, machine learning algorithms, particularly deep learning frameworks, would necessitate a significant quantity of labeled training data [41]. In this regard, [33] used the CheXNet algorithm and was trained on over 100,000 labeled images, which subsequently produced expert-level results. Many researchers, on the other hand, do not have such privilege given due to the limitation in time or resources for data annotation [41], or probably due to the constraint in the number of cases or rare health ramifications in the EHR system. In addition, as previously mentioned, pooling labeled data across different locations may not be a viable option owing to privacy concerns and administrative hurdles [37]. However, innovative solutions such as image data

enhancement and active learning by successively picking the most insightful instances for training can assist in minimizing the portion of training data required to obtain satisfactory performance [42, 43]. In [41], for example, the annotated samples required to obtain an AUC of 0.95 was lowered by 68% when active learning was paired with support vector machines to create an electronic phenotyping approach for rheumatoid arthritis.

B. AI ALGORITHM IN HEALTHCARE SYSTEMS

This article brings machine learning and data mining together for a joint discussion because both disciplines are based on data science and frequently cross [44]. However, there are a few fundamental differences between data mining and machine learning. The study of methods that can extract information automatically is known as machine learning [44]. Forecasting future events requires two sets of data (training data and test data). On the other hand, data mining is an iterative process of uncovering various types of novel and useful patterns in data.

Data mining can employ machine learning, but it can also use other techniques besides or in addition to machine learning to identify new patterns. Machine learning and data mining technologies are employed mainly in the healthcare industry to extract knowledge from vast amounts of electronic health data. Machine learning and data mining approaches were included in the analysis in [45] because they use similar mechanisms for disease prediction and are frequently discussed together in the literature.

1) SUPERVISED ALGORITHM

- Artificial Neural Network (ANN)

Artificial neural networks (ANNs) were first proposed by McCulloch and Pitts [46] and popularized in the 1980s by [47]. They can handle a range of categorization issues. The word "neutral" in their name implies brain-inspired systems designed to mimic how human brains learn categories. ANNs were created to mimic the way the human brain works, in which a vast number of neurons are coupled to one another via many axon junctions. Neuron connections can be strengthened or decreased by reinforcing labeled training data, just as they can be in biological learning. A weighted matrix can be used to represent these neuronal connections. This matrix is referred to as a layer, similar to the cortical layers in the brain. The training data used in ANNs serves as a form of 'biological learning' for people. In an ANN framework, there can be one or more hidden layers in addition to the input and output layers. ANNs are taught to generate an output from a set of input variables.

Several ANN research focused on the survival prediction problem were found in the literature. However, a few research relying on electronic health data were found.

Deep learning is a subfield of machine learning that deals with ANN-inspired algorithms [48]. These algorithms have been utilized to model illness symptoms and hazards in recent years. Liu et al. [49] created a deep learning-based technique for early identification of Alzheimer's disease and mild cognitive impairment in 2014. Neuroimaging data from the Alzheimer's Disease Neuroimaging Initiative database was used.

To get around the bottleneck, they used stacked auto-encoders. Cheng et al. [50] suggested a method for phenotyping patient electronic health records (EHRs) using deep learning. Each patient's EHR was initially represented as a temporal matrix, with time on one axis and events on the other. The researchers built a four-layer convolution neural network (CNN) to extract phenotypes and forecast risk. [51] recently presented Heterogeneous Convolution Neural Network (HCNN), a new predictive learning model representing EHRs as graphs with heterogeneous properties such as diagnosis, procedures, and medicines. They used this information to create a new risk prediction model for numerous comorbid conditions.

- Support Vector Machine (SVM)

SVM is a popular supervised learning approach for classifying linear and non-linear data. SVMs transform the input vector into a higher-dimensional feature space and find the hyperplane that divides the data points into two groups. An SVM may perform classification tasks by increasing the marginal distance between two classes while reducing classification errors. The marginal distance between the decision hyperplane and its nearest instance, which is a member of that class, is the marginal distance for that class [52]. In more technical terms, each data point is first plotted as a point in an n-dimensional space (where n is the number of features), with the value of each part being the coordinate value. We must first locate the hyperplane which separates the two classes by the most significant margin to complete the classification. It has been used for categorization in bioinformatics and healthcare [52].

- Decision Tree Random Forest

A decision tree (DT) is a sophisticated and deterministic data structure that looks like a tree, with internal nodes representing input variables or attributes and leaves representing decision outcomes. All nodes and their accompanying leaves are used to create a plan to attain a categorization goal. The leaves of a DT tree are on the last level of the relevant branch, and the nodes can be organized in more than one level. The root node is the tree's first node. It's similar to a flowchart in which each non-leaf symbolizes a test on a single property, each branch denotes the test's outcome, and each leaf indicates the class label. Many academics in the healthcare sector use decision trees extensively. For example, a decision tree-based prognostic approach was suggested to quantify disease recurrence and predict survival in breast cancer patients [52]. The model was developed for predicting breast cancer survival using two machine learning techniques (ANN and decision tree) and one statistical approach (logistic regression). They used the SEER breast cancer database, regarded as one of the few population-based data repositories for evaluating cancer care quality.

Random forest [52] is an ensemble classifier made up of many decision trees. Individual trees represent the output of the classes. Among the machine learning-based algorithms, it is one of the most accurate. The method in [52] combines Breiman's "Bagging" idea and the random selection of features to create a collection of decision trees with a controlled variation. In [45], researchers suggested a classifier based on the random forest algorithm to estimate illness risk among individuals. The Healthcare Cost and Utilization Project (HCUP) dataset was used in their research. The work in [53] have developed a diabetes risk prediction model using a scalable random forest classification algorithm based on administrative data.

2) UNSUPERVISED ALGORITHM

- Association Analysis

Association analysis has been frequently utilized in data mining and machine learning literature for prediction because it can extract hidden and relevant information from huge datasets [52]. This function generates a collection of dataset item association rules [53]. Power of association is an implication statement with $X \rightarrow Y$, where X and Y are disjoint item sets (i.e., $X \cap Y = \emptyset$). It means that the existence of X things in current transactions may result in one or more Y items appearing in future transactions. As a result, association analysis has been widely utilized with market basket data to forecast retail sales behavior, where each object reflects a customer's purchase [52].

If an item is related to disease and the item set is specified as the patient's set of conditions until now, this method can be applied to the medical context to predict future disease risk.

The Hierarchical Association Rule Model (HARM) was introduced in [55] to predict illness risk from medical data using association analysis and a Bayesian estimate. First, a set of association rules is developed utilizing association analysis methods in this modeling technique. Then, using Bayesian estimation, these association rules are ranked. HARM can anticipate a patient's likely future medical issues based on her previous and present history of reported ailments, assuming that each patient regularly consults healthcare professional.

3) NETWORK APPROACH

A network can be represented as a graph, which is made up of nodes (also known as vertices or actors) and edges (also known as ties or links). Edges represent the relationships between things, while nodes represent the entities themselves. Many scientific problems can be represented as graphs and modeled as networks. Many graphs theory approaches and algorithms for analyzing various problems, including disease prediction in the healthcare area, can be found in the literature.

Many statistical and data mining methods for predicting disease risk from healthcare data do not explicitly take into account the link between diseases and symptoms. Chronic and non-communicable diseases, on the other hand, do not arise in isolation [52]. They frequently share a risk factor, which might be genetic, environmental, or behavioral in nature.

These risk factors have a synergistic influence on health outcomes, which makes it difficult to forecast if they are studied separately. A network method may be more applicable in this scenario. Statistical methods are also used in a network-based approach. Another comparable approach is Social Network Analysis (SNA), which is built on a solid theoretical foundation drawn from network and graph theories. SNA is the study of the pattern of relationships among network entities, such as a group of people, departments, or organizations, as the name suggests. If the elements in the dataset have a lot of relationships between them, SNA can be especially useful. In a healthcare setting, for example, clinicians frequently need to confer among themselves about a patient's illness diagnosis. Patients are additionally cared for by pharmacists, nurses, and medical technicians. As a result, the recordings of these dialogues are bound by a network structure.

Each sort of entity participating in the healthcare data is represented as a node to describe the health care infrastructure as a social network. Edges linking the corresponding node pairs represent relationships between entities. SNA has been utilized to better analyze physician-patient partnerships as well as collaborations throughout a hospital network. Uddin et al. [56] suggested an SNA framework to analyze the process of collaboration (amongst physicians) and coordination (between hospitals).

SNA was created with the intent of being utilized in the social sciences, but it is now frequently employed in medicine and public health. Each sort of entity participating in the healthcare data is represented as a node in the health care infrastructure's social network representation. Edges linking the corresponding node pairs are used to represent relationships between entities. SNA has been used to better understand physician-patient partnerships as well as hospital-to-hospital collaborations. Uddin et al. [56] presented an SNA framework to describe the process of physician collaboration and coordination, for example (between hospitals). Their suggested framework looked at a patient-centric care coordination network, a hospital-rehab coordination network, and a physician collaboration network, all using centrality theories. In the healthcare domain, for example, in obesity research, SNA is utilized to understand research trends and map knowledge structures [54,57].

Large population-level studies aimed at understanding the nature of comorbidities [58] and forecasting the likelihood of comorbid chronic diseases have a lot of potential with electronic health data. [59] established a novel strategy in which they used graph theory and social network analysis methodologies to analyze and comprehend chronic disease progression using electronic health data. Their main goal was to forecast the likelihood of developing a chronic disease in new patients by modeling the health trajectory of chronic disease patients. The data was gathered from hospital admission and discharge records. The diagnoses of the patients (in ICD-10 Australian Modification format), as well as several

socio-demographic characteristics, were taken into account. They created a baseline network based on the diagnosis data to better comprehend and reflect the health trajectory of chronic disease patients. Later, to better understand the comorbidities associated with type 2 diabetes, this approach was expanded and used. They proposed the concept of a 'comorbidity network,' which may be utilized to construct a model for predicting chronic illness risk [60,61].

TABLE I
COMPARISON OF DIFFERENT TYPES OF RISK PREDICTION MODELS WITH STUDY GOALS FOR VARIOUS DISEASES.

Risk prediction model	Diseases Name	Goals	Reference
Artificial neural network (Supervised)	Multiple cancer diseases	Using administrative and registry data, propose a machine learning model for cancer survival prediction.	[62]
	Pancreatic cancer	Using a boosting method and healthcare administrative data, propose a model for predicting in-hospital mortality after pancreatic resection in pancreatic cancer patients.	[63]
	Acute coronary syndrome	A significant volume of EHR data was used to stratify clinical risk and death for individuals with acute coronary syndrome.	[64]
	Heart failure	To offer an EHR-based architecture for heart failure prediction that is both effective and reliable.	[65]
	Alzheimer's disease	Develop a deep learning-based approach for early detection of Alzheimer's disease and Mild Cognitive Impairment.	[49]
	Generic	Propose a deep learning method for phenotyping patients' electronic health records (EHR)	[50]
	Multiple chronic diseases	The goal is to create a new risk prediction model for comorbid disorders.	[51]
Support vector machine (Supervised)	Breast cancer	Using a hybrid SVM method, propose a predictive model for breast cancer diagnosis.	[52]
	Cardiovascular	To create a system that analyses heart valve disease using a genetic SVM classifier.	[53]
	Cardiovascular	To create a model for predicting heart failure patients' 30-day readmission.	[56]
	Diabetes	Using a scalable random forest classification technique, create a model for predicting diabetes risk.	[67]
	Coronary disease artery	Implement and analyze a set of supervised learning approaches for coronary artery disease prediction in a systematic way.	[68]

Association analysis (Unsupervised)	Multiple diseases	Using electronic healthcare data, offer a method for forecasting disease risk in healthcare research.	[54]
Network Approach	Generic	To offer a SNA framework for analyzing the performance of physician collaboration and coordination (between hospitals).	[56]
	Generic	To determine the health trajectory of chronic disease patients and estimate the probability of new disease development.	[59]
	Diabetes	Using graph theory and social network analysis methodologies provides a research framework for understanding and visualizing the evolution of type 2 diabetes.	[42,67]

TABLE II
THE ADVANTAGE AND DISADVANTAGES OF DIFFERENT TYPES OF AI ALGORITHMS IN THE RISK PREDICTION MODEL.

Risk Prediction Model	Advantage	Disadvantage
Artificial Neural Network (ANN)	- When the relationships between variables are nonlinear and complicated, it is appropriate for predicting outcomes. - Requires less formal statistical training, and many training techniques for this methodology are available in the literature. - Can be used to solve both classification and regression issues.	- It is referred regarded as a "black box" technology because the user is unable to see the exact decision-making process. - Training the network for a difficult classification task takes a long time with this technique. - Pre-processing of predictor variables is required.
Support Vector Machine (SVM)	- It introduces the kernel, which allows for non-linear transformation. - The ability to manage a large number of feature spaces. - In SVM, the risk of overfitting is lower. - Even unstructured and semi-structured data, such as words and photos, works well.	- SVMs will not work as a classifier if the points on the boundaries are not informative owing to noise. - Larger, more complicated datasets will take longer to train. - The final model, variable weights, and individual impact are difficult to understand and interpret.
Decision Tree (DT)	- Easy to comprehend and interpret. - Requires minimal data preparation and can handle a variety of data formats, including numeric, nominal, and categorical information. - It is capable of producing robust classifiers that can be validated using statistical tests.	-Classes must mutually exclude one another. - The final decision tree is determined by the order in which variables or attributes are chosen. - They don't perform as well as other classifiers (e.g., Artificial Neural Networks) [62] - When the needed value for the ancestor variable or attribute is absent, it is impossible to select which branch to choose.
Random Forest	- When compared to decision trees, random forest has a lesser likelihood of overfitting training data.	- The number of decision trees in the random forest must be defined.

	- Produce less variance than decision trees since a random forest takes the average value of its constituent decision trees' results. - Random forests are almost always more accurate than decision trees. - It works well with huge datasets. - It can estimate which factors or attributes are most essential in classification.	- When estimating variable importance, it favors variables or qualities that can take a large number of alternative values. - Overfitting is a common occurrence.
Association Analysis	- When diseases have a lot of comorbidities, it can forecast risk. - It can mine massive databases for interesting hidden relationships.	- The methods utilized contain an excessive number of parameters. - The derived rules may be excessively complex and difficult to comprehend.
Network Approach	- It can make clinical decision-making more efficient and effective. - It can disclose the intricate relationships that exist between diseases, patients, and clinicians.	- Traditional network models lack the longitudinal and spatial dimensions necessary to predict illness risks. - When compared to single-attribute networks, healthcare networks are far more complex.

VII. MANAGING EHR USING AI AND BLOCKCHAIN

Machine learning can aid in the optimization of healthcare systems and the provision of intelligent services. How to safely store, exchange, and train sensitive datasets is a major difficulty for practical machine learning systems. Machine learning and blockchain are increasingly being combined to improve the security and privacy of datasets [70,71]

Federated learning is a machine learning technique that is carried out over numerous computing nodes with the confidentiality and privacy of sensitive data protected throughout data sharing as a precondition [194]. By exchanging encrypted datasets, different medical organizations can collaborate to create high-accuracy prediction models. To establish accountability and reliable cooperation, blockchain as a regulator can record associated training transactions in an immutable and transparent manner. Medical organizations and researchers will be more ready to share encrypted datasets to advance medical treatment and public health in this circumstance.

The security of data input is ensured by blockchain as a dependable backbone for machine learning algorithms. The first challenge raised by [72] is the sharing of huge datasets across different applications and domains. In reality, however, homo-morphic encryption has a substantial computational expense. Perhaps sensitive data can be encrypted in the future without affecting machine learning for intelligent services.

If the rate of erroneous predictions is high, blockchain can also be used to store rollback models. The pointers to essential data of retrained models are stored in a safe and immutable manner on the blockchain. In the context of erratic arrhythmia alarm rate, [73] argued that retraining models indexed by pointers in the blockchain can improve accuracies for continuous remote systems.

AI can also be used to automate the production of smart contacts, making processes more secure and adaptable. In both academic research and industry in the form of startups, the use of blockchain in the healthcare sector has been a growing area of interest, [74–79]. Whereas they assert ownership of the first attempt to use blockchain for an EHR management system in their paper [81], they present a system for exchanging EHRs in their report, with a focus on security and ease-of-transfer. The system, however, is still a concept and has yet to be deployed and tested for its stated areas of progress. [74] used blockchain technology to create MedRec, a decentralized EHR management framework. For simplicity and adaptability, their modular architecture was combined with an in-place data storage system. They enticed the medical community and EHR stakeholders to participate as miners in the network's Proof of Work [20] verification. Permission to view aggregated and anonymized data will be granted in exchange. In collaboration with the Harvard Medical School Teaching Hospital, they developed and tested the first working prototype. They suggested that future research focus on areas where miners can rank their preferences for data attributes (demographic, gender, age group, and so on) to allow precision medicine and targeted research.

In [78], researchers built a prototype that differed greatly from the MedRec framework's permissionless mining. From a medical standpoint, they decided to create a closed, access-controlled blockchain EHR system. As a result, cloud storage and access key transfers for encryptions were implemented, while MedRec stored patient data locally at each node.

Although in the most recent literature [79,80], the advantage of providing AI to the context of a blockchain EHR

management system has not been completely realized in both the permissionless and permissioned prototypes.

Blockchain technology and its basic function for the monitoring of health records have been discussed in [81]. It explains how to obtain meaningful results in drug tracking and development, treatment effectiveness, safe patient management [139], and enhance clinical results if healthcare data and big data are combined. on the other hand, [28] focuses on several other critical aspects of an HER such as providing complete reporting, quality assurance, monitoring of a patient's health-related expenses, billing details, and confidentiality. It also discusses how current systems are slow, inflexible, and insecure. The work in [58] highlights the importance of patient records availability. Due to a lack of time and patience, important aspects of a patient's medical history are often overlooked. A patient's medical history can be extremely useful during care. Doctors, on the other hand, are largely unable to access this information because they lack the expertise, time, or desire to retrieve what they need from a patient's medical data repository.

A. METHODOLOGY

In conducting this review, we follow SLR guidelines in [135] as well as the Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines in [136]. An SLR is a methodology for discovering, analyzing, and evaluating all recent literature on a research topic or subject field.

In December 2021, all review papers were chosen by searching for relevant and reliable academic repositories such as Google Scholar, IEEE, ACM, Science Open, Science Direct, Springer, Hindawi, Wiley Online Library, and MDPI.

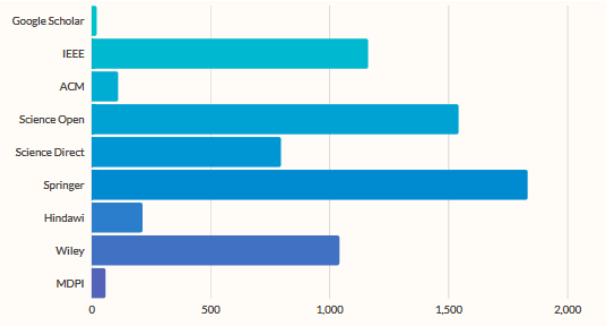

FIGURE 5. Number of articles according to publishers

B. RESEARCH QUESTIONS

The goal of this systematic review paper was to provide answers to the following research questions:

1) To what extent has the blockchain been developed for the management of EHRs, and how has it evolved over time?
2) What standards are used to store EHRs in the blockchain?
3) How large amounts of EHR data are handled?
4) What blockchain platforms/mechanisms are used to manage EHRs?

C. FILTERING THE ARTICLES

After reviewing papers from various categories, selected papers are presented in this portion. As indicated in Section VII-B, the article selection query was intentionally extensive to evaluate as many research issues as feasible.

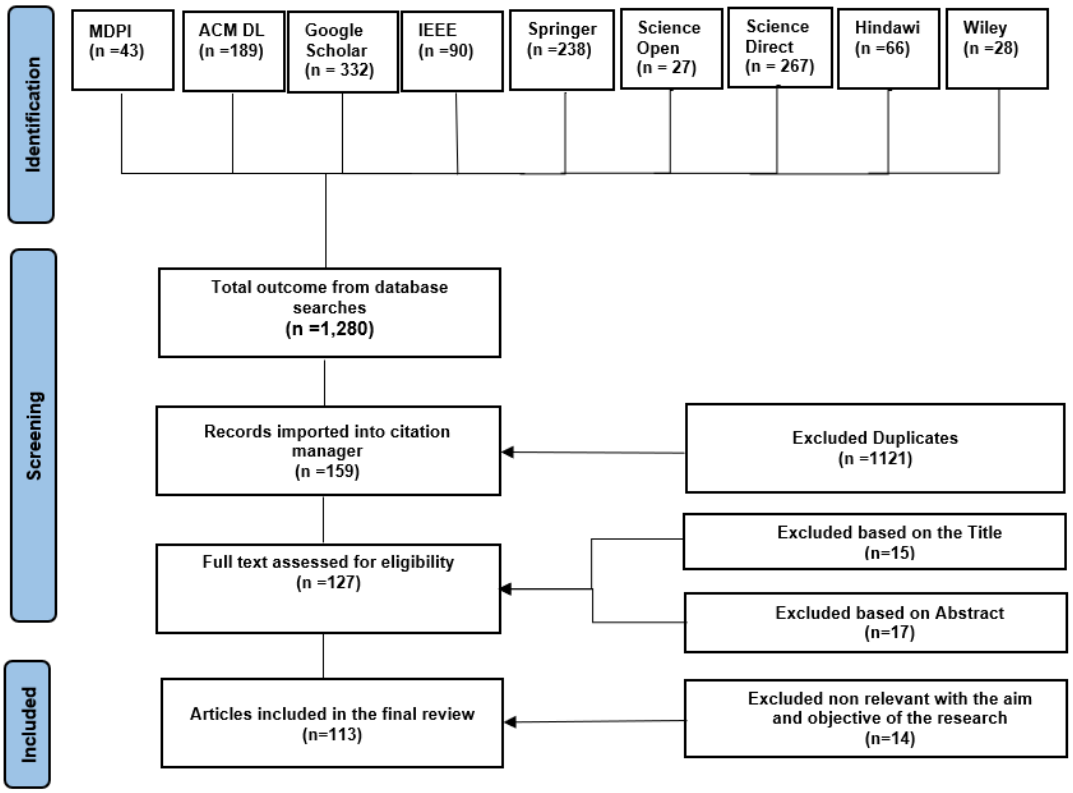

FIGURE 6. PRISMA Chart.

Selected papers are presented in this segment after screening from various categories. The selection query for the articles was purposely long enough to consider as many research questions as possible, as described in SectionVII-B. Using the searching mechanism, we were able to retrieve 1280 research articles from the scientific repositories, as shown in Figure. 6. After the first screening step, we removed duplicates and retrieved 159 papers. Using the second and third screening methods (here, exclusion was based on title and abstract), a total of 32 articles were deleted accordingly, leaving 127 papers for further processing. We uploaded the remaining papers to the Mendeley software for thorough reading. Finally, all articles that did not serve the purpose of the SLR were deducted, and a total of 113 articles were there. The second analysis we ran, as part of our systematic investigation, was to determine the purpose or field of blockchain application in the healthcare industry. As indicated in Table III, the majority of publications in the field of healthcare use blockchain for data interchange, health data records, and access control. A large number of applications of blockchain technology in healthcare (for example, data sharing and access control) are frequently mentioned by authors, which is understandable given that the blockchain technology itself implies specific applications—for example. Essentially, distributed technologies such as blockchain technology are to be used for data sharing, so, understandably, this field of research would be frequently mentioned.

TABLE III
CONTRIBUTIONS IN THE PUBLICATIONS

Contributions	Number of Publication
distributive mechanism	22
Access control	5
decision-making process	3
Increase interoperability	2

TABLE IV
CONTRIBUTIONS IN THE PUBLICATIONS

Field	Number of Publications
Data sharing	20
Health record	18
AI methods	3
Data Security	4
Data Analytics	3
Other	10

Table 4 shows the additional analysis for the selected papers. The table compares papers based on five key characteristics. These characteristics are critical for EHRs. The following properties are discussed further below:

1) Privacy

The concept of privacy refers to a person's right to select when, how, and to what extent they can access, change, and share their own EHRs. [125]. A healthcare provider may purposefully or unintentionally misuse electronic health records (EHRs) to violate patients' privacy, for example [126]. Many patients are concerned about their electronic health records (EHRs), according to the study article [127]. About half of those polled [128] thought that sharing health data would make it more difficult to protect their personal information. As a result, when comparing blockchain-based solutions that claim to protect EHRs' privacy, privacy is an important consideration.

2) Security

EHR security, on the other hand, refers to the extent to which an individual's electronic health records (EHRs) are confined to authorized individuals. According to [129], about half of patients are concerned about the security of their EHRs because they must travel via the Internet.

EHR security is more important to a doctor than to patients, according to [130], and the majority of doctors prefer paper records over EHRs because they believe the former are safer. Because doctors use digital health records, they are more vulnerable to security breaches than paper-based records [131]. Liu et al. in [132] advised that ways of securing EHRs should be thoroughly studied first. These aspects indicate that the security of EHRs should be seriously considered.

3) Accessibility

Controlling and managing access to crucial or sensitive data is an essential part of accessibility. Access to data can be restricted using this method. [133] Role-based, attribute-based and identity-based access control are some of the most common strategies for healthcare systems. Because EHRs deal with sensitive patient health data, access management is a critical consideration.

4) *Storability*

In recent years, the scalability of blockchain technology has become a challenge. Bitcoin's first block had a storage limit of just 1MB when [134] first began mining the cryptocurrency's network. But since then, the popularity of the blockchain has increased, as well as the number of participants and blocks. To understand and validate a transaction, a participant must download all of the chains, which consumes a significant amount of memory and time. On the other hand, conventional blockchain applications have two ways to deal with scalability issues: on-chain and off-chain. Every piece of data that a user uploads will be stored directly on the blockchain. However, off-chain storage means that the true data is held someplace else, but is still linked to the main chain. Off-chain storage, on the other hand, provides less robust security. To store EHRs on-chain, a substantial amount of storage capacity is needed. To keep data safe and secure, it is important to consider storing information outside of the blockchain.

TABLE V
RESEARCH COMPARISON USED BLOCKCHAIN AND AI BASED APPROACHES TO SECURE EHR SYSTEMS.

Ref	Objective	Pros	Cons
[75]	Discovering healthcare intelligence focused on the blockchain with privacy	Patient-controlled documents.	Illustration for concept only.
[109]	For an extensive network to establish a safe health system.	Sharing the network load.	No schemes mature
[110]	To design health sharing based on blockchain with cloud-based services	Mechanism for Access management	Scalability, core leadership
[69]	Usage of blockchain to exchange health information and communicate with mobile health users	Secure Merkle root tree for collaboration on transactions, data sharing, and healthcare.	The interoperability
[111]	To build a medical data exchange blockchain-based framework.	Joins the approach to safety and authenticity of off-chain storage and on-chain verification.	Performance and fairness of the system, and dynamic regulation of access.
[112]	Examination of data security systems in relation to health data	Immutable, memory management and cryptographic algorithms help to handle leaked information	Easily lose paper-based records, slow pace, low memory.
[113]	To strengthen the exchange of effective and safe health information with a blockchain network.	Management and exchanging records from EMR systems, and method of access.	The greater computing capacity of miners contributes to the downstream method.
[114]	To provide the cloud-based support of attribute-based cryptosystem and blockchain to a protected EHR system.	Identity-based encryption guarantees confidentiality and traceability to encrypt databases.	Deployment is not complete yet.
[115]	To propose a stable ABE scheme with multiple blockchain authorities in EHRs	Immutability of the ledger of information	Interoperability, confidentiality
[116]	To discuss continuous monitoring of patients with a patient-centered agent.	Lightweight encryption and authentication, tamper-proof, and single point of failure defense.	Delay End-to-End.
[117]	To suggest a blockchain-based decentralized attribute-based signature for healthcare.	Large-scale and distributed EHR, anonymity, and stable verifiable sharing Non-rebatement.	Certificates attribute, storage space
[118]	To propose access policies for blockchain-based EMR-based systems.	Finer regulation of granular	Proven theoretically.
[119]	To build a blockchain-based secure EHR architecture.	Model for Safe records.	Implementation.
[120]	To assess the efficiency and optimization of blockchain platforms	Ability to simulate network efficiency	Scalability
[121]	For the creation of a blockchain network dependent on permission.	Defined blockchain integrity permission.	Scalability
[122]	Using fabric to scale a blockchain network	Demonstrable network blockchain functionality.	It needs increased computing power.
[123]	Using blockchain to design searchable encryption for EHR.	Analysis of protection with a searchable algorithm for encryption	Scalability
[124]	using Federated Learning (FL) for smart healthcare	coordinating various customers, such as hospitals,.. etc, employing a distributed collaborative AI paradigm is very appealing for smart healthcare.	Implementation

D. INCLUSION AND EXCLUSION CRITERION

The authors selected a clear finding centered on the new technological implications of technology and applications for the development by incorporating AI and blockchain into existing health data management systems. Only those studies meeting the first requirements, which must be updated and published in English, should be selected. The findings received from all electronic databases are evaluated based on the developed parameters, and the papers for this systematic literature review are selected from the aforementioned databases.

The criteria of inclusion and exclusion studies have been defined in the following:

TABLE VI
INCLUSION AND EXCLUSION CRITERION

Inclusion	Exclusion
IC 1: Original research study. **IC 2:** Publication related to the topics of AI-blockchain in healthcare data management system. **IC3:** The study provides ample and strongly correlating research findings in the domain of healthcare data management. **IC4:** The publication year for the study should be between 2016 and 2021.	**EC 1:** Review papers that are based on secondary data or are irrelevant to the targeted domain. **EC 2:** Studies published in the magazine, discussion, and interviews. **EC 3:** Studies not published in English

E. PRIVACY AND SECURITY ISSUES

After reviewing the literature for information extraction, we should answer the following pressing questions.

Q1: How does blockchain ensure privacy by utilizing anonymity?

We see varying degrees of privacy and anonymity [141] depending on the implementation type of the blockchain: public, private, or licensed. According to [142], CORDA [143] protects the transaction's privacy by requiring validation to be performed only by the persons participating in the transaction. In the field of Industry 4.0, we discover the blockchain-based Secure Mutual Authentication System (BSeIn) [144], which aims to provide privacy and security assurances such as anonymous authentication, audit capabilities, and secrecy. It demonstrates the scalability enabled by Smart Contracts. They enable privacy via the various consensus methods employed in blockchain [145]. In other instances, anonymity is used in [146]. While the work in [147] emphasizes conditional privacy, it considers traceability of operations important in the event of a public audit by all entities participating in the blockchain.

The first references we found to anonymization were through pseudonymization [141], which is the process of obliterating some of the information required to identify an entity. Although they assert in [151,148,149] that blockchain does not guarantee completely anonymous transactions and that transactions can be traced using a pseudonym. The authors of [150] state that distributed consensus and anonymity are two critical characteristics of blockchain. Cryptography is critical for ensuring the anonymity of participants on the blockchain, with various levels of anonymity achievable depending on the cryptographic methods utilized. Pseudonymization is one method of implementing blockchain technology [141,151,149,152]. A mechanism in which the identity of the sender is frequently concealed behind a public key, but other transaction characteristics are made public. This presents a difficulty for health data. One option to limit public exposure is to utilize approved blockchain technology. One way to safeguard sensitive data is to implement an out-of-chain solution [141,153]. The approach entails locating sensitive data in a system other than the blockchain and anchoring it to the blockchain's link. This technique is advantageous for systems that manage enormous amounts of data, and it would be impractical to incorporate these data into the blockchain structure. Additionally, it is recommended for systems that handle highly sensitive data and require greater access control, such as health data.

The requirement for confidence and privacy necessitates the development of a mechanism that safeguards cars against forgeries while safeguarding privacy from monitoring threats. The work in [154] proposes a Blockchain-Based Anonymous Reputation System (BARS) to construct a trust model that protects the privacy of Vehicular Ad Hoc Networks (VANETs), which communicate anonymously using a public key as a pseudonym. It tries to prevent the spread of falsified messages using a reputation assessment algorithm that evaluates the message's quality. On the other hand, it exploits the properties of a lexicographical Merkle and eliminates the chance of the public key being linked to the real identity. Such system can be replicated for HER privacy handling too by taking advantage of the features used.

To accomplish anonymization, the approach presented in [144] (BSeIn) uses broadcast encryption and multi-receiver encryption to ensure safe communication between an entity and a collection of previously designated receivers. Additionally, it ensures the confidentiality and anonymity of messages between recipients. It produces one public/private key pair at a time for each transaction, allowing it to withstand replay assaults efficiently. Thus, the system can also be replicated for HER to guarantee the user's privacy without jeopardizing it.

Privacy by design (PbD) is a sequence of procedures aimed at ensuring and retaining the best level of privacy and data protection feasible throughout the design and development of various services, processes, and products. PbD incorporates

privacy and data security considerations throughout the development process, from the beginning to the end, for all sorts of sensitive information, such as healthcare information [156,154]. Ann Cavoukian published the privacy by design (PbD) idea in the mid-1990s [157–159]. Following that, data protection specialists and regulatory authorities began to accredit PbD. In October 2010, at the International Conference of Data Protection and Privacy Commissioners in Jerusalem [160], PbD was overwhelmingly adopted as an international privacy standard. Additionally, PbD is covered by the United States' Commercial Privacy Bill of Rights Act. Similarly, it has been incorporated into the EU's General Data Protection Regulation (GDPR) and accepted by data-protection commissioners worldwide as a concept for ensuring adequate privacy protection in a world of constantly evolving information technology systems capable of collecting and processing massive amounts of data [161]. EHR can definitely benefit from PbD implementation in order to ensure inherent data protection and privacy features throughout the designed system levels.

The strategies for privacy by design are classified into two categories:

A. Data-Driven Approaches

1- Keep it simple: Minimize is the simplest privacy design technique, suggesting that just the barest minimum of personal data should be processed. In [162] describe this method in detail. As a result, it is critical to avoid collecting unneeded data; hence, the probable influence on a system's privacy is minimal.

-Design patterns: "choose before you collect"[163] and the usage of pseudonyms and anonymization [164] are examples of design patterns that put this technique into effect.

2. Hide: This method emphasizes the need of keeping personal information and its interrelationships hidden from plain view. The idea for this method is based on the fact that hiding personal data prevents a variety of abuses [165].

-Design patterns: Within the confines of the "hide strategy", design patterns take on a variety of forms. One such pattern is data encryption (in transit or at rest, anonymization or pseudonymization), which refers to strategies that disentangle certain related events. Data encryption is a type of security that encrypts data so that it may be accessed only with the correct encryption key. It converts data to another format and hence requires a decryption key to retrieve the data [164].

3. Separate: This technique stipulates that personal data should be stored in distinct partitions and, if possible, spread out. By segregating the storage and processing of personal information from a variety of sources associated with the same person, an individual's complete profile cannot be derived [166]. This technique necessitates a distributed processing solution rather than a centralized one. Data from multiple sources should be stored independently and separately.

- Design patterns: No specific design pattern for this strategy has been identified to date [143].

4. Aggregate: According to this technique, personal data should be managed with the fewest feasible details and at the highest level of aggregate possible. As a result, this data becomes less sensitive. When the data is sufficiently uneven, the group over which it is aggregated is large, and only a small quantity of data can be ascribed to a single individual, resulting in privacy protection [143].

- Design patterns: There are two common strategies used. “Granularity of location” design pattern that changes dynamically enables the collection and delivery of data to be as efficient as possible [167]. “K-anonymity” design pattern, on the other hand, is a critical model for privacy protection since it protects against joint attacks. It is a dataset characteristic that is used to describe the dataset's degree of anonymity [168].

B. Process-Oriented Approaches

1. inform: This technique embodies the critical concept of transparency. If personal data is processed, data subjects' information should be kept current. When a user interacts with a system, they should be appropriately informed about the data that is processed and why it is processed. This includes information on the mechanism used to protect the data in question and transparency regarding the system's security [143].

-Design patterns: Both platforms for privacy preferences and notifications of data violation are examples of this type of design pattern. The work in [169] presented an unusual array of privacy design patterns intended to educate the user from the perspective of human-computer interaction.

2. Control: This technique is a necessary complement to the “inform strategy”. It serves little purpose to tell the user that personal data is being gathered unless the user has a realistic means of limiting the use of his data [170]. Users frequently have the right to access, amend, and request deletion of personal data gathered under data protection regulations. This technique accentuates this point and enables users to exercise their data protection rights [143].

-Design patterns: There are no specific design patterns that fit the strategy [143].

3. Implement: This technique ensures that the system operates in a manner that respects user privacy. More significantly, the policy must be implemented. To ensure that the privacy policy is not violated, adequate technical protection measures are developed. Additionally, the policy must be formed through an effective governance system [167].

-Design patterns: This method is carried out using design patterns such as access control and privacy rights management, and license to personal data, which includes the form for managing digital rights [143].

4. Exhibit: This approach establishes the relationship between a data controller and the monitoring of compliance with privacy policies and applicable regulations. In the event of issues, the user should promptly be able to determine the amount of any potential privacy infringement.

-Design patterns: Examples of design patterns that support this strategy include the usage of logging and auditing, as well as a privacy management system [169].

Q2: What are the drawbacks of using blockchain to comply with the GDPR?

There are practical constraints and obstacles associated with blockchain and its applications in the health sector, including ensuring compliance with the GDPR. On the one hand, compliance with an individual's right is to forget about his data. When a transaction is authenticated on the blockchain, it becomes permanent, and information about a patient cannot be deleted if the patient exercises his right to be forgotten [141,171]. The identity associated with the transaction introduced into the blockchain is anonymized, while the remainder of the transaction's information is accessible [153,172,173]. This feature enables the auditing of the entire blockchain if necessary and that, in the case of sensitive information, such as EHR, may result in the exposure of information that enables the transaction's identity to be determined [141].

Q3. How were the arisen issues resolved?

Depending on how blockchain is implemented, various privacy concerns may occur, making it easy to track an entity's transactions. A notable example is given in [141], where an entity's public key corresponds to its identity in the blockchain system, allowing for the discovery of all transactions linked with that public key. This scenario would be catastrophic in a public blockchain and might also present an issue in a private blockchain, as not all members may require access to transaction data. The case in [141] refers to specific blockchain implementations that enable selective publication of private information and rely on zero-knowledge cryptography for verification. How to apply the GDPR-mandated right to be forgotten for a patient's data is one of the disadvantages demonstrated when implementing blockchain in the health area. Among the downsides of blockchain technology are the costs involved with authenticating connected data, auditing different entities and transactions, and the cost of interoperability provided to the network of participants. The pseudonym does not ensure transaction privacy, and it is even feasible to de-anonymize a user's identity through analysis of incoming and outgoing transactions.

Privacy by Blockchain Design (PbBD) Privacy by Blockchain Design develops on data privacy solutions for the disruptive and rapidly growing new tech ecosystem. Blockchains can not only be GDPR-compliant, but they can also help raise data protection levels and truly give back data ownership to individual patients or their legal guardians (e.g., family members or the state), by establishing general principles and methods for handling personal data in blockchain ecosystems. PbBD specifies technical and organizational measures for data protection while taking into account the principle of "privacy by design" as well as specifications that are inspired by legal frameworks, such as GDPR. As such, the Blockchain as a great tool for privacy and want to encourage the industry to take the lead in this area.

VIII. TAXONOMY OF AI-BLOCKCHAIN

A. DECENTRALIZED APPLICATIONS

AI applications are self-contained and execute intelligent decisions by making use of a range of strategizing, discovery, improvement, training, pattern recognition, and information management methodologies. Decentralizing AI activities, on the other hand, is a tough and time-consuming task.

1) AUTONOMOUS COMPUTING

One of the primary aims of AI applications is to facilitate the complete or partial autonomous process. This is achieved when a large number of intelligent agents in the form of small size computer programs identify their component ecosystems, sustain their internal environments, and conduct set actions to produce a response [82]. Modern computer systems must be able to handle tremendous heterogeneity across all verticals to operate autonomously, which often includes datasets, instruments, data processing, storage services, and application linkages, to name a few. Not only the usage of a multiagent approach across all layers makes it more convenient to deal with heterogeneity, but it also enables the easier establishment of the inter-and intra-layer functionality across the whole systems [83]. By ensuring operational decentralization and retaining perpetual records of interactions between the data, users, devices, apps, and systems, the blockchain architecture is significant in developing wholly decentralized autonomous systems.

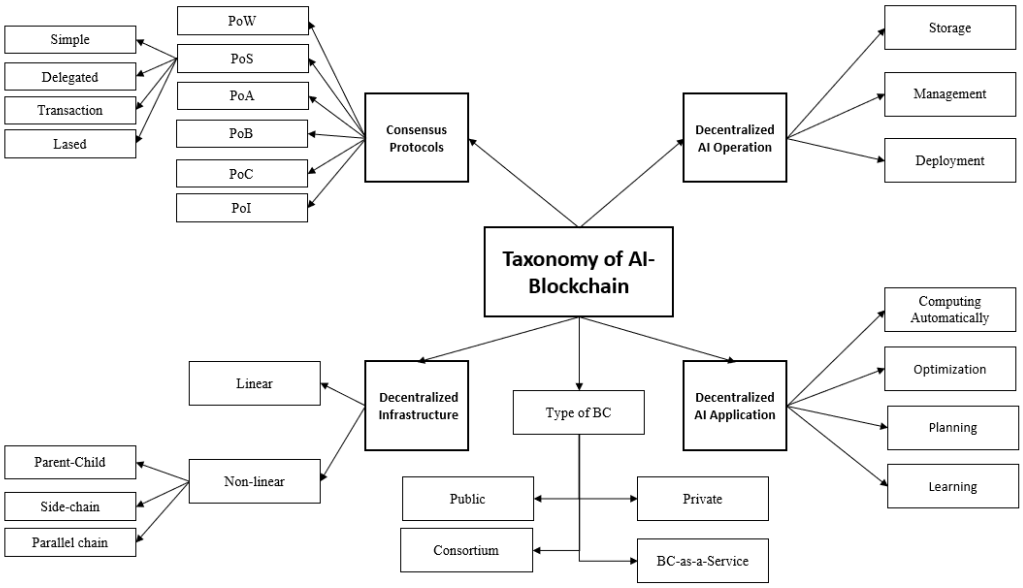

FIGURE 7. Taxonomy of AI-Blockchain

2) OPTIMIZATION

Among the primary characteristics of AI-enabled apps and schemes is the discovery of a collection of optimum solutions from all available alternatives [84]. Mod-ern AI applications and systems can be found in ubiquitous computing such as edge computing systems, infrastructure-restrained environments in mobile devices, spatially confined ecosystems such as wireless local area networks and personal area networks, and centralized enormous parallel computing systems distribution as applied in cloud computing [85]. The optimization algorithms operate in confined or unconstrained environments based on application- and system-level objectives [86]. These strategies facilitate the discovery of the most suitable solutions in identifying the pertinent data sources in pervasive environments, the best cloud or edge servers for processing the data and application, as well as in allowing resource-efficient information management in extensive distribution of computing settings.

The optimization process at present is implemented by centralizing control and taking into account system-wide and application-wide enhancement objectives, causing unnecessary and irrelevant management of data and poor performance of the system or the application itself [87]. The application of blockchain enables decentralized optimization methodologies to bring up new research and development possibilities. By analyzing highly applicable data, the decentralized optimization techniques are advantageous in terms of improving system performance, particularly when numerous techniques are executed concurrently across the systems and applications.

3) PLANNING

AI apps and systems use planning approaches to collaborate with other systems and applications, as well as to solve complex problems in new situations. Planning strategies improve the operational efficiency and resilience of AI systems by gathering current input conditions and performing different logic and rule-based algorithms to achieve preset goals [88]. Currently, centralized planning is a laborious and time-consuming activity. Consequently, decentralized AI planning techniques based on blockchain are required to provide a higher degree of robustness with provenance history and continuous monitoring. It is worth noting that the blockchain ecosystem can also be used to create immutable and critical blueprints for task-essential systems and relevant applications.

4) LEARNING

Learning algorithms, with models such as unsupervised, semi-supervised, supervised, reinforcement, transfer, ensemble, and deep learning, remain to be the heart of AI systems in facilitating knowledge discovery and autonomous processes. These learning models tackle a wide range of machine learning issues, from classification to clustering, besides regression analysis to frequent pattern mining. Traditional learning models are taught and released by utilizing centralized infrastructure to achieve global intelligence.

Dispersed learning models can help in the construction of highly propagated and automated learning systems in contemporary AI systems, allowing for the complete co-ordination of local intelligence across all verticals [89, 90]. Furthermore, by maintaining data provenance and history, the blockchain enables irreversible and highly secure configuration of learning models. Because smart contracts

are irrevocable, learning models must be extensively trained and evaluated before they can be implemented on the blockchain.

B. DECENTRALIZED OPERATION

Large volumes of data are typically handled by AI applications to make superior and more versatile decisions. However, when it comes to designing highly secure and privacy-preserving AI systems, centralized data retention via clouds, data centers and clusters presents a significant challenge. In other cases, learning model development and deployment might also be arduous.

1) STORAGE

A centralized data server raises the issue of vulnerability in terms of privacy and security concerning the users' personal and sensitive data, such as financial information, health records, whereabouts, and activities. Furthermore, as AI applications attempt to analyze, transform, and store massive information, wide-scale data collection would reveal the centralized infrastructure's scalability and capacity constraints. Blockchain-based decentralized storage architecture enables reliable cryptographic data storage across collaborating networks [91, 92, 93]. To maintain data availability for desired clients consisting of an application, user, or a node on the blockchain, every node in the system maintains a client-centric openly secured version of the whole library, which the clients can harvest and utilize their data as needed.

The key technologies for decentralized storage are sharding and swarming [94–96]. Sharding is a technique of dividing a database into logical parts and assigning each one a unique key to be accessed. The shards are then grouped, with the accumulated storage is supported by a swarm of network nodes. In AI applications, the swarms reduce latency by allowing numerous nodes in the network to access data simultaneously. In addition, geographically dispersed multiparty decentralized storage systems would improve storage scalability and dependability.

2) DATA MANAGEMENT

AI applications must manage data in such a way that is highly applicable and precise, with full datasets obtained from credible data sources, along with effective decentralized storage. In the underlying network, AI applications traditionally have used centralized data management techniques operated across all nodes [97]. These strategies include but are not limited to, data segmentation, filtration, context-aware storage systems and transmission in underlying architecture, as well as temporal and intelligent management of data systems. When considering decentralized storage networks and blockchain immutability requirements, inefficient centralized data management may arise, resulting not only in data redundancy in terms of small modifications but also in the transfer of comparable information several times. In the event of large datasets is being utilized, the massive size of data transfer would cause bandwidth to overload quickly and raise the issue of backhaul network traffic, thus, necessitating decentralized data processing for AI systems based on blockchain structure. By taking into account the data's temporal and spatial features, decentralized data infra-structure strategies are intended for application at the network node level. Furthermore, decentralized data management systems may place metadata on the blockchain network to assure data security and provenance while the conventional large-capacity storage solutions, including cloud clusters and data centers, might be utilized to store actual data. For client-centric small datasets, the metadata and real data are maintained on the blockchain, with the management of data being done through the network via token-based incentives for nodes carrying various shards or participants in swarms.

3) DEPLOYMENT

A trained model's true performance is evaluated after the distribution in production settings. Model deployment, on the other hand, is a regular and repetitive process as the developers must constantly improve the models and rectify bias by generating a certain set of findings while disregarding the rest of the options to provide particularly useful and educated judgments. Model deployment is considered a simple iterative process in centralized systems. In decentralized systems, however, poses quite a challenge [98]. Intelligent contract-based model deployment overcomes these difficulties by constantly logging changes and preserving unchangeable model versioning. Furthermore, a model collaboration between various AI applications would be safer and more reliable since developers can monitor the origin and traces of a specific model version.

C. BLOCKCHAIN TYPES FOR AI APPLICATION

The two types of blockchain technologies consist of Permission and Permissionless structures. For the Permission type, only authorized users would be able to handle the blockchain applications in a consortium, cloud-based, or private environment, while it is openly usable for all users over the Internet for the Permissionless type.

1) PUBLIC

Users may retrieve the blockchain codes and save them to their terminal for editing and utilizing based on their needs using the public blockchains [99, 100]. To add to this effect, public blockchains can be easily accessed and available to all network participants, particularly for read and write operations. Because of this feature, blockchains employ complicated security and consensus methods, as well as anonymity and bogus data on the network to handle user credentials and private transactions. For any public blockchain, innate tokens such as valuable pointers and cryptocurrencies are used to move assets and data. Due to its

huge decentralization and transparency, public blockchains are extensively used, even though the users and validators are constantly being anonymous. It was worth noting that due to the obscurity, hostile security assaults such as significant data and value theft on these blockchains are always a possibility.

To reach a consensus, public blockchains would require 51 percent validators at the very least and would perform complicated mathematic works in the background to attempt cracking the security codes, which often results in high energy expenditure and the issue of vulnerability if the attackers obtain control on the 51 percent shares on the network. This might also be the reason for the higher transaction approval times on public blockchains as compared to the consortium and private blockchains.

On a public blockchain, a transaction is often approved in 10 minutes or above, depending on the number of network users and the mathematical complexity of the consensus algorithms used.

2) PRIVATE

A single organization manages a private blockchain, which is structured as a Permission system so that the acknowledged users and participants would be pre-authorized for read and write activities within the network [101]. Since the credentials of pre-approved network participants and validators are known, private blockchains are comparably faster than public blockchain as it requires fewer mathematical operations for transaction validation purposes on the network. In addition, within the network, private blockchains can broadcast any type of indigenous assets, data, and values. Voting or multiparty consensus algorithms are used to approve transactions and asset transfers, which require minuscule energy consumption, allowing for a quick transaction process. For example, on private blockchains, transaction approval times typically take less than one second.

3) BLOCKCHAIN-AS-A-SERVICE

Due to widespread usage and approval by governments and large corporations, blockchain technologies are drawing the attention of cloud service vendors. Customers of major cloud suppliers such as Microsoft, Amazon, and IBM can now create and experiment with blockchain services in their environments [98].

The emergence of BaaS is projected to benefit both consortium and private blockchain firms by allowing them to concentrate on creating value through apps development, validation, and implementation rather than worrying about the infrastructures associated with the storage, underlying network, and computation. Besides the fact that the installation of BaaS facilitates the formation of new cross-industry private-public partnerships, it also helps in the development of new opportunities and company-customer interaction models. To construct smart contracts, developers have access to a single-click setup of BaaS services. On that note, the incorporation of BaaS with AI services opens up a new world of possibilities for apps developers, considering that the main cloud providers currently are offering a plethora of cloud services for AI applications.

C. DECENTRALIZED INFRASTRUCTURE

Traditional blockchain systems built a linear infrastructure using a mixture of a connected list of data frameworks and hashing algorithms. Nonlinear infrastructure, built upon graph theory and buffering data modeling, on the other hand, is growing to meet the needs of instantaneous applications and to manage massive volumes of data.

- Linear: Blockchain system based on a single chain that expands linearly, with new blocks inserted at the chain's end. The early adoption phase of a decentralized system usually uses single chains despite several flaws associated with it. For example, single chains would scale sluggishly, affecting the real-time performance of decentralized applications [99, 100]. Furthermore, because each business situation has its single chain, information, asset, and value exchange in different chains would be a challenging task. Single-chain blockchains instead, may be used for single-task AI systems that conduct search, refinement, and training, as well as autonomous AI applications that function in homogenous environments. Rather than the AI programs themselves being executed via smart contracts, single-chain blockchains may be more advantageous when just the performance records of AI apps need to be preserved in perpetuity. For instance, in radiology applications, a model for deep learning can be used to deliver accurate results for diagnosing liver cancer. The successful search footprints of distant industrial robots could be another example of its use. Since AI applications typically function in unrestrained contexts, placing the entire components on blockchain structure is not a viable option.
- Non-Linear: Multichain architectures are utilized to construct nonlinear blockchain architectures, using topologies and different types of chains such as parallel, parent-child, and main-side [104]. Multi-chain architectures not only offer a broad range of business cases and inter-chain value transfer, but they are also scalable for live performance. One or more chains would serve as the primary chain in a multi-chain structure, holding the data concerning other chains while the remaining ones would be employed as the parallel, side, or child chains. Side and child chains are typically similar in operation, with the principal difference being that the business scenarios in child chains are firmly related to parent chains while the side chains can operate completely independent from the main chains. As for the parallel chains, they could function separately from one another. To transfer the value between several chains, the "pegging" approach is implemented by integrating a two-way peg procedure that allows bidirectional value transfer at a fixed exchange rate. It should also be noted that in the blockchain, native currencies or tokens would

represent the exchange value. For interested readers, the following studies provide a full discussion of nonlinear blockchains.

In decentralized apps, nonlinear blockchains for the AI apps domain grant the operation of several related and independent AI tasks.

Furthermore, the scalability property allows AI applications to be developed and deployed in parallel such that AI parts are installed on the main or parent chain in a production context, while the testing and training apps are loaded on the test nets or side chains. Emerging apps, such as those in adapting and reinforcing learning algorithms, benefit from nonlinear architectures since the principal applications must continually improve their productivity by reconfiguring the learning models. In this case, learning models are built on the side chains and subsequently deployed on the main chains.

D. THE ROLE OF CONSENSUS PROTOCOL

1) PROOF-OF-WORK (POW)

The PoW consensus mechanism is used by popular public blockchain systems, namely Ethereum and Bitcoin to verify transactions after the participation of at least 51 percent of nodes on the underlying network [99, 100].

Because the validating nodes run anonymously and in vast numbers, they must produce the blocks by deciphering complicated and arbitrary mathematical problems, as well as cracking the hash code to access the transactions on the blockchain network. To receive the prizes, the successful nodes send the answer through a peer-to-peer network. Additional transactions and data are irrevocably joined to the blockchain when 51 percent of the nodes successfully solve the mathematical problem. Although PoW has shown to be a standard consensus protocol, it consumes a lot of energy in large networks and causes delays in transaction approvals time. As astute algorithms regularly streamline decision structures to make an educated judgment, AI applications would have a higher prevalence of write operations. As a result, in real-time AI applications, PoW protocols would become a performance barrier, besides the fact that an attack on 51% of the nodes in the underlying network could jeopardize the reliability of AI applications.

2) PROOF-OF-STAKE (POS)

Consensus PoS-based techniques attempt to address the problem of PoW's excessive energy consumption [104]. The PoS protocols function by identifying key players on the blockchain network to allow them to generate new blocks. These methods select validators based on a variety of factors, such as delegated, high frequency transacting, random, or those that maintain coins for a longer period.

PoS has shown to be more energy-efficient than PoW, and it also solves the vulnerability issue by eliminating pseudonymous validators and allowing only those who possess the blockchain's native currency to participate. Validators, on the other hand, have little to risk if they do not authenticate the transactions on the blockchain, which may delay the development of new blocks. Although PoS is useful for the lag-tolerant AI apps, it is not ideal for AI systems, especially in the management of flowing data, changing the identification, and making intelligent decisions on a real-time basis.

3) PROOF-OF-ACTIVITY (POA)

PoAc is a mixture of PoW and PoS protocols. Such protocol aims to address the 51 percent attack problem by implementing the PoW algorithm on blank blockchains [105]. This is done by PoAc protocol solves complicated mathematical problems first and validators begin to receive incentives, increasing their holding on the ledger. This allows for the validators with a sufficient stake in the blockchain to use the PoS algorithm. Additionally, PoAc is effective in terms of security, memory, and network connectivity.

As a result, it may be advantageous for AI programs that require less data accessibility and higher security.

4) PROOF-OF-BURN

According to the PoB protocol, validators can only spend their coins if they send them to a public, valid, unusable, and faulty address. After burning their money, users are instantly authorized to develop new blocks and collect incentives [99]. Users could benefit from PoB since it allows them to contribute in advance and earn interest on the chain while also becoming approved validators. The protocol also gives an advantage by fixing the PoW's energy use problem. Furthermore, coin burning lowers the number of coins on the ledger, resulting in a gradual increase in coin value, amount balancing of currencies on the blockchain, the spending of unsold coins, and payment of the transaction cost. PoB protocols can be used by AI systems to urge participants to keep the value of the underlying judgments. Applications needing a specific degree of precision, a set amount of clusters or items recognized, for example, can consume learning models and search trees to keep value over the ledger.

5) PROOF-OF-CAPACITY (POC)

Traditional PoW algorithms become computationally expensive since they must obtain randomized nonce values to decrypt the blocks. The Proof-of-Concept protocol, commonly called proof of space, is a substitute mechanism for determining the space amount of hard drive on the blockchain network's nodes [107].

Rather than utilizing random numbers, it stores the potential nonce values on the hard drive and looks for matching nonce-hash combinations to decrypt the blocks. Nodes that are having a large amount of disc space would obtain a lot more stake and a high chance of winning with PoC.

6) PROOF-OF-AUTHORITY (POA)

PoA could be used to address the problem of PoW's high energy usage, as well as the issue of the validators should possess a portion of capital invested in the blockchain network. A PoA protocol delegates authoritative power to specified nodes, forming a consensus based on the absolute majority to create additional blocks on the ledger [108].
PoA has been shown as being a resource-effective and low-latency consensus system, albeit it is better suited for networks in private since it allows authorized stakeholders to delegate validation authority. Consequently, blockchain implementers must consider the validators' legal identities, well-defined eligibility requirements, and a common qualification condition for each shareholder to operate as validators. PoA security risks are always present, owing to security attacks on validators, which could be a source of assault on the network, notwithstanding their energy economy and fiscal efficacy. Alternatively, PoA might be used as a substitute consensus approach for AI systems that run on private or consortium networks because all validators are recognized over the system.

IX. DISCUSSION

1) To what extent has the blockchain been developed for the management of EHRs, and how has it evolved over time?
Authors in the literature attempted to propose solutions for managing EHRs from various perspectives. For data encryption, many people used symmetric encryption schemes, while others used asymmetric encryption schemes. A few authors provided solutions for the blockchain's scalability when managing EHRs. Some people brought smart contracts, while others used chain-code for EHR preservation mechanisms. When it comes to EHR storage, there are two options: on-chain storage and off-chain storage. An on-chain storage scheme is focused on storing data on the blockchain, whereas an off-chain storage scheme stores data in the cloud or a local database and links the data's address to the blockchain.
From 2016, when blockchain-based solutions for managing EHRs first became available, to 2021, there has been tremendous progress. The idea of using blockchain as a platform to manage health data was first mentioned in the article [74] in 2016. Later that year, an article [110] discussed the use of private blockchain for EHRs. Following that, researchers attempted to demonstrate the utility of AI-blockchain for handling EHRs.

2) What standards are used to store EHRs in the blockchain?
The standards related to the data format and interoperability principle remain an issue for sharing and storing EHRs. Most authors consider FHIR and HL7 when they defined standard for EHRs data format [74], [24]. However, only a few authors followed the standard of HL7 [78], [101], whereas a small number considered the standard of FHIR [24], [119], [128]. Standardized EHR data model is designed to support interfacing to the clinical decision support system. Among the rest of the papers, authors in [9], [78] and [190] described the standard of ISO 27789 , HL7 and HIPAA, but did not implement those principles.
Despite the references mentioned above, the expected standard for EHRs exchanging, uploading, storing, authenticity checking, and formatting remains a critical issue for blockchain-enabled EHRs solutions. It could be due to the evolving nature of blockchain and the lack of standardized development platforms. While blockchain is a promising technology for EHR management, it still has a long way to go before it can be considered stable enough to support a standardized framework.

3) How large amounts of EHR data are handled?
Handling such massive amounts of data is a significant challenge. When it comes to dealing with large amounts of data via blockchain, the task becomes more difficult because storing data on the blockchain is costly. The blockchain was initially designed to keep data small in size, basically the financial transaction information. However, in order to enjoy the benefits of blockchain while overcoming the limitations of data storage capacity, researchers devised a number of solutions. While many people haven't considered blockchain's scalability for data storage, others have focused on storing data in the cloud or in local databases and linking the address from that storage to the blockchain. Among the papers we examined for the review, slightly less than half did not address the major data storage issue. Authors of [3], [115], [118], have considered the issue, but they haven't discussed the data storage services. In addition, there were other authors who have chosen the Interplanetary File System (IPFS) as a medium of data storage and then linked the address with the blockchain [19], [34], [93], [142], [78], [117], [109]. The rest of the papers proposed using private blockchain or off-chain storage to handle scalability issues.
The solutions mentioned above to overcome big data issues are significant, but more research is required to handle a significant amount of EHRs data.

4) What blockchain platforms/mechanisms are used to manage EHRs?
Because EHRs include sensitive personal information, a private blockchain is at the top of the popularity ranking. Furthermore, a private blockchain can enable access control rules, allowing only particular persons to join the network while adhering to good security policies. A public blockchain, on the other hand, does not have strong access control rules, so anyone can join the web and read the data. A consortium blockchain also provides a private network and restricts access to network data.
The literature review included several potential models or architectures. The majority of the authors concentrated on EHR integrity, availability, transparency, privacy, and security. Almost all of the models offered to support for the storage of EHRs from medical institutions as well as wearable devices. A significant number of papers used the Ethereum platform for the proposed solutions. The number

for Hyperledger Fabric was only one paper [121]. The rest of the offered solutions include Bitcoin [99], [100], [105],[107],[134] consortium blockchain [98], [102], private & consortium blockchain [98], [100], Multichain [104], private blockchain [19], [21], [101],[141], and Permissioned Blockchain [186].

X. OPEN CHALLENGES AND FUTURE RESEARCH OPPORTUNITIES

One may define numerous issues of healthcare Blockchain-based applications based on the proposed prototypes and developed applications discussed above.

With the introduction of wearables and a slew of new IoT devices with data flows harnessed, improved security is required to be readily available to healthcare providers [138, 193]. These issues might be addressed with blockchain technology, which offers interoperability, integrity, and security, as well as portable user-owned data.

Interoperability refers to a system's capacity to seamlessly integrate with another system to share critical data. The ease of transformation of the medical records and the healthcare data information from one provider to another is referred to the interoperability in the EHR system. While health care organizations can connect in a variety of ways, the EHR is generally regarded as one of the simplest and most secure methods that do not result in information blocking [92,93]. To begin with, the EHR must have core interoperability. This enables the entire system to send data to another system while also receiving data. While the data received will not need to be analyzed as part of this level of interoperability, it will be available within the system immediately. This is the lowest degree of functional interoperability, allowing only the most basic data exchange.

Second, the EHR must have structural interoperability, which means that data must flow appropriately through the system so that providers may see unmodified patient data. To establish a new EHR database utilizing structured messages, this intermediate region of health care data exchange ensures that patient information is provided and received in a relevant and shareable fashion. Furthermore, even if the data changes hands, the facts, and meanings will not be altered.

Third, the EHR must have semantic interoperability, which allows data to be accurately reorganized and codified so that any system can receive and interpret the new information. This means that the language used by one EHR system must be readable by the next system. This is the highest level of interoperability possible with significant implications for patients, clinicians in a health system, and scientists and researchers who collect data to study patient populations. Due to the adoption of standardized coding, information is transferrable and usable at this level. In contrast to studies [69,115], which lacked the possibility of interoperability and is not discussed in EMR systems as a result, medical and health data experts must perform manual inspection and mapping of predefined ontologies. At the same time, clinical malpractice is uncontrollable. Furthermore, scalability and interoperability concerns are at the forefront of current and future research in this area. The lack of standards for designing healthcare applications based on blockchain technology is revealed by the interoperability challenge.

The second challenge has to do with questions of privacy and security [115]. The data on the blockchain is spread to all nodes, resulting in non-compliance with privacy rules and vulnerabilities. As a result, to protect data privacy and security, data must be stored off-chain. New privacy technologies, such as homomorphic and attribute-based encryption, secure multiparty computation, zero-knowledge proof, obfuscation, and format-preserving encryption, and may be able to accomplish data privacy [111].

Designing using hybrid privacy approaches and leveraging security-enhancing technology, such as a homomorphic signature, which works better than public-key certificates, could speed up the different security levels in a system. More significantly, any malicious attacker can manipulate health data acquired from hospitals, clinical labs, and patients, rendering AI learning useless. As a result, utilizing federated learning mixed with blockchain technology, it is necessary to collect health data from many sources without any privacy leaks. Each healthcare organization's central entity is responsible for any legal difficulties as well as the overall seamless operation of the centralized healthcare systems. A decentralized, patient-centric system, on the other hand, makes it difficult to resolve any legal disputes or inconsistencies in the public blockchain architecture. When personal data is run on converging AI and blockchain platforms, for example, copyright infringement and defamation issues occur.

On the other hand, scalability is the main issue in blockchain-based healthcare systems [90,100-103], especially when dealing with large amounts of medical data. Due to the high volume of healthcare data, it is not feasible to store it on-chain, as this would result in significant performance degradation.

Due to the consensus method and ledger replication to all network participants, scalability has always been a constraint in blockchain networks [137]. In the case of healthcare blockchain-based networks, scalability has been a barrier to the adoption of any fast-growing technology. Besides the performance bottleneck, the capacity issue with blockchain should be seriously considered. As the size of a blockchain expands, the amount of storage required by all blocks expands as well. As a result, complete nodes, which keep all the network's block data, demand a lot of storage space [117]. Similarly, as the blockchain history grows, the Bootstrap time will climb linearly, slowing the process of new nodes joining the system. All these constraints reduce a blockchain's availability and decentralization and should be carefully considered when creating a large-scale blockchain. Not every entity in such a network needs a comprehensive blockchain ledger. As a result, the strategies should concentrate on interactions between just those in the network who need to

know, i.e. on a need-to-know basis. In every rapidly evolving technology, scalability is a major challenge. Scalability is measured in terms of throughput, latency, storage, and block size in blockchain networks. For that, it should analyze a performance matrix in blockchain networks, such as throughput, consensus latency, and the number of transactions completed per appointment. The bigger the number of verifiers in the block verification phase, the higher the level of security; nevertheless, this increases latency. Healthcare necessitates security with the shortest possible verification time.

In general, there are few future directions that stand clear for the EHR management research efforts, namely; applications of Big Data, AI, Edge Computing and IoMT. Below is our take on these directions.

A. BIG DATA

A significant problem for healthcare data systems seeking to improve the quality of healthcare services is acquiring, processing, and analyzing huge volumes of personal healthcare data, particularly from commonly used mobile and wearable devices, while minimizing privacy violations. Blockchain technology has the potential to address the security concerns associated with big data techniques by providing immutability, security, and traceability. Big data can make the best use of all healthcare data assets to assist necessary improvements in areas of prediction in healthcare diagnosis, analysis in magnetic resonance imaging, and other applications [174].

Two broad categories of big data analysis are data management and data analysis. For data management, blockchain technology can be utilized to securely maintain immutable healthcare records. For data analysis, the blockchain's transactions and records can be extracted and studied for potential trading behaviors.

B. ARTIFICIAL INTELLIGENCE

When blockchain technology is combined with AI in a variety of real-world healthcare applications, the resulting systems become more efficient and stable [175]. Machine learning (ML) and deep learning (DL) are two major branches of AI that are assisting in the automation of real-world applications. In the near future, machine learning will be used in concert with blockchain to manage EHRs. Despite the difficulties associated with storing, distributing, and training vital EHR data to design practical applications, interest among researchers in developing machine learning and blockchain-based EHR applications has grown tremendously [176], [177]. IBM has announced intentions to implement an intelligent blockchain, in which an AI agent performs various duties such as enforcing laws, improving records, detecting suspicious activity, and making recommendations for upgrading smart contracts over a broad network. In the MATRIX project [178], AI is employed to construct a next generation blockchain that enables the automated development of intelligent contracts, enhances protection against malicious attacks, and enables highly scalable operations. Various machine learning techniques can be used to detect fake EHR data, ensuring that only authentic EHRs are maintained on the blockchain. Deep learning enables the recovery and storage of previously damaged scanned medical records in blockchain for the sake of knowledge enhancement (e.g., drug analysis and prediction) [179]. Additionally, deep learning as-a-service (DaaS) is employed on stored EHRs to accurately forecast future diseases based on current patient diagnosis reports [180]. Machine learning techniques can also be employed to protect blockchain networks from large-scale attacks [181]. There are some established projects that mix AI with blockchain. For example, SingularityNET [182] focuses on developing AI and blockchain-based networking for the robot brain, while DeepBrainChain focuses on developing a platform for developing AI algorithms. Additionally, several machine learning and deep learning-based health-related projects are underway, including the Gamalon project, TraneAI [183], and Neureal [184].

C. EDGE COMPUTING

Due to network congestion and data size, sharing huge volumes of EHRs among diverse health care companies is problematic. Recent options for EHR management are limited in terms of scalability, computing cost, and reaction time. Edge computing may provide a solution to these difficulties. It can process a vast amount of data from multiple locations, as edge computing is comprised of a set of servers/computers [185]. Researchers in [186] propose using edge computing to extend cloud services to the network's edge, thereby increasing processing capacity and device QoS. Edge Processing offers the advantages of large data storage, extensive networking, and high computing power, while also enabling secure and regulated scaling for distributed EHR applications. While edge computing has several drawbacks, including security, vulnerability to various attacks during message transmission, and integrity, blockchain-based solutions face several challenges, including storage, scalability, block size constraints, and block creation time, all of which can be addressed using edge computing. Similar approaches for decentralized technology can improve privacy, security, and resource management on an automatic basis [187]. Combining the two can provide several advantages. For example, blockchain can first be used to implement distributed controls across multiple edge nodes. The blockchain mining process verifies the accuracy, consistency, and dependability of data. Then, user privacy can be enhanced further by allowing people to control data using cryptographic keys. Finally, edge computing entails resource sharing across nodes, which can be accomplished securely via blockchain-based smart contracts [188].

D. INTERNET OF MEDICAL THINGS (IOMT)

The IoMT is a collection of medical devices and software that connect to various healthcare providers via online computer networks. The Internet of Medical Things is built on the concept of Machine-to-Machine (M2M) communication between wireless medical devices. Medical care providers and authorities can obtain real-time health updates on patients from remote places using wearable devices via the IoMT. Apart from the benefits of IoMT, there are some disadvantages, as IoMT devices are susceptible to security attacks. Not only has demand for novel medical devices surged dramatically during the Covid-19 outbreak, but so have cyber risks associated with them [189]. Blockchain technology might be viewed as a savior against the hazards posed by IoMT devices. Blockchain's decentralized key management, inseparability, and integrity qualities enable the secure communication of intelligent medical equipment.

XI. CONCLUSION

Blockchain software is attracting considerable interest from people, as well as organizations of almost all kinds and sizes. With its features, which include decentralization, anonymity, persistence, and auditability, it can turn the conventional industry. Blockchain applications are expected to use Artificial Intelligent Approaches to re-shape the healthcare environment. Not only would the mechanism be open and safe, but it will also improve the quality of healthcare at a lower cost. An expanded discussion of various blockchain technologies in the healthcare industry was addressed and major research projects as well as potential prospects for research were identified. In particular, we discussed how a properly designed framework for the management of health data is needed and how blockchain would empower patients and streamline the health data sharing process while maintaining the security and privacy of the patient data. We find that there is a consensus among researchers that patient data would truly be owned and managed by the rightful owner of the data, i.e., the patient, with blockchain technology. The blockchain facilitates timestamping of health records so that after being part of the distributor ledger, no one can tamper with them. Patients have the right to determine who, and for what reason, can and cannot access their data.

21st-century healthcare systems will consist of different technologies that connect patients with their caregivers (e.g., remote healthcare facilities, wearable devices, etc.). Such systems continuously produce data and can be subjected to malicious attacks while being transmitted at different levels of the underlying communication network. In this paper, we addressed several research studies that suggest tamper-resistant systems to ensure the fidelity of health data using blockchain technology and AI methods to improve on current centralized models and enable a patient-centric data-sharing platform by giving the patients complete control over their data.

However, after a thorough review of selected studies, it is found that using blockchain to handle vast amounts of EHR data on a wide scale has drawbacks such as limited storage capacity, computation cost, and communication cost. However, potential solutions to these restrictions include artificial intelligence, IoMT, and edge computing.

The study could be used as a starting point for future research in this area. The collection of all linked publications, their contributions, and their limits will aid potential scholars in developing a new architecture or model.

Furthermore, future research directions using blockchain could aid in the development of more innovative solutions to existing challenges.

REFERENCES

[1] A. Kumari, S. Tanwar, S. Tyagi and N. Kumar, "Fog computing for Healthcare 4.0 environment: Opportunities and challenges", 2022. .

[2] P. Campanella et al., "The impact of electronic health records on healthcare quality: a systematic review and meta-analysis", The European Journal of Public Health, vol. 26, no. 1, pp. 60-64, 2015. Available: 10.1093/eurpub/ckv122.

[3] M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities", Renewable and Sustainable Energy Reviews, vol. 100, pp. 143-174, 2019. Available: 10.1016/j.rser.2018.10.014.

[4] I. Mistry, S. Tanwar, S. Tyagi and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges", Mechanical Systems and Signal Processing, vol. 135, p. 106382, 2020. Available: 10.1016/j.ymssp.2019.106382.

[5] R. Vaishya, M. Javaid, I. Khan and A. Haleem, "Artificial Intelligence (AI) applications for COVID-19 pandemic", Diabetes & Metabolic Syndrome: Clinical Research & Reviews, vol. 14, no. 4, pp. 337-339, 2020. Available: 10.1016/j.dsx.2020.04.012.

[6] P. Tagde et al., "Blockchain and artificial intelligence technology in e-Health", Environmental Science and Pollution Research, vol. 28, no. 38, pp. 52810-52831, 2021. Available: 10.1007/s11356-021-16223-0.

[7] Vora J, Italiya P, Tanwar S, Tyagi S, Kumar N, Obaidat MS, et al. Ensuring privacy and security in E-health records. CITS 2018 - 2018 Int Conf Comput Inf Telecommun Syst. 2018 Aug 17;

[8] S. Tanwar, K. Parekh and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications", Journal of Information Security and Applications, vol. 50, p. 102407, 2020. Available: 10.1016/j.jisa.2019.102407.

[9] [3]T. Kubo, A. Yanasan, T. Herbosa, N. Buddh, F. Fernando and R. Kayano, "Health Data Collection Before, During and After Emergencies and Disasters—The Result of the Kobe Expert Meeting", International Journal of Environmental Research and Public Health, vol. 16, no. 5, p. 893, 2019. Available: 10.3390/ijerph16050893.

[10] T. Davenport and R. Kalakota, "The potential for artificial intelligence in healthcare", Future Healthcare Journal, vol. 6, no. 2, pp. 94-98, 2019. Available: 10.7861/futurehosp.6-2-94.

[11] Q. Feng, D. He, S. Zeadally, M. Khan and N. Kumar, "A survey on privacy protection in blockchain system", Journal of Network and Computer Applications, vol. 126, pp. 45-58, 2019. Available: 10.1016/j.jnca.2018.10.020.

[12] C. Lin, D. He, X. Huang, M. Khan and K. Choo, "DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain", IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2440-2452, 2020. Available: 10.1109/tifs.2020.2969565.

[13] S. Ma, Y. Deng, D. He, J. Zhang and X. Xie, "An Efficient NIZK Scheme for Privacy-Preserving Transactions Over Account-Model Blockchain", IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 641-651, 2021. Available: 10.1109/tdsc.2020.2969418.

[14] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, 1982. Available: 10.1145/357172.357176.

[15] 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.

[16] A. Siyal, A. Junejo, M. Zawish, K. Ahmed, A. Khalil and G. Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives", Cryptography, vol. 3, no. 1, p. 3, 2019. Available: 10.3390/cryptography3010003.

[17] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records", IEEE Access, vol. 7, pp. 147782-147795, 2019. Available: 10.1109/access.2019.2946373.

[18] D. Nguyen, M. Ding, P. Pathirana and A. Seneviratne, "Blockchain and AI-Based Solutions to Combat Coronavirus (COVID-19)-Like Epidemics: A Survey", IEEE Access, vol. 9, pp. 95730-95753, 2021. Available: 10.1109/access.2021.3093633.

[19] M. Cyran, "Blockchain as a Foundation for Sharing Healthcare Data", Blockchain in Healthcare Today, 2018. Available: 10.30953/bhty.v1.13.

[20] J. Kaye, E. Whitley, D. Lund, M. Morrison, H. Teare and K. Melham, "Dynamic consent: a patient interface for twenty-first century research networks", European Journal of Human Genetics, vol. 23, no. 2, pp. 141-146, 2014. Available: 10.1038/ejhg.2014.71.

[21] B. Wang and Z. Li, "Healthchain: A Privacy Protection System for Medical Data Based on Blockchain", Future Internet, vol. 13, no. 10, p. 247, 2021. Available: 10.3390/fi13100247.

[22] "For a meaningful artificial intelligence", Google Books, 2022. [Online]. Available: https://books.google.com/books/about/For_a_meaningful_artificial_intelligence.html?id=9cVUDwAAQBAJ. [Accessed: 02- Aug- 2022].

[23] D. Dimitrov, "Blockchain Applications for Healthcare Data Management", Healthcare Informatics Research, vol. 25, no. 1, p. 51, 2019. Available: 10.4258/hir.2019.25.1.51.

[24] P. Zhang, J. White, D. Schmidt, G. Lenz and S. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data", Computational and Structural Biotechnology Journal, vol. 16, pp. 267-278, 2018. Available: 10.1016/j.csbj.2018.07.004.

[25] K. Salah, M. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges", IEEE Access, vol. 7, pp. 10127-10149, 2019. Available: 10.1109/access.2018.2890507.

[26] "Amazon.com", Amazon.com, 2022. [Online]. Available: https://www.amazon.com/Introduction-Statistical-Learning-Applications-Statistics-ebook/dp/B01IBM7790. [Accessed: 02- Aug- 2022].

[27] F. Jiang et al., "Artificial intelligence in healthcare: past, present and future", Stroke and Vascular Neurology, vol. 2, no. 4, pp. 230-243, 2017. Available: 10.1136/svn-2017-000101.

[28] Y. LeCun, Y. Bengio and G. Hinton, "Deep learning", Nature, vol. 521, no. 7553, pp. 436-444, 2015. Available: 10.1038/nature14539.

[29] M. Resta, M. Sonnessa, E. Tànfani and A. Testi, "Unsupervised neural networks for clustering emergent patient flows", Operations Research for Health Care, vol. 18, pp. 41-51, 2018. Available: 10.1016/j.orhc.2017.08.002.

[30] W. Raghupathi and V. Raghupathi, "Big data analytics in healthcare: promise and potential", Health Information Science and Systems, vol. 2, no. 1, 2014. Available: 10.1186/2047-2501-2-3.

[31] A. Beam and I. Kohane, "Big Data and Machine Learning in Health Care", JAMA, vol. 319, no. 13, p. 1317, 2018. Available: 10.1001/jama.2017.18391.

[32] S. Gehrmann et al., "Comparing deep learning and concept extraction based methods for patient phenotyping from clinical narratives", PLOS ONE, vol. 13, no. 2, p. e0192360, 2018. Available: 10.1371/journal.pone.0192360.

[33] P. Rajpurkar et al., "Deep learning for chest radiograph diagnosis: A retrospective comparison of the CheXNeXt algorithm to practicing radiologists", PLOS Medicine, vol. 15, no. 11, p. e1002686, 2018. Available: 10.1371/journal.pmed.1002686.

[34] I. Omar, R. Jayaraman, K. Salah, I. Yaqoob and S. Ellahham, "Applications of Blockchain Technology in Clinical Trials: Review and Open Challenges", Arabian Journal for Science and Engineering, vol. 46, no. 4, pp. 3001-3015, 2020. Available: 10.1007/s13369-020-04989-3.

[35] Zhou B, Khosla A, Lapedriza A, Oliva A, Torralba A. Learning Deep Features for Discriminative Localization. [cited 2021 Sep 22]; Available from: http://cnnlocalization.csail.mit.edu

[36] E. Ford, J. Carroll, H. Smith, D. Scott and J. Cassell, "Extracting information from the text of electronic medical records to improve case detection: a systematic review", Journal of the American Medical Informatics Association, vol. 23, no. 5, pp. 1007-1015, 2016. Available: 10.1093/jamia/ocv180.

[37] C. Shivade et al., "A review of approaches to identifying patient phenotype cohorts using electronic health records", Journal of the American Medical Informatics Association, vol. 21, no. 2, pp. 221-230, 2014. Available: 10.1136/amiajnl-2013-001935.

[38] D. Carrell et al., "Challenges in adapting existing clinical natural language processing systems to multiple, diverse health care settings", Journal of the American Medical Informatics Association, vol. 24, no. 5, pp. 986-991, 2017. Available: 10.1093/jamia/ocx039.

[39] J. Kirby et al., "PheKB: a catalog and workflow for creating electronic phenotype algorithms for transportability", Journal of the American Medical Informatics Association, vol. 23, no. 6, pp. 1046-1052, 2016. Available: 10.1093/jamia/ocv202.

[40] K. Foster, R. Koprowski and J. Skufca, "Machine learning, medical diagnosis, and biomedical engineering research - commentary", BioMedical Engineering OnLine, vol. 13, no. 1, p. 94, 2014. Available: 10.1186/1475-925x-13-94.

[41] Asperti A, Mastronardo C. The Effectiveness of Data Augmentation for Detection of Gastrointestinal Diseases from Endoscopical Images. BIOIMAGING 2018 - 5th Int Conf Bioimaging, Proceedings; Part 11th Int Jt Conf Biomed Eng Syst Technol BIOSTEC 2018 [Internet]. 2017 Dec 11 [cited 2021 Sep 22];2:199–205. Available from: https://arxiv.org/abs/1712.03689v1

[42] Wong SC, Gatt A, Stamatescu V, McDonnell MD. Understanding Data Augmentation for Classification: When to Warp? 2016 Int Conf Digit Image Comput Tech Appl DICTA 2016. 2016 Dec 22;

[43] R. Kemp and V. Prasad, "Surrogate endpoints in oncology: when are they acceptable for regulatory and clinical decisions, and are they currently overused?", BMC Medicine, vol. 15, no. 1, 2017. Available: 10.1186/s12916-017-0902-9.

[44] R. Lorbieski and S. Nassar, "Impact of an Extra Layer on

the Stacking Algorithm for Classification Problems", Journal of Computer Science, vol. 14, no. 5, pp. 613-622, 2018. Available: 10.3844/jcssp.2018.613.622.

[45] I. Kavakiotis, O. Tsave, A. Salifoglou, N. Maglaveras, I. Vlahavas and I. Chouvarda, "Machine Learning and Data Mining Methods in Diabetes Research", Computational and Structural Biotechnology Journal, vol. 15, pp. 104-116, 2017. Available: 10.1016/j.csbj.2016.12.005.

[46] W. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity", The Bulletin of Mathematical Biophysics, vol. 5, no. 4, pp. 115-133, 1943. Available: 10.1007/bf02478259.

[47] D. Rumelhart, G. Hinton and R. Williams, "Learning representations by back-propagating errors", Nature, vol. 323, no. 6088, pp. 533-536, 1986. Available: 10.1038/323533a0.

[48] J. Schmidhuber, "Deep learning in neural networks: An overview", Neural Networks, vol. 61, pp. 85-117, 2015. Available: 10.1016/j.neunet.2014.09.003.

[49] Liu S, Liu S, Cai W, Pujol S, Kikinis R, Feng D. Early diagnosis of Alzheimer's disease with deep learning. 2014 IEEE 11th Int Symp Biomed Imaging, ISBI 2014. 2014 Jul 29;1015–8.

[50] Cheng Y, Wang F, Zhang P, Hu J. Risk prediction with electronic health records: A deep learning approach. Proceedings [Internet]. 2016 [cited 2021 Sep 22];432–40. Available from: https://epubs.siam.org/page/terms

[51] Zhang J, Gong J, Barnes L. HCNN: Heterogeneous Convolutional Neural Networks for Comorbid Risk Prediction with Electronic Health Records. Proc - 2017 IEEE 2nd Int Conf Connect Heal Appl Syst Eng Technol CHASE 2017. 2017 Aug 14;214–21.

[52] M. Hossain, A. Khan, M. Moni and S. Uddin, "Use of Electronic Health Data for Disease Prediction: A Comprehensive Literature Review", IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 18, no. 2, pp. 745-758, 2021. Available: 10.1109/tcbb.2019.2937862.

[53] Rallapalli S, Suryakanthi T. Predicting the risk of diabetes in big data electronic health Records by using scalable random forest classification algorithm. Proc - 2016 3rd Int Conf Adv Comput Commun Eng ICACCE 2016. 2017 Oct 18;281–4.

[54] S. Uddin, A. Khan and L. Baur, "A Framework to Explore the Knowledge Structure of Multidisciplinary Research Fields", PLOS ONE, vol. 10, no. 4, p. e0123537, 2015. Available: 10.1371/journal.pone.0123537.

[55] T. McCormick, C. Rudin and D. Madigan, "A Hierarchical Model for Association Rule Mining of Sequential Events: An Approach to Automated Medical Symptom Prediction", SSRN Electronic Journal, 2011. Available: 10.2139/ssrn.1736062.

[56] Uddin S, Khan A, Piraveenan M. Administrative claim data to learn about effective healthcare collaboration and coordination through social network. Proc Annu Hawaii Int Conf Syst Sci. 2015 Mar 26;2015-March:3105–14.

[57] A. Khan, N. Choudhury, S. Uddin, L. Hossain and L. Baur, "Longitudinal trends in global obesity research and collaboration: a review using bibliometric metadata", Obesity Reviews, vol. 17, no. 4, pp. 377-385, 2016. Available: 10.1111/obr.12372.

[58] A. Khan, S. Uddin and U. Srinivasan, "Comorbidity network for chronic disease: A novel approach to understand type 2 diabetes progression", International Journal of Medical Informatics, vol. 115, pp. 1-9, 2018. Available: 10.1016/j.ijmedinf.2018.04.001.

[59] Khan A, Uddin S, Srinivasan U. Adapting graph theory and social network measures on healthcare data-a new framework to understand chronic disease progression. Proc Australas Comput Sci Week Multiconference [Internet]. 2016 [cited 2021 Sep 22]; Available from: http://dx.doi.org/10.1145/2843043.2843380

[60] Khan A, Uddin S, Srinivasan U. Chronic disease prediction using administrative data and graph theory: The case of type 2 diabetes. Expert Syst Appl. 2019 Dec 1;136:230–41.

[61] E. Kang, S. Kim, Y. Rhee, J. Lee and Y. Yun, "Self-management strategies and comorbidities in chronic disease patients: associations with quality of life and depression", Psychology, Health & Medicine, vol. 26, no. 8, pp. 1031-1043, 2020. Available: 10.1080/13548506.2020.1838585.

[62] S. Gupta et al., "Machine-learning prediction of cancer survival: a retrospective study using electronic administrative records and a cancer registry", BMJ Open, vol. 4, no. 3, p. e004007, 2014. Available: 10.1136/bmjopen-2013-004007.

[63] J. Velez-Serrano et al., "Prediction of in-hospital mortality after pancreatic resection in pancreatic cancer patients: A boosting approach via a population-based study using health administrative data", PLOS ONE, vol. 12, no. 6, p. e0178757, 2017. Available: 10.1371/journal.pone.0178757.

[64] Z. Huang, W. Dong, H. Duan and J. Liu, "A Regularized Deep Learning Approach for Clinical Risk Prediction of Acute Coronary Syndrome Using Electronic Health Records", IEEE Transactions on Biomedical Engineering, vol. 65, no. 5, pp. 956-968, 2018. Available: 10.1109/tbme.2017.2731158.

[65] B. Jin, C. Che, Z. Liu, S. Zhang, X. Yin and X. Wei, "Predicting the Risk of Heart Failure With EHR Sequential Data Modeling", IEEE Access, vol. 6, pp. 9256-9261, 2018. Available: 10.1109/access.2017.2789324.

[66] Q. Pham, D. Nguyen, T. Huynh-The, W. Hwang and P. Pathirana, "Artificial Intelligence (AI) and Big Data for Coronavirus (COVID-19) Pandemic: A Survey on the State-of-the-Arts", IEEE Access, vol. 8, pp. 130820-130839, 2020. Available: 10.1109/access.2020.3009328.

[67] Xu W, Zhang J, Zhang Q, Wei X. Risk prediction of type II diabetes based on random forest model. Proc 3rd IEEE Int Conf Adv Electr Electron Information, Commun Bio-Informatics, AEEICB 2017. 2017 Jul 7;382–6.

[68] Forssen H, Patel R, Fitzpatrick N, Hingorani A, Timmis A, Hemingway H, et al. Evaluation of Machine Learning Methods to Predict Coronary Artery Disease Using Metabolomic Data. Stud Health Technol Inform. 2017;235:111–5.

[69] X. Liang, S. Shetty, D. Tosh, D. Bowden, L. Njilla and C. Kamhoua, "Towards Blockchain Empowered Trusted and Accountable Data Sharing and Collaboration in Mobile Healthcare Applications", EAI Endorsed Transactions on Pervasive Health and Technology, vol. 4, no. 15, p. 159338, 2018. Available: 10.4108/eai.24-7-2018.159338.

[70] Zheng X, Mukkamala RR, Vatrapu R, Ordieres-Mere J. Blockchain-based personal health data sharing system using cloud storage. 2018 IEEE 20th Int Conf e-Health Networking, Appl Serv Heal 2018. 2018 Nov 9;

[71] S. Lee and C. Yang, "Fingernail analysis management system using microscopy sensor and blockchain technology", International Journal of Distributed Sensor Networks, vol. 14, no. 3, p. 155014771876704, 2018. Available: 10.1177/1550147718767044.

[72] Yaji S, Bangera K, Neelima B. Privacy preserving in blockchain based on partial homomorphic encryption system for ai applications. Proc - 25th IEEE Int Conf High Perform Comput Work HiPCW 2018. 2019 Feb 4;81–5.

[73] Juneja A, Marefat M. Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. 2018 IEEE EMBS Int Conf Biomed Heal Informatics, BHI 2018. 2018 Apr 6;2018-January:393–7.

[74] Ekblaw A, Azaria A, Halamka JD, Lippman A, Vieira T.

A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data White Paper MedRec: Using Blockchain for Medical Data Access and Permission Management IEEE Original Authors. 2016;

[75] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control", Journal of Medical Systems, vol. 40, no. 10, 2016. Available: 10.1007/s10916-016-0574-6.

[76] Gem [Internet]. [cited 2021 Sep 22]. Available from: https://gem.co/health/

[77] P. Beninger and M. Ibara, "Pharmacovigilance and Biomedical Informatics: A Model for Future Development", Clinical Therapeutics, vol. 38, no. 12, pp. 2514-2525, 2016. Available: 10.1016/j.clinthera.2016.11.006.

[78] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annu Symp Proc [Internet]. 2017 [cited 2021 Sep 22];2017:650. Available from: /pmc/articles/PMC5977675/

[79] D. Randall, P. Goel and R. Abujamra, "Blockchain Applications and Use Cases in Health Information Technology", Journal of Health & Medical Informatics, vol. 08, no. 03, 2017. Available: 10.4172/2157-7420.1000276.

[80] Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for eHealth data access management. Int Conf Adv Biomed Eng ICABME. 2017 Dec 5;2017-October.

[81] Z. Wang and M. O'Boyle, "Machine Learning in Compiler Optimization", Proceedings of the IEEE, vol. 106, no. 11, pp. 1879-1901, 2018. Available: 10.1109/jproc.2018.2817118.

[82] D. Ye, M. Zhang and A. Vasilakos, "A Survey of Self-Organization Mechanisms in Multiagent Systems", IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 47, no. 3, pp. 441-461, 2017. Available: 10.1109/tsmc.2015.2504350.

[83] Y. Rizk, M. Awad and E. Tunstel, "Decision Making in Multiagent Systems: A Survey", IEEE Transactions on Cognitive and Developmental Systems, vol. 10, no. 3, pp. 514-529, 2018. Available: 10.1109/tcds.2018.2840971.

[84] F. Fioretto, E. Pontelli and W. Yeoh, "Distributed Constraint Optimization Problems and Applications: A Survey", Journal of Artificial Intelligence Research, vol. 61, pp. 623-698, 2018. Available: 10.1613/jair.5565.

[85] M. Rehman, C. Liew, T. Wah and M. Khan, "Towards next-generation heterogeneous mobile data stream mining applications: Opportunities, challenges, and future research directions", Journal of Network and Computer Applications, vol. 79, pp. 1-24, 2017. Available: 10.1016/j.jnca.2016.11.031.

[86] M. ur Rehman, A. Batool, C. Liew, Y. Teh and A. ur Rehman Khan, "Execution Models for Mobile Data Analytics", IT Professional, vol. 19, no. 3, pp. 24-30, 2017. Available: 10.1109/mitp.2017.53.

[87] L. Bottou, F. Curtis and J. Nocedal, "Optimization Methods for Large-Scale Machine Learning", SIAM Review, vol. 60, no. 2, pp. 223-311, 2018. Available: 10.1137/16m1080173.

[88] Contreras-Cruz M, … JL-P-2017 IC, 2017 undefined. Distributed path planning for multi-robot teams based on artificial bee colony. ieeexplore.ieee.org [Internet]. [cited 2021 Dec 12]; Available from: https://ieeexplore.ieee.org/abstract/document/7969358/

[89] Kurtulmus AB, Daniel K. Trustless Machine Learning Contracts; Evaluating and Exchanging Machine Learning Models on the Ethereum Blockchain. 2018 Feb 27 [cited 2021 Dec 12]; Available from: http://arxiv.org/abs/1802.10185

[90] H. Kim, J. Park, M. Bennis and S. Kim, "Blockchained On-Device Federated Learning", IEEE Communications Letters, vol. 24, no. 6, pp. 1279-1283, 2020. Available: 10.1109/lcomm.2019.2921755.

[91] Mcconaghy T, Marques R, Müller A, De Jonghe D, Mcconaghy TT, Mcmullen G, et al. Bigchaindb: a scalable blockchain database. git.berlin [Internet]. 2016 [cited 2021 Dec 12]; Available from: https://git.berlin/bigchaindb/site/raw/commit/b2d98401b65175f0fe0c169932ddca0b98a456a6/_src/whitepaper/bigchaindb-whitepaper.pdf

[92] Shafagh H, Burkhalter L, … AH-P of the 2017, 2017 undefined. Towards blockchain-based auditable storage and sharing of iot data. dl.acm.org [Internet]. 2017 Nov 3 [cited 2021 Dec 12];45–50. Available from: https://dl.acm.org/doi/abs/10.1145/3140649.3140656

[93] Cui S, Asghar M, International GR-2018 27th, 2018 undefined. Towards blockchain-based scalable and trustworthy file sharing. ieeexplore.ieee.org [Internet]. [cited 2021 Dec 12]; Available from: https://ieeexplore.ieee.org/abstract/document/8487379/

[94] Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. dl.acm.org [Internet]. 2016 Oct 24 [cited 2021 Dec 12];24-28-October-2016:17–30. Available from: https://dl.acm.org/doi/abs/10.1145/2976749.2978389

[95] Zamani M, Movahedi M, ACM MR-P of the 2018, 2018 undefined. Rapidchain: Scaling blockchain via full sharding. dl.acm.org [Internet]. 2018 Oct 15 [cited 2021 Dec 12];18. Available from: https://dl.acm.org/doi/abs/10.1145/3243734.3243853

[96] K. Ozyilmaz and A. Yurdakul, "Designing a Blockchain-Based IoT With Ethereum, Swarm, and LoRa: The Software Solution to Create High Availability With Minimal Security Risks", IEEE Consumer Electronics Magazine, vol. 8, no. 2, pp. 28-34, 2019. Available: 10.1109/mce.2018.2880806.

[97] Vo H, Kundu A, EDBT MM-, 2018 undefined. Research Directions in Blockchain Data Management and Analytics. dke.jku.at [Internet]. 2018 [cited 2021 Dec 12]; Available from: http://www.dke.jku.at/general/news/res/N000026/Mohania EDBT paper-227.pdf

[98] Lai L, Suda N. Rethinking Machine Learning Development and Deployment for Edge Devices. 2018 Jun 20 [cited 2021 Dec 12]; Available from: http://arxiv.org/abs/1806.07846

[99] N. Nakamoto, "Centralised Bitcoin: A Secure and High Performance Electronic Cash System", SSRN Electronic Journal, 2017. Available: 10.2139/ssrn.3065723.

[100] paper GW-E project yellow, 2014 undefined. Ethereum: A secure decentralised generalised transaction ledger. files.gitter.im [Internet]. [cited 2021 Dec 12]; Available from: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf

[101] Dinh TTA, Wang J, Chen G, Liu R, Ooi BC, Tan KL. BLOCKBENCH: A framework for analyzing private blockchains. Proc ACM SIGMOD Int Conf Manag Data. 2017 May 9;Part F127746:1085–100.

[102] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things", IEEE Transactions on Industrial Informatics, pp. 1-1, 2017. Available: 10.1109/tii.2017.2786307.

[103] Hwang GH, Chen PH, Lu CH, Chiu C, Lin HC, Jheng AJ. InfiniteChain: A multi-chain architecture with distributed auditing of sidechains for public blockchains. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics). 2018;10974 LNCS:47–60.

[104] King S, paper SN, August undefined, 2012 undefined.

Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. chainwhy.com [Internet]. 2012 [cited 2022 Jan 10]; Available from: https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf

[105] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, "Proof of Activity", ACM SIGMETRICS Performance Evaluation Review, vol. 42, no. 3, pp. 34-37, 2014. Available: 10.1145/2695533.2695545.

[106] Slimcoin A Peer-to-Peer Crypto-Currency with Proof-of-Burn "Mining without Powerful Hardware." 2014 [cited 2022 Jan 11]; Available from: www.slimcoin.org

[107] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, 2016. Available: 10.1109/comst.2016.2535718.

[108] Angelis S De, Aniello L, Baldoni R, Lombardi F. PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. 2018 [cited 2022 Jan 11]; Available from: https://iris.uniroma1.it/bitstream/11573/1337256/1/DeAngelis_PBFT_2018.pdf

[109] J. Zhang, N. Xue and X. Huang, "A Secure System For Pervasive Social Network-Based Healthcare", IEEE Access, vol. 4, pp. 9239-9250, 2016. Available: 10.1109/access.2016.2645904.

[110] Q. Xia, E. Sifah, K. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain", IEEE Access, vol. 5, pp. 14757-14767, 2017. Available: 10.1109/access.2017.2730843.

[111] Jiang S, Cao J, Wu H, Yang Y, Ma M, He J. Blochie: A blockchain-based platform for healthcare information exchange. Proc - 2018 IEEE Int Conf Smart Comput SMARTCOMP 2018. 2018 Jul 26;49–56.

[112] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao and S. Liu, "Blockchain-Based Data Preservation System for Medical Data", Journal of Medical Systems, vol. 42, no. 8, 2018. Available: 10.1007/s10916-018-0997-3.

[113] K. Fan, S. Wang, Y. Ren, H. Li and Y. Yang, "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain", Journal of Medical Systems, vol. 42, no. 8, 2018. Available: 10.1007/s10916-018-0993-7.

[114] H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain", Journal of Medical Systems, vol. 42, no. 8, 2018. Available: 10.1007/s10916-018-0994-6.

[115] R. Guo, H. Shi, Q. Zhao and D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems", IEEE Access, vol. 6, pp. 11676-11686, 2018. Available: 10.1109/access.2018.2801266.

[116] M. Uddin, A. Stranieri, I. Gondal and V. Balasubramanian, "Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture", IEEE Access, vol. 6, pp. 32700-32726, 2018. Available: 10.1109/access.2018.2846779.

[117] Sun Y, Zhang R, Wang X, Gao K, Liu L. A decentralizing attribute-based signature for healthcare blockchain. Proc - Int Conf Comput Commun Networks, ICCCN. 2018 Oct 9;2018-July.

[118] Zhang X, Poslad S. Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR). IEEE Int Conf Commun. 2018 Jul 27;2018-May.

[119] Yang G, Li C. A design of blockchain-based architecture for the security of electronic health record (EHR) systems. Proc Int Conf Cloud Comput Technol Sci CloudCom. 2018 Dec 26;2018-December:261–5.

[120] Thakkar P, Nathan S, Viswanathan B. Performance benchmarking and optimizing hyperledger fabric blockchain platform. Proc - 26th IEEE Int Symp Model Anal Simul Comput Telecommun Syst MASCOTS 2018. 2018 Nov 7;264–76.

[121] Sukhwani H, Martínez JM, Chang X, Trivedi KS, Rindos A. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). Proc IEEE Symp Reliab Distrib Syst. 2017 Oct 13;2017-September:253–5.

[122] Thakkar P, Natarajan S. Scaling Hyperledger Fabric Using Pipelined Execution and Sparse Peers. PVLDB [Internet]. 2020 Mar 11 [cited 2021 Sep 22];14(1):2150–8097. Available from: https://arxiv.org/abs/2003.05113v2

[123] L. Chen, W. Lee, C. Chang, K. Choo and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing", Future Generation Computer Systems, vol. 95, pp. 420-429, 2019. Available: 10.1016/j.future.2019.01.018.

[124] D. Nguyen et al., "Federated Learning for Smart Healthcare: A Survey", ACM Computing Surveys, vol. 55, no. 3, pp. 1-37, 2022. Available: 10.1145/3501296.

[125] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges", Egyptian Informatics Journal, vol. 22, no. 2, pp. 177-183, 2021. Available: 10.1016/j.eij.2020.07.003.

[126] M. Cifuentes, M. Davis, D. Fernald, R. Gunn, P. Dickinson and D. Cohen, "Electronic Health Record Challenges, Workarounds, and Solutions Observed in Practices Integrating Behavioral Health and Primary Care", The Journal of the American Board of Family Medicine, vol. 28, no. 1, pp. S63-S72, 2015. Available: 10.3122/jabfm. 2015.s1.150133.

[127] K. Win, "A Review of Security of Electronic Health Records", Health Information Management, vol. 34, no. 1, pp. 13-18, 2005. Available: 10.1177/183335830503400105.

[128] J. Ancker, M. Silver, M. Miller and R. Kaushal, "Consumer experience with and attitudes toward health information technology: a nationwide survey", Journal of the American Medical Informatics Association, vol. 20, no. 1, pp. 152-156, 2013. Available: 10.1136/amiajnl-2012-001062.

[129] G. Perera, A. Holbrook, L. Thabane, G. Foster and D. Willison, "Views on health information sharing and privacy from primary care practices using electronic medical records", International Journal of Medical Informatics, vol. 80, no. 2, pp. 94-101, 2011. Available: 10.1016/j.ijmedinf.2010.11.005.

[130] S. B. Wikina, ''What caused the breach? An examination of use of information technology and health data breaches,'' Perspect. Health Inf. Manage., vol. 11, pp. 1–16, Oct. 2014.

[131] C. Kruse, B. Smith, H. Vanderlinden and A. Nealand, "Security Techniques for the Electronic Health Records", Journal of Medical Systems, vol. 41, no. 8, 2017. Available: 10.1007/s10916-017-0778-4.

[132] V. Liu, M. Musen and T. Chou, "Data Breaches of Protected Health Information in the United States", JAMA, vol. 313, no. 14, p. 1471, 2015. Available: 10.1001/jama.2015.2252.

[133] B. Yüksel, A. Küpçü and Ö. Özkasap, "Research issues for privacy and security of electronic health services", Future Generation Computer Systems, vol. 68, pp. 1-13, 2017. Available: 10.1016/j.future.2016.08.011.

[134] S. Squarepants, "Bitcoin: A Peer-to-Peer Electronic Cash System", SSRN Electronic Journal, 2008. Available: 10.2139/ssrn.3977007.

[135] S. Keele et al., ''Guidelines for performing systematic literature reviews in software engineering,'' Citeseer, 2007.

[136] D. Moher, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement", Annals of Internal Medicine, vol. 151, no. 4, p. 264, 2009. Available: 10.7326/0003-4819-151-4-200908180-00135.

[137] B. Houtan, A. Hafid and D. Makrakis, "A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare", IEEE Access, vol. 8, pp. 90478-90494, 2020. Available: 10.1109/access.2020.2994090.
[138] M. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges", IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188-2204, 2019. Available: 10.1109/jiot.2018.2882794.
[139] E. De Aguiar, B. Faiçal, B. Krishnamachari and J. Ueyama, "A Survey of Blockchain-Based Strategies for Healthcare", ACM Computing Surveys, vol. 53, no. 2, pp. 1-27, 2021. Available: 10.1145/3376915.
[140] L. Rundo, R. Pirrone, S. Vitabile, E. Sala and O. Gambino, "Recent advances of HCI in decision-making tasks for optimized clinical workflows and precision medicine", Journal of Biomedical Informatics, vol. 108, p. 103479, 2020. Available: 10.1016/j.jbi.2020.103479.
[141] Tzanou, M. The Fundamental Right to Data Protection: Normative Value in the Context of Counter Terrorism Surveillance, 1st ed.; Bloomsbury Publishing: London, UK, 2017.
[142] Ahmed, A.; Parvez, M.M.R.; Hasan, M.H.; Nur, F.N.; Moon, N.N.; Karim, A.; Azam, S.; Shanmugam, B.;Jonkman, M. An Intelligent and Secured Tracking System for Monitoring School Bus. In Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, Tamil Nadu, India, 23–25 January 2019.
[143] Hoepman, J.H. Privacy Design Strategies. In Proceedings of the 29th IFIP International Information Security Conference, Merrakech, Morocco, 2–4 June 2014.
[144] M. van Lieshout, L. Kool, B. van Schoonhoven and M. de Jonge, "Privacy by Design: an alternative to existing practice in safeguarding privacy", info, vol. 13, no. 6, pp. 55-68, 2011. Available: 10.1108/14636691111174261.
[145] A. Appari and M. Johnson, "Information security and privacy in healthcare: current state of research", International Journal of Internet and Enterprise Management, vol. 6, no. 4, p. 279, 2010. Available: 10.1504/ijiem.2010.035624.
[146] C. O'Keefe and C. Connolly, "Privacy and the use of health data for research", Medical Journal of Australia, vol. 193, no. 9, pp. 537-541, 2010. Available: 10.5694/j.1326-5377.2010.tb04041.x.
[147] A. Cavoukian, "Understanding How to Implement Privacy by Design, One Step at a Time", IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 78-82, 2020. Available: 10.1109/mce.2019.2953739.
[148] Sweeney, L. Privacy-preserving surveillance using selective revelation. IEEE Intelligent Systems. 2005, 1, 83-84.
[149] Privacy by Design: Effective Privacy Management in the Victorian Public Sector; Commissioner for Privacy and Data Protection: Melbourne, Victoria, Australia, 2018.
[150] Australian Governemnt—Office of the Australian Information Commissioner. 1 January 2019. Available online: https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design/ (accessed on 8 November 2019).
[151] Skinner, G.; Chang, E.; Miller, M.; Aisbett, J. Privacy shield Hippocratic Security Method for Virtual Communities. IECON2004. In Proceedings of the 30th Annual Conference of the IEEE Industrial Electronics Society, Busan, South Korea, 2–6 November 2004.
[152] Spiekermann, S.; Cranor, L.F. Engineering privacy. IEEE Trans. Softw. Eng. 2009, 35, 67–82
[153] Gkoulalas-Divanis, A.; Loukides, G. Medical Data Privacy Handbook, 1st ed.; IBM Research-Divanis: Dublin, Ireland, 2015.
[154] L. Dang, M. Piran, D. Han, K. Min and H. Moon, "A Survey on Internet of Things and Cloud Computing for Healthcare", Electronics, vol. 8, no. 7, p. 768, 2019. Available: 10.3390/electronics8070768.
[155] M. van Lieshout, L. Kool, B. van Schoonhoven and M. de Jonge, "Privacy by Design: an alternative to existing practice in safeguarding privacy", info, vol. 13, no. 6, pp. 55-68, 2011. Available: 10.1108/14636691111174261.
[156] G. Iachello and J. Hong, "End-User Privacy in Human-Computer Interaction", Foundations and Trends® in Human-Computer Interaction, vol. 1, no. 1, pp. 1-137, 2007. Available: 10.1561/1100000004.
[157] Office of the Victorian Information Commissioner. Privacy by Design: Effective Privacy Management in the Victorian public sector. 2019. Available online: https://ovic.vic.gov.au/resource/privacy-by-designeffective-privacy-management-in-the-victorian-public-sector/ (accessed on 5 December 2019).
[158] A. Cavoukian, "Privacy by Design [Leading Edge]", IEEE Technology and Society Magazine, vol. 31, no. 4, pp. 18-19, 2012. Available: 10.1109/mts.2012.2225459.
[159] J. Miller, "Who knows: Safeguarding your privacy in a networked world", Library & Information Science Research, vol. 19, no. 1, pp. 97-98, 1997. Available: 10.1016/s0740-8188(97)90008-6.
[160] Spitzer, J. 6.1M Healthcare Data Breach Victims in 2018: 5 of the Biggest Breaches So Far. Becker's Health IT & CIO Report: Chicago, IL, USA, 2019
[161] Donnelly, C. The GDPR: Why you Need to Adopt the Principles of Privacy by Design. IT Governance. 16 March 2019. Available online: https://www.itgovernance.eu/blog/en/the-gdpr-why-you-need-to-adoptthe-principles-of-privacy-by-design (accessed on 17 December 2019).
[162] Gürses, S.; Troncoso, C.; Diaz, C. Engineering privacy by design. Comput. Priv. Data Prot. 2011, 14, 25
[163] Jacobs, B. Select before you collect. Ars Aequi 2005, 54, 1006–1009.
[164] Pfitzmann, A.; Hansen, M. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management—A Consolidated Proposal for Terminology; Institute of Systems Architecture, Faculty of Computer Science, Tu Dresden, Dresden, Germany, 2010
[165] International Standard ISO/IEC 29100. Privacy Framework Technologies 29100; International Organization for Standardization, Vernier, Switzerland, 2011.
[166] Warren, S.D.; Brandeis, L.D. The Right to Privacy. Harv. Law Rev. 1990, 5, 193–220.
[167] J.H. Privacy Design Strategies. In ICT Systems Security and Privacy Protection. IFIP Adv. Inf. Commun. Technol. 2014, 428, 446–459.
[168] Sweeney, L. k-anonymity: A model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl. Based Syst. 2002, 10, 557–570.
[169] Graf, C.; Wolkerstorfer, P.; Geven, A.; Tscheligi, M. A pattern collection for privacy enhancing technology. In Proceedings of the 2nd Int. Conf. on Pervasive Patterns and Applications, Lisbon, Portugal, 21–26 November 2010.
[170] M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements", Requirements Engineering, vol. 16, no. 1, pp. 3-32, 2010. Available: 10.1007/s00766-010-0115-7.
[171] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 2019. Available online: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed on 9 November 2019).
[172] 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.
[173] A. Cavoukian, "Understanding How to Implement Privacy by Design, One Step at a Time", IEEE Consumer

Electronics Magazine, vol. 9, no. 2, pp. 78-82, 2020. Available: 10.1109/mce.2019.2953739.
[174] W. Hersh, A. Jai Ganesh and P. Otero, "Big Data: Are Biomedical and Health Informatics Training Programs Ready?", Yearbook of Medical Informatics, vol. 23, no. 01, pp. 177-181, 2014. Available: 10.15265/iy-2014-0007.
[175] M. Kamel Boulos, J. Wilson and K. Clauson, "Geospatial blockchain: promises, challenges, and scenarios in health and healthcare", International Journal of Health Geographics, vol. 17, no. 1, 2018. Available: 10.1186/s12942-018-0144-x.
[176] X. Zheng, X. Geng, L. Xie, D. Duan, L. Yang, and S. Cui, ''A SVM-based setting of protection relays in distribution systems,'' in Proc. IEEE Texas Power Energy Conf. (TPEC), Feb. 2018, pp. 1–6.
[177] S. Lee and C. Yang, "Fingernail analysis management system using microscopy sensor and blockchain technology", International Journal of Distributed Sensor Networks, vol. 14, no. 3, p. 155014771876704, 2018. Available: 10.1177/1550147718767044.
[178] L. Tzu. (2017). Matrix Technical Whitepaper. [Online]. Available:https://www.matrix.io/html/MATRIXTechnical WhitePaper.pdf
[179] D. E. O'Leary, ''Artificial intelligence and big data,'' IEEE Intell. Syst., vol. 28, no. 2, pp. 96–99, Mar. 2013.
[180] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi and N. Kumar, "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications", IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1242-1255, 2021. Available: 10.1109/tnse.2019.2961932.
[181] S. Dey, "A Proof of Work: Securing Majority-Attack in Blockchain Using Machine Learning and Algorithmic Game Theory", International Journal of Wireless and Microwave Technologies, vol. 8, no. 5, pp. 1-9, 2018. Available: 10.5815/ijwmt.2018.05.01.
[182] Singularitynet. A Decentralized, Open Market and InterNetwork for AIS, 2017, [Online]. Available: https://public.singularitynet.io/whitepaper.pdf
[183] F. Corea. The Convergence of AI and Blockchain: What is the Deal, 2017, [Online]. Available: https://francesco-ai.medium.com/theconvergence-of-ai-and-blockchain-whats-the-deal-60c618e3accc
[184] N. Team. What is Neureal. Accessed: Feb. 16, 2021. [Online]. Available: https://neureal.net/
[185] A. Awad Abdellatif et al., "MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange", IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15762-15775, 2021. Available: 10.1109/jiot.2021.3052910.
[186] K. Gai, Y. Wu, L. Zhu, L. Xu and Y. Zhang, "Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks", IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7992-8004, 2019. Available: 10.1109/jiot.2019.2904303.
[187] R. Yang, F. Yu, P. Si, Z. Yang and Y. Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges", IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1508-1532, 2019. Available: 10.1109/comst.2019.2894727.
[188] P. De Filippi, ''The interplay between decentralization and privacy: The case of blockchain technologies,'' J. Peer Prod., no. 7, 2016. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689
[189] P. Dialani. IoMT Devices are Vulnerable to Cybersecurity Risks. [Online]. Available: https://www.analyticsinsight.net/iomt-devices-are-vulnerableto-cybersecurity-risks/
[190] R. Nosowsky and T. Giordano, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule: Implications for Clinical Research", Annual Review of Medicine, vol. 57, no. 1, pp. 575-590, 2006. Available: 10.1146/annurev.med.57.121304.131257.
[191] X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, "A survey on the security of blockchain systems", Future Generation Computer Systems, vol. 107, pp. 841-853, 2020. Available: 10.1016/j.future.2017.08.020.
[192] Li C, Palanisamy B. Incentivized blockchain-based social media platforms: A case study of steemit. InProceedings of the 10th ACM conference on web science 2019 Jun 26 (pp. 145-154).
[193] Srivastava G, Crichigno J, Dhar S. A light and secure healthcare blockchain for iot medical devices. In2019 IEEE Canadian conference of electrical and computer engineering (CCECE) 2019 May 5 (pp. 1-5). IEEE.
[194] Dwivedi, "BRISK: Dynamic Encryption Based Cipher for Long Term Security", Sensors, vol. 21, no. 17, p. 5744, 2021. Available: 10.3390/s21175744.