Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.034448

ARTICLE

Medi-Block Record Secure Data Sharing in Healthcare System: Issues, Solutions and Challenges

Zuriati Ahmad Zukarnain[1,*], Amgad Muneer[2,3], Nur Atirah Mohamad Nassir[1] and Akram A. Almohammedi[4,5]

[1]Faculty of Computer Science and Information Technology, University Putra Malaysia, Seri Kembangan, 43400, Malaysia

[2]Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Seri Iskandar, 32160, Malaysia

[3]Centre for Research in Data Science (CeRDaS), Universiti Teknologi PETRONAS, Seri Iskandar, 32610, Malaysia

[4]Automobile Transportation Department, South Ural State University, Chelyabinsk, 454080, Russia

[5]Electrical and Electronics Engineering Department, Karabük University, Karabük, 78050, Turkey

*Corresponding Author: Zuriati Ahmad Zukarnain. Email: zuriati@upm.edu.my

Received: 17 July 2022 Accepted: 03 November 2022 Published: 09 November 2023

ABSTRACT

With the advancements in the era of artificial intelligence, blockchain, cloud computing, and big data, there is a need for secure, decentralized medical record storage and retrieval systems. While cloud storage solves storage issues, it is challenging to realize secure sharing of records over the network. Medi-block record in the healthcare system has brought a new digitalization method for patients' medical records. This centralized technology provides a symmetrical process between the hospital and doctors when patients urgently need to go to a different or nearby hospital. It enables electronic medical records to be available with the correct authentication and restricts access to medical data retrieval. Medi-block record is the consumer-centered healthcare data system that brings reliable and transparent datasets for the medical record. This study presents an extensive review of proposed solutions aiming to protect the privacy and integrity of medical data by securing data sharing for Medi-block records. It also aims to propose a comprehensive investigation of the recent advances in different methods of securing data sharing, such as using Blockchain technology, Access Control, Privacy-Preserving, Proxy Re-Encryption, and Service-On-Chain approach. Finally, we highlight the open issues and identify the challenges regarding secure data sharing for Medi-block records in the healthcare systems.

KEYWORDS

Medi-block record; healthcare system; Blockchain technology; secure data sharing

1 Introduction

The healthcare system is the collection of institutions, resources and people working together to offer healthcare services to specific populations [1,2]. In Malaysia, different hospitals use different systems or private electronic databases for information storage [3]. Besides, they also use paper/files to keep and track their patient's medical records. The current healthcare system in every hospital will not integrate or be connected to protect patients' privacy [4]. However, this kind of old fashion system has its weakness when some patients who need to go to a different hospital in the way of emergency, the new hospital cannot check the existing health problem or any treatment that needs to continue [3]. This will lead to time-consuming in checking of the patient's health from the start. Although this way is good for protecting patient's privacy, this way is no longer relevant since the world is evolving into a new era of digitalization [3]. To be aligned with today's digitalization world, Medi-blocked record has been introduced in the healthcare system, where the data will be stored on the cloud [5]. Medi-block is a patient-oriented health record t to overcome the issue where the patient records are usually kept in a separate system or papers/files at the specific hospital. However, this method has led to a new issue: privacy and integrity of the data since it is shared on the cloud and can be accessed by many hospitals [6]. Data sharing is the collection of practices, technologies, cultural elements, and legal frameworks relevant to digital transactions in any type of information exchange between various organizations. To put the patient's medical record on a centralized system online and accessible from every hospital, protecting data privacy and integrity is vital and needs to be maintained [7]. Several studies have been conducted to analyze the methods on how to secure data sharing in Medi-block records in the healthcare system.

For example, the authors in [3] have introduced a bilinear mapping method for the authentication phase in Blockchain technology. This architecture includes comprehensive security authentication, access control and authorization techniques to authenticate identity management for data-sharing devices, services, and users. In [7], safeguarding user data privacy using a secret sharing system in a smart city environment to manage and secure large amounts of real-time data remains an issue. Therefore, there are still security challenges in cloud-assisted electronic health (e-health) which led the author in [8] to propose blockchain-based privacy preservation to guarantee the security and confidentiality of patients' medical records. This method introduced pairing-based cryptography to create tamper-proof records to protect them from illegal modification. One of the benefits to secure data sharing for Medi-block records in the healthcare system is to protect the privacy of confidential data for every patient at the hospitals, maintain the integrity of the data and enhance the security level [3]. Furthermore, enhancing the level of security to protect privacy and integrity will give every patient peace of mind that their confidential data is completely secured and protected at every level. Many challenges should be tackled to secure data sharing in Medi-block records to successfully protect the privacy and confidentiality of patient's medical records and maintain the integrity of the data in the healthcare system [3].

There have been many research studies in secure data sharing that aimed to increase the security level [9,10,4,11], protect the privacy and integrity of medical data, and overcome the problem of asymmetric information. Nonetheless, detailed assessments of research that evaluate various aspects of secure data exchange in Medi-block records, including requirements and challenges, are mainly absent. The author in [11] discussed enabling the proxy re-encryption to secure data sharing on the Internet of Things (IoT), the same as the author in [9], which proposed key-aggregate proxy re-encryption. In [12], the authors discussed sharing data in the government sector and proposed a Service-On-Chain (SOC) approach to provide trustworthiness in data content and controllability in data ownership. The authors in [13] discussed sharing health data among companies regarding COVID-19 infection data to protect the community and individual health. Authors in [14], also discussed protecting healthcare systems using blockchain and other formal methods. This method aimed to protect information exchanged in hospital networks, particularly for magnetic resonance images (MRI), where each host network must authenticate the transition data network. Ahmed et al. [15] evaluated the security approaches used to maintain healthcare devices and presents a mathematical methodology for ranking them in order of priority and preference. In [16] work, attribute-based searchable honey encryption with a functional neural network framework is introduced to analyze disease and give improved security in IoT-cloud healthcare data. Ahmad et al. [17] discussed 10 different methods to secure healthcare devices and propose a quantitative framework to list them in order of significance. However, many studies in the literature focused on cloud storage issues and it is still challenging to realize secure sharing of records over the network. Hence, the Medi-block record in the healthcare system has brought a new digitalization method for patients' medical records and believe to be a state-of-the-art method.

Therefore, this work contribution can be summarized in threefold. First, we have conducted extensive research on the issues, solutions, current advancements, and challenges associated with safe data exchange for Medi-block records in healthcare systems. Second, we draw inferences from recent research by examining their problem areas, suggested solutions, and considered techniques. Third, we have identified the merit and demerit of the available, secure data-sharing Medi-block methods in the literature and provide a guideline for future research. In contrast to past surveys, this article discusses current difficulties, solution methodologies, the limitations of suggested solutions, and new obstacles in safe data sharing for Medi-block records in the healthcare system. Additionally, most of the research cited in this study is current and was not discussed prior to this survey. We have omitted all out-of-date publications cited in previous surveys and focused on the most recent directions in secure data exchange. Thus, the main aim of this work is to present the latest works of proposed solutions (suggested methods, outcomes, and limitations) on secure data sharing and the challenges that still require to be addressed. Table 1 shows the secure data-sharing methods in the existing related works.

Table 1: Secure data sharing methods in existing related works

Authors	Years	Methods
Singh et al. [3]	2021	Bilinear Mapping
Cha et al. [7]	2021	Secret Sharing Algorithm
Zhang et al. [8]	2022	Privacy-Preserving
Pareek et al. [9]	2021	Proxy Re-Encryption
Piao et al. [12]	2021	Service-On-Chain (SOC)
Brunese et al. [14]	2019	Formal Method

The remainder of the article is organized as follows. Section 2 presents an analysis and review of data sharing in Medi-block records. Section 3 provides the review and comparison between all methods used in secure data sharing, such as Bilinear Mapping, Secret Sharing Algorithm, Access Control, Privacy-Preserving, Proxy Re-Encryption, Service-On-Chain and Formal Method and its limitations. After that, we summarize the conclusion in Section 4 of this paper.

2 Medi-Block Record

Blockchain technology is a distributed database, and it is best at maintaining a secure and decentralized record of transactions [18]. Blockchain is based on cryptography and the peer-to-peer (P2P) network concept. Data integrity and security are ensured by algorithm and cryptography techniques [19]. The Medi-blocked record has been introduced in the Healthcare system, where the data will be stored decentralized on a cloud. Medi-block is a patient-oriented health record built to overcome the issue of the patient records being kept in separate systems or papers/files at the specific hospital. However, this method has led to a new issue: privacy and integrity of the data since it is shared on the cloud, and many hospitals can access it. Medi-block presents tamper-proof for medical records sharing for hospitals and patients. One of the approaches employed for the authentication step is bilinear mapping, which eliminates the need for third-party trust. It establishes bidirectional authentication between patients and the hospital. The authentication scheme suggested is examined by Burrows Abadi Nidham (BAN) logic, storage overhead and computing cost [20]. Many other available methods can be used, applied, and proposed in Blockchain technology to protect the medical record's confidentiality and integrity [21]. In Section 3, we will review a comparison between all methods discussed in this paper. Fig. 1 is the basic overview of the Medi-Block record.

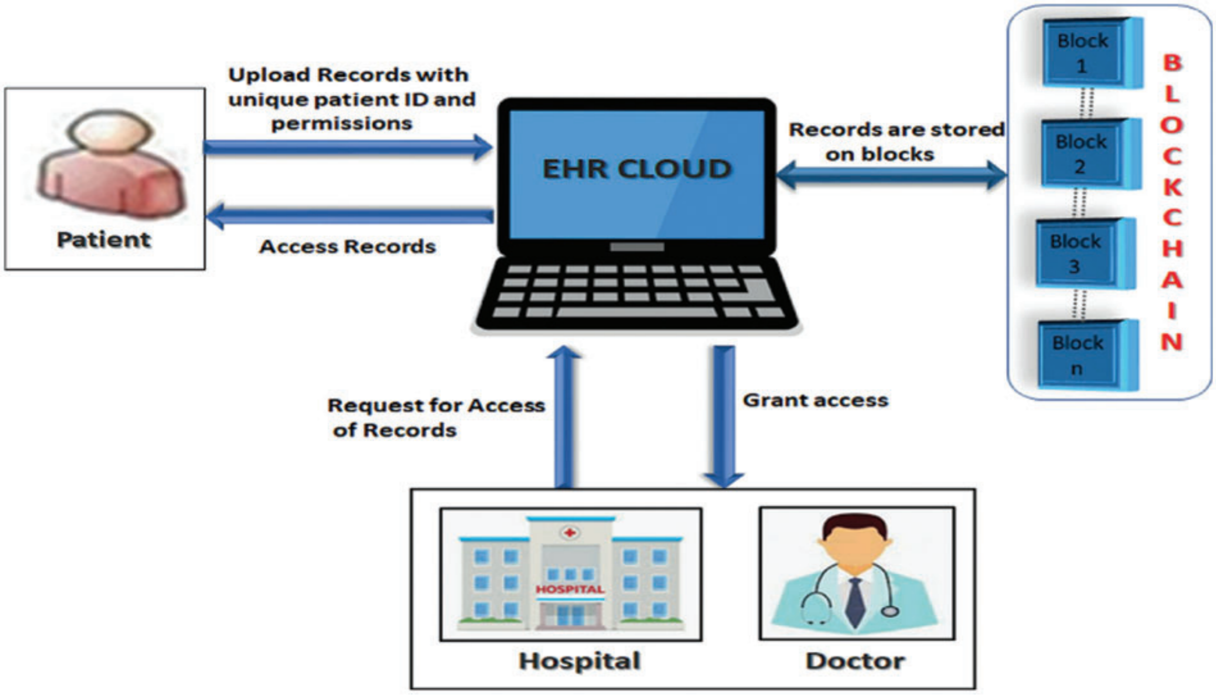

Upload Records with unique patient ID and permissions
Patient
Access Records
EHR CLOUD
Records are stored on blocks
Block 1
Block 2
Block 3
Block n
BLOCKCHAIN
Request for Access of Records
Grant access
HOSPITAL
Hospital
Doctor

Figure 1: Basic overview of Medi-block record

3 Methods in Secure Data Sharing

In existing related surveys, researchers proposed many methods in the Blockchain technology to protect medical records data to maintain privacy and confidentiality and retain the data's integrity. The methods proposed by recent surveys are Bi-linear Mapping, Secret Sharing, Access Control, Privacy-Preserving, Proxy Re-Encryption, SOC, and Formal Method. We will look at and discuss in detail each method proposed.

3.1 Bilinear Mapping

Bilinear mapping is the technique or method applied for the authentication phase. The suggested authentication approach is analyzed by BAN logic, storage overhead, and cost of computing. The three steps of secure authentication for Medi-block are a start-up, registration, and authentication [3]. This concept of the method is a pairing concept to the elliptic curve. Bilinear denotes that *h1*, *h2* goes to *G,* and *a*, *b* goes to Z_p. The Bilinear formula is given in Eq. (1):

$$e\ (ha1, hb2) = (h1, h2) * a * b \tag{1}$$

As blockchain has storage memory constraints, hospitals store their records as cypher text, hashes, abstracts, and cloud storage locations in consortium chains' central nodes. L symbolizes a cloud storage location where medical records are stored; M is the hash of every hospital. In order to be sent to the blockchain network, L would constantly be encrypted with the hospital public key. Below is a flow diagram that illustrates each of the steps involved. Medical records from each hospital are used as input; the output is the trading results of the data from those records.

1. Stage 1: Produce the corresponding Epubkey $\{Mac|\ |H(M)||L\}$.
2. Stage 2: On the medical consortium chain, save the information generated in Step 1.
3. Stage 3: A blockchain network is used to broadcast all transactions.
4. Stage 4: This step's output reflects the updated medical record.

3.2 Secret Sharing

A smart city is a digital system that is intelligent and efficient. By digitizing all data, smart cities can manage it. CSPs are connected via a blockchain to ensure user data's integrity and facilitate data access via Transactions [22]. CSP stores user information on the blockchain using the Secret Sharing algorithm, significantly improving the security of existing centralized systems [23]. The suggested method enhanced security and privacy through security analysis and increased transaction speed and data storage efficiency over prior studies [7]. The blockchain-empowered secret sharing for the smart city concept is shown in Fig. 2.

The challenges in secret sharing have difficulty restoring data if the scattered data's components do not capture enough data to meet the threshold. In some previous research, blockchain and secret sharing were utilized to create a P2P electronic cash system that permitted centralized financial systems to be transacted P2P via third parties. This study can help mitigate the security weakness of a centralized network, as numerous nodes share the same blocks. Using the blockchain, data blocks can be separated from each other, preventing them from staying altered between blocks and preventing block contents from being amended arbitrarily. As a result, data integrity can be confirmed between dispersed nodes without the involvement of a third party.

3.3 Access Control

There is a proposed biometric identity-based hybrid signcryption (BIOIBHSC) scheme for access control in wireless body area networks (WBAN). This scheme used to build public keys and streamlines vital generation [24]. This also combines two mechanisms: biometric identity-based signcryption tag-key encapsulation mechanism (BIO-IBSCTK) and data encapsulation mechanism (DEM) to attain confidentiality, integrity, authenticity, and anonymity non-repudiation in data sharing. In this proposed scheme, they use bilinear pairings and fuzzy extractor methods. Fig. 3 shows an example of a healthcare system model using an access control scheme.

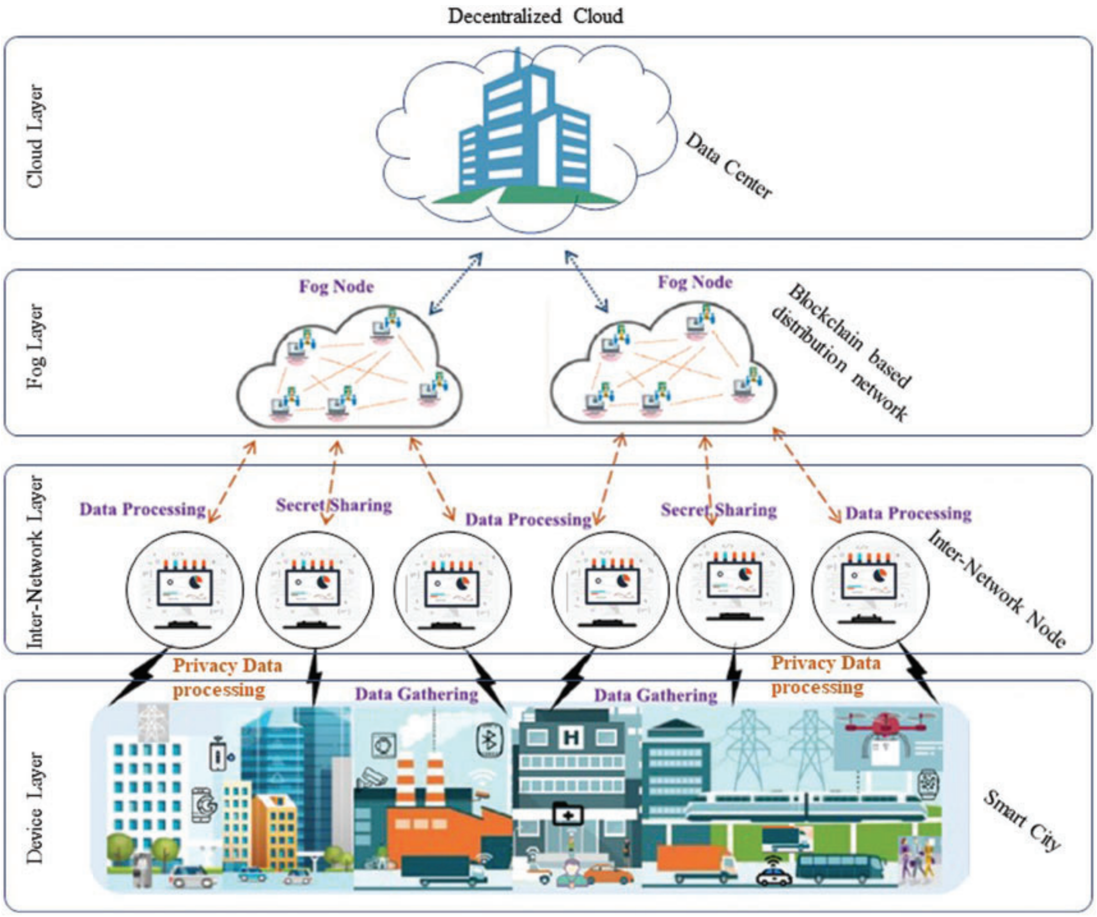


Figure 2: Blockchain-empowered on secret sharing for the smart city

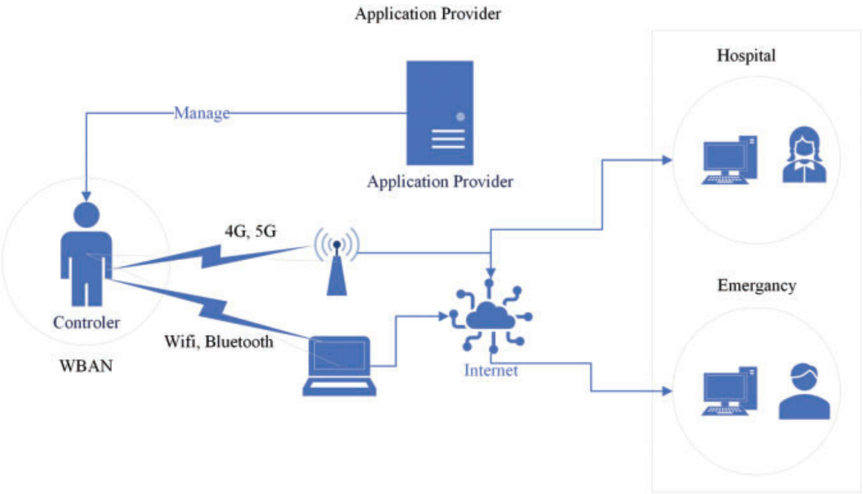


Figure 3: Healthcare system model using an access control scheme

Another access control mechanism has been introduced to ensure healthcare information security and confidentiality. This mechanism is called the La-grange-interpolation-driven access control mechanism (LIDACM). This LIDACM strictly controls privacy settings and access authority and prevents unauthorized users from accessing personal health records on the cloud. Hence, this simultaneously increases the hacking difficulties of databases and stealing private health records and medical information [25]. Since this mechanism randomly generates a private key, it is not easy to analyze and increases the difficulties cyberattacks face. LIDACM ensures data security when multiple users are accessing it. Two components are used in LIDACM: when the user intends to retrieve medicinal data. The method utilizes A(x) to validate if an access request comes from an authorized user. Then B(y) is utilized to check the PHR (Personal Health Record) system if the file requested by the user is permitted to be accessed. Hence, an example of access control mechanisms for PHR based system is presented in Fig. 4.

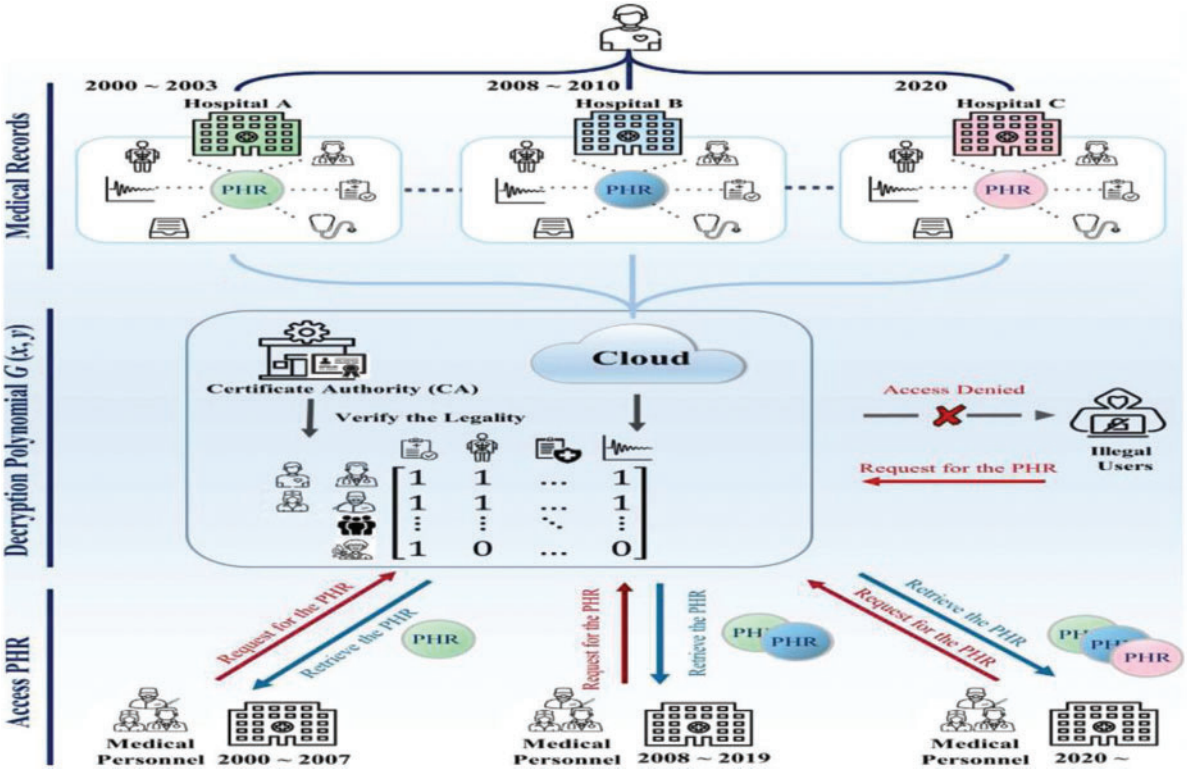


Figure 4: An example of access control mechanisms for PHR based system

3.4 *Privacy Preserving*

Privacy-Preserving is the method of protecting confidentiality and privacy, and data sharing. This resolves traditional data sharing, which were P2P and centralized data sharing modes [12].

3.4.1 Privacy-Preserving Using Off-Chain Blockchain Systems (OCBS)

Off-chain is the data that is structured externally to the blockchain network. The key features of off-Chain Blockchain Systems (OCBS) are improving scalability, reducing requirements of data storage, and enhancing data privacy. Nevertheless, various kinds of health data are also subordinate to severe regulatory, security, and legal constraints, which impede blockchain implementation in the industry [1]. The OCBS system employed multiple layers of cryptography in conjunction with an innovative data storage and privacy-by-design infrastructure. Several of the fundamental principles are as follows:

- Hashing
- Public Key Infrastructure (PKI)
- Asymmetric Encryption
- Digital Signatures
- Secure Multiparty Computation (SMPC)
- Trusted Execution Environments (TEE)
- Verifiable Computation

These cryptographic mechanisms for validating data stored in connected databases and several layers of protection are employed to prevent system errors and misuse. This method has been used in Government data sharing (GDS) in the existing work. Government agencies may transfer information or data between themselves to comply with applicable laws and regulations to eliminate data silos and maximize the value of data. Typically, government data contains a substantial number of personal and business-related information. Personal data may include, but is not limited to, information on a person's salary income, real estate ownership, and records of violations of laws and regulations. The term "business data" refers to information about company partners, income, bonds, trademark patents, and investment funds, among other things. Sensitive data that individuals and corporations may like to keep private and specific aspects of the data are frequently described as privacy.

3.5 Proxy Re-Encryption

In proxy re-encryption, this method will ensure the confidentiality and integrity of the data, allowing the data to be only visible to the owner and the smart contract [11]. In this method, they proposed the Ethereum blockchain and Hyperledger Fabric blockchain. However, the Ethereum blockchain has a limitation where the delay time increases when multiple users' request or retrieve the data, as shown in the proxy re-encryption architecture in Fig. 5. An intelligent contract is a well-known protocol that enables, verifies, and enforces the negotiation or fulfilment of a contract digitally. Unlike traditional contracts, which rely on counterparties' reputations, smart contracts can be entered between untrusted, anonymous individuals. Contractual terms are automatically enforced and do not rely on any third party. On the other hand, smart contracts were not conceivable in many traditional systems because the participants maintained separate databases and lacked an appropriate trust model. Therefore, the ability to construct a trusted and shared database based on a blockchain has removed this constraint.

Another way for proxy re-encryption is Key-aggregate cryptosystems. This is an efficient way to enforce access control policies. This key aggregate proxy re-encryption (KAPRE) method secures data sharing on cloud storage [9]. Fig. 6 shows the suggested two variants of KAPRE by [9].

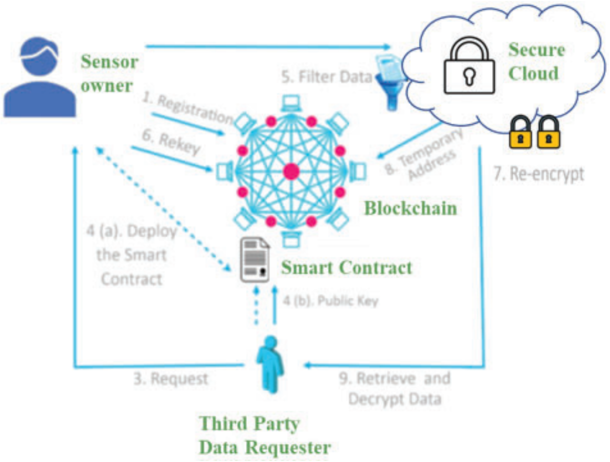
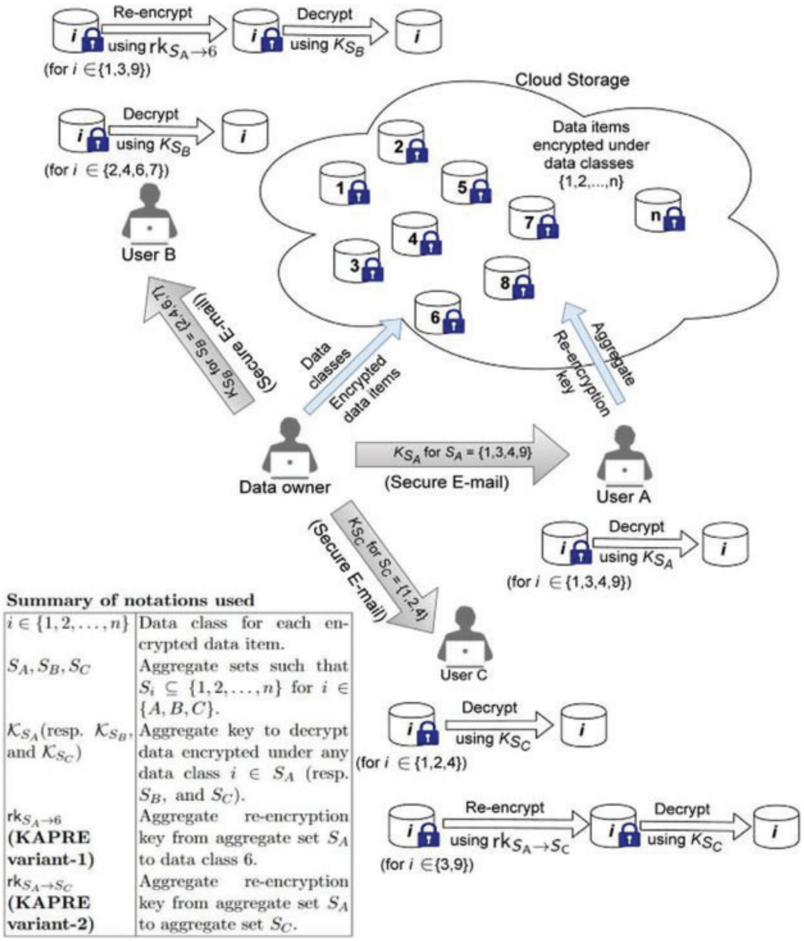


Figure 5: Proxy re-encryption method architecture



Summary of notations used

$i \in \{1,2,\ldots,n\}$	Data class for each encrypted data item.
S_A, S_B, S_C	Aggregate sets such that $S_i \subseteq \{1,2,\ldots,n\}$ for $i \in \{A,B,C\}$.
$\mathcal{K}_{S_A}$(resp. $\mathcal{K}_{S_B}$, and $\mathcal{K}_{S_C}$)	Aggregate key to decrypt data encrypted under any data class $i \in S_A$ (resp. S_B, and S_C).
$\mathrm{rk}_{S_A \to 6}$ **(KAPRE variant-1)**	Aggregate re-encryption key from aggregate set S_A to data class 6.
$\mathrm{rk}_{S_A \to S_C}$ **(KAPRE variant-2)**	Aggregate re-encryption key from aggregate set S_A to aggregate set S_C.

Figure 6: Key-aggregate proxy re-encryption in two variants proposed [9]

Table 2: Comparison of proposed methods and limitations

Method	Algorithm	Process/scheme	Limitations
Bilinear mapping [3]	Burrows Abadi Nidham (BAN) logic	X	It cannot be directly applicable to the medical sector
Secret sharing [7]	Secret sharing algorithm (SSA)	X	Not efficient privacy data in real-time
Privacy-Preserving [8]	Cryptography	Off-chain blockchain systems (OCBS)	Interoperability, integration and data standardization with existing health information systems
Proxy re-encryption Key-aggregate cryptosystems [9]	Setup, CertifiedUserKeyGen, Encrypt, ReKeyGen, ReEncrypt, Decrypt1, and Decrypt2	Ethereum blockchain	The delay time increase when multiple users request the data
Service-On-Chain (SOC) [12]	Algorithm of data sharing process	Off-chain privacy-preserving	Data sharing architecture construction, diversified data, smart contracts, and operational security need further study
Formal method [14]	X	Equivalence checking	It has not been deployed in a real hospital network
Access control: Fuzzy extractor [19]	$\{Gen, Rep\}$ algorithms	Biometric identity-based	No limitations
Access control: Lagrange-interpolation-driven access control mechanism (LIDACM) [25]	Polynomial	X	Access control management & system compatibility are essential challenges that must be addressed
A widespread social network-based healthcare record [26]	X	X	The proposed protocol operates with a small number of nodes but is inefficient for real-world applications
A blockchain-based privacy preservation solution for an IoT-enabled healthcare network [27]	Purpose-centric access model	X	The system is susceptible to communication overhead and increased execution chain code costs
Blockchain-based secure and privacy-preserving PHI sharing BSSP scheme [28]	X	X	The proposed method is vulnerable to a 50% attack

3.6 Service-On-Chain (SOC)

The Service-On-Chain concept was proposed to circumvent the restrictions associated with traditional data exchange methods. The central concept is SOC, data off the chain. By leveraging the blockchain's smart contract mechanisms, each department's data is extended to the blockchain-based on a service-oriented architecture [29], while sensitive data is maintained on the blockchain [12].

- *Off-Chain Privacy-Preserving:* Off-chain data preservation can improve data security, reducing the danger of privacy leaks to a particular level. This will ensure data security in the event of a leak or an attack while also increasing shared data integrity and controllability [30]. To re-establish data's trustworthiness and controllability, each government department saves original data in a local database, while data sharing is kept in the network file system (NFS) after privacy processing. To get pre-shared data, the service provider pre-screens the obtained data in line with applicable laws, rules, and policies. A metadata information file is produced and saved in the network file system based on the comprehensive information included in the pre-shared data (including information like "data size, data acquisition time, and data digest"). The service provider then packages it as a service and publishes it to the blockchain via the client, creating a service directory. The service provider can handle pre-shared data in various ways depending on the data. The process and data sharing will be saved on the network file system, and a data digest will be generated for authentication purposes through shared data. This off-chain data storage technique ensures the security of processed data and mitigates hazards associated with knowledge asymmetry throughout the data exchange process.

3.7 Formal Method

A blockchain is a collection of documents, referred to as blocks, that are connected together via cryptography [30]. They utilize the equivalency verification procedure in the proposed formal technique to determine whether two systems are equal to one another according to some theoretically specified equivalence. For example, formal equivalence checking takes two systems and an equivalence relation as inputs, precisely two systems s1 and s2 and an equivalence relation x, and asks, "Is the model of s1 equivalent to the model of s2 with regard to x?". The solution to this question is conditional on the equivalence relation x that is being considered. The suggested approach is intended to undertake a distributed verification of data passing over the hospital network [14]. This technology has been used previously to detect manipulated areas in medical photographs. It employed a block-based method, dividing the picture into eight 8-pixel chunks that were not overlapping. After dividing each block into four 4-pixel subblocks, a 9-bit watermark is formed. The watermark information is then inserted in the first nine pixels of each of the four 4-pixel subblocks' least significant bits (LSBs). The changed areas are detected during tamper detection using a three-level hierarchical technique. Additionally, this approach creates the joint photographic experts' group (JPEG) bit string for the specified area of interest (ROI) and then segments it into fixed-length segments. The approach divides the medical picture into chunks and calculates the hash bits for each block, omitting the block with the ROI [14]. Table 2 summarizes the suggested methods in the literature and their limitations.

4 Challenges for Proposed Methods in Existing Works

To develop a system that protects data privacy and confidentiality and maintains the integrity of the data, many methods have been proposed to overcome the issues arising. However, we need also to investigate the challenges in implementing all those methods in the existing systems. This section also discusses the challenges in all methods proposed in existing works done by previous researchers.

4.1 Challenges in Bilinear Mapping

The research in [31] proposed proxy re-encryption without bilinear mapping or pairing because of its costly operation. The suggested approach is unidirectional, key optimal, collision-proof, non-transitive, proxy visible, offers original access, and meets the temporary condition. Another challenge in this proposed blockchain-based architecture method is the BAN logic method, which is inapplicable directly to the medical field [3]. They use blockchain and cloud storage concepts to offer a safe platform for exchanging electronic medical data records.

4.2 Challenges in Secret Sharing

The secret-sharing method is disseminated and shared amongst n secret-keeping shareholders [32]. To reinstate secret T, the hidden parts of secret T preserved by n shareholders must be accumulated to the required level. Assume that such Secret Sharing is reinstated for nefarious reasons in the external cloud without erasing the original data at the user's request. In such instances, public encryption may result in an offline Brute force Attack against the same domain or in security risks that gradually decrypt the encryption using increased computer capabilities. Secret Sharing, in which the original data T is disseminated, has trouble recovering data if the distributed data samples do not gather enough data to meet the restoration threshold. Another challenge in implementing this secret sharing method is that it is not efficient in protecting private data when running in real-time [7]. In the upcoming work, the author aims to conduct extensive research using smart city services to distribute sharing algorithms that can convey safe, efficient privacy data in real-time and offer benefits in various sophisticated smart city applications.

4.3 Challenges in Access Control

Access control is another method of protecting data privacy and confidentiality in data sharing. However, access control management and system compatibility are fundamental challenges that must be addressed [33]. For example, the smart contract is an access control method and one of the most critical components in Blockchain technology, where data owners can define access control policies [34]. If large organizations with many workers or users utilize this strategy, it will be costly and impose significant computational overhead on the blockchain. Additionally, such systems cannot support attribute revocation, which enables the data owner to withdraw permissions for a set of users simultaneously.

4.4 Challenges in Privacy Preserving

In privacy-preserving, we found the potential challenges. This Off-Chain Block-Chain Systems (OCBS) model is challenged regarding interoperability, integration, and data standardization. The use of industry data format standards, such as "HL7 Fast Healthcare Interoperability Resources or the IEEE P2418.6 standard for Framework of Distributed Ledger Technology Use in Healthcare and the Life and Social Sciences". Another challenge found in the Genomic data reference model of maintaining privacy while maintaining accuracy is the primary challenge with this methodology, owing to the massive file size of Whole Genome Sequenced (WGS) data [1]. The genomics data reference pattern is the highly dynamic and extensible model available. Additionally, the genomics reference pattern is created with the flexibility to evolve over time in response to evolving regulatory guidelines on genomes data. The genomics data reference model was created to maximize data sharing and transfer mediated by individuals, which is required given the tremendous significance of genome data in advancing precision medicine and public health challenges.

4.5 Challenges in Proxy Re-Encryption

In the proxy re-encryption method using Key-aggregate cryptosystems, prior to implementing a public-key cryptosystem for safe data sharing and access control, it is critical to examine the overall length of time required for end-users to access the data. We found a challenge where the delay time increases when multiple users request the data simultaneously. This might also slow the application's performance in retrieving the required data [9].

4.6 Challenges in Service-On-Chain (SOC)

An off-chain privacy-preserving service was proposed for the SOC approach [12]. This is good for protecting the privacy and confidentiality of the data [35]. However, some challenges need to be considered, and further research is necessary on building data-sharing architectures, diversified data, smart contracts, and operational security. The suggested Service-On-Chain architecture can serve as a model for implementing Blockchain technology in government data sharing. The following two areas will be the focus of future development. For off-chain privacy preservation, the optimal parameters of the universal privacy-preserving model may be investigated using game theory to strike a balance between data availability and privacy preservation. The author will also research ways to enhance and deploy the scheme method on popular consortium blockchain frameworks, such as FISCO BCOS and Hyperledger Fabric.

4.7 Challenges in Formal Method

The formal method using the equivalence checking process is to perform a distributed verification of data passing over the hospital network. It is offered to safeguard critical information on hospital networks. The suggested method makes use of tools for formal verification. When a host requests access to magnetic resonance pictures, each host that requests the same resource does an integrity check. Thus, the suggested technique guarantees that an attacker does not alter the received information. However, the challenge we found is that it has not been deployed in a real hospital network, so we would not know the success of this method yet [14]. Table 3 presents the summary of the existing methods and their key challenges.

Table 3: Summary of methods and challenges

No.	Method	Challenges
1	Bilinear mapping	A costly operation cannot be applied directly to the medical field when Burrows Abadi Nidham (BAN) logic is used
2	Secret sharing	Not efficient in protecting privacy data when running in real-time
3	Access control	Highly costly and incur high computation overhead on the blockchain if big companies with large employees use this method
4	Privacy-preserving	The interoperability, integration, and data standards of health information systems are now in use
5	Proxy re-encryption	Delay time increases when multiple users request the data simultaneously
6	Service-On-Chain (SOC)	Further research is needed on data sharing architecture development, diverse data, smart contracts, and operational security
7	Formal method	It has not been deployed in a real hospital network

5 Conclusions

In this paper, we can conclude that many methods, algorithms, processes, and schemes can be used or implemented in Blockchain technology to protect the privacy and confidentiality of data sharing on cloud storage, IoT and decentralized system. We have observed that the Medi-block record in the healthcare system shows great potential to be the central decentralized system in sharing medical data across hospitals and clinics and will become the most effective system for retrieving medical data or records from any authorized healthcare location. The survey reviews various proposed solutions to achieve secure data sharing for Medi-block records into secure data sharing for Medi-block records in the healthcare system. Therefore, the existing solutions have been summarized by highlighting the proposed solutions' issues. We identified problems and challenges that required further research based on the analysis work. Hopefully, the detailed discussion in this extensive review may provide insights to the audience to better understand data sharing, the methods, research gaps, and future work that can be done for secure data sharing for Medi-block records in the healthcare system.

Acknowledgement: Authors contributed equally to this paperwork. Present a primer addressing to some of the problems, solutions, and challenges in secure data sharing in electronic medical records. The authors focus on their issues, proposed methods, and techniques for the solutions. All authors have read and agreed to the published version of the manuscript.

Funding Statement: The authors would like to acknowledge the support of University Putra Malaysia for paying the article processing charges (APC) of this publication.

Author Contributions: Study conception, design, analyzing and interpretation of results: Zuriati Ahmad Zukarnain, Amgad Muneer; draft manuscript preparation, investigation, and resources: Nur Atirah Mohamad Nassir, Akram A. Almohammedi. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data used to support the findings of this review paper are derived from existing sources, which are appropriately cited throughout the article.

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

References

[1] K. Miyachi and T. K. Mackey, "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design," *Information Processing & Management*, vol. 58, no. 3, pp. 102535, 2021.

[2] D. Kim, S. Min and S. Kim, "A DPN (delegated proof of node) mechanism for secure data transmission in IoT services," *Computers, Materials & Continua*, vol. 60, no. 1, pp. 1–14, 2019.

[3] C. Singh, D. Chauhan, S. A. Deshmukh, S. S. Vishnu and R. Walia, "Medi-block record: Secure data sharing using block chain technology," *Informatics in Medicine Unlocked*, vol. 24, pp. 100624, 2021.

[4] C. Zhang, C. Xu, K. Sharif and L. Zhu, "Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications," *Computer Standards & Interfaces*, vol. 77, pp. 103520, 2021.

[5] P. K. Sahoo and C. K. Dehury, "Efficient data and cpu-intensive job scheduling algorithms for healthcare cloud," *Computers & Electrical Engineering*, vol. 68, pp. 119–139, 2018.

[6] R. Ganiga, R. M. Pai, M. M. M. Pai and R. K. Sinha, "Private cloud solution for securing and managing patient data in rural healthcare system," *Procedia Computer Science*, vol. 135, pp. 688–699, 2018.

[7] J. Cha, S. K. Singh, T. W. Kim and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *Journal of Information Security and Applications*, vol. 57, pp. 102686, 2021.

[8] G. Zhang, Z. Yang and W. Liu, "Blockchain-based privacy preserving e-health system for healthcare data in cloud," *Computer Networks*, vol. 203, pp. 108586, 2022.

[9] G. Pareek and B. Purushothama, "KAPRE: Key-aggregate proxy re-encryption for secure and flexible data sharing in cloud storage," *Journal of Information Security and Applications*, vol. 63, pp. 103009, 2021.

[10] Q. Miao, H. Lin, X. Wang and M. M. Hassan, "Federated deep reinforcement learning based secure data sharing for internet of things," *Computer Networks*, vol. 197, pp. 108327, 2021.

[11] A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila and M. Liyanage, "Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain," *Journal of Network and Computer Applications*, vol. 176, pp. 102917, 2021.

[12] C. Piao, Y. Hao, J. Yan and X. Jiang, "Privacy preserving in blockchain-based government data sharing: A Service-On-Chain (SOC) approach," *Information Processing & Management*, vol. 58, no. 5, pp. 102651, 2021.

[13] E. Balistri, F. Casellato, C. Giannelli and C. Stefanelli, "BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten," *ICT Express*, vol. 7, no. 3, pp. 308–315, 2021.

[14] L. Brunese, F. Mercaldo, A. Reginelli and A. Santone, "A blockchain based proposal for protecting healthcare systems through formal methods," *Procedia Computer Science*, vol. 159, pp. 1787–1794, 2019.

[15] S. Ahmed and A. Alhumam, "Unified computational modelling for healthcare device security assessment," *Computer Systems Science and Engineering*, vol. 37, no. 1, pp. 1–18, 2021.

[16] M. Vedaraj and P. Ezhumalai, "A secure IoT-cloud based healthcare system for disease classification using neural network," *Computer Systems Science and Engineering*, vol. 41, no. 1, pp. 95–108, 2022.

[17] M. Ahmad, J. F. Al-Amri, A. F. Subahi, S. Khatri, A. Hussain Seh *et al.,* "Healthcare device security assessment through computational methodology," *Computer Systems Science and Engineering*, vol. 41, no. 2, pp. 811–828, 2022.

[18] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, pp. 108500, 2021.

[19] R. Zhang and Z. Hu, "Access control method of network security authentication information based on fuzzy reasoning algorithm," *Measurement*, vol. 185, pp. 110103, 2021.

[20] M. O. Alassafi, "Success indicators for an efficient utilization of cloud computing in healthcare organizations: Saudi healthcare as case study," *Computer Methods and Programs in Biomedicine*, vol. 212, pp. 106466, 2021.

[21] 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.

[22] K. Fan, S. Wang, Y. Ren, H. Li and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–11, 2018.

[23] D. Datta, L. Garg, K. Srinivasan, A. Inoue, G. T. Reddy *et al.,* "An efficient sound and data steganography based secure authentication system," *Computers, Materials & Continua*, vol. 67, no. 1, pp. 723–751, 2021.

[24] C. Jin, Y. Xu, G. Chen, C. Yu, Y. Jin *et al.,* "EBIAC: Efficient biometric identity-based access control for wireless body area networks," *Journal of Systems Architecture*, vol. 121, pp. 102317, 2021.

[25] Y. T. Huang, D. L. Chiang, T. S. Chen, S. D. Wang, F. P. Lai *et al.,* "Lagrange interpolation-driven access control mechanism: Towards secure and privacy-preserving fusion of personal health records," *Knowledge-Based Systems*, vol. 236, pp. 107679, 2022.

[26] J. Zhang, N. Xue and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[27] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 1–8, 2016.

[28] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of Medical Systems*, vol. 42, pp. 1–18, 2018.

[29] A. AL-Ashmori, S. Basri, P. Dominic, A. Muneer, Q. Al-Tashi *et al.,* "Blockchain-oriented software development issues: A literature review," *Proceedings of the Computational Methods in Systems and Software*, vol. 232, pp. 48–57, 2021.

[30] N. A. Akbar, A. Muneer, N. ElHakim and S. M. Fati, "Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses," *Future Internet*, vol. 13, no. 11, pp. 285, 2021.

[31] S. Prasad and B. Purushothama, "CCA secure and efficient proxy re-encryption scheme without bilinear pairing," *Journal of Information Security and Applications*, vol. 58, pp. 102703, 2021.

[32] M. S. Rahman, I. Khalil and X. Yi, "A lossless dna data hiding approach for data authenticity in mobile cloud based healthcare systems," *International Journal of Information Management*, vol. 45, pp. 276–288, 2019.

[33] D. K. Sharma, D. S. Chakravarthi, A. A. Shaikh, A. A. A. Ahmed, S. Jaiswal *et al.,* "The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique," *Materials Today: Proceedings*, vol. 7, pp. 2214–7853, 2021.

[34] M. Sookhak, M. R. Jabbarpour, N. S. Safa and F. R. Yu, "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues," *Journal of Network and Computer Applications*, vol. 178, pp. 102950, 2021.

[35] S. Dash, S. K. Shakyawar, M. Sharma and S. Kaushik, "Big data in healthcare: Management, analysis and future prospects," *Journal of Big Data*, vol. 6, pp. 1–25, 2019.