International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Encrypting the Electronic Health Record using the Cloud Computing and Blockchain Technologies

Ebtisam Ali Abdullah[1], Anwar Al Shamiri[2], Abdualmajed A. G. Al-Khulaidi[3]

Submitted: 02/12/2023 **Revised**: 11/01/2024 **Accepted**: 22/01/2024

Abstract: Although safeguarding electronic health records (EHRs) is crucial, there has yet to be a thorough and exhaustive investigation into EHR protection methods specifically within the context of cloud computing and blockchain. The objective of this article is to bridge that gap by conducting a systematic review of the literature on EHR protection mechanisms in cloud and blockchain environments. The results are presented in the form of a traditional taxonomy, which identifies the most recent approaches taken to address this important issue and highlights any remaining unresolved concerns. The classification system introduced in this study is divided into four main categories: algorithms used for safeguarding electronic health records and the platforms utilized in blockchain technology, factors employed to assess the effectiveness of EHR protection, and lastly, tools implemented to ensure the security of electronic health records in cloud computing and blockchain environments. We conducted a review of scientific articles spanning from 2010 to 2022 specifically addressing the safeguarding of electronic health records in cloud computing environments. Additionally, we surveyed scientific articles from 2017 to 2023 that focused on the protection of EHRs in both cloud computing environments and blockchain technology.
In cloud computing, security of electronic health records and minimizing communication costs are critical factors in ensuring security and the timely sharing of EHRs to potentially save a patient's life. These areas have been classified into three categories: approximate, exact, and hybrid methods. Furthermore, this article explores EHR protection measures while also taking into account the advantages and limitations of EHR protection mechanisms within networks.

Keywords: *Cloud Computing, Electronic health records, Blockchain.*

1. Introduction

The traditional model for storing Electronic Health Records (EHRs) with the assistance of cloud technology involves a cloud-based system that offers patients and healthcare organizations an efficient and user-friendly way to manage their sensitive EHRs[3], However, since EHRs contain highly confidential and critical information, the security and privacy of outsourced EHRs often pose challenges for cloud-based storage systems [4]. To protect patients' privacy against internal threats, the entire EHRs are encrypted before outsourcing. Over time, multiple strategies have been proposed to guarantee the confidentiality and integrity of outsourced Electronic Health Records (EHRs) within a cloud-based framework. A review of existing schemes by Zhang et al. [5] found that a significant portion of the EHRs stored by cloud service providers (CSP) are duplicates. In order to minimize the storage overhead for Cloud Service Providers (CSPs), a proposal was made by the authors in [5] for an efficient model that allows CSPs to eliminate duplicate Electronic Health Records (EHRs), thereby reducing storage costs. Wei et al. [6] introduced a secure EHR-sharing model based on the CPABE scheme within the cloud paradigm. Their model achieved user revocation, EHR confidentiality, and key delegation for users. However, user revocation is per-formed periodically to ensure security against internal threats posed by malicious users, and the model utilized a less expressive LSSS access structure. While these methodologies offer secure and efficient EHR storage within CSPs, challenges still remain, such as preventing internal adversaries and addressing CSP failures or breakdowns.

In the last few years, there has been a notable increase in interest in using blockchain technology to improve security in cloud models. Alongside these efforts, numerous advancements in blockchain-related techniques have been introduced for current cloud environment models.Traditional security requirements, such as privacy protection, data protection, communication protection, and access control, are essential considerations. The highly centralized and flexible architecture of the cloud environment model allows for centralized pro-cessing of security requirements, resulting in guaranteed security benefits. How-ever, there are instances of dishonest behavior that can occur in the cloud envi-ronment, such as unsuccessful deletion of data, inaccurate services provided during cloud service transactions by CSPs, and

[1,2,3]*Sana'a University, Yemen*
ORCID ID : 0009-0003-7448-7229
** Corresponding Author Email: ibt.alselwi@su.edu.ye*
[2]*anwarsaif@su.edu.ye*
[3]*alkhulaidi@su.edu.ye*
[1]*Information Technology,* [2]*Information Systems,* [3]*Software Engineering*

unguaranteed Service Level Agreements (SLAs) of the cloud. Consequently, it's crucial to take data operation security issues, audit problems , log security problems, and data source security challenges in the cloud seriously. To address these concerns, cloud providers must offer security services like secure authentication, secure auditing, identity manage-ment, secure access control, and data encryption [5].Subsequent paragraphs, however, are indented.

1.1. Blockchain

The blockchain represents a novel solution to the challenges posed by centralized security measures for storing and sharing data in cloud computing, as high-lighted in various sources [7] [8] [2], it introduces a modern paradigm for information documentation on the internet and has potential applications in a wide range of are-as, including social networks, online shopping, voting systems, games [9] [10], messengers, storage platforms, online education, and prediction markets [11] [12]. The blockchain can accommodate various types of data, including medical re-ports sharing, money transfers, individual identities, ownership[13] [14], and sensitive information. Fig. 1 provides a step-by-step depiction of how blockchain technology operates [13] [15].

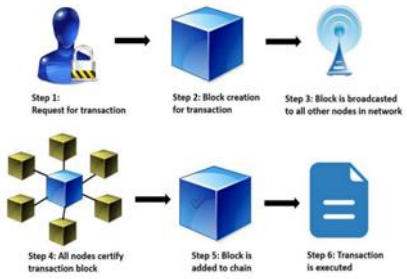


Fig. 1. Step-by-step blockchain working[2]

1.1.1 Blockchain Characteristics

The blockchain has some characteristics such as encryption, decentralization , tokenization ,immutability and distribution [3]

1. Encryption allows for safe and semi-anonymous recording of data with participants using pseudonyms. Participants maintain control over their personal identification and only share what is necessary for a transaction [4].

2. Immutability: finished transactions are timestamped, cryptographically signed, and sequentially appended to the ledger [5]. Records cannot be changed or altered unless all participants concur that it is required.

3. The process of tokenization, in which value is exchanged for tokens that can stand in for a variety of asset classes, including cash, data units, and user identities. Tokenization is how blockchain expresses and allows for a native value that can be traded in currency [6].

4. Decentralization, whereby no single entity controls or dictates the rules to a majority of nodes. A consensus method verifies and authorizes transactions, eliminating the need for a central network administrator. Built-in attributes in blockchain technology include member pseudonymity [7], automation usability [8] , and peers' participation in versatility development [9].

5.the distributed network, in which nodes that uphold the business rules of the blockchain are operated by blockchain members connected by a distributed network. A complete copy of the ledger is also kept on nodes, and it updates automatically as new transactions take place. [10].Blockchain technology doesn't store information at a central point like traditional security methods [11] [12] . Instead, multiple copies of the same data are stored in various locations and on various devices, making it a distributed technology [13].

The presence of multiple copies of data ensures that the loss of any single point of storage doesn't compromise the security of the original data [14].

Moreover, if an attacker hacks and alters data at one point, multiple identical copies of the same data are accessible to retrieve the true information [15]. In summary, data is packaged into blocks, which are linked to build a chain with other blocks containing the same information [16]. This process of linking various blocks into a chain ensures that information is securely stored in a blockchain.

Once a chain of blocks is built [17] , it becomes extremely difficult to compromise the security of blockchain technology since altering a single block requires altering all other blocks in the chain.

1.1.2 Blockchain types

Three broad forms of blockchain technologies can be distinguished: federated blockchain, private blockchain, and public blockchain.

(a) The public blockchain technology is available to everyone without the need for permission [18]. In a public blockchain, any transaction is valid for all end-users[19] .

(b) private blockchain, Conversely, private blockchain is a centralized system with lower transaction costs and easier document handling, but higher security risks [20]. Examples of private blockchain technologies includes Multichain and MONAX [21].

(c) Federated blockchains, also known as Consortium Blockchains, are the opposite of public blockchain as they

do not allow everyone to access them. These blockchains are processed by a group of leaders, and privacy is superior in transactions compared to private blockchain [22] [23] .

The Cloud over Blockchain(CoB)model deploys blockchain on the cloud as a functional tool to protect data in the cloud. Blockchain over Cloud (BoC) involves using cloud computing resources to handle part of the blockchain workload. Mixed Blockchain-Cloud (MBC) represents a significant example of integrating blockchain technology with cloud environments. By employing MBC, the system efficiently tracks data usage in cloud systems and authenticates user identities utilizing blockchain's security features. In this model, the blockchain and cloud environment operate as separate, independent networks[1]. Building upon Gai's work, The blockchain and cloud environment integration models were improved and made explicit in the study [1]. Three categories of integration models exist [1]: Three scenarios are possible: (1) Cloud as a Blockchain Service (CaaBS), in which the cloud environment is managed using blockchain technology; (2) Blockchain as a Cloud Service (BaaCS), in which blockchain-based services are offered on platforms for cloud environments; and (3) MBC, which combines the two distinct networks to allow for the recording, witnessing, or verification of data from one or more layers within a cloud computing model using blockchain[1]. [1]. Regarding MBC, "witness" refers to the blockchain's practice of logging a particular piece of data's hash value as reliable proof because of the technology's immutability and security[1]. Fig. 2 shows the architectures of the CaaBS and BaaCS in the third combination, which is more complicated.

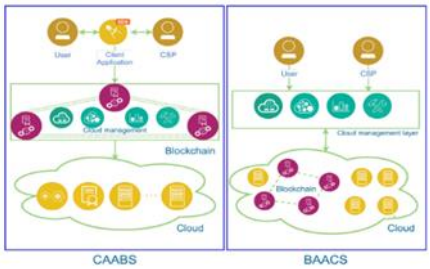


Fig. 2. BAACS and CAABS[1]

Fig. 3 demonstrates the architecture of the MBC model. When considering the third combination of blockchain and cloud for security services, the model can be classified into several types.[1]:

1) Users at the user layer have the ability to engage in the trading of cloud resources through the utilization of smart contracts. Additionally, their identity data can be effectively managed and authenticated using blockchain technology. The actions performed by users, such as sharing, uploading , deleting ,modifying, or downloading data, can be meticulously supervised, verified, and securely recorded through the implementation of blockchain. To illustrate, users can be closely monitored either by event listeners or smart contracts, as they interact with data through smart contracts. Integration of the user layer with the blockchain network is not required when a user is only a visitor to the blockchain service and is not actively involved in the network[1].

(2) The management layer can be thought of as the main center for Cloud Service Provider (CSP) administration. A decentralized platform built on blockchain technology can be created to provide cloud resource management, price settlement, and data exchange between CSPs in situations when several of them are offering resources for the same cloud. The adoption of blockchain technology allows for secure recording, careful monitoring, and verification of the activities conducted by CSPs, just like in the user layer. This layer allows users to interact with cloud resources, and at this layer, designers can combine blockchain technology with logging, access control, and identity authentication features[2].

(3) The use of blockchain technology to the cloud layer facilitates data movement, resource scheduling, and activity tracking and recording.

(4) Blockchain technology can be used in the access layer for efficient logging, authentication, and device access control. Traffic from IoT devices and the fog layer can be routed to the access layer by utilizing Software Defined Networking (SDN) technologies.

(5) The coherence of the decisions taken by the fog nodes is ensured by the integration of blockchain technology with the fog layer. Additionally, this stage of blockchain deployment offers automated supervision of IoT devices and discourages malicious activity by Byzantine nodes [2].

(6) Blockchain is frequently used in the Internet of Things layer to help with device management, authentication, and information processing for devices.

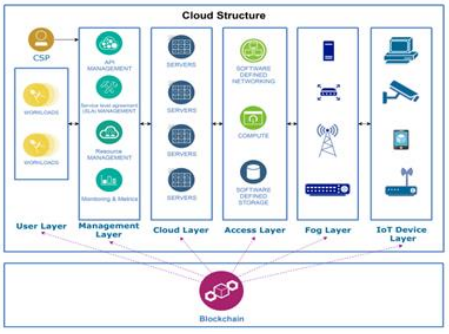


Fig. 3. Mixed blockchain-cloud[1]

Drawing from the preceding discussions, The research conducted in[1] presents a concise summary of the functions performed by the cloud within the context of blockchain, which can be outlined as follows:

(1) Client: The cloud computing acts as a client of the blockchain network, using blockchain for data storage, authentication, or witnessing.

(2) Resources that can be traded [2] .Blockchain can be used to trade, provide, and manage cloud services as a resource within a network.

(3) Platform for Management: The cloud can function as a blockchain management platform. Customers can purchase a blockchain that has already been implemented using the cloud trading platform. It is possible to build the blockchain's nodes using cloud-hosted virtual computers.

(4) Computational Resources: Additionally, the cloud can function as a valuable source of computational resources for the blockchain network, especially when certain operations necessitate extensive computation.

(5) Storage Resources: The cloud can be effectively utilized as a storage resource for blockchain, enabling the storage of data within its infrastructure.

(6) Peers: Within the blockchain network, the cloud can assume the role of a peer node. In order to facilitate data exchange and mutual oversight, this can entail the use of Cloud Service Providers (CSPs) or even a sophisticated blockchain network made up of numerous peer nodes, in which the cloud server functions as a common participant[1].

1.1.3. Blockchain based EHR storage model

Recent advancements in the utilization of blockchain for maintaining electronic health records (EHRs) in cloud-based environments have been made[24] [25] [26]. Yu et al. [27] introduced a different approach by using attribute-based signatures, which encompassed a diverse range of authorities to safeguard the EHRs' integrity. Following diagnosis, the patient's treatment details were combined into a single block. Nonetheless, healthcare data often exceeds considerable dimensions and possesses intricate relationships, necessitating comprehensive searching capabilities. To address this issue. Huang et al. [28] introduced a HealthBlock blockchain model, a patient-centric system designed to handle large amounts of data. By supporting computational infeasibility against modification attacks on stored EHRs, HealthBlock ensures data integrity. Only individuals with the correct password can access their EHRs from the blockchain.The researchers also created a proof-chain, a record-keeping system, to store manipulation logs of patients' stored EHRs. These logs can serve as evidence to protect patients' rights.

HealthBlock suffers from weaknesses against offline-dictionary and replay attacks. In 2021, Li et al. [29] advanced a blockchain-based EHR storage model, employing an attribute-based model to safeguard security while maintaining privacy. Nevertheless, the EHRs are directly stored on the blockchain at CSP, which leads to potential centralization concerns, To address this issue Li et al. [30] presented a blockchain-assisted EHR storage model, incorporating an effective provenance method that utilizes the public blockchain to guarantee EHR records' provenance. However, the limited storage capacity in blockchain blocks may result in authentication delays when EHRs' size or number expands. Hussien et al. [31] developed a "smart contract-based searchable attribute-based encryption (ABE) - SC-ABE" model that integrates smart contracts, CPABE, searchable symmetric encryption, and IPFS storage for secure EHR storage in the cloud paradigm. Despite this improved approach, the model remains susceptible to denial of service (DoS) attacks. Dagher et al. [32] developed a data management model that uses blockchain technology to securely store electronic health record (EHR) data. By generating hash-values for each EHR and storing them in blockchain blocks, this approach enhances data privacy and integrity. Additionally, the model can handle specific query requests by sending relevant transaction link information via HTTPS. Despite its efficiency, the system still faces challenges in combating distributed denial-of-service (DoS) attacks. In a separate study, Benil et al. [33] the researchers highlight the vital problem of scalability and ensuring the safety of medical records in Electronic Health Record (EHR) systems using Blockchain technology. By creating a test case, they utilize smart contracts to strengthen data scalability.

Furthermore, the researchers emphasize that while doctors can generally be trusted during the diagnosis phase, their trustworthiness is limited. In a real-world scenario, if any corrupt doctors incentivize the Cloud Service Provider (CSP) to modify the outsourced EHRs, it becomes challenging to identify such malicious activities by dishonest doctors [34].

Recently, Yang et al. [35] the attribute-based outsourcing decryption model, presented by the researchers, aims to alleviate users' computational burdens. Despite its potential benefits, the proposed system raises fresh centralization worries in the consortium blockchain framework. Critical concerns regarding the loss of control over EHR storage keys make secure EHR storage even more challenging.

Additionally, the centralization issues caused by key-escrow compound the risk of severe malfunctions and data

breaches in secure EHR storage systems.

Scheme [36] presented a decentralized EHR storage model that utilized IPFS and a permissioned blockchain for proper availability of EHR data in the cloud paradigm. Nonetheless, the scheme continued to experience limitations, including controlled access, the timeliness of EHR records, and challenges related to the functionalities of stored data in the blockchain. Chelladurai et al. [37] proposed an alternative approach to share healthcare records by employing a decentralized blockchain structure with a modified merkle hash tree (MMHT). This novel MMHT offered an efficient hashing procedure to ensure the secure validation and verification of all transactions for EHR sharing.

2. Related Work

Several studies have examined the integration of cloud computing and blockchain technologies for securing electronic health records. While blockchain technology offers robust security, its limited storage capacity presents a challenge. As a solution, records are typically encrypted and stored in the cloud computing environment, which offers ample storage space. The following studies have explored this ap-proach:

To store, share, and manage patient medical records, electronic health records (EHR) and electronic medical records (EMR) are essential. The implementation of an EHR system in a cloud environment offers many advantages, such as easy access, elastic computing resources, high-grade fault tolerance, and differentiation from other systems. However, cloud storage introduces privacy and security concerns, as cloud service providers are typically not responsible for the confidentiality and accessibility of EHRs in transit. To address these issues, various cryptographic techniques are used, including the use of Trusted Third Parties (TTPs) for authentication and auditing, as well as protecting authorized confidential data from unauthorized users. However, trust remains a significant obstacle to sharing electronic data in cloud environments, as clients are often unaware of the location of their stored data and the risks associated with third-party compromise. Blockchain technology has been implemented in cloud environments to securely move EHR data between authorized entities in order to address these issues[3]. Blockchain technology enables tamper-proof data-ledger-based features that can be given to all organizations on the network, offering a tamper-proof platform for health transaction information. This approach provides confidentiality, integrity, availability , authentication , and Enabling convenient access control to user data in the cloud, both during data transfer and when at rest.

The exchange of patient health record (PHR) information through cloud computing presents a significant security risk to user privacy, primarily due to the reliance on trustworthy third parties to share data. While many conventional cryptographic algorithms employ various keying approaches to exchange data securely, this approach compromises the privacy of consumers' data by involving a third party. To address this issue and offer secure communication without the involvement of a third party, a distributed blockchain-based (DBC) ciphertext-policy attribute-based encryption (CP-ABE) approach is employed in this study[38]. The proposed CP-ABE system is entirely dependent on elliptic curve cryptography to reduce complexity, leveraging bilinear pairing and simple scalar multiplication factors. The data requester provides dynamic attributes, and a user-centric access policy is created, allowing multiple authorities to manage the attributes and provide data access. The suggested method guarantees data confidentiality, data authentication, user authentication, and tamper-proof data. The DBC-CP-ABE method is used to provide user-centric access policies and effective key management.

The peculiar nature of medical data necessitates robust privacy protection measures. Therefore, it is crucial to design a secure solution to ensure data privacy. However, many existing schemes are based on single-server architecture, which has inherent drawbacks, such as single-point faults. While blockchain technology can help address these issues, some privacy protection deficiencies remain. To tackle these challenges, a medical data privacy protection system is proposed in [39]. Blockchain, group signatures, and asymmetric encryption are all integrated into the system to safeguard patient privacy and enable dependable medical data sharing between healthcare facilities. Through system implementation, the study shows the system's practicality and theoretically proves that it satisfies security and privacy requirements.

This work in [40] presents an enhanced structure of cloud relational databases (RDB) called BC over cloud-RDB, which is based on blockchain technology (BC). The proposed system includes a self-verification mechanism that enables clients to detect and prevent erroneous RDB manipulation. To improve cloud-RDB, two systems are proposed: agile BC-based RDB and secure BC-based RDB, both of which are distributed among multiple cloud service providers based on the Byzantine Fault Tolerance consensus. Both systems link records to each other using SHA-256, while the secure BC-based RDB uses a proof-of-work consensus to prevent data offensive operations. Based on performance and security analysis, the agile BC-

based RDB is recommended for high throughput databases, while the secure BC-based RDB is recommended for RDBs that contain sensitive data and have low throughput performance. The improved RDB is flexible and can be operated according to the data owner's specifications.

The researchers in [41] proposed a security solution against DoS and DDoS attacks in distributed and parallel (cloud) applications, with an Online Ticket Booking (OTB) application selected as an example. To ensure secure data transmission for booking tickets and payment, blockchain security is integrated into the system. The entire system is then experimented with, and the results demonstrate that blockchain security (BCS) can provide high levels of security. The dataset used in the experiment involves electronic healthcare records containing patients' private data, financial information, and medicinal details, which should not be disclosed to insurance companies, medical industries, or competitors. The processing time and time consumption are evaluated and compared with other existing systems. Based on the experimental results and discussion, it is concluded that BCS-OTB provides high performance in terms of time, cost, and improved security compared to existing approaches. The performance of BCS-OTB is summarized as having less time complexity, high success rate, low cost, and very high-performance factors.

Table 1. Research Questions

RQ1	What kind of classification is exhibited in cloud and blockchain systems to protect EHR?
RQ2	What platforms are presented in the evaluating the EHR security approaches?
RQ3	Which tools are used for assessing the security of Electronic Health Record (EHR) approaches?
RQ4	What are the usual factors assessed to evaluate EHR security approaches and promote their improvement?
RQ5	What are the open issues for research in using blockchain technology and cloud computing to protect medical records?

In traditional electronic health record (EHR) management systems, each medical service center maintains its own health records, limiting the sharing of data across diverse medical platforms. To overcome this challenge, blockchain technology has gained prominence as it facilitates the secure sharing of EHRs across platforms.However, the cost of storing the entire EHR data in blockchain makes it impractical due to its size. Cloud computing presents a potential solution, offering storage availability and scalability. Nevertheless, cloud-based EHR systems are susceptible to various attacks because sensitive data is transmitted via a public channel.To safeguard against these vulnerabilities, we propose a secure protocol for cloud-assisted EHR systems utilizing blockchain technology. The suggested protocol ensures data integrity and access control through blockchain transaction logs while the cloud server manages patient EHRs securely. This innovative approach combines the strengths of both blockchain and cloud computing, providing a reliable and efficient solution for the healthcare sector. The researchers in [42], presents a secure protocol for cloud-assisted EHR systems using blockchain technology, which includes six phases: registration, authentication, smart contract uploading, EHR storing, EHR requesting, and log.

3. Research Methodology

In this section, we provide an overview of the literature studies that are relevant to our research focus. To ensure that we identified the most pertinent articles in the areas of Cloud Computing, Blockchain, and Healthcare, we conducted a systematic literature review (SLR)based on established principles . Our approach involved defining a set of keywords and using them to create a search query, which we applied to multiple article databases:

"blockchain" AND ("cloud computing" OR "cloud") AND ("healthcare" OR "health") AND ("health record" OR "medical record" OR "EHR" OR "PHR" OR "EMR")

The a systematic literature review (SLR) method employs research questions (RQs) to establish a clear motivation for the study, with the aim of obtaining an evidence-based review of Encrypting the Electron-ic Health Record using the Cloud Computing and Blockchain technologies. Five distinct research questions are typically defined, which serve to guide the development of a search strategy for identifying and extracting relevant literature. These RQs are designed to clarify the basis for the systematic review and are presented in Table I for reference.

For the search process, studies published between 2010 and 2022 for encrypting the Electronic Health Record using the Cloud Computing were exclusively considered. Also, studies published between 2016 and 2023 for encrypting the Electronic Health Record using the Cloud Computing and Blockchain technologies were exclusively considered.

The search was conducted in Springer, Google Scholar, CMA Digital Library, ScienceDirect, and IEEE Databases,

as shown in Table 2 In addition, numerous research papers have been published as books, conferences and journals.

The search process involved the inclusion of studies that featured the search string in either their titles, abstracts, or keywords.

Table 2. Databases from which the research was taken

No	Academic Database	link
1	Springer	https://www.springer.com/gp
2	Google Scholar	https://scholar.google.com/
3	CMA Digital Library	https://dl.acm.org/
4	ScienceDirect	https://www.sciencedirect.com/
5	IEEE	https://ieeexplore.ieee.org/Xplore/home.jsp

The criteria for selecting studies involved excluding those that were only identified by their title and abstract. Instead, we focused on examining publications from a prominent magazine in the field of Cloud Computing. These publications were filtered based on their relevance to the topics of Secure EHR, as well as the use of cloud computing and blockchain technologies. We applied an inclusion and exclusion process throughout the paper to ensure that only the most relevant studies were considered, as shown in Table 3.

Table 3 . Criteria for selection

Relevance	Criteria
Title	Title: Secure Electronic Health Records (EHR) in Cloud Computing and Blockchain Technologies: Language Considerations (English)
By search	Search query: Publication year range (2010-2023) format
Abstract/ introduction/ conclusion	Background of cloud computing and blockchain technologies within their respective domains
Full text	Comprehensive examination of challenges, issues, and techniques for securing Electronic Health Records (EHR) in the context of cloud computing and blockchain technologies: An empirical study.

3.1. EHR security Algorithms classification

We classified the algorithms that were used to security electronic health records using cloud computing and using cloud computing with blockchain technology for scientific papers from 2010 to 2023 and the categorization of this approach can be based on the algorithms or models employed to tackle the literature problem. Three main classifications have been recognized: approximate, exact, and hybrid methods. In this section, we will analyze a selection of 52 articles that fulfill the mentioned criteria. We will classify the algorithms, determine platforms, evaluation parameters, utilized tools, as shown in Table 4.

A. Exact Methods

The efficient solution to optimization problems is typically achieved by utilizing exact search techniques. Despite their ability to provide optimal solutions, these techniques may take longer for larger instances due to the increased complexity of the problem. Exact search is indeed slower than some alternative approaches [35]. This section highlights the findings of articles in the literature review that utilize exact search techniques, including encryption algorithms, graph theory, and combinatorial optimization methods.

1. **Encryption algorithms** can be categorized into various groups according to their functions and structures , as shown in fig. 4. Here are some common categories of data protection algorithms:

- Symmetric Key Algorithms[43] [44] [45] [46].
- Asymmetric Key Algorithms [44] .
- Hashing Algorithms [47] .
- Key Exchange Algorithms [48] .
- Digital Signature Algorithms [49]

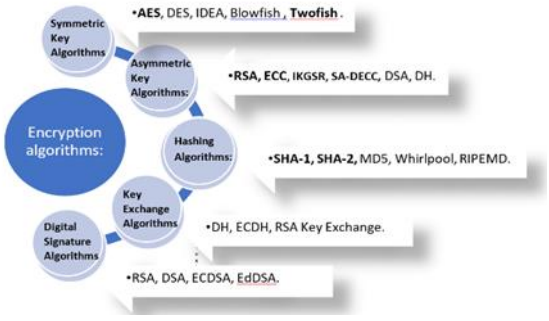


Fig. 4. Encryption algorithms

- **Symmetric Key Algorithms:** These algorithms use a single secret key for both data encryption and decryption. This key remains confidential between the communicating partiesThe key makes it easier to

convert plaintext into ciphertext and vice versa..Symmetric key algorithms are employed in numerous applications, such as internet communication security, and data protection on local storage devices. The Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish algorithm are a few instances of frequently utilized symmetric key algorithms. According to the collected papers, the algorithm was the most used two algorithms : AES algorithm [39] [50] [94] [105] [51], and two fish based encryption algorithm[52]

- **Asymmetric Key Algorithms:** Asymmetric key algorithms, also known as public-key cryptography, are cryptographic systems that use pairs of keys: a public key and a private key. The public key is made available to everyone, while the private key is kept secret. Messages encrypted with the public key can only be decrypted with the corresponding private key, and vice versa. Applications for asymmetric key algorithms are numerous and include key exchange protocols, digital signatures, and secure communication. Asymmetric key algorithms include Elliptic Curve Cryptography (ECC), Diffie-Hellman, and RSA.According to the collected papers, the mostly used algorithms are: RSA algorithm [38] [39] [53] [77] [54] [51] , ECC algorithm [3] [33] [50] [55] [56] [57] [58] , IKGSR algorithm [59], SA-DECC algorithm [60], CP-ABE algorithm [38] [42] [61], ABPRE algorithm [28], HOM algorithm [77] , and DDSA algorithm [62].

- **Symmetric-key and Asymmetric Key**

  According to the reviewed works, the mostly used algorithms are : DET algorithm [[63], CryptDB[63]] and user registration algorithm[64]].

- **Hashing Algorithms :** Hashing algorithms are mathematical functions that take input data of arbitrary size and produce a fixed-size output, called a hash or message digest. The purpose of a hashing algorithm is to provide a unique digital fingerprint of the input data, such that any change to the input data will result in a different hash value. Hashing algorithms are commonly used for data integrity checks, digital signatures, and password storage.Commonly used hashing algorithms include the Secure Hash Algorithm (SHA) family, such as SHA-256 and SHA-3, and the Message Digest (MD) family, such as MD5. However, some of these algorithms have known vulnerabilities, and it is recommended to use modern, secure hashing algorithms such as SHA-3 whenever possible.According to the collected papers, the algorithm was the most used SHA algorithm [65] [66] [67] and MPHT algorithm [62].

- **Digital signature**

  According to the collected papers, the algorithm was the most used DDSA algorithm [62].

- **Graph theory**

  According to the collected papers, the algorithm was the most used GNNSC algorithm [66].

- **Game theory**

  According to the collected papers, the algorithm was the most used NBS- based resource allocation[68] and KeywordSearch [69].

- **Computational theory**

  According to the collected papers, the algorithm was the most used NTRU algorithm[97], Chord algorithm [70] and search algorithm[50].

B. Approximate Methods

In this part, we delve into research concerning approximate methods, which encompass stochastic, probabilistic, and statistical techniques. Section I focuses on examining stochastic methods, which involve heuristic and metaheuristic approaches within the research domain. Subsequently, in Section II, we explore probabilistic/statistical methods.

I. Stochastic methods

1- Heuristic Methods

Heuristic methods are problem-solving techniques that use practical and efficient methods to find approximate solutions to complex problems. Here are some examples of heuristic algorithms:

Greedy Algorithm[71] [72], simulated annealing[73], and tabu search[74],Randomized Algorithm, as shown in fig. 5.

In our classification of the compiled research, we found two examples of heuristic methods, which are as follows: Greedy algorithm [70] and Optimal algorithm[63].

Fig. 5. Heuristic Methods

2- Meta-Heuristic Methods

A class of optimization algorithms known as metaheuristic approaches is intended to find approximations for complicated optimization problems. The term

"metaheuristic" refers to the fact that these algorithms are general-purpose and can be applied to a wide variety of optimization problems, without requiring problem-specific knowledge. Metaheuristic algorithms are often inspired by natural phenomena or physical processes, such as evolutionary processes, swarm intelligence, or simulated annealing[75] [76] [77][78] .Some commonly used metaheuristic algorithms include genetic algorithms[79], ant colony optimization[80], particle swarm optimization[81], Harmony Search[77], Biogeography-based Opt[77] , Cuckoo Search[77] , Bat Algorithm [77], as shown in fig. 6.

Fig. 6. Meta-Heuristic Methods

In our classification of the compiled research, we found examples of metaheuristic methods, which are as follows: Genetic algorithm [82] [83] [84], particle swarm optimization algorithm [83] [85], ant colony optimization algorithm [86], harmony Search [60], Biogeography-based Opt algorithm [87], Cuckoo Search algorithm [101] [66], Bat algorithm [[88], Enhanced Fuzzy Particle Swarm Optimization algorithm [[89], EFPSO algorithm [90], HU-GA algorithm [90], PSOSAA algorithm [91] [92] , AGOGT-VNM algorithm [93], vigenere encryption [52].

3-Neural network

As a result of the classification , we found two examples of Neural network methods,: MKE algorithm [94] and buildindex algorithm[50].

4-Evolutionary algorithm

Additionally, EF-RBAC algorithm [95],a sophisticated algorithm [96],MKE system algorithm[94] and voting and counting algorithm [64] are classified as Evolutionary algorithm.

II. Probabilistic/statistic methods

In this section, probabilistic/statistic methods, including machine learning , and game theory .

1-Machine learning

According to the classification. , we found nine examples of Machine learning methods, which are as follows: K-NN algorithm [53], ABSB algorithm [56], HBTL algorithm [66], SBVM algorithm [66], DataGen algorithm [121],Data redundancy algorithm [97],a recursive algorithm[98],consensus algorithm [24] [110] [99] [69] ,(EF-RBAC) Framwork algorithm and Access control policy algorithm[100].

2.Game theory

Game theory class of classification evolves the following algorthims:

NBS- based resource allocation algorithm [68] and KeywordSearch algorithm[69].

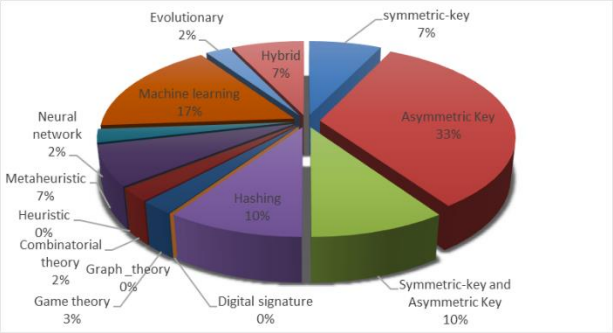
A. Hybrid Methods

Hybrid methods apply various methods, such as approximate, exact, and fundamental, for accomplishing . Studies with hybrid methods are reviewed in this section. including : RSA + AES algorithm [39] [51],Packagetransaction model [18] and keylnGen [69].

Table 4: illustrates the classification of the used algorithms from 2010 to 2023.

Category	Method	Algorithm	Papers
Ex Act	symmetric-key (deterministic or probabilistic)	AES	[39, 50][94] [105] [51].
		Two fish	[52]
	Asymmetric Key (deterministic or probabilistic)	RSA	[38] [39] [53] [77] [54] [51]]
		IKGSR	[59]]
		ECC	[3] [33] [50] [55] [56] [57] [58]
		SA-DECC	[60]
		CP-ABE	[38] [42] [61]
		ABPRE	[28]
		HOM	[77]
		DDSA	[62]
	Symmetric-key and Asymmetric Key	DET	[63]]
		CryptDB	[63]]
		User registration algorithm	[64]]

Approximate		ABE	[42] [50] [101]	Machine learning	K-NN	[53]
		BABSC	[65]		ABSB	[56]
		ABAC	[102]		HBTL	[103]]
	Hashing	SHA	[65] [66] [67]		SBVM	[66]
		MPHT	[62]		DataGen	[121]
	Digital signature	DDSA	[62]		Data redundancy	[97]]
	Graph _theory	GNNSC	[66]		Recursive	[98]
	Game theory	NBS-based resource allocation	[68]		Consensus	[24] [110] [99] [69]
					Access control policy	[100]
		KeywordSearch	[69]	Evolutionary	EF-RBAC	[95]
	Combinatorial theory	NTRU	[97]		Sophisticated	[96]
		Chord	[70]		MKE	[94]]
		Search	[50]		Voting and counting	[106]
	Heuristic	Greedy	[70]	Hybrid	RSA + AES	[39] [[51].
		Optimal	[63]]		Packagetransaction model	[18]
	Metaheuristic	Genetic	[82] [83]] [84]		keylnGen	[69]
		PSO	[83]] [85]			
		ACO	[86]]			
		HSO	[60]]			
		BBO	[87]			
		CS	[101] [66]			
		Bat	[88]]			
		EFPSO	[89]]			
		HU-GA	[90]			
		PSOSAA	[91] [92]]			
		AGOGT-VNM	[93]			
		Vigenere encryption	[52]			
	Neural network	MKE	[94]]			
		Buildindex	[50]			



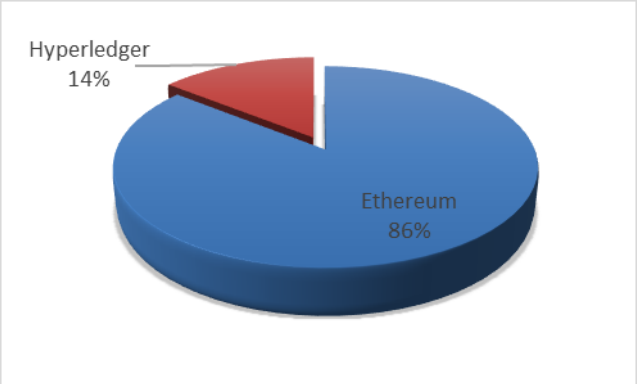


Fig. 8. Platform used in cloud computing with blockchain

- **Platforms used to protect the electronic health record using cloud computing with blockchain technologies** :

Table 5: Platform used to protect the electronic health record in cloud computing with blockchain

Platform type	Papers
Ethereum	[3] [24] [45] [50] [55] [59] [64] [104] [101] [116] [117] [123]
Hyperledger	[39] [100]

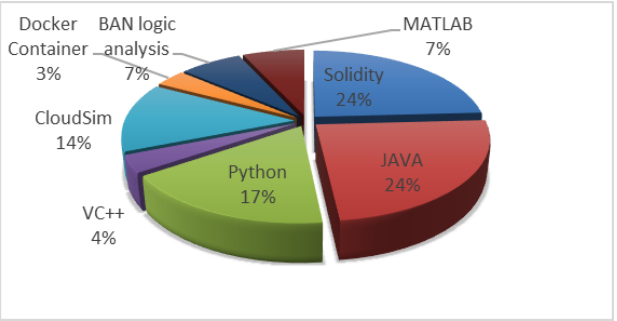


Fig. 9. Tools used in cloud computing with blockchain technologies

- **Tools used to protect the electronic health record using cloud computing with blockchain technologies:**

Table 6:Tools used to protect the electronic health record in cloud computing with blockchain technologies

Tools	Papers
Solidity	[3] [18]] [55] [[59] [104] [101] [105]
JAVA	[55] [58] [61] [62] [59]] [108] [[106]
Python	[38] [50] [66] [67] [108]
VC++	[65]
CloudSim	[84] [87] [61] [99]
Docker Container	[100]
BAN logic analysis	[42] [57]
MATLAB	[33] [102]

- **Factors used to protect the electronic health record using cloud computing with blockchain technologies:**

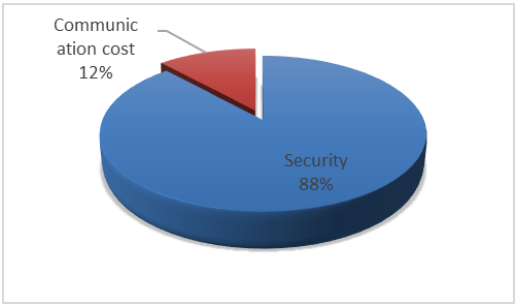


Fig. 10. Factors used in cloud computing with blockchain technologies

Table 7. Factors used protect the electronic health record in cloud computing with blockchain technologies.

Factors	studies
Security	[3] [[18] [24] [28] [33] [38] [39] [54] [50] [65] [55] [57] [69] [59]] [65 ,60] [66] [67] [62] [61] [84] [102] [64] [104] [101] [100] [105] [106]] [99] [69]
Communication cost	[28] [42] [57] [65]

4. Discussion and Comparison

This part shows an analytical assessment and discussion of Encrypting the Electronic Health Record using the Cloud Computing and Blockchain technologies. This work conducted a comparison between 60 studies related to the protection of sensitive data, such as electronic medical records, using cloud computing alone and also using both cloud computing and blockchain. The comparison was based on the following criteria: the technology used, the platform, the applications, the metrics, and the tools employed in each study, as shown in Table 8.The analytical assessment :

Q1: What kind of classification is exhibited in cloud and blockchain systems to protect EHR?

In Figs.7 the different applied encryption EHR methods are discussed. The usage of these methods is demonstrated through the statistical percentage of their applications. It can be observed that the Asymmetric Key algorithms are the most frequently utilized in EHR encryption assessments, comprising 18 studies and representing 33% of the applied methods.

Asymmetric key algorithms offer several advantages for protecting Electronic Health Records (EHR) in healthcare settings:

1. Secure Key Exchange: Asymmetric key algorithms facilitate secure key exchange between parties. In the context of EHR protection, this means that the encryption keys used to encrypt and decrypt the sensitive data can be securely shared between authorized entities, such as healthcare providers and patients. Asymmetric key algorithms, such as RSA or elliptic curve cryptography (ECC), enable the establishment of secure communication channels without the need for a pre-shared secret key.

2. Public/Private Key Pair: Asymmetric key algorithms use a public/private key pair for encryption and decryption of data. The public key is shared openly, while the private key is kept secret by the key owner. This enables the encryption of EHR data using the recipient's public key, ensuring that only the intended recipient with the corresponding private key can decrypt and access the sensitive information. This provides a strong level of confidentiality for EHR protection.

3. Digital Signatures: Asymmetric key algorithms also facilitate the use of digital signatures. Digital signatures provide a means to verify the authenticity and integrity of EHR data. By using the private key to sign the data, the entity can provide a verifiable proof of identity and ensure that the data has not been tampered with during transmission or storage. This helps to establish trust and non-repudiation in healthcare transactions, such as sharing medical records or prescriptions.

4. Scalability and Flexibility: Asymmetric key algorithms offer scalability and flexibility in managing access control and encryption in EHR systems. With asymmetric key algorithms, multiple users can have their own unique key pairs, enabling granular access control to specific EHR records. Additionally, as the number of users increases, the system can accommodate new users by generating and distributing their unique key pairs without compromising the security of existing users.

5. Regulatory Compliance: Asymmetric key algorithms align industry, such as the Health Insurance Portability and Accountability Act (HIPAA). These algorithms provide strong encryption and data protection mechanisms, which are essential for meeting privacy and security standards mandated by healthcare regulations.

It's important to note that while asymmetric key algorithms offer these advantages, their computational overhead is typically higher than symmetric key algorithms. Therefore, a common practice is to pair asymmetric key algorithms with symmetric key algorithms for efficient and secure EHR protection, combining the benefits of both approaches.

Q2: which evaluation platform are applied for evaluating the Encrypting the Electronic Health Record approaches?

In Fig.8, the utilization of the Ethereum and Hyperledger platforms in evaluating and analyzing existing case studies is demonstrated. The study reveals that the Ethereum platform is employed by 86% of the research articles, while the Hyperledger platform is applied by 14% of the articles. Thus, when it comes to utilizing blockchain technology to encrypt an electronic health record in a cloud computing setting, the Ethereum platform is the most effective and popular choice.

Q3: Which tools are used for assessing the security of Electronic Health Record (EHR) approaches?

There many tools used in encrypting the Electronic Health Record , According to Fig. 9, 24% of the research articles applied the java tool to evaluate and analyze the existing case studies,24% of the research articles applied the solidity tool to evaluate and analyze the existing case studies, 17% of the research articles applied the python tool to evaluate and analyze the existing case studies, In comparison, 14% of the research articles applied the CloudSim tool to evaluate and analyze the existing case studies, In addition, 7% , 7% , 4% , 3% of the research

papers used the Matlab environment, BAN logic analysis , VC++ and Docker tools .

As a result, the most suitable, effective, and popular tools for encrypting electronic health records in cloud environments utilizing blockchain technology on the Ethereum platform are Java and solidity technologies.

Q4: What are the usual factors assessed to evaluate EHR security approaches and promote their improvement?

According to Fig. 10, there two factors important for EHR security to evaluate and analyze the existing case studies,88% of the research articles used the security factor to evaluate and analyze the existing case studies , 14% used communication cost factor.

Q5: What are the open issues for research in using blockchain technology and cloud computing to protect medical records?

The use of cloud computing and blockchain technology for protecting medical records raises several open issues for research. Some of the key areas that require further investigation and exploration include:

1. **Scalability:** Blockchain technology, while providing transparency and immutability, faces scalability challenges when it comes to handling a large volume of transactions and data. Research is needed to develop scalable blockchain architectures and consensus mechanisms that can efficiently handle the storage and processing requirements of medical records in cloud-based systems.

2. Privacy and Security: Ensuring privacy and confidentiality of medical records stored on the blockchain or in cloud environments is crucial. Research is needed to develop privacy-preserving mechanisms and encryption techniques that allow for secure storage and sharing of sensitive medical data while maintaining patient confidentiality.

3.Interoperability and Standards: Integration and interoperability between different healthcare systems, blockchain networks, and cloud platforms pose significant challenges. Research efforts are needed to establish standards and protocols that enable seamless data exchange and interoperability while maintaining security and privacy.

These open research issues highlight the complexity and multidisciplinary nature of leveraging cloud computing and blockchain technology for protecting medical records. Addressing these challenges will contribute to the development of secure, privacy-preserving, and efficient systems for managing and sharing sensitive healthcare data.

4-Comminucation cost :

When considering the cost of communication in using blockchain technology and cloud computing to protect medical records, there are several open research issues to be explored:

1. Network Scalability: Blockchain networks can face scalability challenges, particularly in terms of transaction throughput and network latency. Research is needed to develop scalable blockchain architectures that can handle the increasing volume of medical record transactions while minimizing the associated communication costs.

2. Efficient Data Transfer: In cloud computing environments, efficient data transfer mechanisms are crucial to minimize costs. Research is required to optimize data transfer protocols, compression techniques, and bandwidth management strategies to reduce communication overhead when transferring medical records to and from the cloud.

3. Data Synchronization: In distributed blockchain networks, maintaining data consistency and synchronization across multiple nodes can be costly in terms of communication. Research is needed to devise efficient consensus mechanisms and synchronization protocols that minimize communication overhead while ensuring the integrity and consistency of medical records.

4. Off-Chain Data Storage: Storing all medical records directly on the blockchain can be expensive due to the associated storage costs and transaction fees. Research is required to explore hybrid approaches where selective data is stored off-chain in cloud environments, and only the necessary metadata or references are stored on the blockchain. This can help reduce storage and communication costs while maintaining data integrity and security.

5. Bandwidth Optimization: Optimizing bandwidth usage is crucial to reduce communication costs. Research is needed to develop techniques such as data compression, differential updates, or delta encoding to minimize the amount of data transferred during synchronization or when accessing medical records from the cloud.

6. Cost Models and Economic Incentives: Designing cost models and economic incentive mechanisms is essential to encourage participation and contribution to the blockchain network while managing communication costs. Research is required to explore incentive mechanisms that align the interests of network participants with the efficient use of communication resources.

7. Edge Computing and Local Processing: Leveraging edge computing capabilities can reduce communication costs by processing and analyzing medical records closer to the data source. Research is needed to explore edge computing architectures and algorithms that can handle privacy and security requirements while minimizing communication overhead.

8. Quality of Service (QoS): Ensuring adequate QoS levels, such as response time and reliability, is essential in healthcare applications. Research is required to develop communication protocols and resource allocation strategies that meet QoS requirements while minimizing costs in blockchain-based medical record systems.

Addressing these research issues related to the cost of communication will help optimize the use of blockchain technology and cloud computing for protecting medical records, making the systems more efficient, cost-effective, and scalable.

5. Conclusion

In this paper, the systematic literature review focuses on examining the state-of-the-art of secure EHR approaches in the cloud computing environment, using blockchain technology. This thorough evaluation highlights the latest and most effective strategies for securing EHRs in the cloud, emphasizing the importance of blockchain-based solutions in addressing these challenges.

The work conducted a comparison between 60 studies related to the protection of sensitive data, such as electronic medical records, using cloud computing alone and also using both cloud computing and blockchain. The comparison was based on the following criteria: the technology used, the platform, the applications, the Factors used protect the electronic health record, and the tools employed in each study.

Then the work classified the algorithms that were used to security electronic health records using cloud computing and using cloud computing with blockchain technology for scientific papers from 2010 to 2023 and the categorization of this approach can be based on the algorithms or models employed to tackle the literature problem. Three main classifications have been recognized: approximate, exact, and hybrid methods based on reviewing a 52 articles. The classification is based on the algorithms used , platforms, evaluation parameters, and utilized tools.

Through the analysis, this work reached the following results:

The statistical percentage of the applied used strategies presents that the Asymmetric Key algorithms have the best use in encryption EHR assessment with 18 studies and represent 33%.

Additionally, when it comes to utilizing blockchain technology to protect electronic health records in a cloud computing setting, the Ethereum platform is the most effective and popular 86%. Regarding the tools, Java and Solidity are the most suitable, effective, and popular tools 24%, 24%. for utilizing blockchain technology on the Ethereum platform to secure the electronic health record in a cloud environment. And there are two important EHR security factors to evaluate and analyze existing case studies, 88% of research articles used the security factor to evaluate and analyze existing case studies, and 14% used the communication cost factor.

Recommendations

Here are the recommendations we can provide to researchers interested in studying the protection of electronic health records using cloud computing and blockchain technologies:

1. Deep Understanding of Technologies: Researchers should have a deep understanding of both cloud computing and blockchain technologies. They should be familiar with the core concepts, algorithms used, and the challenges and benefits associated with each technology.

2. Security Model Design: Researchers should design an appropriate security model for electronic health records using cloud computing and blockchain. This includes identifying and evaluating potential threats, and determining suitable algorithms and mechanisms to protect data and privacy.

3. Use of Encryption: Strong encryption techniques should be employed to protect sensitive data in electronic health records. Advanced encryption methods such as public key encryption and end-to-end encryption can be used to ensure data confidentiality and integrity.

4. Identity and Access Management: Robust identity and access management procedures should be implemented to maintain data integrity. This includes using techniques such as two-factor authentication and access control to ensure that sensitive data is accessed only by authorized individuals.

Researchers should study and evaluate the available tools and platforms, and choose those that meet their needs and align with security and privacy requirements.

Table 8: Comparison of previous studies based on the specified criteria.

Ref	Authors	Years	Technology	Platform		Application	Metrics	Tools
				Cloud computing √	Cloud and blockchain			
1[70]	Kim, I.K., et al	2010	Chord Algorithm			Health records	- Security. - Processing load.	• CloudSim
2[107]	Nordin, M.I., A.H.M. Amin, and S.N.M. Shah	2012	ABSB algorithm	√		Medical Informatics	- Security. - Delay - Response time . - Processing time - Performance time .	• CloudAnalyst • JAVA • JADE . • Cloudsim simulation toolkits.
3[108]	Hussein, S.E. and H. Arafat	2013	-Resource consumption algorithms -Scheduling algorithms	√		Healthcare	- Security - Efficiency - Scalability.	• OpenStack, • DeltaCloud, • OpenShift. • CloudSim cloud simulator
4[109]	Qu, X., Z. Wei, and J. Zhang	2013	Scheduling algorithm	√		Medical Data	- Tasking total time - Processing and the times of peak appearance	• CloudSim
5[68]	Hassan, M.M	2015	NBS based allocation algorithm	√		E-health	- Cost - Average resource utilization on servers. - Time	• CloudSIm
6[90]	Jrad, F., et al	2015	HU-GA algorithm	√		Health data , like the DNA sequencing	-Execution costs ,improving the QoS.	• CloudSim • WorkflowSim • java-based Opt4J

								genetic framework • Match-Maker performs
7[91]	**Liu, Y., et al**	**2015**	**Effective PSOSAA algorithm**	√ √		Health records	- Execution time - The efficiency	• CloudSim • cloud simulator • Windows XP platform
8[53]	**Azeez, N. and H. Iliyas**	**2016**	**(K-NN) algorithm ,** **RSA algorithms**			PMR	-Security -Confidentiality	• CloudSim
[82] 9	**Wen, Z., et al.**	**2016**	**GA, NCF** **Algorithms**	√		Sensitive data	-Security, - Execution time -Monetary cost of the deployment.	• CloudSim
[63] 10	**Althebyan, Q., et al**	**2016**	**Optimal algorithm,** **CryptDB, (HOM), (DET)**	√		Patients health records	- Security,privacy - Delay, health costs -Power consumption	• CloudExp simulator simulator • CloudSim
[92] 11	**Luo, S. and B. Ren**	**2016**	**PSOSAA algorithm**	√		Health records	- Execution time - Energy cost	• CloudSim • Windows XP platform
[103] 12	**Mohan, K. and M. Aramudhan**	**2017**	**(HBTL) algorithm,** **Patient Turned Queuing Scheduling (PTQS) mechanism**	√		Healthcare data	-Trust (security and privacy) -Response time -number of users - number of health service providers, deadline of tasks -The execution time	• JADE 4.3.0 platform • Windows 7 (64 bits)
[97] 13	**Gorata, M., et al.**	**2017**	**Data redundancy algorithm**	√ √		Health information	- Security - Availability	• CloudSim simulation

14[96]	**Kadarla, K., et al**	**2017**	**A sophisticated algorithm**			Healthcare data	- Response time	• Cloudsim platform
[88] 15	**Eslami, P. and M.S. Hajmohammadi**	**2017**	**Bat algorithm**	√		E-health systems	- Resource management Time - Performance.	• CloudSim • Java programming language
[18] 16	**Xia, Q., et al.**	**2017**	**Smart Contract on Data Algorithm, Packagetransaction model Algorithm.**		√	Medical Data	- Security - Confidentiality - Privacy - Latency	• Solidity • JMeter
[83] 17	**Elhoseny, M., et al.**	**2018**	**GA, PSO and PPSO based algorithms**	√ √		EMR	- Data processing speed, - Execution time - System efficiency	• MATLAB • CloudSim package.
[94] 18	**Chandavale, A.A. and A.J. Gade**	**2018**	**(NTRU) algorithm,** **MKE system algorithm.**			Medical information	- Security - Confidentiality - Time ,Delivery	• MKE system algorithm
19[98]	**Roy, S., et al**	**2018**	**A recursive algorithm**	√		Patients' records	- Security - Computation Costs - Communication Costs	• ProVerif 1.93 tool
20[52]	**Chennam, K. and L. Muddana**	**2018**	**Vigenere encryption and two fish based encryption algorithm**	√		PHR	- Security(encryption and decryption time) - clustering accuracy, - memory	• JAVA • CloudSim
[60] 21	**Pourvahab, M. and G. Ekbatanifard**	**2019**	**(HSO) algorithm,** **(SA-DECC) algorithm ,** **SDN controller .**		√	Digital forensic system	- Security(encryption , decryption times) - Hash computation time - Response time - Evidence insertion time	• Net Beans-8.2 • NS-3.26 • CloudSim

							- Evidence verification time - Computational overhead	
[64] 22	**Zhu, L., et al**	**2019**	**User Registration algorithm , Voting And Counting Algorithm**		√	Sensitive data	- Financial cost - Efficiency - User amount - Document size	• Ethereum client Geth (1.8.3-stable) • Ethereum Wallet 0.10.0 • MacOS 10.13.4
[86] 23	**Kavitha, K. and S.C. Sharma,**	**2019**	**ACO algorithm**	√		Healthcare applications	-Response time	• CloudSim
24[104]	**Nguyen, D.C., et al**	**2019**	**RSA**		√	EHR	- Security - Access control - Network overheads - Flexibility - Availability - Integrity - Data privacy	• Ethereum blockchain network. • Amazon cloud computing. • Ubuntu 16.04 LTS • Solidity programming language. • And deployed on AWS Lambda functions. • web3.js API. • Geth client • The web3.js library • IPFS • BioKin platform .
25[69]	**Wang, Y., et al**	**2019**	**The DataGen algorithm , The KeyInGen , KeywordSearch**		√	EHR	Security,privacy computational overhead , communication	• Ethereum platform.

			algorithm, consensus mechanism				overhead.	
26[110]	**Liu, Y., et al.**	**2019**	**AI algorithms(machine learning algorithms)**	√		PHR	- Security - Reduce risks - save costs - fast, accurate and efficient medical services using DT technology	• CloudDTH platform • ECG device (Huake HKW-10) • WIFI module • TCP protocol • ZigBee • DTH
27[55]	**Al Omar, A., et al**	**2019**	**(ECC) algorithm**		√	EHR	-Security,privacy -transaction cost, -execution cost -Computation time.	• Solidity 0.4.11 • Ethereum Network • JAVA 1.8. • Win 8, 64-bit
28[50]	**Chen, L., et al.**	**2019**	**ABE Algorithm, BuildIndex algorithm, AES algorithm, search algorithm .**		√	EHR	- Security , - Overhead. - Accuracy of query	• Ethereum network(TestRPC) • Python 2.7. • MongoDB 3.4 enterprise edition. • Windows 10 (64 bit) . • (UCI) dataset.
[89] 29	**Anandaraj, A.P.S. and G. Indumathi**	**2020**	**EFPSO Algorithm**	√		Healthcare	- Time. - Memory usage. Number of Virtual Machines. - Attack detection rate	• CloudSim • Windows 7 64-bit . • Amazon EC2 X • Linux .
30[111]	**Raja, J., N. Balamurugan, and R. Pitchai**	**2020**	**AGOGT algorithm, (AGOGT-VNM) algorithm**	√	√	Patient medical records	- performance, - processing time	• Java Language • CloudSim simulator

31[65]	**Eltayieb, N., et al**	**2020**	**BABSC scheme , SHA-256 algorithm.**			Sensitive data	Security, communication cost .	• VC++ 6.0 using PBC library. • Windows 10- 64-bit.
32[87]	**Gupta, P., et al**	**2020**	**(BBO) algorithm**	√		E-health services	- Execution time - Waiting Time - Delay - Network cost	• Cloudsim 3.0 API
33[102]	**Wei, P., et al.**	**2020**	**(ABAC) is an (ABE) algorithm**		√		Security , Storage overhead, Time overhead	• Simulation software MATLAB7.0
34[93]	**Balamurugan, N., J. Raja, and R. Pitchai**	**2020**	**(MD-GTROVNM) algorithm**	√		Heart diseases patient's	- Computation time - Memory consumption - Request acceptance ratio	• Java language • CloudSim network simulator
35[56]	**Kumari, A., et al.**	**2020**	**ECC**	√		Medical record	- Security, - Privacy - Authentication - Computing time -Communication cost	Not mentioned
36[95]	**Harnal, S. and R. Chauhan**	**2020**	**(EF-RBAC) framework Algorithm**	√		Hospital e-Record	- Security, - Cost - Server usage, - Guarantees privacy	• JAVA • CMD • CloudSim (version 3.0)
37[42]	**Son, S., et al.**	**2020**	**ABE ,(CP-ABE), (PoA) algorithm**		√	Patient health data	- Security - Communication Cost, - Computation Cost.	• BAN logic analysis • AVISPA simulation tool . • Ubuntu 12.04.1 LTS 32 bit os

38[57]	**Kim, M., et al**	**2020**	**(ECC) algorithm**		√	EHR	- Security, - Computation Cost, - Communication Cost,	• BAN logic analysis. • AVISPA simulation tool. • HLPSL
39[33]	**Benil, T. and J. Jasper**	**2020**	**(ECC) algorithm**		√	EHR	- Security, - Delay , - Computational time - Computation cost.	• MATLAB R-2018b • Windows 10 with Platform 64 • **Ethereum**
40[54]	**Mubarakali, A.**	**2020**	**RSA algorithm**		√	HER	- Security - Delay, - System execution time.	• Net Beans 8.2, JDK 1.8, • Apache Tomcat 8.0.15, • MYSQL 5.7, • Jelastic cloud environment . • Windows 8 with a 64-bit .
41[100]	**Tanwar, S., K. Parekh, and R. Evans**	**2020**	**Access Control Policy Algorithm**		√	EHR	- Security,Privacy - Llatency, - Throughput, - Network scalability , - Round Trip Time (RTT), - CPU usage, - Memory consumption, - Disk write/read, - Network I/O.	• Hyperledger network • Caliper tool • Composer, • Docker Container
42[84]	**Tang, J., et al**	**2020**	**GA algorithm**			Dynamic files	- Execution time, - Response time - Load balancing.	• Linux server . • CloudSim. • Ant tool .

							- Energy consumption	
43[112]	**Anuradha, M., et al.**	**2021**	**AES algorithm**	√		Cancer patients	- Security - Authentication	• CloudSim • Java programming
[51] 44	**Saravanan, N. and A. Umamakeswari**	**2021**	**AES and RSA**	√		PHR	-Security -Access Time -Space Complexity -Avalanche Effect -Time Complexity	• CloudSim simulator • windows 10 • BLP and lattice models
45[28]	**Huang, H., et al.**	**2021**	**BCES system, Proof Chain, ABPRE scheme**		√	EHR	- Security - Computation cost - Communication cost - Consensus cost	• Ubuntu 18.04 • Prime-order bilinear groups with 128 bits
46[58]	**Mayuranathan, M., M. Murugan, and V. Dhanakoti,**	**2021**	**ECC algorithm.**		√	EHR	- Security, - Computational time complexity - Time consumption - Cost.	• JAVA • Cloud Simulator
47[101]	**Verma, G., N. Pathak, and N. Sharma.**	**2021**	**ABE**		√	EHD	- Security - Cost - Number of Transactions - Time taken in Accessing of record	• Ethereum TestRpc. • solidity language . • The AWS cloud. • Ubuntu 14.04 LTS virtual machine.
48[39]	**Wang, B. and Z. Li**	**2021**	**AES algorithm, RSA algorithm**		√	Medical data	- Security, - Privacy, - Throughput, - Scalability.	• Hyperledger • Ubuntu 16.04 (64-bit).
49[66]	**Khan, Y. and S. Verma**	**2021**	**(SHA)-version 3 of 512-bit hash-based tree, cuckoo search**		√	Forensic system	- Response time, - Cloud evidence insertion time,	• Cloud environment . • Python .

			algorithm , CB- EL GAMAL) algorithm , GNNSC, SBVM, SDN controller				- Cloud evidence verification time, - Computational overhead, - Hash calculation time, - Key generation times, - Entire overall change rate.	• Network simulator-3.30 .
50[61]	**Sharma, P., R. Jindal, and M.D. Borah**	**2021**	**CP-ABE algorithm Honey bee optimization algorithm**		√	Sensitive data	- Security, - Response Time - Execution Time - Throughput , - Delay, - Computation Time, - Transmission Time. - Average Resource Utilization.	• Java programming language. • Netbeans 7.0 IDE with JDK 1.7. • CloudSim 3.0.3 . • Window 10 .
51[99]	**Alzubi, J.A.**	**2021**	**Consensus algorithm**		√	MHEALTH dataset	- Security, privacy - Communication overhead - Communication Time , - Authentication accuracy - Authentication time - Data integrity	• CloudSim 3.0.
52[85]	**Kumar, P. and K. Silambarasan**	**2022**	**CS, PSO, and ABC Algorithms**	√		Healthcare area.	- Security, - Execution time - Speed of live data processing, - System efficiency.	• MATLAB • Cloud Sim package
53[38]	**Sammy, F. and S. Vigila**	**2022**	**CP-ABE (ECC,RSA)**		√	PHR	- Security(encryption, decryption time) ,	• Python and charm library

							- Computation cost, - Communication overhead, - Performance.	• Ubuntu platform
54[62]	**Jayasudha, M. and C. Vijayalakshmi**	**2022**	**(DDSA) Architecture ,(MPHT) algorithm**		√	EHR	- Security , - Encryption Time & Decryption Time - Encryption & Decryption Cost .	• Java • Windows 8.
55[24]	**Ramesh, D., et al**	**2023**	**Consensus algorithm**		√	EHR	- Security, - Computational overhead. (latency, throughput, . Block capacity and block size) , - Communication overhead.	• Ethereum platform. • web3js API. • Ganache. • Ganache client Geth 1:9:0. • The web3js library • Ubuntu 16.04 LTS. • Amazon cloud , PBC-(0.5.14) and OpenSSL crypto-library .
56[67]	**RM, M.S.K. and A. Jayachandran**	**2023**	**(SHA) Algorithm, (CNN), hybridization Algorithm (EOA , HEPRO) Algorithms**		√	EHR, EEG Psychiatric Disorders Dataset	- Security	• Python platform
57[105]	**Zakzouk, A., A. El-Sayed, and E.E.-D. Hemdan**	**2023**	**consensus algorithms**		√	**(EMR)**	- Security , - Execution Time, - Response time - Throughput, - Latency.	• Solidity programming language. • Ethereum. • JavaScript and Python. • Ganache.

								• Apache JMeter version 5.1.1.
58[3]	**Murala, D.K., S.K. Panda, and S.K. Sahoo**	**2023**	**ECC algorithm, a tampered proof mechanism**		√	**EHR**	- Security , - tamper-proof, - trust, - confidentiality, - integrity, uthentication, - availability.	• Solidity language. • Remix IDE . • Ethereum blockchain platform. • web3js, JSON-RPC, and Infura. • SmartCheck tool. • Oyente .
106] 59[	**Kumar, M., et al**	**2023**	**BigchainDB, Tendermint, Inter-Planetary-File-System (IPFS), MongoDB, and AES encryption algorithms.**		√	**EHR**	- Privacy - Security	• Ubuntu 21.04 • Java Script (React Library and Express Js) • Node Js
[59] 60	**Chinnasamy, P., et al**	**2023**	**PoW, IKGSR algorithm**		√	**EHR**	- Security - Time overhead - Encryption Time - Decryption time	• Ethereum network • Solidity scripting language • Amazon Web Computing (AWS) • Ubuntu 16.04 LTS VMs • Geth client • web3.js. web3.js toolkit • Android OS type 7.0 • java

References

[1] J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. R. Choo, "Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges," *ACM Computing Surveys (CSUR)*, vol. 54, pp. 1-36, 2021.

[2] H. B. Mahajan, A. S. Rashid, A. A. Junnarkar, N. Uke, S. D. Deshpande, P. R. Futane, *et al.*, "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," *Applied Nanoscience*, vol. 13, pp. 2329-2342, 2023.

[3] D. K. Murala, S. K. Panda, and S. K. Sahoo, "Securing electronic health record system in cloud environment using blockchain technology," in *Recent advances in blockchain technology: real-world applications*, ed: Springer, 2023, pp. 89-116.

[4] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, pp. 1-8, 2016.

[5] X.-Y. Wu, Z.-P. Fan, and B.-B. Cao, "An analysis of strategies for adopting blockchain technology in the fresh product supply chain," *International Journal of Production Research*, pp. 1-18, 2021.

[6] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016, pp. 1-11.

[7] S. Mohapatra and S. Parija, "A brief overview of blockchain algorithm and its impact upon cloud-connected environment," *Bitcoin and Blockchain*, pp. 99-113, 2020.

[8] S. Mohapatra and A. Roy, "A study on mediclaim processing in connected healthcare system," *Trends in Wireless Communication and Information Security: Proceedings of EWCIS 2020*, pp. 363-374, 2021.

[9] M. A. Cyran, "Blockchain as a foundation for sharing healthcare data," *Blockchain in Healthcare Today*, 2018.

[10] S. Shubbar, "Ultrasound medical imaging systems using telemedicine and blockchain for remote monitoring of responses to neoadjuvant chemotherapy in women's breast cancer: concept and implementation," Kent State University, 2017.

[11] H. S. Hasan, A. A. Abdallah, I. Khan, H. S. Alosman, A. Kolemen, and B. Alhayani, "Novel unilateral dental expander appliance (udex): a compound innovative materials," *Computers, Materials and Continua*, pp. 3499-3511, 2021.

[12] W. Yahya, K. Ziming, W. Juan, M. Al-Nehari, L. Tengyu, R. Qichao, *et al.*, "Study the influence of using guide vanes blades on the performance of cross-flow wind turbine," *Applied Nanoscience*, vol. 13, pp. 1115-1124, 2023.

[13] K. Aldiabat, A. Kwekha Rashid, H. Talafha, and A. Karajeh, "The extent of smartphones users to adopt the use of cloud storage," *J Comput Sci*, vol. 14, pp. 1588-1598, 2018.

[14] A. S. Rashid, K. Tout, and A. Yakan, "The critical human behavior factors and their impact on knowledge management system–cycles," *Business Process Management Journal*, vol. 27, pp. 1677-1702, 2021.

[15] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, *et al.*, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Transactions on Computational Social Systems*, vol. 5, pp. 942-950, 2018.

[16] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," *CAAI Transactions on Intelligence Technology*, vol. 3, pp. 114-118, 2018.

[17] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, p. 44, 2017.

[18] 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, 2017.

[19] Y. ZHANG, R. H. DENG, J. SHU, K. YANG, and D. ZHENG, "Trustworthy Keyword Search over Encrypted Data with Two-side Verifiability via Blockchain."

[20] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools and Applications*, vol. 79, pp. 9711-9733, 2020.

[21] M. Jmaiel, M. Mokhtari, B. Abdulrazak, H. Aloulou, and S. Kallel, *The Impact of Digital*

Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, June 24–26, 2020, Proceedings vol. 12157: Springer Nature, 2020.

[22] G. Yang, C. Li, and K. E. Marstein, "A blockchain-based architecture for securing electronic health record systems," *Concurrency and Computation: Practice and Experience*, vol. 33, p. e5479, 2021.

[23] L. Huang and H. Lee, "Decentralization and security issues in blockchain enabled internet of things," *Wirel Commun Mob Comput*, 2020.

[24] 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, 2023.

[25] R. Ch, G. Srivastava, Y. L. V. Nagasree, A. Ponugumati, and S. Ramachandran, "Robust cyber-physical system enabled smart healthcare unit using blockchain technology," *Electronics*, vol. 11, p. 3070, 2022.

[26] 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 (TOMM)*, vol. 17, pp. 1-17, 2021.

[27] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava, and P. Chatterjee, "Efficient and privacy-preserving medical research support platform against COVID-19: a blockchain-based approach," *IEEE consumer electronics magazine*, vol. 10, pp. 111-120, 2020.

[28] H. Huang, X. Sun, F. Xiao, P. Zhu, and W. Wang, "Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments," *Journal of Parallel and Distributed Computing*, vol. 148, pp. 46-57, 2021.

[29] F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, "Ehrchain: a blockchain-based ehr system using attribute-based and homomorphic cryptosystem," *IEEE Transactions on Services Computing*, vol. 15, pp. 2755-2765, 2021.

[30] S. Li, Y. Zhang, C. Xu, N. Cheng, Z. Liu, and X. S. Shen, "Besure: Blockchain-based cloud-assisted ehealth system with secure data provenance," in *2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS)*, 2021, pp. 1-6.

[31] H. M. Hussien, S. M. Yasin, N. I. Udzir, and M. I. H. Ninggal, "Blockchain-based access control scheme for secure shared personal health records over decentralised storage," *Sensors*, vol. 21, p. 2462, 2021.

[32] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable cities and society*, vol. 39, pp. 283-297, 2018.

[33] T. Benil and J. Jasper, "Cloud based security on outsourcing using blockchain in E-health systems," *Computer Networks*, vol. 178, p. 107344, 2020.

[34] M. J. Iqbal, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C.-W. Lin, "RThreatDroid: A Ransomware Detection Approach to Secure IoT Based Healthcare Systems," *IEEE Transactions on Network Science and Engineering*, 2022.

[35] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access*, vol. 8, pp. 45468-45476, 2020.

[36] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE access*, vol. 8, pp. 59389-59401, 2020.

[37] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-11, 2022.

[38] F. Sammy and S. Vigila, "An efficient blockchain based data access with modified hierarchical attribute access structure with CP-ABE using ECC scheme for patient health record," *Security and Communication Networks*, vol. 2022, 2022.

[39] B. Wang and Z. Li, "Healthchain: A privacy protection system for medical data based on blockchain," *Future Internet*, vol. 13, p. 247, 2021.

[40] R. Awadallah and A. Samsudin, "Using Blockchain in Cloud Computing to Enhance Relational Database Security," *IEEE Access*, vol. 9, pp. 137353-137366, 2021.

[41] M. Mayuranathan, M. Murugan, and V. Dhanakoti, "Enhanced security in cloud applications using emerging blockchain security algorithm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 6933-6945, 2021.

[42] 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.

[43] M. Sohal and S. Sharma, "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, pp. 1417-1425, 2022.

[44] M. Al-Shabi, "A survey on symmetric and asymmetric cryptography algorithms in information security," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, pp. 576-589, 2019.

[45] A. H. Alwan and A. H. Kashmar, "FCNN Model for Diagnosis and Analysis of Symmetric Key Cryptosystem," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, pp. 53-61, 2023.

[46] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *International Journal on Computer Science and Engineering*, vol. 4, p. 877, 2012.

[47] P. P. Pittalia, "A comparative study of hash algorithms in cryptography," *International Journal of Computer Science and Mobile Computing*, vol. 8, pp. 147-152, 2019.

[48] H. H. Hadi and A. A. Neamah, "Diffie-Hellman Key Exchange Based on Block Matrices Combined with Elliptic Curves," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, pp. 353-360, 2023.

[49] M. Bedoui, B. Bouallegue, A. M. Ahmed, B. Hamdi, M. Machhout, Mahmoud, *et al.*, "A Secure Hardware Implementation for Elliptic Curve Digital Signature Algorithm," *Comput. Syst. Sci. Eng.*, vol. 44, pp. 2177-2193, 2023.

[50] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future generation computer systems*, vol. 95, pp. 420-429, 2019.

[51] N. Saravanan and A. Umamakeswari, "Lattice based access control for protecting user data in cloud environments with hybrid security," *Computers & Security*, vol. 100, p. 102074, 2021.

[52] K. Chennam and L. Muddana, "An efficient two stage encryption for securing personal health records in cloud computing," *International Journal of Services Operations and Informatics*, vol. 9, pp. 277-296, 2018.

[53] N. Azeez and H. Iliyas, "Implementation of a 4-tier cloud-based architecture for collaborative health care delivery," *Nigerian Journal of Technological Development*, vol. 13, pp. 17-25, 2016.

[54] A. Mubarakali, "Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach," *Mobile Networks and Applications*, vol. 25, pp. 1330-1337, 2020.

[55] 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, 2019.

[56] A. Kumari, V. Kumar, M. Y. Abbasi, S. Kumari, P. Chaudhary, and C.-M. Chen, "Csef: cloud-based secure and efficient framework for smart medical system using ecc," *IEEE Access*, vol. 8, pp. 107838-107852, 2020.

[57] 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*, vol. 20, p. 2913, 2020.

[58] M. Mayuranathan, M. Murugan, and V. Dhanakoti, "Enhanced security in cloud applications using emerging blockchain security algorithm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 6933-6945, 2021.

[59] P. Chinnasamy, A. Albakri, M. Khan, A. A. Raja, A. Kiran, and J. C. Babu, "Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System," *Applied Sciences*, vol. 13, p. 3970, 2023.

[60] M. Pourvahab and G. Ekbatanifard, "Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology," *IEEE Access*, vol. 7, pp. 153349-153364, 2019.

[61] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based decentralized architecture for cloud storage system," *Journal of Information Security and Applications*, vol. 62, p. 102970, 2021.

[62] M. Jayasudha and C. Vijayalakshmi, "Blockchain meets healthcare: Architecture for secure data

sharing in unobtrusive medical applications," in *AIP Conference Proceedings*, 2022.

[63] Q. Althebyan, Q. Yaseen, Y. Jararweh, and M. Al-Ayyoub, "Cloud support for large scale e-healthcare systems," *Annals of telecommunications*, vol. 71, pp. 503-515, 2016.

[64] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Generation Computer Systems*, vol. 91, pp. 527-535, 2019.

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

[66] Y. Khan and S. Verma, "An intelligent blockchain and software-defined networking-based evidence collection architecture for cloud environment," *Scientific Programming*, vol. 2021, pp. 1-19, 2021.

[67] M. S. K. RM and A. Jayachandran, "ENSURING DATA SECURITY FOR PATIENT HEALTH RECORDS WITH CLOUD-BASED BLOCKCHAIN MONITORING AND ACCURATE DISEASE CLASSIFICATION USING CNN."

[68] M. M. Hassan, "Cost-effective resource provisioning for multimedia cloud-based e-health systems," *Multimedia Tools and Applications*, vol. 74, pp. 5225-5241, 2015.

[69] 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.

[70] I. K. Kim, Z. Pervez, A. M. Khattak, and S. Lee, "Chord based identity management for e-healthcare cloud applications," in *2010 10th IEEE/IPSJ International Symposium on Applications and the Internet*, 2010, pp. 391-394.

[71] S. Boettcher, "Inability of a graph neural network heuristic to outperform greedy algorithms in solving combinatorial optimization problems," *Nature Machine Intelligence*, vol. 5, pp. 24-25, 2023.

[72] X. Han, Y. Han, Q. Chen, J. Li, H. Sang, Y. Liu, *et al.*, "Distributed flow shop scheduling with sequence-dependent setup times using an improved iterated greedy algorithm," *Complex System Modeling and Simulation*, vol. 1, pp. 198-217, 2021.

[73] P. Ghannadi, S. S. Kourehli, and S. Mirjalili, "A review of the application of the simulated annealing algorithm in structural health monitoring (1995-2021)," *Frattura ed Integrità Strutturale*, vol. 17, pp. 51-76, 2023.

[74] J. P. Gabhane, S. Pathak, and N. M. Thakare, "A novel hybrid multi-resource load balancing approach using ant colony optimization with Tabu search for cloud computing," *Innovations in Systems and Software Engineering*, vol. 19, pp. 81-90, 2023.

[75] F. S. Gharehchopogh, "Quantum-inspired metaheuristic algorithms: comprehensive survey and classification," *Artificial Intelligence Review*, vol. 56, pp. 5479-5543, 2023.

[76] M. Abdel-Basset, L. Abdel-Fatah, and A. K. Sangaiah, "Metaheuristic algorithms: A comprehensive review," *Computational intelligence for multimedia big data on the cloud with engineering applications*, pp. 185-231, 2018.

[77] T. Dokeroglu, E. Sevinc, T. Kucukyilmaz, and A. Cosar, "A survey on new generation metaheuristic algorithms," *Computers & Industrial Engineering*, vol. 137, p. 106040, 2019.

[78] Z. Beheshti and S. M. H. Shamsuddin, "A review of population-based meta-heuristic algorithms," *Int. j. adv. soft comput. appl*, vol. 5, pp. 1-35, 2013.

[79] M. Gen and L. Lin, "Genetic algorithms and their applications," in *Springer handbook of engineering statistics*, ed: Springer, 2023, pp. 635-674.

[80] A. Rezvanian, S. M. Vahidipour, and A. Sadollah, "An Overview of Ant Colony Optimization Algorithms for Dynamic Optimization Problems," 2023.

[81] W. Huang and J. Xu, "Particle Swarm Optimization," in *Optimized Engineering Vibration Isolation, Absorption and Control*, ed: Springer, 2023, pp. 15-24.

[82] Z. Wen, R. Qasha, Z. Li, R. Ranjan, P. Watson, and A. Romanovsky, "Dynamically partitioning workflow over federated clouds for optimising the monetary cost and handling run-time failures," *IEEE Transactions on Cloud Computing*, vol. 8, pp. 1093-1107, 2016.

[83] M. Elhoseny, A. Abdelaziz, A. S. Salama, A. M. Riad, K. Muhammad, and A. K. Sangaiah, "A hybrid model of internet of things and cloud computing to manage big data in health services

applications," *Future generation computer systems*, vol. 86, pp. 1383-1394, 2018.

[84] J. Tang, C. Huang, H. Liu, and N. Al-Nabhan, "Cloud Storage Strategy of Blockchain Based on Genetic Prediction Dynamic Files," *Electronics*, vol. 9, p. 398, 2020.

[85] P. Kumar and K. Silambarasan, "Enhancing the performance of healthcare service in IoT and cloud using optimized techniques," *IETE Journal of Research*, vol. 68, pp. 1475-1484, 2022.

[86] K. Kavitha and S. C. Sharma, "Performance analysis of ACO-based improved virtual machine allocation in cloud for IoT-enabled healthcare," *Concurrency and Computation: Practice and Experience*, vol. 32, p. e5613, 2020.

[87] P. Gupta, M. K. Goyal, A. Mundra, and R. P. Tripathi, "Biogeography-based meta-heuristic optimization for resource allocation in cloud for E-health services," *Journal of Intelligent & Fuzzy Systems*, vol. 38, pp. 5987-5997, 2020.

[88] [88] P. Eslami and M. S. Hajmohammadi, "A Real Time Memory Resource Management Algorithm in E-health Systems," *International Journal of Software Engineering and Its Applications*, vol. 11, pp. 7-14, 2017.

[89] A. P. S. Anandaraj and G. Indumathi, "Enhanced Fuzzy Particle Swarm Optimization Load Distribution (EFPSO-LD) for DDOS Attacks Detection and Prevention in Healthcare Cloud Systems," *Journal of Internet Technology*, vol. 21, pp. 435-445, 2020.

[90] F. Jrad, J. Tao, I. Brandic, and A. Streit, "SLA enactment for large-scale healthcare workflows on multi-cloud," *Future Generation Computer Systems*, vol. 43, pp. 135-148, 2015.

[91] Y. Liu, B. Dong, B. Guo, J. Yang, and W. Peng, "Combination of cloud computing and internet of things (IOT) in medical monitoring systems," *International Journal of Hybrid Information Technology*, vol. 8, pp. 367-376, 2015.

[92] S. Luo and B. Ren, "The monitoring and managing application of cloud computing based on Internet of Things," *Computer Methods and Programs in Biomedicine*, vol. 130, pp. 154-161, 2016.

[93] N. Balamurugan, J. Raja, and R. Pitchai, "Multicriteria dragonfly graph theory based resource optimized virtual network mapping technique for home medical care service provisioning in cloud," *Peer-to-Peer Networking and Applications*, vol. 13, pp. 1872-1885, 2020.

[94] A. A. Chandavale and A. J. Gade, "Cloudlet based Healthcare and Medical Knowledge Extraction System for Medical Big Data," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 16, 2018.

[95] S. Harnal and R. Chauhan, "Towards secure, flexible and efficient role based hospital's cloud management system: case study," *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 6, 2020.

[96] K. Kadarla, S. C. Sharma, T. Bhardwaj, and A. Chaudhary, "A simulation study of response times in cloud environment for iot-based healthcare workloads," in *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2017, pp. 678-683.

[97] M. Gorata, A. M. Zungeru, M. Mangwala, and J. Chuma, "Design andImplementation of Security in Healthcare Cloud Computing," 2017.

[98] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 457-468, 2018.

[99] J. A. Alzubi, "Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare," *Computer Communications*, vol. 170, pp. 200-208, 2021.

[100] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, p. 102407, 2020.

[101] G. Verma, N. Pathak, and N. Sharma, "A secure framework for health record management using blockchain in cloud environment," in *Journal of Physics: Conference Series*, 2021, p. 012019.

[102] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Future Generation Computer Systems*, vol. 102, pp. 902-911, 2020.

[103] K. Mohan and M. Aramudhan, "Broker based trust architecture for federated healthcare cloud system," *Intelligent Automation & Soft Computing*, vol. 23, pp. 477-483, 2017.

[104] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE access*, vol. 7, pp. 66792-66806, 2019.

[105] A. Zakzouk, A. El-Sayed, and E. E.-D. Hemdan, "A blockchain-based electronic medical records management framework in smart healthcare infrastructure," *Multimedia Tools and Applications*, pp. 1-19, 2023.

[106] M. Kumar, H. Raj, N. Chaurasia, and S. S. Gill, "Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0," *Internet of Things and Cyber-Physical Systems*, 2023.

[107] M. I. Nordin, A. H. M. Amin, and S. N. M. Shah, "Agent based Resource Broker for medical informatics application in clouds," in *2012 International Conference on Computer & Information Science (ICCIS)*, 2012, pp. 802-807.

[108] S. E. Hussein and H. Arafat, "An Open Cloud Model for Expanding Healthcare Infrastructure," *International Journal of Advanced Computer Science and Applications*, vol. 4, 2013.

[109] X. Qu, Z. Wei, and J. Zhang, "Research on architecture of medical data interaction platform based on cloud services," in *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology*, 2013, pp. 130-133.

[110] Y. Liu, L. Zhang, Y. Yang, L. Zhou, L. Ren, F. Wang, *et al.*, "A novel cloud-based framework for the elderly healthcare services using digital twin," *IEEE access*, vol. 7, pp. 49088-49101, 2019.

[111] J. Raja, N. Balamurugan, and R. Pitchai, "Annealed glowworm optimization graph theory-virtual network mapping for home healthcare in cloud," *MOBILE NETWORKS & APPLICATIONS*, vol. 25, pp. 609-619, 2020.

[112] M. Anuradha, T. Jayasankar, N. Prakash, M. Y. Sikkandar, G. Hemalakshmi, C. Bharatiraja, *et al.*, "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," *Microprocessors and Microsystems*, vol. 80, p. 103301, 2021.