












Research Article

Healthcare Security in Edge-Fog-Cloud Environment using Blockchain: A Systematic Review

Zaid J. Al-Araji¹, *, Najwa N. Hazem Al-Sheikh², Abdullah A. Ibrahim Al-Dulaimi², Ayad Yassen², Namaa N. Hikmat³, Sharifah Sakinah Syed Ahmad⁴, Hussein M. Farhood⁵, Zaid Ali Abdulkadhim⁶, Ammar Awad Mutlag⁷, Mahmood S. AlKhaldee⁸, Ammar Hashim Ali⁸

¹ College of Information Technology, Ninevah University, Ninevah 41001, Iraq

² Technical Computer Engineering Department, Al-Hadba University, Ninevah 41001, Iraq

³ Ninevah Health Directorate, Ministry of Health, Ninevah 41001, Iraq

⁴ Faculty of Information Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka 76100, Malaysia

⁵ Department of Computer Engineering, College of Engineering Mustansiriyah University, 10047 Baghdad, Iraq

⁶ Al-Forat Al-Awsat Technical University (ATU), Al-Diwaniyah Technical Institute, 58006 Al-Qadisiyah, Iraq

⁷ Ministry of Education/General Directorate of Curricula, Pure Science Department, Baghdad 10065, Iraq

⁸ Ninevah Education Directorate, Ministry of Education, Ninevah 41001, Iraq

ARTICLE INFO

Article history

Received 1 Jan 2025

Revised 24 Apr 2025

Accepted 17 May 2025

Published 6 Jul 2025

Keywords

Blockchain

Healthcare

Edge Computing

Fog Computing

Cloud Computing



ABSTRACT

Context: Our domain of expertise is healthcare security, which protects the sensitive information of patients and the integrity of the healthcare services provided to them. As health record digitization grows, along with the adoption of advanced technologies, data protection becomes more complex and vital. Realizing the transformative potential of blockchain (BC) in healthcare security requires critical exploration into the prevailing centralization of sensitive patient information, shedding traditional paradigms, and embracing the digital decentralization enabled by the BC realm. **Objectives:** The purpose of this study was to analyse prior research and provide a comprehensive overview of the literature on BC-based healthcare security in edge-fog-cloud (EFC) scenarios. Face and researchers, outlining the obstacles they face and offering recommendations to analysts for enhancing this crucial area of study. **Methods:** The analyses systematically examined healthcare security utilizing BC within the EFC domain across all studies; additionally, four databases—Web of Science (WoS), ScienceDirect, IEEE Xplore Digital Library, and Scopus—were employed from 2019–2024 to analyse their architecture, applications, and performance evaluation. **Results:** In accordance with our inclusion and exclusion criteria, 97 publications concerning healthcare security utilizing BC in edge, fog, and cloud systems with various approaches and strategies were chosen. Four classes were created from the taxonomy results according to the BC location: healthcare security using BC at the edge, healthcare security using BC in fog, healthcare security using BC in the cloud, and review articles. **Discussion:** BC facilitates secure and efficient sharing of patient data among different healthcare systems, promoting seamless interoperability of electronic health records (EHRs). Data are also stored in a decentralized manner, which diminishes the danger of breaches because there is no singular point of failure. Additionally, with national tracking protocols via BC, full lifecycle monitoring of pharmaceutical products is ensured, guaranteeing transparency and minimizing counterfeit medication. **Conclusion:** Although the research domains of healthcare security using BC in EFC differ, they are generally equally important. Through this review, research capabilities are highlighted, and new research domains are expanded.

1. INTRODUCTION

The number of connected devices is rapidly increasing with their design and development. The number of devices connected to modern networks and infrastructure is thought to be continuously increasing. The Internet of Things (IoT) has

*Corresponding author. Email: zaid.jasim@uoninevah.edu.iq

given most manufacturing companies a fresh perspective on the internet [1]. The IoT is growing and becoming a crucial component of the internet's future. Note that cloud computing offers several IoT services that have revolutionized technology, including computing resources, storage capacities, heterogeneity, high processing, etc. There are different levels of computing resource virtualization in the cloud [2], [3]. Cloud computing is an operational framework that offers customers across numerous industrial and application areas network-based services such as networking, storage, and processing power. It provides various virtualized computing resources at different levels, including platforms, software, and infrastructure, which are made available to customers as cloud-based on-demand services [2]. However, the cloud suffers from several issues, such as high delay, high bandwidth, high cost, and high energy needed, which affect performance, especially the response time. To address the shortcomings of cloud computing, Cisco unveiled a new computing idea in 2012 called fog computing (FC) [4]. However, FC still suffers from the same issues as cloud computing. For this reason, edge computing has been used to overcome fog and cloud limitations. Using the edge computing concept, the data processing, storage, and computing tasks that the cloud initially needed can be offloaded to the network's edge close to terminal devices [5]. In addition to achieving decentralization, this approach lessens the strain on network bandwidth, lowers data transmission costs, and speeds up device response times and data transmission [5]. The implementation of the IoT in the edge-fog-cloud (EFC) environment is promising in healthcare, and it is important for patients and doctors [6]. It is a collection of several devices that communicate with each other and measure a patient's vital statistics in terms of medical information. The IoT is emerging as a transformative ingredient of the healthcare system, providing significant advantages across different segments. This includes medication development, predictive illness analysis, early epidemic warning, preventative healthcare, and patient health monitoring. A critical concern in electronic and ubiquitous healthcare is the security of IoT devices and the foundational healthcare information infrastructure [7]. As the IoT advances and healthcare devices and applications proliferate, substantial volumes of medical data are gathered and transmitted hourly, daily, weekly, and beyond. Current healthcare systems encounter obstacles, including interoperability issues, protracted procedures, delays in processing and diagnosis, sluggish information exchange, elevated operational expenses, laborious insurance processes, privacy concerns, security vulnerabilities, and challenges related to data ownership and control [8].

This work presents a systematic literature review (SLR) of healthcare security within the EFC environment, examining the application of blockchain (BC) across several domains and analysing prior research on BC enhancement. The criteria and qualities that enhance the understanding of pertinent aspects of this topic in the literature include motivation, limitations, and recommendations for analysts, advancing this vital study domain. This study focuses on healthcare security using BC issues, problems, and challenges in an EFC environment. As the number and diversity of methods, approaches, and theories used in EFC increase, it is imperative to study and identify the role of BC in implementing EFC in healthcare. An SLR can determine, categorize, and synthesize a comparative study of state-of-the-art studies. Therefore, it would help move knowledge transfer in the scientific domain [9], [10]. The SLR was conducted to locate, classify taxonomically, and systematically compare existing research on the planning, execution, and validation of healthcare security using BC in the EFC. Through a systematic evaluation of the current literature, we seek to address the following inquiries:

1. What are the main practical motivations for using BC in EFC for healthcare security?
2. Which type of classification in research approaches can be applied to healthcare security via blockchain in EFC?
3. What are the current research trends for blockchain use in healthcare in the EFC environment?
4. What are the metrics measured in previous research?
5. What datasets and simulations are used to implement and evaluate the blockchain in EFC environments?
6. What types of blockchains are used in healthcare in EFC environments?
7. Which environment is the most effective for implementing and applying blockchain?
8. What are the limitations of healthcare security using blockchain in EFC?

The guidelines in [3], [11], [12], [13] were followed in this study. We aim to perform a comprehensive comparison to examine the limitations and possibilities of previous research and to perform a systematic determination and taxonomy classification of the evidence on healthcare security using BC in EFC. Note that the SLR of this work was created by focusing on the proposed solutions, techniques, and algorithms for healthcare security using BC in EFC. Hence, 97 studies were selected, classified, and compared by applying characterization taxonomy. The characterization taxonomy based on these fields comprises three groups on the basis of the location of the BC: edge, fog, or cloud. Furthermore, limitations related to healthcare security in the use of BC in EFC are also presented.

2. EDGE-FOG-CLOUD ENVIRONMENTS

Driven by increasing applications and services, large numbers, and various devices, these situations result in vast amounts of data and stress on the network infrastructure. In this edge, fog, and cloud environment, users/clients cross multiple domains or networks, as shown in Figure 1. This affects network performance and leads to network functionality issues.

There is a new trend to comprehensively use three kinds of resources to benefit the end-to-end network service. In this section, these environments are explained as follows.

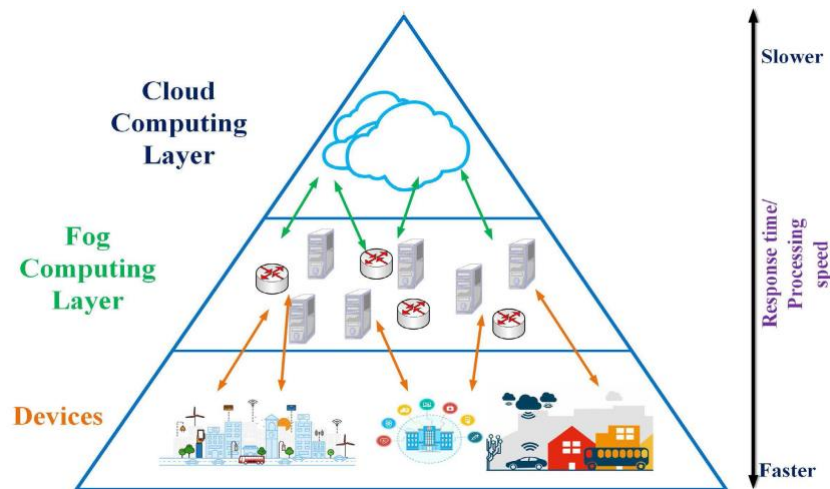


Fig. 1. Edge-Fog-Cloud environment [16], [18].

2.1 Edge Computing

Edge computing describes a novel computing paradigm that computes sensor and actuator data at the network's edge. Computation is performed at the network edge via a novel computing paradigm. The main concept involves bringing processing closer to the data source. [15]. According to this theory, certain services and applications that do not need much processing power can be handled on the edge, near the data source, and are not required to get over the network to be handled by the cloud or fog [16]. Therefore, the edge could decrease the processing load and the volume of data sent to and from the cloud or fog data centres, guarantee real-time processing, and enhance data transmission performance [16]. Edge computing is used in many aspects to provide better performance, and healthcare is one of them. Because edge computing provides greater efficiency and more thorough treatment everywhere, it helps enhance healthcare standards [17]. By implementing devices that may present computational capabilities for disease diagnosis and patient monitoring, the widespread use of health sensors can minimize the number of patients who visit hospitals and clinics. By continuously monitoring vital signs, these edge sensor devices make it easy for patients to maintain and provide new information in healthcare [17]. From medical devices and sensors, edge computing helps in real-time data analytics, which helps patients and doctors perform instant responsive actions. This is a critical element for crucial applications such as monitoring life and providing timely help. Moreover, it enables the healthcare sector to improve patient support, as the data are processed near the source, improving the speed of decision-making [18]. Processing data at the edge decreases the need to transmit sensitive patient information over the internet, reducing the likelihood of data breaches and maintaining adherence to privacy regulations [19]. Thus, edge computing greatly minimizes the latency in transmitting data to centralized cloud servers. This is especially crucial for applications needing instant responses, such as emergency medical services and remote surgeries.

2.2 Cloud Computing

"Cloud computing," also known as "on-demand computing" or "platform computing," refers to a broad range of resources and uses, such as device deployment, server and database administration, and file storage. This computing style is known as "on-demand computing" or "platform computing." Given that the cloud service provider's servers are actual computers, additional infrastructure must be set up, which takes resources and time. The phrase "cloud computing" describes providing computer services where users can use a shared pool of reconfigurable computing resources (such as processing power and data storage) with minimal human participation. Another name for cloud computing is "utility computing" [20]. Cloud computing is used in many fields to increase performance, and in the context of healthcare, it is important. It is changing the healthcare industry by providing scalable, secure, and efficient solutions to improve patient care and make operations more efficient. In addition, cloud platforms enable healthcare practitioners to store and process large amounts of data, such as EHRs, medical images, and patient data, securely and in an easily accessible way [21]. This also allows for concomitant sharing and integration of real-time data among healthcare professionals, enhancing the accuracy and speed of diagnosis and therapy [21]. Cloud computing also facilitates telemedicine and remote patient surveillance, allowing patients to obtain medical attention and care given the comfort and convenience of their homes. Furthermore, cloud-based analytics can analyse big data to identify insights leading to improved clinical decisions and customized therapies. The cost-effectiveness and flexibility of cloud solutions enable healthcare organizations to scale up their IT infrastructure to meet healthcare needs, thus

reducing the effort needed to maintain in-house infrastructure (e.g., storage, databases, and server platforms). Cloud computing improves healthcare efficiency, security, and quality, thus benefiting patients.

3. BLOCKCHAIN

At its core, a BC is a distributed database consisting of an ordered sequence of records linked together by chains [22], [23]. Only authorized users can access the information stored in these blocks pertaining to distinct transactions. Here, a sophisticated collection of self-managed encryption keys is used to preserve user authorization. Every authorized user receives a unique, time-sensitive key that automatically stops it if the allotted time for decryption expires [24]. The block structure of the BC is displayed in Figure 2. Endpoint workstations are block nodes, which hold a full copy of the ledgers on which they are independently updated and kept. The transaction is the main item of the blockchain, which is the record of the blockchain. The chain refers to a chain of blocks, which is a format defining the distributed transactions across the network. Note that all blocks contain a hash of the blocks preceding and following the current block. Miners are vertices that validate and add blocks to the BC topology. Specifically, every BC block follows rules that are intended to protect it from the network [25].

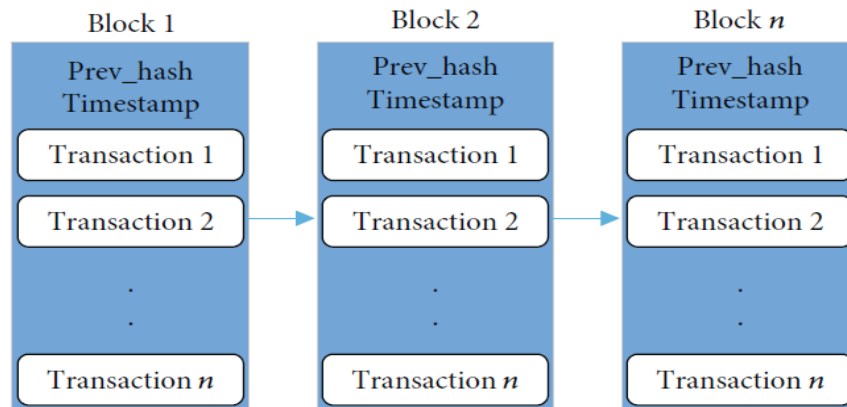


Fig. 2. Configuration of blocks in the blockchain [25].

3.1 Types of Blockchain

BCs can be divided into four distinct types: consortium, private, hybrid, and public. BC systems can be divided into two primary categories: access to BC data and access to the BC system. Table 1 compares these types.

TABLE I. BLOCKCHAIN TYPE COMPARISON.

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain	Hybrid Blockchain
Access	Open to anyone	Restricted	Restricted	Combination
Control	Decentralized	Centralized	Semidecentralized	Flexible
Transparency	High	Limited	Selective	Customizable
Security	High	High	High	High
Performance	Slower, energy-intensive	Faster, efficient	Faster, efficient	Scalable, efficient
Use Cases	Cryptocurrencies, DeFi	Enterprise applications	Industry collaborations	Healthcare, government

A. Public Blockchain

A public BC is a decentralized network that is open to anyone. This means that anyone with an internet connection can join the network, participate in the consensus process, and validate transactions. Public BCs are characterized by transparency and security, as all transactions are recorded on a public ledger that is accessible to everyone [26]. Public BCs are the first kind of BC technology. This region featured the development of cryptocurrencies such as Bitcoin, which increased interest in distributed ledger technology (DLT). The process becomes more effective by eliminating centralization's drawbacks, such as security and transparency. Instead of being stored in a single location, DLT distributes information as a peer-to-peer network. Its decentralized nature requires a way to guarantee data validity. In essence, it is a process by which the BC's members agree on the ledger's present state. The two common approaches to consensus building are proof of stake and proof of work. Hence, anyone with internet connectivity can register as a node to a BC network because of permissionless and unrestricted BC technology. A user can perform mining operations, which are intricate calculations that confirm and add transactions to the ledger, as well as see both recent and historical records [27]. The most public BC, Bitcoin, with the broadest adoption, employs proof-of-work consensus to verify transactions and secure the network [26]. Another popular

public BC, Ethereum, is a platform that supports smart contracts and decentralized applications (dApps), opening the door to a diverse range of applications [28].

B. Private Blockchain

A private BC is a type of BC network restricted to a specific group of participants. Unlike public BCs, private BCs are not open to everyone. They are typically used within a single organization or among organizations that need to share data and processes securely and privately [29]. Note that private BCs function in constrained settings, such as closed networks or networks under the management of one organization. This kind of BC network is far smaller than a public BC, even though it is decentralized and peer-to-peer. Private BCs function on a network of individuals within an organization, as opposed to public BCs, which allow participation from everyone with computing capability. Permission BCs are another name for enterprise and permission-based BCs [27]. The Linux Foundation developed a widely used private BC framework designed for enterprise use and supported a modular architecture, allowing organizations to customize their BC solutions [30]. Developed by R3, Corda is a private BC platform specifically designed for financial institutions. It focuses on privacy and scalability, making it suitable for complex financial transactions [31].

C. Hybrid Blockchain

A hybrid BC combines elements of public and private BCs. This allows organizations to leverage the benefits of both types of BCs, such as the transparency and security of public BCs and the privacy and control of private BCs [32]. Hybrid BC is used by many organizations interested in profiting from both simultaneously. An organization can manage which data on the BC are publicly available by implementing a private permission system and a public permissionless system. Furthermore, smart contracts can be used to verify transactions and records on a hybrid BC, which usually does not publish them. The secrecy of the data within the network can still be confirmed. A private entity may possess a hybrid BC. Nevertheless, it cannot alter transactions. A user gains full access to the network upon joining a hybrid BC. The user's identity remains safeguarded unless a transaction involves other users. Upon this occurrence, the identities of the other parties are disclosed [27]. A hybrid BC platform designed for global trade and finance combines the best features of public and private BCs [33]. Originally developed by Disney, the Dragon chain is a hybrid BC platform allowing businesses to control public and private data [43].

D. Consortium Blockchain

A consortium BC, also known as a federated BC, is a type of BC network where a preselected group of nodes controls the consensus process. Unlike public BCs, which are open to everyone and private BCs are restricted to a single organization, consortium BCs are managed by a group of organizations [34]. However, a decentralized network enables different members of an organization to work together. The risks associated with a single party running the network are removed by consortium BCs, which are private BCs exclusively accessible by a particular group. Nodes in a consortium BC are in charge of the consensus processes. Note that validator nodes initiate, receive, and authenticate transactions. Thus, any system node can send and receive transactions [27]. A BC platform is designed specifically for financial institutions, allowing secure and private transactions between parties [35]. It is an open-source BC framework hosted by the Linux Foundation, designed for enterprise use, and supports modular architecture [36].

4. HEALTHCARE SECURITY USING BLOCKCHAIN

BC is used in healthcare and has many other uses. Healthcare researchers may unlock the genetic code, control a medication supply chain, and securely transfer patient medical records with the aid of ledger technology [37]. According to [38], BC can be used in many aspects of health, as illustrated in Figure 3. Public healthcare is one of the many BC technology applications previously limited to the financial sector. One of the most exciting directions of current research is BC-based medical solutions. The medical information that is gathered must not be altered. The researcher, the patient, the patient's family, or anybody else who requests the data should be required to attest to its veracity. Some scholars have attempted to integrate BC technology with other technologies to securely transfer data, whereas several have used BC to combine different technologies [39].

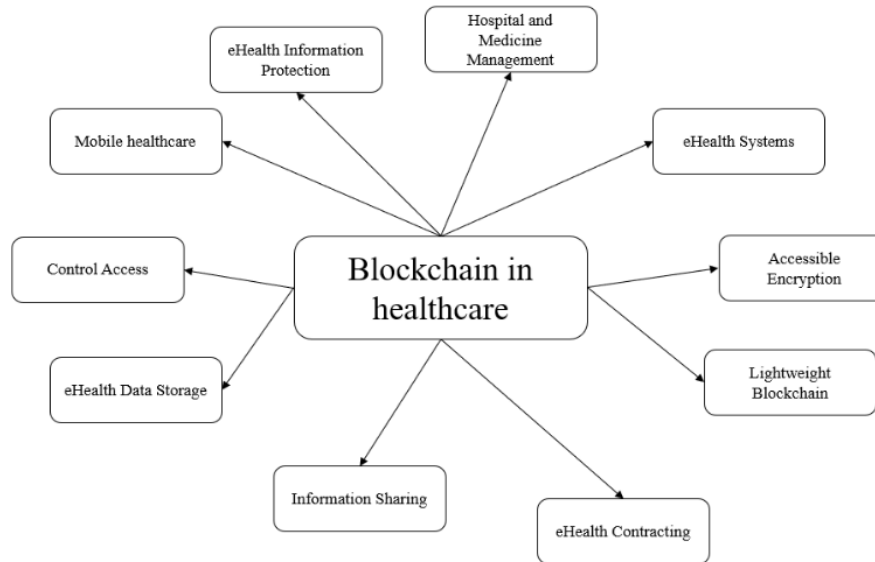


Fig. 3. Blockchain in healthcare classification [51].

In addition to improving overall efficiency in promoting patient treatment and the gradual transition of present medical systems into distributed eHealth, the application of the BC idea in eHealth may effectively address essential concerns of confidentiality and protection [40], [41]. Researchers want to utilize EFC and BC technologies to develop eHealth models or frameworks for the secure provision of information, data management, and network management. Researchers have identified a promising area for BC-based healthcare architecture research [42]. This technology aids in the creation of dependable storage health data and the granular tracking of real-time data [43]. To better comprehend complicated diseases, develop new medications, and create individualized therapies, researchers in the healthcare sector may require access to enormous datasets [44]. The BC provides a shared ecosystem of various exchange datasets [44]. It allows patients of different socioeconomic and ethnic backgrounds to be included. Using BC in healthcare also presents many advantages for improving patient outcomes and ensuring data security. By introducing BC functionality in medical transactions, the inherent properties of distributed and irreversible ledgers can support the robustness of data provenance and privacy [45]. This security upgrade is significant in ensuring the security of patient information from illegal acquisition and modification. In addition, using BC technology in healthcare can enhance interoperability and enable seamless data sharing among healthcare personnel while ensuring confidentiality in healthcare information [46]. Second, BC's decentralized characteristics improve transparency and trust in medical transactions, lowering fraud or human error. In particular, BC technology can facilitate more efficient administration, subsequently increasing efficiency and reducing healthcare costs. Globally, the use of BC to transform the health industry is great, with the potential to change healthcare delivery by adopting secure, efficient, and patient-controlled care delivery.

5. HEALTHCARE SECURITY VIA BLOCKCHAIN IN EFC COMPUTING

Protecting healthcare information is very challenging for researchers. For this reason, scientists have invented and developed many methods and techniques to improve healthcare information security. In this work, we focus on healthcare security via BC. However, healthcare security, in general, still suffers from many issues. The following sections review previous work to highlight the current issues.

5.1 Research Methodology

A comprehensive literature review was conducted via standard methods for extracting, analysing, and reporting results. We obtained the guidelines [3], [13], [14], A three-phase research methodology encompassing planning, execution, and documentation.

The initial phase is the planning and evaluation process for EFC computing's use of BC in healthcare security. The actions listed below are as follows: (1) Describe and examine the research gaps, questions, and issues encountered by prior research; (2) highlight the need and requirements for a literature review of healthcare security using BC in EFC computing; and (3) enhance/evaluate the process for conducting a systematic literature review on the topic of healthcare security using BC in EFC computing. Therefore, identifying healthcare security via BC in EFC computing research, choosing the literature, and extracting information for healthcare security via BC in EFC computing are the steps in guiding the systematic literature

review of healthcare security via BC in EFC computing. The documentation review phase looks at how to choose research and applies the findings of the SLR of BC-based healthcare security in EFC computing.

5.2 Planning the Review

Understanding the reasons behind systematic work and the outcomes of a review procedure is the first step in review planning.

A. Motivation

This systematic literature review identifies, categorizes, and compares current evidence on healthcare security using BC in EFC computing. Its main objective is to classify and compare BC technology in the healthcare industry. The significance of healthcare security in EFC networks necessitates the use of BC technology to compile the available data.

B. Identifying the Research Questions

The reason for the study is shaped by the research questions, and the responses provide evidence-based analysis of BC-based healthcare security. As indicated in Table 2, eight research questions were created to establish the foundation for determining the search strategy for gathering literature. Note that motivation was the driving force behind each question's investigation. On the other hand, comparative analysis makes it possible to examine the overall impact of research, which is expressed in terms of similar characteristics.

TABLE II. RESEARCH QUESTIONS.

Number	Questions
RQ1	What are the main practical motivations for healthcare security using blockchain in EFC?
RQ2	Which type of classification in research approaches can be applied to healthcare security using blockchain in EFC?
RQ3	What are the current research trends for blockchain use in healthcare in the Edge-Fog-Cloud environment?
RQ4	What are the metrics measured in previous research?
RQ5	What datasets and simulations are used to implement and evaluate the blockchain in EFC environments?
RQ6	What types of blockchains are used in healthcare in EFC environments?
RQ7	Which environment is the most effective for implementing and applying blockchain?
RQ8	What are the limitations of healthcare security using blockchain in EFC?

C. Study Selection

Four databases—Web of Science (WoS), ScienceDirect, Scopus, and the IEEE Xplore Digital Library—were used methodically to conduct the research. An index showing both basic and sophisticated computer science journals and conference research papers was used to choose the study. As a result, technical factors were considered during the selection process, providing a more comprehensive view of research projects and considering a wide range of scientific fields.

The query used in the search was divided into three parts. The first was about healthcare ("health" OR "healthcare" OR "health care"). In contrast, the second part was about BC ("blockchain" OR "blockchain"), and the last part was about the EFC environment ("fog" OR "fog computing" OR "cloud" OR "cloud computing" OR "edge" OR "edge computing" OR "end devices"). For each database, we selected two types of articles, research articles and review articles, as presented in Table 3.

TABLE III. INCLUDED AND EXCLUDED ARTICLES.

Criteria	Type of data
Included	Research articles (frameworks, models, architecture, review, and survey) related to healthcare security using blockchain in an edge-fog-cloud environment.
Excluded	Books, books, chapters, theses, and non-English articles.

Finding relevant articles was the next stage. Figure 4 illustrates the three processes that make up the selection process. Duplicates were first eliminated. Of the 6495 items we discovered, 1949 were duplicates. The second phase involved scanning abstracts and titles to identify related and irrelevant articles. Here, 97 of the 4546 publications applied BC technology to EFC healthcare security.

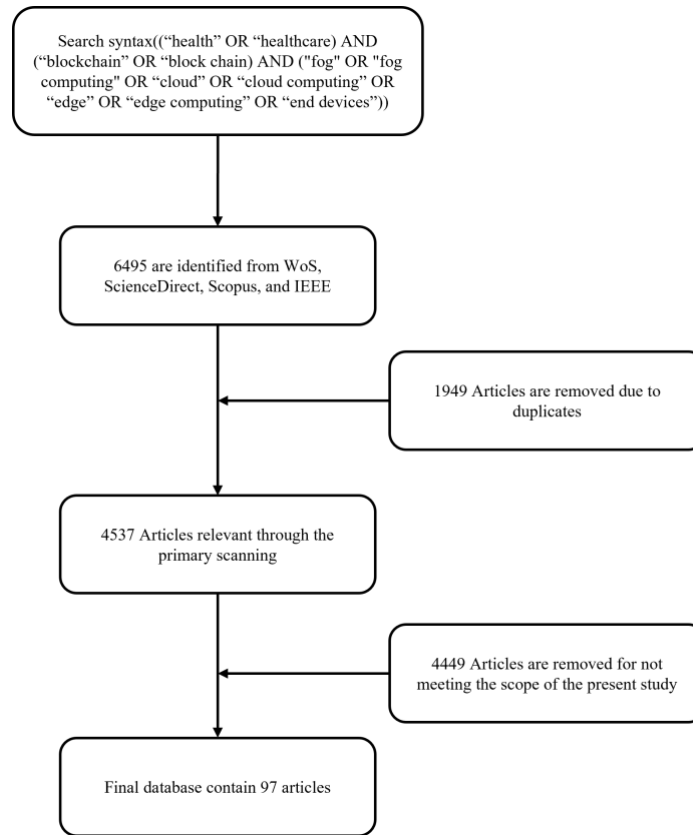


Fig. 4. The protocol for a systematic literature review.

6. HEALTH SECURITY USING A BLOCKCHAIN IN EFC CLASSIFICATION

This section defines a systematic classification of related literature. The BC position within the EFC environment served as the basis for classification.

6.1 Healthcare Security Using Blockchain in Edge Computing

Blending BC technology with an edge for healthcare changes the management, processing, and security of patient data and offers new opportunities to uncover original and valuable insights that have remained obscure. Edge computing places computational power at the data source, e.g., medical devices and sensors. Hence, it is possible to perform real-time data processing and analysis. This proximity reduces latency and increases application responsiveness to healthcare applications, a highly critical functionality for various critical tasks (e.g., remote patient care and emergency response). On the other hand, BC technology provides an immutably and permanently logged history of transaction(s) and transfer(s) of data. Through the integration of these technologies, healthcare systems can guarantee the integrity, confidentiality, and availability of patient data and enhance operational efficiency. This synergy solves numerous problems familiar with traditional biomedical IT frameworks, including data leaks, slow processing, and low operational costs. Note that BC technology on the edge of the cloud also leads to more efficient sharing of data by clinicians, which will facilitate better teamwork as well as better patient outcomes. These technologies promise to transform healthcare delivery, making it more patient-focused, secure, and efficient as the technologies mature [18], [47]. This subsection summarizes the recent efforts in the use of BC technology in edge computing for health care, as shown in Table 4.

TABLE IV. HEALTHCARE SECURITY USING BLOCKCHAIN IN EDGE COMPUTING.

Authors	Proposed	Health section	Metrics	Strength	Limitations
[48]	An innovative, secure, and decentralized healthcare system	eHealth information protection	Convergence behavior	Allow the sharing of massive amounts of medical data	The time, cost, and energy consumption are not considered
[25]	SecureMed framework	eHealth information protection	Delay, bandwidth, running time, and accuracy	Decentralized privacy	The dataset is not explained

[49]	Security and Privacy Mechanisms	eHealth system	-	The eHealth system is a stable and efficient fault-handler	The dataset is not explained
[50]	Privacy-preserved Secure Medical Data Sharing	Information Sharing	-	Used three different keys	The dataset is not explained
[51]	Reliable Low-Delay Digital Healthcare	eHealth system	Delay, energy, and cost	Establish decentralized trust, and dependable access in real time	The dataset is not explained.
[52]	A Fast Blockchain-Assisted	eHealth system	Energy consumption, throughput, delay, packet loss rate, and running time	Increase energy savings by using duty cycle MAC scheduling and virtual clustering.	Lack of scalability considerations
[53]	Secure Cross-Domain Sharing	Information Sharing	Running time	combine cryptography technologies and Blockchain for data traceability	Time-checking complexity must be improved
[54]	Edge intelligent Agent Hybrid Hierarchical Blockchain	eHealth system	Energy, accuracy, throughput, delay, packet loss, and authentication time	Proposing a blockchain-based, decentralized solution that guarantees the confidentiality and privacy of medical records	Need for additional mechanisms for device legitimacy
[55]	Protected key sharing and robust authentication between IoT devices	Information Sharing	-	Evaluate their approach on 48 attack traces from 23 different vulnerable protocols.	Comparison with only two state-of-the-art schemes
[56]	Medical record privacy and security	eHealth information protection	Running time and throughput	The system can handle big data scenarios	The paper does not discuss the details of the implementation of the AAL system.
[57]	data integrity auditing scheme based on blockchain	Information Sharing	Delay, authentication time, energy consumption, and running time	Better quality of service with assurances of data security and privacy	The proposed scheme involves multiple phases and complex cryptographic operations

[48] proposed an innovative, secure, decentralized healthcare model that uses BC in edge technologies to conveniently share data among multiple entities. Moreover, [25] suggested a unique framework (SecureMed) that enforces privacy protection through distributed authentication based on BC technology deployed at the edge of cloudlets. Smart contracts are used in SecureMed to connect internet of Medical Things (IoMT) devices to edge cloudlets. Coviblock is a revolutionary, decentralized, BC-based healthcare aid system presented by [56] to enhance health record security during pandemic mitigation while maintaining the system. Alternatively, [49] proposed a distributed e-health system with three levels secured by BC technology: 1) Intelligent clinical sensors that provide information to the mobile device within a patient's body are part of the sensing network region sensor system. 2) Single-hop equipment constructed using IoT sensors for data sensing makes up the closer processing level of the edge networks. 3) Fast-processing-level networks are composed of extensive cloud services. [51] focused on the latter scenario, aiming to deliver user-friendly, dependable, and secure remote monitoring and assistance for older individuals in their residences. They proposed a framework to amalgamate edge computing and BC technology functionalities to fulfil the essential requirements of advanced remote healthcare systems. [52] offered a BC-enabled infrastructure that utilizes distributed edge servers for rapid data processing. They create smart contracts to authenticate the identities of network entities and ensure data integrity. [54] introduced an innovative edge intelligent agent hybrid hierarchical blockchain (EIA-H2B) model for healthcare observation and recommendation systems utilizing IoT devices within the WBAN-5G framework. On the other hand, [50] utilized BC technology's transparency, security, and efficiency, as well as computing and storage facilities at the edge level, to establish privacy-preserving storage and tracking schemes for electronic health records (EHRs). [53] demonstrated an effective and secure cross-domain sharing framework for EHRs via edge computing. The application allows the physician access to the patient's EHRs with the patient's consent, facilitating an understanding of the health history and the subsequent creation of a new medical record. [55] introduced a novel and safe approach termed IoToDChain for an e-health system, which uses cryptographic techniques, particularly the elliptic curve Diffie-Hellman-RSA and the BC paradigm. On the other hand, [57] presented a BC-based data integrity auditing scheme. A method for distributed data integrity verification without the involvement of a third-party auditor is developed.

6.2 Healthcare Using Blockchain in Fog Computing

Combining BC technology with FC lays the foundation for a secure, efficient, and scalable healthcare infrastructure. Note that FC layers have extra functionality on top of cloud computing by placing computational assets at the edge between the data sources (e.g., medical devices and sensors) and the cloud. Such proximity allows data to be processed and analysed in time, which is particularly relevant in the context of remote patient monitoring as well as emergency response activities. This aids in the real-time processing of health and safety data. Decentralization and immutability are key properties of BC technology that can enhance the integrity and protection of health data within the FC environment. Using BC, medical

institutions can guarantee that patient information is securely logged and transmitted to appropriate stakeholders without the risk of manipulation or unauthorized reading. This integration overcomes several issues that conventional healthcare information technology systems are usually subject to, including data privacy breaches, delays, and data centralization and preparation limitations. The security provided by the BC's cryptographic method and consensus mechanism is strengthened. The delay provided by the FC is minimized, and the response ability of the healthcare application is enhanced. Second, the decentralization of BC guarantees the consistency and integrity of data among all nodes in a network, increasing confidence in the functioning of the healthcare system. With the advancement of these technologies, there is great promise for incorporation to change the healthcare delivery system in terms of better security, efficiency, and patient-centeredness [58], [59]. This section outlines the literature on the use of BC technology as a fog computer in healthcare (Table 5).

TABLE V. HEALTHCARE SECURITY USING BLOCKCHAIN IN FOG COMPUTING.

Authors	Proposed	Health section	Metrics	Strength	Limitations
[60]	BEdgeHealth	Information Sharing	Delay, energy consumption, and authentication time	They have conducted several practical tests to confirm the efficacy of the work	- Use of classic IPFS with global DHT for data sharing, leading to high data retrieval delay
[61]	Edge-Cloud-Enabled Nursing System	eHealth system	Energy consumption and delay	The proposed system supports dynamically increasing healthcare datasets	The proposed system is complex in implementation and maintenance.
[62]	protect the innovative health system	eHealth system	Accuracy	Tested four machine learning algorithms	Scalability problems because of the large amount of health data
[63]	Task Offloading Method Using Blockchain Security and Emergency Management	eHealth system	Delay and throughput	Enhances the system's dependability and time efficiency.	The energy consumption is not calculated.
[64]	IoT infrastructure softwarization for safe and intelligent healthcare	eHealth system	-	Integrating Blockchain and Tor ensures robust security for patient information.	The proposed work is complex.
[65]	Secure IoMT architecture with blockchain support	Information Sharing	Accuracy	successfully identifies cybersecurity ransomware attacks	There is no calculation of the cost or energy use.
[66]	Assisted deep reinforcement learning with mobile fog and cloud	eHealth system	-	Utilize blockchain work scheduling and multicriteria offloading based on deep reinforcement learning policies.	The cost, energy, and delay constraints are not considered
[67]	IoT-fog-based healthcare 4.0 system	eHealth system	Accuracy, running time, and cost	Provide high accuracy	The limitations of cost and energy are not taken into account.
[68]	Health Record Management	Hospital and medicine management	Reliability, accuracy, Running Time, and delay	The proposed technique achieves 95% reliability	The limitations of cost and energy consumption are not taken into account.
[69]	Identification and Authentication in Healthcare	eHealth information protection	Delay, Throughput, Energy consumption, running time, and accuracy	Provide a high accuracy in fog computing	The complexity is high
[70]	Proposed FogChain	eHealth system	running time, delay, and throughput	Reduce the delay	The CPU and memory utilization are high under heavy load.
[71]	Blockchain-enabled job scheduling system with federated learning	eHealth system	Delay and energy consumption	Reduce the energy consumption and delay	The cost and running time are not considered
[72]	Federated Learning and Blockchain-Enabled	eHealth information protection	Accuracy	Improve the accuracy	The cost, energy, and delay constraints are not considered
[73]	Self-monitoring of Blood Glucose	eHealth data storage	response time, throughput, and delay	Suggested a method for diagnosing, tracking, researching, and taking public health action.	The cost and energy are not considered
[74]	Predicting Diabetic-Cardio Disease with a Secure Healthcare App	eHealth system	Running time and accuracy	Reduce the running time	The cost and energy are not considered

[75]	An interplanetary file system and blockchain are merged into a three-level/tier network.	Information Sharing	Accuracy and running time	Improve the accuracy	The cost and energy are not considered
[76]	bioinspired robotics-enabled schemes	eHealth information protection	Energy consumption and running time	Improve the energy consumption for different IoT activities	The cost is not considered
[77]	AISCM-FH: AI-Enabled Secure Communication	eHealth system	Cost, accuracy, throughput, and running time	Reduce the cost	The energy consumption is not considered
[78]	Group Authentication Framework for IoT Systems	eHealth system	Running time and accuracy	Improve the execution time	The cost and energy are not considered
[79]	IoT security model	Control access	Delay and throughput	Reduce the delay	The cost and energy are not considered
[80]	Blockchain-Based Lightweight Encryption Technique	eHealth system	running time, cost, and delay	Improve the execution time	The energy consumption is not considered
[81]	Fog-enabled, lightweight blockchain-based remote patient monitoring system	eHealth system	Running time, delay, and energy consumption	Low execution and delays were accomplished.	The cost is not considered.
[82]	blockchain-based fog monitoring framework	eHealth system	Accuracy	The processing of minimum and optimal features relative to other features	The cost, delay, execution time, and energy are not considered
[83]	patient electronic health Data method	eHealth data storage	Cost, running time, and reliability	The model supports many service requests	The paper includes simulation results, practical implementation, and real-world testing are limited.

[60] suggested a decentralized health architecture named BEdgeHealth, which incorporates MEC and BC for data offloading and sharing between distributed hospital networks. Moreover, [65] introduced the secure BC IoMT architecture for the data fusion processing of lung cancer data within the fog and cloud networks. The BC IoMT architecture presents the BC Data Fusion Secure algorithm framework, which consists of task scheduling and BC validation mechanisms. A three-layer network incorporating BC and the Interplanetary File System (IPFS) was proposed to achieve data security for patients and IoMT sensors [75]. Alternatively, [61] presented an innovative distributed combined edge–cloud architecture to more effectively meet these needs. To address security concerns, they incorporate BC technology to authenticate the identity of data exchanges and implement differential privacy in the NS to safeguard the data privacy of healthcare providers. [62] demonstrated a novel system for healthcare models based on many emerging technologies: BC, IoT, fog, and artificial intelligence. [63] developed a centralized task-offloading method featuring a low-latency, secure, and dependable decision-making algorithm with robust emergency management capabilities to assist resource-limited edge devices in task-offloading. [64] provided an agile software architecture for the flexible, cost-efficient, safe, and privacy-preserving implementation of the IoT in novel healthcare applications and services. The research examined offloading and scheduling issues related to healthcare workflows within an IoMT fog-cloud network [66]. Consequently, the study regarded the issue as an offloading and scheduling dilemma and framed deep reinforcement learning as a Markov problem. The proposed approach centers on an electronic healthcare system that concurrently manages essential and noncritical patients [67]. The fog layer is bifurcated into a crucial and noncritical fog cluster. [70] introduced an architectural concept called FogChain, which integrates BC, FC, and the IoT for the healthcare sector. The primary contribution is the FogChain model, which addresses IoT limitations through a differentiated approach by introducing an intermediary Fog layer proximate to the edge, enhancing capabilities and resources. [71] proposed a system for task scheduling based on federated learning and blockchain technology (FL-BETS) with various dynamic heuristics. This research examines various healthcare applications characterized by intricate limitations and energy usage during execution on distributed fog and cloud nodes. [74] advocated for efficient and secure healthcare services for disease prediction within FC environments. On the other hand, [77] proposed an AI-enhanced secure communication framework within a fog computing-based healthcare system (AISCM-FH), which employs the conventional random oracle model alongside a heuristic (nonmathematical) security evaluation. [78] introduced an innovative group authentication architecture for IoMT systems. The group authentication protocol is executed via a four-phase procedure: setup, registration, secret construction, and authentication. [80] created a distinctive, lightweight encryption technique that uses fog for the IoT. The fog bus offers a platform-agnostic interface for the execution and interaction of IoT applications and computational entities. [81] established a three-tier remote patient monitoring system that utilizes BC technology for enhanced security and fog technology to deliver low-latency services to IoT devices and healthcare customers. Moreover, [82] proposed a framework for activity monitoring and recognition that uses a multiclass cooperative categorization method to increase the accuracy of activity classification in videos within fog or cloud computing-based BC architectures. [68] presented a BC-enabled FC framework for the IoMT. The proposed method integrates a BC with another consensus (YAC)

protocol, establishing a security framework within the FC to store and transmit IoMT data across the network. A unique method utilizing FC and BC was presented by [69]. The system comprises an FC-based three-tier architecture, an analytical model, a mathematical framework, and an advanced signature-based encryption (ASE) algorithm for the identification and verification of healthcare IoT devices, as well as the authentication of patient health data (PHD). [72] presented a federated learning (FL) platform and private BC technology in a fog-IoT network. On the other hand, [76] developed bioinspired robotics-enabled strategies within the BC-fog-cloud-assisted IoMT ecosystem. The objective is to reduce execution expenses and BC apps. This work develops bioinspired robotics function blockchain task scheduling (BIR-FBTS) algorithms to ascertain the optimal allocation of jobs to the available nodes. [73] designed and constructed a system that augments commercial continuous glucose monitoring (CGM) by incorporating IoT functionalities, enabling remote patient monitoring and providing alerts regarding potentially hazardous conditions. A secure IoT model is proposed to monitor the health of players and spectators and conduct tactical analyses of matches [79]. In the proposed model, the system becomes more efficient with the help of FC. [83] presented a novel approach to processing PEHDs that enhances security. Note that PEHD is processed and centralized via conventional cloud servers. Servers consolidated in a singular location are susceptible to failure.

6.3 Healthcare Using Blockchain in Cloud Computing

Combining the cloud with BC technology in managing healthcare data is a major step in protecting integrity and easing access to the data. According to [84], a hybrid healthcare data management system (HDMS) has been suggested to utilize the best features of cloud computing and Ethereum BC to ensure safe and efficient storage and management of healthcare data. It combines new privacy features, such as decentralized identifiers (DIDs) and homomorphic encryption, to enhance the security and privacy of HDMS data and, in turn, makes them compliant with the health level 7 (HL7) standard and the data protection act. Furthermore, [85] stated that using BC technology solves the problems posed by centralized medical device data systems since it provides a dependable audit trail and guarantees that health data in cloud settings are secure and that their origin is remembered. In this progressive world, combining BC and cloud computing will increase trust in data and shareability. This will encourage a shift towards a healthcare environment with easy, safe, private sharing of health information and quality clinical decisions.

TABLE VI. HEALTHCARE SECURITY USING BLOCKCHAIN IN CLOUD COMPUTING

Authors	Proposed	Health section	Metrics	Strength	Limitations
[86]	Multiple access control scheme for EHRs	eHealth system	Running time	the encryption scheme has proved to be more efficient and feasible.	Key generation center might lead to failure and key escrow problems
[87]	develop a tamper-proof cloud-based EPIHR management solution	eHealth information protection	-	prevent existing data management system transactions from being altered	The paper does not address the potential challenges of transaction speed, storage requirements, and network scalability.
[88]	propose a blockchain-empowered security and privacy protection	eHealth information protection	Running time, throughput, and delay	Reduce the delay	The cost and energy consumption are not collected
[89]	protect privacy and enhance access management	Information Sharing	running time	Reduced the running time	The energy consumption is not calculated
[90]	enhance the health insurance process	eHealth system	-	-	The cost and energy consumption are not collected.
[91]	Secure Storage in Cloud-Based eHealth Systems	eHealth system	Cost and delay	Reduce the delay	The energy consumption is not calculated
[92]	Private blockchain for multimedia medical data processing	eHealth system	Running time, Peak to Signal Noise Ratio, and Mean Square Error	Reduce Encryption time and Decryption time	The cost and energy consumption are not collected
[93]	Security and Privacy of Patient Information in Medical Systems	eHealth information protection	Running time	Reduce running time	The cost and energy consumption are not collected
[94]	Securing e-health records	eHealth information protection	Running time and cost	The results demonstrate that the KSIBC framework significantly improves response time and storage costs.	The energy consumption is not calculated.

[95]	Securing and Managing Healthcare Data	eHealth information protection	-	This innovative approach adds a layer of security by encrypting the block hashes using DNA sequences, making it potentially difficult for unauthorized access to compromise the data.	They didn't consider the framework's cost, efficiency, and implementation constraints.
[96]	Secure Cross-domain Medical Data Sharing	Information Sharing	Running time and cost	Reduce the running time	The energy consumption is not calculated
[97]	Secure Cloud-Based EHR System	eHealth information protection	-	Using identity-based signatures (IBS) further enhances data authenticity and integrity.	The energy consumption and cost are not calculated.
[98]	Protecting Vaccine Safety	Hospital and medicine management	Computation, communication, and storage consumption	improve the safety of vaccine circulation	The proposed system imposes a more considerable computation and storage burden.
[99]	Privacy-friendly platform for healthcare data	Hospital and medicine management	Running time and cost	Reduce the running time	the energy consumption is not calculated
[100]	IoT-based skin surveillance system	eHealth system	-		The energy consumption and cost are not calculated.
[101]	Practical Homomorphic Authentication	eHealth system	Cost and running time	Reduce the running time	the energy consumption is not calculated
[102]	wearable medical sensor-assisted framework	eHealth information protection	Accuracy and Cost	Improve the accuracy	the energy consumption is not calculated
[103]	A Blockchain Framework for Secure Remote Monitoring	eHealth system	Throughput and running time	It works very well with large networks	the energy consumption and cost are not calculated
[104]	Block Chain Technique for Data Privacy and Access Anonymity	eHealth system	Running Time and Cost	The proposed method allows for better data privacy in the innovative healthcare network.	The energy consumption is not calculated.
[105]	Multitier Blockchain Framework	eHealth information protection	Running time	Reduce the processing time	the energy consumption and cost are not calculated
[106]	Trust-Less Medical Data Sharing	Information Sharing	Delay	The proposed system is designed to be practical and applicable in real-world scenarios, potentially improving the efficiency and security of medical data sharing among cloud service providers.	The paper mentions that delay increases with the number of requests per cloud service provider, which could raise concerns about the system's scalability in high-demand environments.
[107]	Patient-centric interoperability through blockchain	eHealth information protection	Running time	Allow patients to securely store, share, and manage access to their health data	the cost and energy consumption are not considered
[108]	A Medical Data Sharing Scheme	Information Sharing	Throughput and running time	Reduce the running time	the cost and energy consumption are not considered
[109]	Keyword search over encrypted cloud data	eHealth information protection	Running time	the integration of blockchain enhances data integrity and confidentiality	the complexity of the system, including key generation and trapdoor generation processes, could lead to performance issues
[110]	Improving the Financial Security of National Health Insurance	Hospital and medicine management	-	reduce fraud by ensuring transparent and tamper-proof claims processing through blockchain technology	the cost and energy consumption are not considered
[111]	hierarchical architecture of blockchain networks	eHealth data storage	Running time	The system ensures immutability, redundancy, and tamper-proof protection by storing all data on-chain.	The hierarchical structure may introduce complexity in implementation and maintenance.
[112]	Trustworthy Blockchain-Based Multi-Cloud Broker	eHealth system	Running time, Mean absolute deviation, and reliability	The architecture ensures compliance with data protection laws by limiting access on a need-to-know basis, thus respecting user privacy	The testing was conducted in simulated environments, which may not fully capture the complexities and variety of real-world healthcare settings
[113]	Forward Transparency and Secure Provenance	eHealth system	Delay, cost, and running time	the system is resistant to common threats like offline	While the blockchain component enhances

				dictionary attacks and maintains the integrity of provenance records	security, it might face scalability issues, particularly with increasing records and user demands in cloud environments
[114]	Healthcare Services Monitoring	eHealth system	Delay, running time, and accuracy	minimizes system execution time (SET) and average delays	the scalability of the blockchain solution in a real-world environment with numerous users and transactions might require further validation
[115]	Decentralized blockchain-based secure storage	eHealth data storage	Running time and accuracy	Utilizes blockchain technology to eliminate third-party involvement, ensuring data confidentiality and integrity	The performance may be affected as the number of IoT nodes increases, potentially leading to higher computational overhead.
[116]	Flexible and Efficient Blockchain-Based ABE Scheme	Control access	Cost and running time	The scheme supports multiple authorities, which is more realistic for distributed telemedicine systems and enhances flexibility and scalability.	The complexity of managing multiple authorities could lead to potential coordination challenges and increased overhead.
[117]	Flexible Access Control Mechanism	Control access	Running time	It allows patients to control access to their EHRs with attribute-based encryption, enhancing user privacy.	Patients must deploy smart contracts and manage key generation, which may demand high computational resources.
[118]	Extended Validation Certification-based Fischer Neural Network optimization	eHealth system	Delay	Addresses critical quality of service parameters like network delay and end-to-end delay, which are essential for eHealth applications.	The discussion on cryptographic techniques is minimal, which may impact the overall security framework.
[119]	Federated Intrusion Detection System for Blockchain-Enabled	eHealth information protection	Accuracy and running time	Demonstrated superior performance, mainly when tested with the BoT-IoT dataset, achieving 99.99% accuracy and a 0% false alarm rate	Incorporating blockchain increases system complexity, and while the time overhead is relatively small, it could still impact resource-constrained environments.
[120]	Electronic Health Records Sharing Model	Information Sharing	Delay and throughput	Enhancing the robustness and efficiency of data sharing in EHR systems	the proposed model may face challenges in environments with high transaction volumes or large numbers of participating entities
[121]	EHR storage model based on a deletable consortium blockchain	eHealth data storage	Cost and delay	Implements mechanisms such as tamper-proof and time-stamped transactions, multilayer encryption, and a secure password-based key exchange protocol to ensure data confidentiality and integrity	The lack of deployment in real-world scenarios raises questions about practical scalability and robustness.
[122]	Secure Protocol for Cloud-Assisted Electronic Health Record System	Control access	Cost	The proposed system is designed to be practical for real-world healthcare applications, considering factors like storage efficiency and scalability.	Integrating blockchain, cloud computing, and ECC adds complexity to the system.
[123]	Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information	Control access	Cost	the paper ensures data integrity and scalability while maintaining low computation costs.	The integration of blockchain, cloud computing, and CP-ABE adds complexity to the system
[124]	protect outsourced EHRs from illegal modification	eHealth information protection	Cost and delay	The proposed system is efficient regarding computational and communication overhead, making it practical for real-world deployment.	The scalability of the blockchain itself could be a limiting factor as the number of transactions and participants increases.

[125]	Health Resource Sharing Based on Consensus-Oriented Blockchain	Information Sharing	Accuracy, reputation, and cost	Block generation is performed using the Proof of Authority (PoA) consensus algorithm, which is efficient and does not require significant computational power.	The scalability of the blockchain could be a limiting factor as the number of transactions and participants increases.
[126]	Elliptical Curve Certificateless Aggregate Cryptography Signature scheme	eHealth information protection	Running time, delay, and cost	The proposed scheme is designed to resist various attacks, including collusion attacks, forgery, and malicious data modification.	The proposed scheme involves multiple cryptographic operations and blockchain transactions, which can be complex to implement and manage.
[127]	Livestock monitoring	eHealth system	-	The integration of blockchain technology ensures that all data related to livestock are tamper-proof and traceable.	The proposed system can be complex to implement and manage.
[128]	EHR sharing protocol	Information Sharing	Running time	The proposed scheme combines searchable encryption and conditional proxy re-encryption to preserve data security and privacy.	The scalability of the blockchain could be a limiting factor as the number of transactions and participants increases.
[129]	searchable encryption	Information Sharing	Running time	The paper proposes an improved consensus algorithm that enhances resource utilization and accelerates block generation. This makes the blockchain more efficient and suitable for innovative healthcare applications.	The proposed scheme involves multiple cryptographic operations and blockchain transactions, which can be complex to implement and manage.
[130]	complex Smart Healthcare computations	eHealth system	Delay and throughput	The proposed architecture is designed to be scalable, accommodating the fast-growing volume and variety of medical big data.	The feasibility of implementing the proposed architecture is evaluated based on the cost of quantum cloud services and the performance of the proposed PBFT algorithm.
[131]	efficient tamper-proof model for EHR storage	eHealth data storage	Throughput, running time, and delay	The proposed model supports batch outsourcing and storage of EHRs, allowing multiple doctors to outsource EHRs for multiple patients simultaneously.	The proposed model involves multiple advanced technologies, including blockchain, IPFS, and cryptographic techniques.
[132]	A privacy-preserving blockchain-based tracing model	eHealth system	Energy consumption, error rate, and running time	The immutability and traceability of blockchain enhance the overall security and reliability of the system.	The proposed model involves multiple advanced technologies, including blockchain, LDP, CP-ABE, and smart contracts.
[133]	a blockchain-assisted, verifiable, outsourced attribute-based encryption	Information Sharing	Cost, running time	The scheme is designed to have a constant ciphertext size, which reduces bandwidth utilization and storage overhead.	The proposed scheme involves multiple advanced technologies, including blockchain, attribute-based encryption, and smart contracts.

[86] presented an efficient ABE system that delegates a portion of the computational burden to the FNs. This framework securely disseminates data with less overhead and facilitates user and attribute revocation. Moreover, [90] demonstrated a smart healthcare insurance framework for fraud detection and prevention (SHINFDP) that utilizes advanced technologies, including BC, 5G, cloud computing, and machine learning (ML), to improve the health insurance process. [91] identified threats to the security of outsourced EHRs and delineated the system and security criteria that a safe cloud-based eHealth system must fulfil. They subsequently presented a BC-enabled eHealth framework for safeguarding outsourced EHRs that fulfil the specified criteria. [92] examined a unique BC-based secure biomedical image processing system that preserves anonymity. [100] established a BC-based skin surveillance system for the IoT that incorporates safety and data protection features. In a distributed architecture, a safe data transfer method for IoT devices is suggested. [101] examined a workable homomorphic authentication system for cloud-assisted VANETs that offers medical monitoring for all passengers. [103] introduced PharmaChain 2.0, which employs the PoAh consensus algorithm to attain reduced processing demands and enhanced scalability while ensuring requisite security. A distinctive BC-based method was proposed by [104] to enhance anonymity regarding data access and privacy. The registration phase is initially conducted for both the device and the user.

[112] addressed data security and trust issues by introducing Healthy Broker, an innovative brokering architecture designed to enhance trust across various cloud environments. [113] suggested a server-assisted password-based subsequent key-locked encryption method to safeguard the confidentiality of outsourced EHRs. The encryption approach ensures conditional forward transparency: a physician may examine a patient's EHRs pertinent to the current diagnosis just with the patient's authorization. The methodology suggested by [114] is a safe and resilient healthcare-oriented blockchain (SRHB) that employs attribute-based encryption (ABE) for the secure transmission of healthcare data. [118] introduced an extended validation certification-based Fischer neural network optimization (EVC-FNNO) approach for secure mobile cloud-based e-Health systems. [127] introduced an innovative approach to utilize BC technology to ensure traceability and authenticity throughout the livestock supply chain, enhancing the scientific rigor and reliability of cattle production practices. [130] demonstrated a quantum cloud-as-a-service that offers an efficient, scalable, and secure solution for intricate smart healthcare computations. A verifiable ABE scheme utilizing BC and local differential privacy was proposed by [132], which employs LDP to locally perturb the original data to mitigate collusion attacks. It outsources encryption and decryption to designated service providers to alleviate the burden on mobile terminals and implements smart contracts in conjunction with BC for equitable execution by all parties to address the issue of erroneous search results in a semihonest cloud server. [87] presented a BC management system architecture that controls the EHRs and personal information of every person (EPIHR). [88] suggested a security and privacy protection plan for COVID-19 medical records driven by BC technology that involves direct and traceable revocation. [93] employed BC technology to safeguard private information in medical systems and successfully implemented antitheft measures for private data. Authentication is guaranteed via the keyless signature architecture that [94] uses to protect the confidentiality of digital signatures. Additionally, data integrity is managed by the proposed BC technology. [95] created and suggested a novel framework for sensor machine data generation and cloud storage. BC technology can secure transactions. The framework encrypts the hashes of the blocks via DNA cryptography. [97] proposed a safe EHR system built on BC technology and an attribute-based cryptosystem. Medical data are encrypted by the authors via identity-based encryption (IBE) and ABE, and digital signatures are implemented via identity-based signatures (IBSs). [102] presented PMHE, a BC-based architecture that uses fully homomorphic encryption technology to protect the privacy of medical data. [105] provided an innovative protocol designed to ensure complete patient privacy protection, referred to as pseudonym-based encryption with different authorities (PBE-DA), by integrating BC technology with healthcare communication systems within an e-health platform. [107] presented MediTrans, a BC-based, secure, interoperable solution for managing patient-centric data access. In the proposed architecture, patients possess their treatment-related data and keep it in a secure personal health record (PHR) cloud. [109] examined a BC-based attribute-centric searchable encryption technique that facilitates ciphertext verification and implemented it within an electronic medical record system. The FIDChain IDS was proposed by [119] and uses lightweight artificial neural networks (ANNs) within an FL framework to safeguard healthcare data privacy. This approach leverages BC technology, which offers a distributed ledger for aggregating local weights and subsequently broadcasting the updated global weights after averaging. [124] presented a secure cloud-assisted eHealth solution to safeguard outsourced EHRs from unauthorized alterations. This system would utilize BC technology, such as BC-based currencies such as Ethereum. [126] determined a novel elliptic curve certificateless aggregate cryptography signature (EC-ACS) technique for public verification and auditing within the medical cloud server (MCS) to safeguard EHRs via approved BC technology. Alternatively, [89] presented a novel user-centric health data-sharing solution utilizing a decentralized yet permissioned BC to safeguard privacy and improve access control. [96] suggested a safe, cross-domain medical data exchange system that protects patient privacy. The authors deploy a distributed cloud to enable cross-domain medical data sharing to overcome data isolation from different hospital sites. [106] introduced MeDShare, a system designed to address the challenge of medical data sharing across custodians of extensive medical data in a trustless setting. [108] presented a medical data-sharing framework utilizing cloud-chain collaboration and policy integration within the IoT. It presents a conflict resolution and fusion technique that allows physicians and patients to coauthorize medical data about asymmetrical access control rights. [120] introduced an ABE method and a multikeyword encryption technique for encrypting EHRs. Additionally, they propose a node-state-checkable practical Byzantine fault tolerance (sc-PBFT) consensus method to prevent Byzantine nodes from infiltrating the consortium BC. [125] assessed a cloud-based health resource-sharing paradigm utilizing consensus-oriented BC technology and conducted a simulation study on breast tumor diagnostics. [128] presented a BC-based framework for secure and privacy-preserving EHR sharing. Upon obtaining the data owner's authorization, the data requester may query the specified keyword from the data provider to locate pertinent EHRs on the EHR consortium BC and retrieve the re-encryption ciphertext from the cloud server. [129] presented a secure encryption approach featuring fine-grained access control for sharing cloud-based EHRs facilitated by BC technology. It delegates computing duties to edge servers and allows users to regulate access to their EHRs. [133] established a BC-enabled Verifiable Outsourced Attribute-Based Signcryption (BVOABSC) system that facilitates the secure sharing of EHRs inside a multiauthority cloud storage framework. [98] provided a better, storage-efficient, BC-based vaccine safety protection system. In particular, first, the vaccination circulation mechanism is simulated. [99] proposed a patient-centered healthcare data management solution that helps achieve privacy by storing data via BC technology. Cryptographic features provide pseudonymity and encrypt patient data. [110] designed and implemented a BC-based system to safeguard the NHIS against financial decline. This study delineates the conceptual architecture of the proposed system, including sequence and use case diagrams, a data management framework, an innovative notification system, and an intelligent claim processing

system. [111] investigated an innovative method for addressing the scalability issue through a hierarchical structure of BC networks. A three-tier hierarchical BC framework comprises hospital, city, and state layers. [115] proposed a decentralized BC-based secure storage system. This system uses BC technology to store patient health information rather than relying on a cloud service provider's storage solution. [121] presented a model called "DS-Chain," an innovative deletable consortium BC-based secure EHR storage architecture inside a multicloud framework. [131] determined an innovative BC-based, efficient, tamper-proof solution for EHR storage via decentralized IPFS cloud storage, termed "TAC-EHR." [116] introduced an ABE framework designed to facilitate dynamic authentication and authorization, enhancing flexibility and efficiency for MoD services in telemedicine. A consortium BC-based cloud-stored EHR was proposed by [117] that uses smart contracts. [122] presented a safe protocol for a BC-based, cloud-assisted EHR system. The suggested approach uses BC technology to ensure data integrity and access control through log transactions, while the cloud server stores and administers patients' EHRs to offer safe storage resources. [123] assessed a secure authentication methodology for a cloud-assisted Traffic Management Information System (TMIS) that incorporates access control via BC technology.

6.4 Review Papers

The review and survey articles were included in this category to describe healthcare using BC in an EFC environment.

TABLE VII. REVIEW PAPERS.

Authors	Metrics	Blockchain type	Environment	Health department
[134]	x	X	Cloud	x
[135]	x	X	Fog	x
[136]	x	X	Edge	x
[39]	x	X	Cloud	x
[137]	x	X	Edge	x
[138]	x	X	Fog – Cloud	x
[139]	Y	Y	Edge	x
[140]	x	X	Cloud	x
[141]	Y	X	Edge – Fog – Cloud	Y
[142]	Y	Y	Cloud	x
[143]	x	Y	Fog	x
[144]	x	X	Fog	x
[145]	x	X	Fog	x
[146]	x	X	Cloud	x
Our work	Y	Y	Edge – Fog – Cloud	Y

[134] Assess different aspects in which m-health is implemented, particularly the best practices regarding security in the area and the BC protocol in mHealth. [135] discussed the advantages and disadvantages of an FC-supported architecture that utilizes BC for healthcare, focusing on potential uses of BC technology in healthcare. An SLR of published works on BC applications in edge-enabled innovative healthcare systems was undertaken by [136]. A comprehensive examination of BC technology in cloud storage was presented by [39] to increase the security of healthcare systems. The authors analyse the advantages and disadvantages of utilizing a fundamental cloud storage system. These methods provide a concise summary of BC cloud storage technology. [137] examined the integration of edge computing, BC technology, and IPFS to increase eHealth's quality of service and address security concerns. They assessed recent research in this area to ascertain the primary requirements that must be addressed in the design of eHealth applications. They concluded by presenting a proposal informed by the current literature that addresses the stated problems throughout the whole lifespan of eHealth data management. [138] provided a comprehensive examination of sophisticated methods for safeguarding cloud-based healthcare data management systems through the use of BC technologies. It offers a classification and emphasizes the advantages and disadvantages of the analysed methodologies. [139] provided a comprehensive evaluation of integrating BC technology and edge computing within the healthcare sector. [140] presented an extensive comprehension of the concepts, problems, and future prospects associated with this integration. Initially, they examined the concepts of BC and cloud computing, emphasizing their distinct functionalities and advantages. They subsequently deliberated on the benefits of integrating these technologies inside the healthcare sector: improved security, data integrity, interoperability, and decentralized control. [141] presented an extensive examination of the integration of the IoT, AI, EFC, and BC paradigms by addressing a range of subjects related to all critical aspects from design to deployment. The paper commences with a comprehensive examination of the primary requirements, cutting-edge reference architectures, applications, and obstacles. [142] examined trust issues in cloud computing and evaluated how BC technology mitigates these concerns through BC-based trust management frameworks. [143] Determine the security challenges of the IoMT framework and investigate how FC and BC technologies can address the latency and security issues inherent in conventional IoMT systems. [144] provided a comprehensive review of the IoT, BC, and FC tools and their roles in healthcare via the smart city concept approach. [145] investigated the use of BC technology in conjunction with FC for the storage and processing of distributed data with cloud-based storage and the processing of data generated by these solutions. [146] described the processes of deploying cloud-based solutions and blockchain technologies for storing and managing acquired healthcare data.

7. ANALYSIS OF RESULTS

This section analyses the systematic review results. In response to the RQs, we review the chosen articles in Section A before comparing them with the articles in Section B.

7.1 Overview of Selected Studies

Figure 5 illustrates that 57% of the papers originated from ScienceDirect, 21% from Scopus, 14% from WoS, and 8% from IEEE. A total of 6,495 articles were included across all the databases. A total of 1949 papers were identified as replicated across the databases following the initial filter, which entailed the elimination of duplicates. In the second filter, irrelevant papers were excluded by reviewing titles and abstracts. Among the 4546 remaining papers, 4449 were unrelated to the topic, whereas 97 papers used BC in healthcare in the EFC environment.

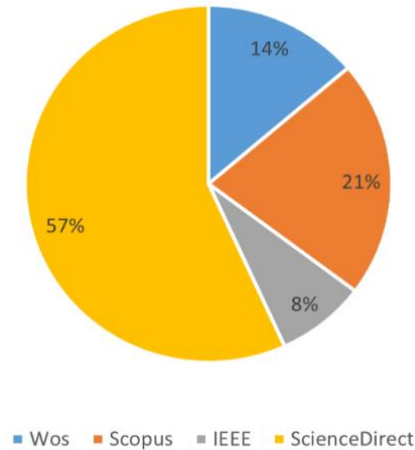


Fig. 5. Article percentages based on the database.

7.2 Research Objective and Techniques

The review process of the selected articles on BC in healthcare in the EFC is covered in Section 5 within four main categories on the basis of the location of BC in the EFC: BC in edge computing, BC in FC, BC in cloud computing, and review papers. The analytical and statistical results of the research questions are presented in Section 5.2 as follows:

RQ2: Which type of classification in research approaches can be applied to healthcare security via blockchain in EFC?

The use of BC in EFC healthcare fell into four categories. Figure 6 shows the statistical percentage of each category. Healthcare using BC in cloud computing studies accounted for the largest percentage of studies (50%), followed by healthcare using BC in FC (25%), review papers (14%), and healthcare using BC in edge computing (11%).

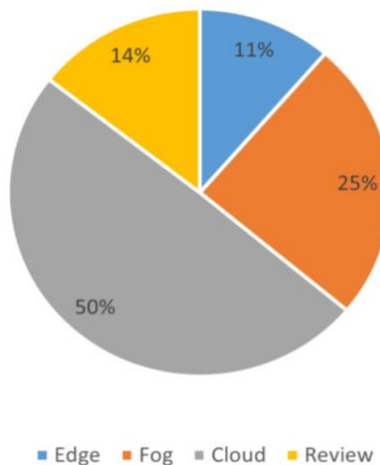


Fig. 6. The use of blockchain in the EFC percentage.

RQ3: What are the current research trends for blockchain use in healthcare in the edge-fog-cloud environment?

The areas of healthcare addressed in the analysed publications demonstrate current research trends in BC in edge computing. Table 7 shows that eHealth systems and information sharing were the areas in healthcare targeted by the researchers the most. Notably, many papers have used BC for eHealth information protection, as shown in Figure 7.

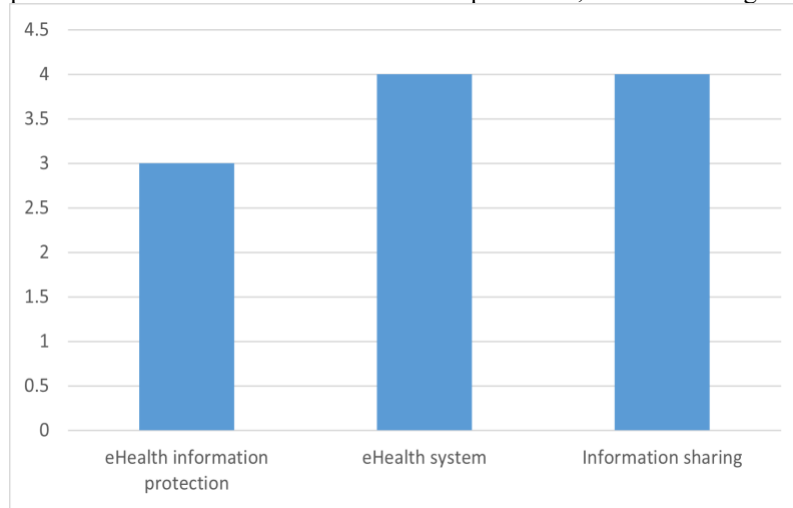


Fig. 7. Healthcare areas used by blockchain in edge computing.

The areas of healthcare addressed in the analysed publications demonstrate current research trends in BC in FC. Table 8 shows that researchers highly used and improved the eHealth system, while the hospital medicine management system was the lowest.

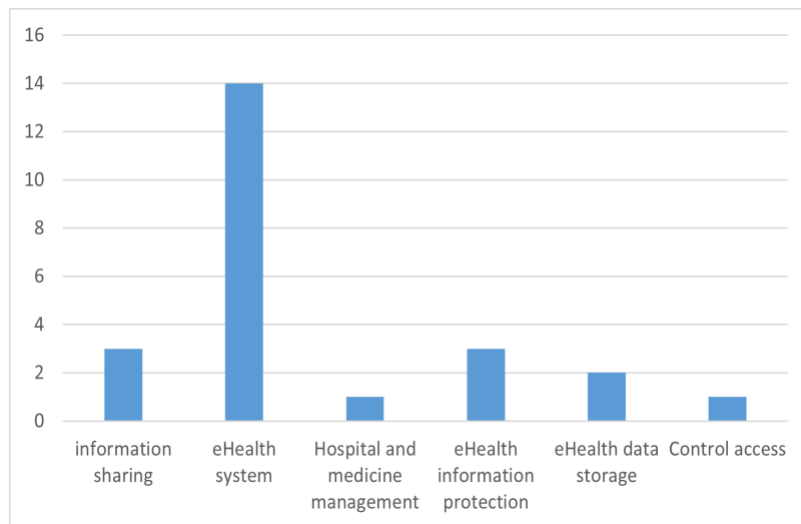


Fig. 8. Healthcare areas used by blockchain in fog computing.

The areas of healthcare addressed in the analysed publications demonstrate current research trends in BC in cloud computing. The results presented in Table 9 show that researchers used the eHealth system more than eHealth information protection did. Hospital and medicine management was the lowest, as shown in Figure 9.

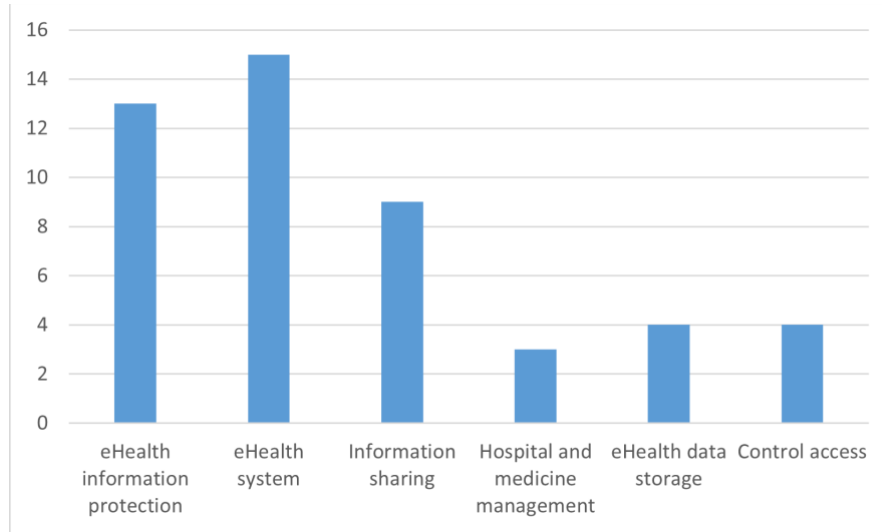


Fig. 9. Healthcare areas used by blockchain in cloud computing.

As depicted in Figure 9, the results show that the researchers focused on improving the eHealth system more than other areas in healthcare. Moreover, there are many areas in which no researchers, such as mobile healthcare, accessible encryption, lightweight BC, and eHealth contracting, have used.

RQ4: What are the metrics measured in previous research?

As shown in Figure 10, the running time is the metric most commonly measured in previous works. The delay was the second highest metric, indicating that the time metric is the most critical metric for the previous works. The results show that energy consumption, accuracy, and cost were not measured by many works, indicating high energy consumption, accuracy, and cost, which is still a limitation for using the BC in EFC.

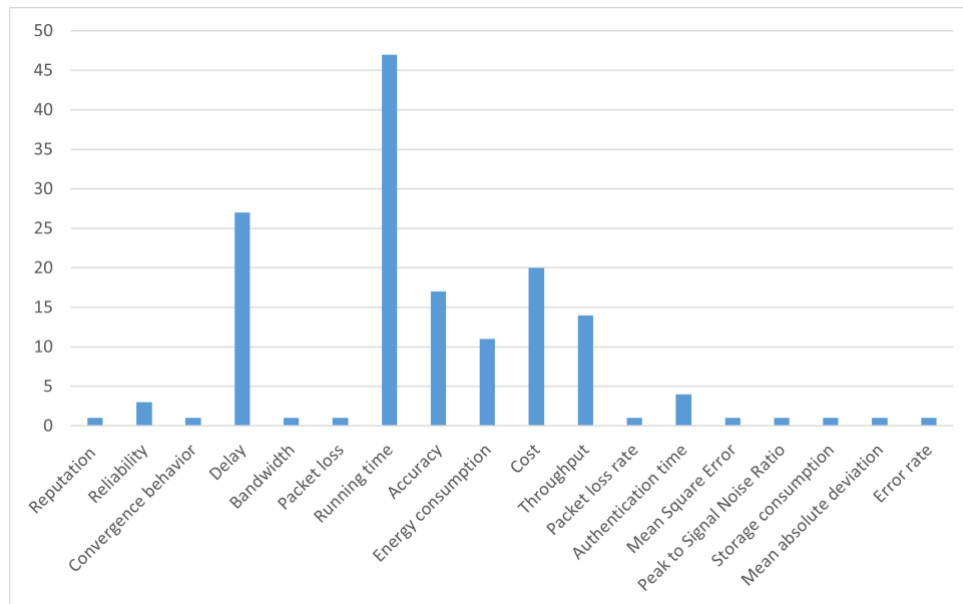


Fig. 10. Number of each metric used in previous works.

RQ5: What datasets and simulations are used to implement and evaluate blockchain in EFC environments?

The dataset plays a significant role in evaluating and testing any model or framework. In recent works, most researchers have not mentioned which datasets are used or even explained the features used. Only a few researchers mention the name of the dataset, such as CSE-CIC-IDS2018, Bot Net IoT, KDD Cup 99, Wisconsin Diagnosis Breast Cancer, Cancer DNA Patients, Oropharynx Radiomics HPV, and a few other datasets. In contrast, others explained the collected data and the parameters they set in the simulations. The same thing occurred with the simulation or the tool they used to implement and

apply the proposed model or framework. Most researchers did not mention the simulation or the tool they used, whereas others explained it in detail. Figure 11 illustrates the simulation or the tool they used in previous work.

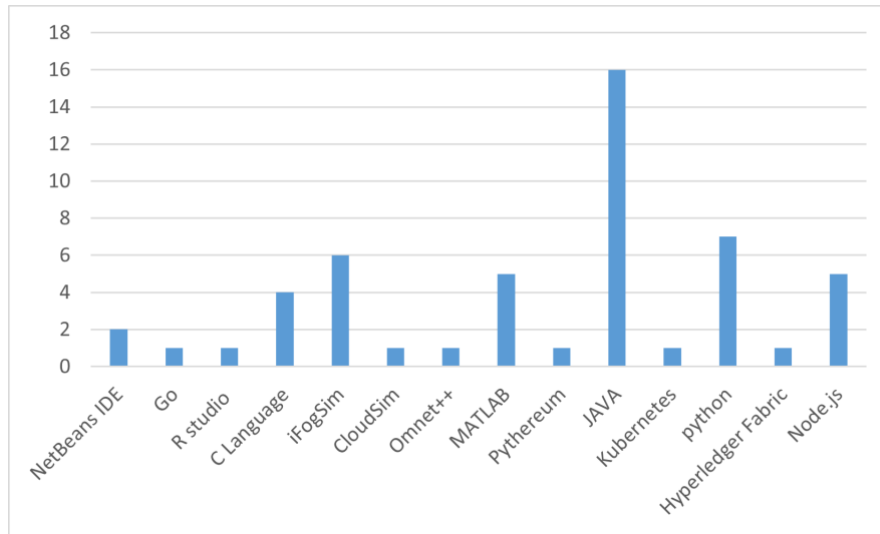


Fig. 11. Percentages of experimental tools.

RQ6: What types of blockchains are used in healthcare in EFC environments?

As mentioned above, BC can be divided into four types: private, public, hybrid, and consortium. Note that recent works have used these types to implement BC for healthcare security in the EFC environment. The results of analyses of recent works based on BC types show that public and consortium BCs are highly used in cloud computing. In contrast, private BCs are highly used in FC, as depicted in Figure 12.

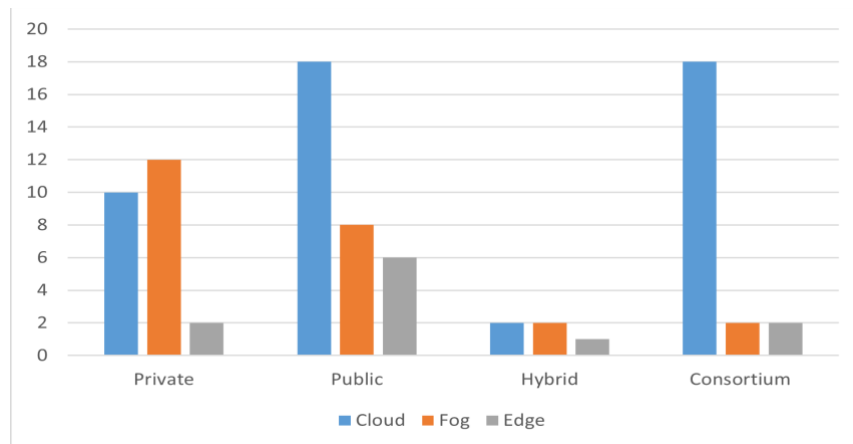


Fig. 12. Number of blockchain types in EFC.

RQ7: Which environment is the most effective for implementing and applying blockchain?

Many factors, such as time, play a central role in choosing the location of BC application in EFC. Time is the most effective metric that researchers must consider when they implement or design their proposed work, specifically in healthcare and security. In previous works, most researchers measured time in different ways. Some researchers have measured the response time, which is the time needed to finish the task. Others measured the encryption and decryption time, whereas others measured the total time from sending the task until storing the data. These different ways to measure time show how important time is in any framework or model. In terms of time, edge computing provides a better response time than does fog and cloud computing. For example, [25] recorded (650 ms) 20 transactions in the response time of his model. This minimum time indicates that edge computing provides a fast response. For other factors depending on time, [69] reported a minimum delay time of (1 ms) for 100 users in the FC, which indicates that the FC is better at distributing the task to reduce the delay. Another important factor is energy consumption, which refers to the energy needed to operate the proposed system. Note that edge computing needs a minimum amount of energy to process the system because of the minimum number of

transactions needed, whereas cloud computing needs high energy because of centralized data centers and extensive cooling needs. For example, [51] compared the implementation of the algorithm at the edge and cloud computing, showing that the energy needed at the edge was recorded (63.75 watts). In comparison, the energy needed for cloud computing is 548 watts.

Time and energy consumption are critical factors in applying any EFC model or system, especially BC. For these factors, on the basis of previous works, edge computing provides the low running time and low energy needed to operate the BC because of low data transmission. It leverages the local processing power and low latency, as data are processed at the source, minimizing delay and running time since data are processed directly at or near the source.

RQ8: What are the limitations of healthcare security using blockchain in EFC?

In recent years, the use of BC for healthcare security in EFC has increased to overcome healthcare security challenges. Although BC has many advantages in healthcare, it also has many limitations, which will be explained in this section. Researchers mostly face a scalability problem in their proposed work. The scalability challenge might be problematic for BC networks since the volume of transactions and data from healthcare IoT devices could be very high. This could increase latency and slow down the time taken for processing. [113] Presented a secure and efficient HealthFort. However, it can suffer from scalability issues, which grow rapidly with increasing records and user demands in the cloud environment. Similarly, [114], [124], [125], and [143] observed scalability issues due to large transactions and participants. Energy consumption is another challenge associated with the use of BC in EFC healthcare. In particular, BC, with its proof-of-work, is considered energy intensive. This is a significant concern in healthcare environments where energy efficiency is crucial. Most of the papers did not consider evaluating their work with energy consumption factors because it might record a high amount of energy needed in their work. [61] decreased the energy consumption factor by 50%. Nonetheless, the energy consumption remained significantly greater when the experiment time increased. The energy consumption was reduced by 35%–45% in the work of [54]. The system still records high energy consumption, especially when the BC is used in edge computing. Another limitation is complexity and integration: integrating BC with existing healthcare systems and ensuring their compatibility across edge, fog, and cloud layers is complex. It requires a great deal of technical expertise and resources. [129] proposed a scheme that involves multiple cryptographic operations and BC transactions, which can be complex to implement and manage. The proposed system involves multiple components and technologies (RFID, sensors, BC, and cloud computing), which can be complex to implement and manage. [127]. Finally, previous works have recorded many other factors, such as running time, throughput, and delay. Nevertheless, many papers have reported excellent results, especially in terms of delay. On the basis of our observations, these limitations are the most noticeable and might not be the only limitations in healthcare security using BC in EFC.

8. Open Issues and Future Work

The transformational potential of blockchain (BC) technology in improving healthcare security in edge-fog-cloud (EFC) environments is highlighted in the systematic review presented in this research. To further develop the field, future studies can fill the gaps in a few areas that are yet understudied. Below are some potential directions for future work:

1. Scalability is the main issue for blockchain in healthcare. There is a main reason for the scalability issue, which is the increase in the number of IoT devices, which leads to an increase in transactions. Future work must focus on developing a system that can handle a massive amount of data without compromising performance.
2. Performance adaptation is another issue that researchers should consider and concentrate on. Researchers must develop a technique to reduce computational overhead and energy consumption, especially in resource-computing environments such as fog computing. Techniques such as sharding, off-chain transactions, and lightweight consensus algorithms can be examined.
3. Although interest in blockchain applications for healthcare security is increasing, numerous important technological issues still impede its practical use, especially in edge-fog-cloud (EFC) systems. Latency, which results from time-consuming consensus processes—e.g., Proof of Work or Practical Byzantine Fault Tolerance—which many blockchain platforms rely on, is one of the most serious concerns. Time-sensitive healthcare activities, including real-time patient monitoring, emergency response, and remote diagnostics, cannot tolerate this delay since data must be processed and acted upon with minimal delay.
4. Another major challenge is storage overhead. Given that all transactions are permanently stored and copied across several nodes, blockchains are naturally append-only ledgers. The requirement for scalable off-chain storage solutions becomes critical in healthcare, where high-resolution imaging, genetic data, and continuous sensor feeds produce large amounts of data. Especially at the edge or fog levels where storage capabilities are constrained, on-chain storage might rapidly become impractical without effective hybrid architectures.
5. To increase privacy, although blockchain provides transparency and immutability, it may also reveal sensitive patient information. Future research should develop advanced privacy-preserving techniques, such as zero-

knowledge proofs, homomorphic encryption, and differential privacy, to ensure that patient data remain confidential while still being accessible to authorized users.

6. To increase the ability of healthcare systems, researchers can explore ways to combine blockchain with artificial intelligence (AI) and machine learning in healthcare to enable predictive analytics and personalized medicine and improve the automation of decision-making.
7. Another challenge is the cost of implementing blockchain; although there are many benefits of using blockchain, the cost is high. Researchers, in future work, should consider reducing the cost of using blockchain in healthcare, such as shared infrastructure and cloud computing, and use open source blockchain.
8. Future work can detect the use of decentralized identity management systems, such as self-confident identity (SSI), to give patients more control over their personal health data. This can enhance privacy and security by enabling comfortable data from various healthcare providers.

9. CONCLUSION

In this study, obtaining an understanding of and insights into healthcare security via BC in the EFC domain is considered significant. This study will add to such understanding and knowledge by reviewing and arranging applicable research. Hence, a few specific examples are provided and categorized into four classes: healthcare security using BC at the edge, healthcare security using BC in fog, healthcare security using BC in cloud computing, and reviews and surveys. A high volume of indispensable data was acquired by seriously perusing and investigating different review articles, such as issues, difficulties and challenges, motivation, and advantages in healthcare security. In this study, we identified issues, difficulties, and challenges and provided different suggestions to determine current and potential difficulties and issues associated with the use of BC technology in healthcare. Moreover, we have provided a methodical review that depicts BC methods in EFC healthcare. Furthermore, we have examined the weaknesses of the current methods, systems, and frameworks and determined the scope of improvements that can be used for future research studies. The results of the analysis of the previous works revealed that 50% of the papers used blockchain in healthcare for cloud computing, 25% for fog computing, 11% for edge computing and 14% for review. Additionally, the eHealth system was targeted by researchers more than other categories in all environments. For the metrics, the running time was measured by most of the papers, whereas energy consumption and cost were measured as 12% and 20%, respectively. These numbers indicate that the energy consumption and cost are not mentioned by the authors because the proposed methods require high energy and cost, which is the main issue for blockchain in EFC. The open issues and future research directions have been lined through the current knowledge shown in this review through a synthesis structure created by integrating insight from existing obstacles, recommendations and newly identified insights. For future work, the solving latency and resource constraints depend on the creation of energy-efficient consensus techniques designed for the edge and fog computing layers. Particularly in situations with wearable medical equipment and remote monitoring, lightweight blockchain designs with safe data offloading, dynamic authentication, and privacy-preserving analytics need to be investigated. Moreover, future studies should use multidisciplinary methods that combine healthcare policy, ethics, and organizational management to address sociotechnical issues, including regulatory compliance, data ownership, and institutional acceptance resistance.

Conflicts of interest

The authors declare no conflicts of interest.

Funding

This research received no external funding.

Acknowledgment

The authors would like to thank their respective universities for their support. They also acknowledge the contributions of colleagues and reviewers whose feedback helped improve the quality of this manuscript.

REFERENCES

- [1] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology," *Journal of Supercomputing*, vol. 77, no. 8, pp. 7916–7955, Aug. 2021, doi: 10.1007/s11227-020-03570-x.

- [2] S. Mubeen, P. Nikolaidis, A. Didic, H. Pei-Breivold, K. Sandstrom, and M. Behnam, "Delay Mitigation in Offloaded Cloud Controllers in Industrial IoT," *IEEE Access*, vol. 5, pp. 4418–4430, 2017, doi: 10.1109/ACCESS.2017.2682499.
- [3] A. A. Mutlag, M. K. Abd Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, Jan. 2019, doi: 10.1016/j.future.2018.07.049.
- [4] A. M. Elmisery, S. Rho, and M. Aborizka, "A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services," *Cluster Comput*, vol. 22, no. 1, pp. 1611–1638, 2019.
- [5] H. Hua, Y. Li, T. Wang, N. Dong, W. Li, and J. Cao, "Edge Computing with Artificial Intelligence: A Machine Learning Perspective," *ACM Comput Surv*, vol. 55, no. 9, Sep. 2023, doi: 10.1145/3555802.
- [6] C. Kotronis *et al.*, "Evaluating Internet of Medical Things (IoMT)-Based Systems from a Human-Centric Perspective," Dec. 01, 2019, *Elsevier B.V.* doi: 10.1016/j.iot.2019.100125.
- [7] L. Soltanisehat, R. Alizadeh, H. Hao, and K. K. R. Choo, "Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review," Jan. 01, 2023, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/TEM.2020.3013507.
- [8] J. Adler-Milstein, A. J. Holmgren, P. Kralovec, C. Worzala, T. Searcy, and V. Patel, "Electronic health record adoption in US hospitals: The emergence of a digital 'advanced use' divide," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1142–1148, Nov. 2017, doi: 10.1093/jamia/ocx080.
- [9] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud Migration Research: A Systematic Review," *IEEE Transactions on Cloud Computing*, vol. 1, no. 2, pp. 142–157, Jul. 2013, doi: 10.1109/TCC.2013.10.
- [10] Z. J. Al-Araji, S. S. S. Ahmad, N. Kausar, A. Farhani, E. Ozbilgekahveci, and T. Cagin, "Fuzzy Theory in Fog Computing: Review, Taxonomy, and Open Issues," *IEEE Access*, vol. 10, pp. 126931–126956, 2022, doi: 10.1109/ACCESS.2022.3225462.
- [11] M. Haghi Kashani and E. Mahdipour, "Load Balancing Algorithms in Fog Computing: A Systematic Review," *IEEE Trans Serv Comput*, 2022, doi: 10.1109/TSC.2022.3174475.
- [12] Z. J. Al-Araji, S. S. S. Ahmad, N. Kausar, A. Farhani, E. Ozbilgekahveci, and T. Cagin, "Fuzzy Theory in Fog Computing: Review, Taxonomy, and Open Issues," 2022, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2022.3225462.
- [13] Z. J. Al-Araji, S. S. S. Ahmad, H. M. Farhood, A. A. Mutlag, and M. S. Al-Khaldee, "Attack graph-based security metrics: concept, taxonomy, challenges and open issues," in *BIO Web of Conferences*, EDP Sciences, Apr. 2024. doi: 10.1051/bioconf/20249700085.
- [14] H. Rafique, M. A. Shah, S. U. Islam, T. Maqsood, S. Khan, and C. Maple, "A Novel Bio-Inspired Hybrid Algorithm (NBIHA) for Efficient Resource Management in Fog Computing," *IEEE Access*, vol. 7, pp. 115760–115773, 2019, doi: 10.1109/ACCESS.2019.2924958.
- [15] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An Overview on Edge Computing Research," 2020, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2020.2991734.
- [16] H. A. Alharbi and M. Aldossary, "Energy-Efficient Edge-Fog-Cloud Architecture for IoT-Based Smart Agriculture Environment," *IEEE Access*, vol. 9, pp. 110480–110492, 2021, doi: 10.1109/ACCESS.2021.3101397.
- [17] M. Hartmann, U. S. Hashmi, and A. Imran, "Edge computing in smart health care systems: Review, challenges, and research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3710.
- [18] A. Rancea, I. Anghel, and T. Cioara, "Edge Computing in Healthcare: Innovations, Opportunities, and Challenges," *Future Internet*, vol. 16, no. 9, p. 329, Sep. 2024, doi: 10.3390/fi16090329.
- [19] I. Singh, A. Kaur, P. Agarwal, and S. M. Idrees, "Enhancing Security and Transparency in Online Voting through Blockchain Decentralization," *SN Comput Sci*, vol. 5, no. 7, Oct. 2024, doi: 10.1007/s42979-024-03286-2.
- [20] H. S. Malallah, R. Qashi, L. M. Abdulrahman, M. A. Omer, and A. A. Yazdeen, "Performance Analysis of Enterprise Cloud Computing: A Review," *Journal of Applied Science and Technology Trends*, vol. 4, no. 01, pp. 01–12, Feb. 2023, doi: 10.38094/jastt401139.
- [21] L. Griebel *et al.*, "A scoping review of cloud computing in healthcare," *BMC Med Inform Decis Mak*, vol. 15, no. 1, 2015, doi: 10.1186/s12911-015-0145-7.
- [22] Q. Xia, E. B. Sifah, K. O. 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, Jul. 2017, doi: 10.1109/ACCESS.2017.2730843.
- [23] C. Zhang and Y. Chen, "A review of research relevant to the emerging industry trends: Industry 4.0, iot, blockchain, and business analytics," Mar. 01, 2020, *World Scientific*. doi: 10.1142/S2424862219500192.
- [24] A. Gorkhali, L. Li, and A. Shrestha, "Blockchain: a literature review," *Journal of Management Analytics*, vol. 7, no. 3, pp. 321–343, Jul. 2020, doi: 10.1080/23270012.2020.1801529.

- [25] W. Rafique, M. Khan, S. Khan, and J. S. Ally, "SecureMed: A Blockchain-Based Privacy-Preserving Framework for Internet of Medical Things," *Wirel Commun Mob Comput*, vol. 2023, 2023, doi: 10.1155/2023/2558469.
- [26] G. Piccardo, L. Conti, and A. Martino, "Blockchain Technology and Its Potential to Benefit Public Services Provision: A Short Survey," Aug. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/fi16080290.
- [27] K. K. Vaigandla, M. Siluveru, M. Kesoju, and R. Karne, "Review on Blockchain Technology: Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications," Dec. 10, 2023, *Mesopotamian Academic Press*. doi: 10.58496/MJCS/2023/012.
- [28] P. Bustamante *et al.*, "Government by Code? Blockchain Applications to Public Sector Governance," 2022, *Frontiers Media SA*. doi: 10.3389/fbloc.2022.869665.
- [29] F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, "Blockchain from the perspective of privacy and anonymisation: A systematic literature review," *Sensors (Switzerland)*, vol. 20, no. 24, pp. 1–21, Dec. 2020, doi: 10.3390/s20247171.
- [30] V. Buterin, J. Iillum, M. Nadler, F. Schär, and A. Soleimani, "Blockchain privacy and regulatory compliance: Towards a practical equilibrium," *Blockchain: Research and Applications*, vol. 5, no. 1, Mar. 2024, doi: 10.1016/j.bcr.2023.100176.
- [31] D. C. G. Valadares, A. Perkusich, A. F. Martins, M. B. M. Kamel, and C. Seline, "Privacy-Preserving Blockchain Technologies," Aug. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/s23167172.
- [32] Y. Li, J. Wang, Z. Zhao, and D. Lv, "Hague: a hybrid scaling stateless blockchain," *Peer Peer Netw Appl*, vol. 18, no. 1, pp. 1–16, 2025.
- [33] A. Alkhateeb, C. Catal, G. Kar, and A. Mishra, "Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review," Feb. 01, 2022, *MDPI*. doi: 10.3390/s22041304.
- [34] X. Chen, S. He, L. Sun, Y. Zheng, and C. Q. Wu, "A Survey of Consortium Blockchain and Its Applications," *Cryptography*, vol. 8, no. 2, p. 12, 2024.
- [35] L. Qu, F. Wen, H. Huang, and Z. Wang, "Aggregation-chain: a consortium blockchain based multi-chain data sharing framework with efficient query," *Cluster Comput*, vol. 28, no. 1, pp. 1–16, 2025.
- [36] S. Lu *et al.*, "CCIO: a cross-chain interoperability approach for consortium blockchains based on oracle," *Sensors*, vol. 23, no. 4, p. 1864, 2023.
- [37] S. Sharma, H. K. Shakya, and A. Mishra, "Medical Data Security Using Blockchain With Soft Computing Techniques: A Review," in *The Internet of Medical Things (IoMT): Healthcare Transformation*, Wiley, 2021, pp. 269–288. doi: 10.1002/9781119769200.ch14.
- [38] J. Almalki, "State-of-the-Art Research in Blockchain of Things for HealthCare," *Arab J Sci Eng*, 2023, doi: 10.1007/s13369-023-07896-5.
- [39] M. Mustafa, M. Alshare, D. Bhargava, R. Neware, B. Singh, and P. Ngulube, "Perceived Security Risk Based on Moderating Factors for Blockchain Technology Applications in Cloud Storage to Achieve Secure Healthcare Systems," *Comput Math Methods Med*, vol. 2022, 2022, doi: 10.1155/2022/6112815.
- [40] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry (Basel)*, vol. 10, no. 10, 2018, doi: 10.3390/sym10100470.
- [41] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Applied Sciences (Switzerland)*, vol. 9, no. 9, May 2019, doi: 10.3390/app9091736.
- [42] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," Nov. 01, 2017, *Oxford University Press*. doi: 10.1093/jamia/ocx068.
- [43] D. Randall, P. Goel, and R. Abujamra, "Blockchain Applications and Use Cases in Health Information Technology," *J Health Med Inform*, vol. 08, no. 03, 2017, doi: 10.4172/2157-7420.1000276.
- [44] N. Kshetri, "Blockchain and Electronic Healthcare Records [Cybertrust]," *Computer (Long Beach Calif)*, vol. 51, no. 12, pp. 59–63, Dec. 2018, doi: 10.1109/MC.2018.2880021.
- [45] N. S. Talwandi and N. Kaur Walia, "Enhancing Security of Cloud Computing Transaction using Blockchain," in *2023 International Conference on Advances in Computation, Communication and Information Technology, ICAICCIT 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1133–1139. doi: 10.1109/ICAICCIT60255.2023.10466075.
- [46] A. K. Bashir *et al.*, "A Survey on Federated Learning for the Healthcare Metaverse: Concepts, Applications, Challenges, and Future Directions," *IEEE Internet Things J*, vol. 10, no. 24, pp. 21873–21891, Apr. 2023, [Online]. Available: <http://arxiv.org/abs/2304.00524>
- [47] M. Humayun, A. Alsirhani, F. Alserhani, M. Shaheen, and G. Alwakid, "Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency," *Journal of Cloud Computing*, vol. 13, no. 1, Dec. 2024, doi: 10.1186/s13677-024-00602-2.
- [48] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, and A. Refaey, "SSHealth: Toward Secure, Blockchain-Enabled Healthcare Systems," *IEEE Netw*, vol. 34, no. 4, Jun. 2020, doi: 10.1109/MNET.011.1900553.

- [49] J. Singh and K. Ghai, "Security and Privacy Mechanisms for the New Generation Healthcare Applications Using Blockchain Technology," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICRITO51393.2021.9596107.
- [50] R. I. Emon *et al.*, "Privacy-preserved Secure Medical Data Sharing Using Hierarchical Blockchain in Edge Computing," *Annals of Emerging Technologies in Computing*, vol. 6, no. 4, pp. 38–48, Oct. 2022, doi: 10.33166/AETiC.2022.04.005.
- [51] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, and E. Harjula, "Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications," *Sensors*, vol. 21, no. 7, Apr. 2021, doi: 10.3390/s21072502.
- [52] Z. Ming, M. Zhou, L. Cui, and S. Yang, "FAITH: A Fast Blockchain-Assisted Edge Computing Platform for Healthcare Applications," *IEEE Trans Industr Inform*, vol. 18, no. 12, pp. 9217–9226, Dec. 2022, doi: 10.1109/TII.2022.3166813.
- [53] Y. Cheng, B. Gong, Z. J. Jia, Y. Y. Yang, Y. He, and X. Zhang, "Efficient and Secure Cross-Domain Sharing of Blockchain Electronic Medical Records Based on Edge Computing," *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/7310771.
- [54] A. H. Sharmila and N. Jaisankar, "Edge Intelligent Agent Assisted Hybrid Hierarchical Blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT," *Computer Networks*, vol. 200, Dec. 2021, doi: 10.1016/j.comnet.2021.108508.
- [55] H. Reffad, A. Djenaoui, and A. Alti, "Distributed Secure Services Based on IoT and Blockchain for e-Health Remote Care," in *Proc. Int. Conf. Computer Science's Complex Systems and Their Applications*, 2020.
- [56] B. S. Egala, A. K. Pradhan, S. Gupta, K. S. Sahoo, M. Bilal, and K. S. Kwak, "CoviBlock: A Secure Blockchain-Based Smart Healthcare Assisting System," *Sustainability (Switzerland)*, vol. 14, no. 24, Dec. 2022, doi: 10.3390/su142416844.
- [57] Y. Li and M. Tang, "Blockchain-powered distributed data auditing scheme for cloud-edge healthcare system," *Cyber Security and Applications*, vol. 1, p. 100017, Dec. 2023, doi: 10.1016/j.csa.2023.100017.
- [58] I. Ahmad, S. Abdullah, and A. Ahmed, "IoT-fog-based healthcare 4.0 system using blockchain technology," *Journal of Supercomputing*, vol. 79, no. 4, pp. 3999–4020, Mar. 2023, doi: 10.1007/s11227-022-04788-7.
- [59] S. R. Mallick, R. K. Lenka, P. K. Tripathy, D. C. Rao, S. Sharma, and N. K. Ray, "A lightweight, secure, and scalable blockchain-fog-iomt healthcare framework with ipfs data storage for healthcare 4.0," *SN Comput Sci*, vol. 5, no. 1, p. 198, 2024.
- [60] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain," *IEEE Internet Things J*, vol. 8, no. 14, pp. 11743–11757, Jul. 2021, doi: 10.1109/JIOT.2021.3058953.
- [61] J. Wu, P. Zhou, Q. Chen, Z. Xu, X. Ding, and H. Jiang, "Blockchain-Based Privacy-Aware Contextual Online Learning for Collaborative Edge-Cloud-Enabled Nursing System in Internet of Things," *IEEE Internet Things J*, vol. 10, no. 8, pp. 6703–6717, Apr. 2023, doi: 10.1109/JIOT.2021.3133653.
- [62] L. Fetjah, K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "Towards a Smart Healthcare System: An Architecture Based on IoT, Blockchain, and Fog Computing," *International Journal of Healthcare Information Systems and Informatics*, vol. 16, no. 4, 2021, doi: 10.4018/IJHISI.20211001.0a16.
- [63] J. Ren, J. Li, H. Liu, and T. Qin, "Task Offloading Strategy with Emergency Handling and Blockchain Security in SDN-Empowered and Fog-Assisted Healthcare IoT," *Tsinghua Sci Technol*, vol. 27, no. 4, pp. 760–776, 2022, doi: 10.26599/TS.
- [64] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of internet of things infrastructure for secure and smart healthcare," *Computer (Long Beach Calif)*, vol. 50, no. 7, pp. 74–79, 2018.
- [65] A. Lakhan *et al.*, "Secure blockchain assisted Internet of Medical Things architecture for data fusion enabled cancer workflow," *Internet of Things*, vol. 24, p. 100928, Dec. 2023, doi: 10.1016/j.iot.2023.100928.
- [66] A. Lakhan, M. A. Mohammed, S. Kozlov, and J. J. P. C. Rodrigues, "Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows," *Transactions on Emerging Telecommunications Technologies*, 2021, doi: 10.1002/ett.4363.
- [67] I. Ahmad, S. Abdullah, and A. Ahmed, "IoT-fog-based healthcare 4.0 system using blockchain technology," *Journal of Supercomputing*, vol. 79, no. 4, pp. 3999–4020, Mar. 2023, doi: 10.1007/s11227-022-04788-7.
- [68] M. Al Duhayyim *et al.*, "Integration of fog computing for health record management using blockchain technology," *Computers, Materials and Continua*, vol. 71, no. 2, pp. 4135–4149, 2022, doi: 10.32604/cmc.2022.022336.
- [69] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, "Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model," *Internet of Things (Netherlands)*, vol. 15, Sep. 2021, doi: 10.1016/j.iot.2021.100422.
- [70] A. H. Mayer, V. F. Rodrigues, C. A. Da Costa, R. Da Rosa Righi, A. Roehrs, and R. S. Antunes, "FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records," *IEEE Access*, vol. 9, pp. 122723–122737, 2021, doi: 10.1109/ACCESS.2021.3109822.

- [71] A. Lakhan *et al.*, “Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare,” *IEEE J Biomed Health Inform*, vol. 27, no. 2, pp. 664–672, Feb. 2023, doi: 10.1109/JBHI.2022.3165945.
- [72] M. J. Baucas, P. Spachos, and K. N. Plataniotis, “Federated Learning and Blockchain-Enabled Fog-IoT Platform for Wearables in Predictive Healthcare,” *IEEE Trans Comput Soc Syst*, vol. 10, no. 4, pp. 1732–1741, Aug. 2023, doi: 10.1109/TCSS.2023.3235950.
- [73] T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, “Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and iot based continuous glucose monitoring system for diabetes mellitus research and care,” *Sensors (Switzerland)*, vol. 19, no. 15, Aug. 2019, doi: 10.3390/s19153319.
- [74] P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry, and Y. Nam, “Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing,” *IEEE Access*, vol. 9, pp. 45706–45720, 2021, doi: 10.1109/ACCESS.2021.3065440.
- [75] C. and M. Methods in Medicine, “Retracted: Blockchain and IPFS Integrated Framework in Bilevel Fog-Cloud Network for Security and Privacy of IoMT Devices,” *Comput Math Methods Med*, vol. 2023, pp. 1–1, Aug. 2023, doi: 10.1155/2023/9851401.
- [76] A. lakhan, M. A. Mohammed, D. A. Ibrahim, and K. H. Abdulkareem, “Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment,” *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 1, pp. 1–12, Jan. 2023, doi: 10.1016/j.jksuci.2021.11.009.
- [77] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and M. Guizani, “AISCMS-FH: AI-Enabled Secure Communication Mechanism in Fog Computing-Based Healthcare,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 319–334, 2023, doi: 10.1109/TIFS.2022.3220959.
- [78] N. Alsaed, F. Nadeem, and F. Albalwy, “A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing,” *Future Generation Computer Systems*, vol. 151, pp. 162–181, Feb. 2024, doi: 10.1016/j.future.2023.09.032.
- [79] A. Karakaya and S. Akleylek, “A novel IoT-based health and tactical analysis model with fog computing,” *PeerJ Comput Sci*, vol. 7, pp. 1–34, 2021, doi: 10.7717/peerj-cs.342.
- [80] J. J. Naidu N S S and G. E. N, “A Novel Blockchain-Based Lightweight Encryption Technique in Fog Based IoT for Personal Healthcare Data Application,” *International Journal of Intelligent Systems and Applications in Engineering IJISAE*, vol. 2023, no. 3s, pp. 119–128, 2023, [Online]. Available: www.ijisae.org
- [81] O. Cheikhrouhou, K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi, “A lightweight blockchain and fog-enabled secure remote patient monitoring system,” *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100691.
- [82] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, “A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services,” *Future Generation Computer Systems*, vol. 100, pp. 569–578, Nov. 2019, doi: 10.1016/j.future.2019.05.059.
- [83] V. Mani *et al.*, “A new blockchain and fog computing model for blood pressure medical sensor data storage,” *Computers and Electrical Engineering*, vol. 102, Sep. 2022, doi: 10.1016/j.compeleceng.2022.108202.
- [84] A. Ginavane and S. Prasanna, “Integration of Ethereum Blockchain with Cloud Computing for Secure Healthcare Data Management System,” *Journal of Electrical Systems*, vol. 20, no. 4, pp. 111–124, 2024.
- [85] O. Akinola, A. Akinola, B. Oyekan, O. Oyerinde, H. Folashade Adebisi, and B. Sulaimon, “Blockchain-Enabled Security Solutions for Medical Device Integrity and Provenance in Cloud Environments,” *International Journal of Innovative Science and Research Technology (IJISRT)*, pp. 123–135, Apr. 2024, doi: 10.38124/ijisrt/IJISRT24APR225.
- [86] Y. Yang, R. hua Shi, K. Li, Z. Wu, and S. Wang, “Multiple access control scheme for EHRs combining edge computing with smart contracts,” *Future Generation Computer Systems*, vol. 129, pp. 453–463, Apr. 2022, doi: 10.1016/j.future.2021.11.002.
- [87] M. S. Rahman, F. F. Tura, and S. Mahamud, “Unlocking the Power of Blockchain for Safe and Secure Electronic Personal Information and Health Record Management with the Use of Cloud Storage,” *Institute of Electrical and Electronics Engineers (IEEE)*, Aug. 2023, pp. 495–500. doi: 10.1109/sist58284.2023.10223495.
- [88] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, “Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach,” *IEEE Trans Netw Sci Eng*, vol. 9, no. 1, pp. 271–281, 2022, doi: 10.1109/TNSE.2021.3101842.
- [89] 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 Trans Pervasive Health Technol*, vol. 4, no. 15, 2018, doi: 10.4108/eai.24-7-2018.159338.
- [90] F. Al-Quayed, M. Humayun, and S. Tahir, “Towards a Secure Technology-Driven Architecture for Smart Health Insurance Systems: An Empirical Study,” *Healthcare (Switzerland)*, vol. 11, no. 16, Aug. 2023, doi: 10.3390/healthcare11162257.

- [91] S. Cao, X. Zhang, and R. Xu, "Toward secure storage in cloud-based ehealth systems: A blockchain-assisted approach," *IEEE Netw*, vol. 34, no. 2, pp. 64–70, Mar. 2020, doi: 10.1109/MNET.001.1900173.
- [92] H. B. Mahajan and A. A. Junnarkar, "Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing," *Multimed Tools Appl*, Nov. 2023, doi: 10.1007/s11042-023-15204-4.
- [93] H. Wu, A. D. Dwivedi, and G. Srivastava, "Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 17, no. 2s, Jun. 2021, doi: 10.1145/3408321.
- [94] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Comput Appl*, vol. 32, no. 3, pp. 639–647, Feb. 2020, doi: 10.1007/s00521-018-3915-1.
- [95] H. Kaur, R. Jameel, M. A. Alam, B. Alankar, and V. Chang, "Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography," *Journal of Enterprise Information Management*, vol. 36, no. 4, pp. 861–878, Jun. 2023, doi: 10.1108/JEIM-02-2021-0084.
- [96] J. Cui, L. Duan, W. Ni, and C. Li, "Secure Cross-domain Medical Data Sharing based on Distributed Cloud and Blockchain Services," in *2023 IEEE International Conference on Web Services (ICWS)*, Institute of Electrical and Electronics Engineers (IEEE), Sep. 2023, pp. 698–700. doi: 10.1109/icws60048.2023.00089.
- [97] H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain," *J Med Syst*, vol. 42, no. 8, Aug. 2018, doi: 10.1007/s10916-018-0994-6.
- [98] L. Cui, Z. Xiao, F. Chen, H. Dai, and J. Li, "Protecting Vaccine Safety: An Improved, Blockchain-Based, Storage-Efficient Scheme," *IEEE Trans Cybern*, vol. 53, no. 6, pp. 3588–3598, Jun. 2023, doi: 10.1109/TCYB.2022.3163743.
- [99] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, Jun. 2019, doi: 10.1016/j.future.2018.12.044.
- [100] S. Juyal, S. Sharma, A. Harbola, and A. S. Shukla, "Privacy and Security of IoT based Skin Monitoring System using Blockchain Approach," in *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 2020, pp. 1–5.
- [101] H. Tan, P. Kim, and I. Chung, "Practical homomorphic authentication in cloud-assisted vanets with blockchain-based healthcare monitoring for pandemic control," *Electronics (Switzerland)*, vol. 9, no. 10, pp. 1–21, Oct. 2020, doi: 10.3390/electronics9101683.
- [102] J. Zhao, W. Wang, D. Wang, X. Wang, and C. Mu, "PMHE: a wearable medical sensor assisted framework for health care based on blockchain and privacy computing," *Journal of Cloud Computing*, vol. 11, no. 1, Dec. 2022, doi: 10.1186/s13677-022-00373-8.
- [103] A. K. Bapatla, S. P. Mohanty, E. Kougianos, and D. Puthal, "PharmaChain 2.0: A Blockchain Framework for Secure Remote Monitoring of Drug Environmental Parameters in Pharmaceutical Cold Supply Chain," in *Proceedings - 2022 IEEE International Symposium on Smart Electronic Systems, iSES 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 185–190. doi: 10.1109/iSES54909.2022.00046.
- [104] J. Priya and C. Palanisamy, "Novel Block Chain Technique for Data Privacy and Access Anonymity in Smart Healthcare," *Intelligent Automation and Soft Computing*, vol. 35, no. 1, pp. 243–259, 2023, doi: 10.32604/iasc.2023.025719.
- [105] S. Badr, I. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," in *Procedia Computer Science*, Elsevier B.V., 2018, pp. 159–166. doi: 10.1016/j.procs.2018.10.162.
- [106] Q. Xia, E. B. Sifah, K. O. 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, Jul. 2017, doi: 10.1109/ACCESS.2017.2730843.
- [107] M. George and A. Mary Chacko, "MediTrans—Patient-centric interoperability through blockchain," *International Journal of Network Management*, vol. 32, no. 3, May 2022, doi: 10.1002/nem.2187.
- [108] H. Pan, Y. Zhang, X. Si, Z. Yao, and L. Zhao, "MDS2-C3PF: A Medical Data Sharing Scheme with Cloud-Chain Cooperation and Policy Fusion in IoT," *Symmetry (Basel)*, vol. 14, no. 12, Dec. 2022, doi: 10.3390/sym14122479.
- [109] S. Niu, M. Song, L. Fang, F. Yu, S. Han, and C. Wang, "Keyword search over encrypted cloud data based on blockchain in smart medical applications," *Comput Commun*, vol. 192, pp. 33–47, Aug. 2022, doi: 10.1016/j.comcom.2022.05.018.
- [110] A. A. Amponsah, A. F. Adekoya, and B. A. Weyori, "Improving the Financial Security of National Health Insurance using Cloud-Based Blockchain Technology Application," *International Journal of Information Management Data Insights*, vol. 2, no. 1, Apr. 2022, doi: 10.1016/j.jjime.2022.100081.
- [111] A. Thamrin and H. Xu, "Hierarchical Cloud-Based Consortium Blockchains for Healthcare Data Storage," in *Proceedings - 2021 21st International Conference on Software Quality, Reliability and Security Companion, QRS-C 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 644–651. doi: 10.1109/QRS-C55045.2021.00098.

- [112] H. Kurdi, S. Alsalamah, A. Alatawi, S. Alfaraj, L. Altoaimy, and S. H. Ahmed, "Healthybroker: A trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services," *Electronics (Switzerland)*, vol. 8, no. 6, Jun. 2019, doi: 10.3390/electronics8060602.
- [113] S. Li *et al.*, "HealthFort: A Cloud-Based Ehealth System With Conditional Forward Transparency and Secure Provenance Via Blockchain," *IEEE Trans Mob Comput*, Nov. 2022, doi: 10.1109/TMC.2022.3199048.
- [114] A. Mubarakali, "Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN(SRHB)Approach," *Mobile Networks and Applications*, vol. 25, no. 4, pp. 1330–1337, Aug. 2020, doi: 10.1007/s11036-020-01551-1.
- [115] M. Sumathi, S. P. Raja, N. Vijayaraj, and M. Rajkamal, "Healthcare Data Collection Using Internet of Things and Blockchain Based Decentralized Data Storage," *Advances in Distributed Computing and Artificial Intelligence Journal*, vol. 12, no. 1, 2023, doi: 10.14201/adcaij.28612.
- [116] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, "Flexible and Efficient Blockchain-Based ABE Scheme with Multi-Authority for Medical on Demand in Telemedicine System," *IEEE Access*, vol. 7, pp. 88012–88025, 2019, doi: 10.1109/ACCESS.2019.2925625.
- [117] C. Eben and S. Nagarajan, "Flexible Access Control Mechanism for Cloud stored EHR using Consortium Blockchain," *International Journal of System Assurance Engineering and Management*, pp. 1–16, 2022.
- [118] N. R. Sivakumar, S. A. Ghorashi, N. Ahmed, H. E. A. Elsrej, and S. Basheer, "Fischer machine learning for mobile cloud computing in eHealth systems using blockchain mechanism," *Microprocess Microsyst*, vol. 103, Nov. 2023, doi: 10.1016/j.micpro.2023.104969.
- [119] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "FIDChain: Federated Intrusion Detection System for Blockchain-Enabled IoT Healthcare Applications," *Healthcare (Switzerland)*, vol. 10, no. 6, Jun. 2022, doi: 10.3390/healthcare10061110.
- [120] Z. Pang, Y. Yao, Q. Li, X. Zhang, and J. Zhang, "Electronic Health Records Sharing Model based on Blockchain with Checkable State PBFT Consensus Algorithm," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3186682.
- [121] R. Mishra, D. Ramesh, D. R. Edla, and L. Qi, "DS-Chain: A secure and auditable multi-cloud assisted EHR storage model on efficient deletable blockchain," *J Ind Inf Integr*, vol. 26, Mar. 2022, doi: 10.1016/j.jii.2021.100315.
- [122] M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of secure protocol for cloud-assisted electronic health record system using blockchain," *Sensors (Switzerland)*, vol. 20, no. 10, May 2020, doi: 10.3390/s20102913.
- [123] S. Son, J. Lee, M. Kim, S. Yu, A. K. Das, and Y. Park, "Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain," *IEEE Access*, vol. 8, pp. 192177–192191, 2020, doi: 10.1109/ACCESS.2020.3032680.
- [124] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Inf Sci (N Y)*, vol. 485, pp. 427–440, Jun. 2019, doi: 10.1016/j.ins.2019.02.038.
- [125] X. Zhu, J. Shi, and C. Lu, "Cloud health resource sharing based on consensus-oriented blockchain technology: Case study on a breast tumor diagnosis service," *J Med Internet Res*, vol. 21, no. 7, Jul. 2019, doi: 10.2196/13767.
- [126] T. Benil and J. Jasper, "Cloud based security on outsourcing using blockchain in E-health systems," *Computer Networks*, vol. 178, Sep. 2020, doi: 10.1016/j.comnet.2020.107344.
- [127] L. Yang, X. Y. Liu, and J. S. Kim, "Cloud-based Livestock Monitoring System Using RFID and Blockchain Technology," in *Proceedings - 2020 7th IEEE International Conference on Cyber Security and Cloud Computing and 2020 6th IEEE International Conference on Edge Computing and Scalable Cloud, CSCloud-EdgeCom 2020*, Institute of Electrical and Electronics Engineers Inc., Aug. 2020, pp. 240–245. doi: 10.1109/CSCloud-EdgeCom49738.2020.00049.
- [128] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019, doi: 10.1109/ACCESS.2019.2943153.
- [129] H. Gao, H. Huang, L. Xue, F. Xiao, and Q. Li, "Blockchain-Enabled Fine-Grained Searchable Encryption with Cloud-Edge Computing for Electronic Health Records Sharing," *IEEE Internet Things J*, vol. 10, no. 20, pp. 18414–18425, Oct. 2023, doi: 10.1109/JIOT.2023.3279893.
- [130] A. EL Azzaoui, P. K. Sharma, and J. H. Park, "Blockchain-based delegated Quantum Cloud architecture for medical big data security," *Journal of Network and Computer Applications*, vol. 198, Feb. 2022, doi: 10.1016/j.jnca.2021.103304.
- [131] D. Ramesh, R. Mishra, P. K. Atrey, D. R. Edla, S. Misra, and L. Qi, "Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage," *Alexandria Engineering Journal*, vol. 68, pp. 205–226, Apr. 2023, doi: 10.1016/j.aej.2023.01.012.
- [132] C. Qin, L. Wu, W. Meng, Z. Xu, S. Li, and H. Wang, "A privacy-preserving blockchain-based tracing model for virus-infected people in cloud," *Expert Syst Appl*, vol. 211, Jan. 2023, doi: 10.1016/j.eswa.2022.118545.
- [133] X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, "A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRS sharing in the cloud," *IEEE Access*, vol. 8, pp. 170713–170731, 2020, doi: 10.1109/ACCESS.2020.3025060.

- [134] J. A. Santos, P. R. M. Inácio, and B. M. C. Silva, "Towards the Use of Blockchain in Mobile Health Services and Applications," *J Med Syst*, vol. 45, no. 2, Feb. 2021, doi: 10.1007/s10916-020-01680-w.
- [135] C. Awasthi, M. Nawal, and P. K. Mishra, "Security Concerns of Fog Computing in Field of Healthcare using Blockchain: A Review," in *Proceedings - International Conference on Communication, Information and Computing Technology, ICCICT 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICCICT50803.2021.9510166.
- [136] Ž. Kodrič, S. Vrhovec, and L. Jelovčan, "Securing edge-enabled smart healthcare systems with blockchain: A systematic literature review," *Journal of Internet Services and Information Security*, vol. 11, no. 4, pp. 19–32, Nov. 2021, doi: 10.22667/JISIS.2021.11.30.019.
- [137] H. Makina and A. Ben Letaifa, "Bringing intelligence to Edge/Fog in Internet of Things-based healthcare applications: Machine learning/deep learning-based use cases," *International Journal of Communication Systems*, vol. 36, no. 9, Jun. 2023, doi: 10.1002/dac.5484.
- [138] A. Mudheher Badr, L. Chaari Fourati, and S. Ayed, "Investigation on the Integrated Cloud and BlockChain (ICBC) Technologies to Secure Healthcare Data Management Systems," in *Proceedings - International Conference on Developments in eSystems Engineering, DeSE*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 19–26. doi: 10.1109/DeSE58274.2023.10100065.
- [139] R. Kothari, "Integration of Blockchain and Edge Computing in Healthcare: Accountability and Collaboration," 2023, doi: 10.22545/2020/00230.
- [140] Y. Zhang and D. Wang, "Integrating blockchain technology and cloud services in healthcare: a security and privacy perspective," *Proceedings of the Indian National Science Academy*, 2023, doi: 10.1007/s43538-023-00202-9.
- [141] F. Firouzi *et al.*, "Fusion of IoT, AI, Edge-Fog-Cloud, and Blockchain: Challenges, Solutions, and a Case Study in Healthcare and Medicine," *IEEE Internet Things J*, vol. 10, no. 5, pp. 3686–3705, Mar. 2023, doi: 10.1109/JIOT.2022.3191881.
- [142] M. K. I. Rahmani *et al.*, "Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review," 2022, *Hindawi Limited*. doi: 10.1155/2022/9766844.
- [143] S. Alam *et al.*, "Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration," Nov. 01, 2022, *MDPI*. doi: 10.3390/su142215312.
- [144] M. M. Kamruzzaman, B. Yan, M. N. I. Sarker, O. Alruwaili, M. Wu, and I. Alrashdi, "Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities," *J Healthc Eng*, vol. 2022, 2022, doi: 10.1155/2022/9957888.
- [145] C. Awasthi, S. Prakash Awasthi, and P. K. Mishra, "A review on FOG supported architecture in healthcare using blockchain," *J. Integr. Sci. Technol*, vol. 12, no. 1, pp. 721–727, 2024, [Online]. Available: <http://pubs.thesciencein.org/jist>
- [146] H. Kaur, M. A. Alam, R. Jameel, A. Kumar Mourya, and V. Chang, "A Proposed Solution and Future Direction for Blockchain based Heterogeneous Medicare data in Cloud Environment," *J Med Syst*, vol. 2018, no. 4, pp. 1–11, 2018.