Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6486 - 6495
Received 16 February 2021; Accepted 08 March 2021.

Blockchain-Based Framework for Interoperable Electronic Health Record

Faheem A Reegu[1], Maher O Al-Khateeb[2], Waleed A Zogaan[3], Mohammad R AL-Mousa[4], Shadab Alam[5],Ibrahim Al-Shourbaji[6].

Department of Computer and Network Engineering, Jazan University,Jazan, Saudi Arabia[1]
Department of Computer Science, Zarqa University, Zarqa, 13132, Jordan[2]
Department of Computer science, Jazan University, Jazan 45142, Saudi Arabia[3]
Department of Computer Science, Zarqa University, Zarqa, 13132, Jordan[4]
Department of Computer science, Jazan University, Jazan 45142, Saudi Arabia[5]
Department of Computer and Network Engineering, Jazan University, Jazan, Saudi Arabia[6],
alshourbajiibrahim@gmail.com

Abstract

Electronic Health Record (EHR) is being used in most healthcare institutions through the advancement in computer technologies to preserve and share health records instead of a paper-based method. Data information should be exchanged amongst various parties and users' privileges to manage access to their records should also be provided. In addition to the basic standards of secrecy, confidentiality and integrity of information, these acts further demonstrate the need for interoperability and consumer access to personal data. EHR frameworks face problems in the protection of data collection, reputation and management. Blockchain technology has arisen as a powerful technology that can offer the immutability, confidentiality and user access properties of stored information without the need for centralized storage. This paper discusses the different EHR norms, specifications and problems and also offers a comparative analysis of various EHR specifications and current blockchain-based EHR systems. Finally, it suggests an interoperable EHR system focused on blockchain.

Keywords—Blockchain, Interoperability, Security, EHR Standards.

INTRODUCTION

EHR is a real-time official health record of a patient in a digital version that can be shared easily, securely, and instantly among different facilities and departments. It includes every data required to get the patient's details, including medical history, radiology images, diagnoses, medications, immunization dates, treatment plans, allergies, laboratory results, etc. It plays a significant role in healthcare because it delivers easy access to health records used in -making related to patient care.

: The deficiency of standardisation and regulation of sharing files create EHR interoperability, which healthcare providers have to consider. According to [1], divergence and discrepancy in health IT standards usage render several administrations powerless for exchanging records among different EHR solutions [1]. Healthcare providers are not entirely satisfied with the available EHR system. According to the study in[2], Heterogeneity in the EHR system and EHRs present additional complications and obstructions in sharing information among health care organisations and medical professionals. Determining confidentiality and security during information sharing increases the complication in attaining interoperability [2]. "Medicare and Medicaid Promoting Interoperability Programs" in 2019, was intended to encourage EHR interoperability amongst suppliers [3][4]. The reality is that owing to the inadequate coordination requirements among the various EHRs, increased costs of participation, the low engagement of patients in data sharing and the absence of patient identity in health data sharing are not coordinated efficiently and interoperable across different EHRs, and other Health Information Exchanges (HIE)[5] [6].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6486 - 6495
Received 16 February 2021; Accepted 08 March 2021.

A blockchain is defined as a digitized record of the transaction. This technology is referred to as blockchains, owing to its architecture. It contains individual records, referred to as inter-linked blocks, organised into a discrete sequence, referred to as a chain. Each transaction is applied to the blockchain after validation by separate interconnected validating nodes [7][8]. The blockchain is a simple illustration of Distributed Ledger Technology (DLT) [9]. Organised to monitor the various forms of blockchain transactions, these networks form a peer-to-peer transaction-related network [10]. They make attempts to validate in an organised manner that every transaction is verified right before it is added to the blockchain. This distributed network of computer nodes certifies that null or unwanted blocks have not been linked to a unique chain by a solitary unit [11]. Whenever a unique block is added to a blockchain, it is interlinked with the previous blocks using a "cryptographic hash" generated from within the former block. It assures that the chain is not in any way broken and that any block is permanently recorded. It is also deliberately difficult to modify earlier transactions in the blockchain when all the active blocks had to be transformed first. Block-chain is sometimes referred to as a

"Distributed Ledger Technology (DLT)" has established a special history connected to a decentralised asset that can be unchanged and translucent by utilising cryptographic hashing and decentralisation. Blockchain is one such unique technology that can play a role in enhancing encryption and security. Because of its immutability features, blockchain is a unique technology that can improve security and security [12].

Different studies[12,14] has been conducted to identify challenges and provide a future recommendation to improve the state of the art blockchain-based framework with less emphasis on interoperability attribute. This study, however specifically conducted to identify the interoperability challenges in a blockchain-based framework linked with electronic health records and proposed a conceptual framework to address interoperability challenges. The rest of the paper is organized as follows. Section 2 provides the background of the study. Section 3 described blockchain in EHR. Section 4 proposed a conceptual framework, and the last section concludes the study.

BACKGROUND STUDY

A. EHR

Before the 1960s, all therapeutic records were documented and reported by using papers and is filed manually. Lab reports, diagnoses, medicine directions, and visit notes, were all maintained and written by using the simple paper sheets arranged together for maintaining the records of the patients. Moreover, these medical records were retrieved and filed from specifically designed shelves to carry these records' file folders. Afterward, in the 1960s, things started to revolutionise, developing electronic healthcare records systems [13].

According to [12,13], the initial use of EHRs comprises the exchange of information for the processing of claims and scanning images to capture documents [14]. This advancement was found to be helpful and save time by obsoleting the method of retrieval and filing of documents or charts, controlling the location of the chart, and photocopying. Representing the data become easy through the graphical representation technique. Microcomputer network workstations were designed to transcribe all patient orders that are related to an EHR. Hence, patient charges were lower down significantly along with the hospital costs [15].

Automated management for the records makes the patient records accessible that can be linked easily to the monitoring gadgets for recording and interpreting patients' data in the EHR. Rapidly with the growing period, the EHRs started to use in production and enormous amounts to maintain the medical data found to be effective in doing research related to epidemiology. Though, subordinate use of data related to EHR highlighted the problems or errors with the quality of the recorded data for analysis and evaluation soon. Data usage with the goals except for the purpose for which it was obtained displayed that poor quality of data frequently directed to noteworthy misrepresentation and impending patient harm [16].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6486 - 6495
Received 16 February 2021; Accepted 08 March 2021.

Most of the EHRs are designed on web/client-server bases in the modern world, use data access, relational databases, and entry screens that are circumnavigated by using mouse like scrolling and pointer devices. In the United States, the upsurge in the adoption of EHR was enthused by the year 2009. Automatically allocating healthcare information from one department to another department has now developed frequently, and numerous medical administrations have applied HIE and EHRs networks [17].

There have been considerable progressions in few years in EHR; however, most of the previous expectations have not been understood, and present EHRs require more improvement to meet the requirement of the present speedily altering the environment in healthcare. Advancing EHR technology will help in delivering interoperable solutions based on international standards.

B. *EHR Requirements*

There are several specifications for and they are as follows:

(a) Interoperability: High-performance transfers, enhanced patient outcomes, improved health status, decreased duplication practices, and reduced uncertainty are facilitated through interoperability and inter-party data sharing [18]. The degree to which devices and systems can transfer data and translate shared data is known as interoperability in the EHR. In clinical decision-making, this understanding of the data expressed will assist [19].

(b) Privacy and Security: Encryption is expected to preserve confidentiality of information [20][21]. Administrative, open and physical protection measures are the three dependencies that ensure confidential health records' confidentiality as defined by the HIPAA. In the healthcare context, privacy is meant to enable patients to have the right to manage their medical records by authorisation as exists in the EHRs patients can use and change their private records [22].

(c) Confidentiality: An expansion of privacy is associated with data security, in particular. If it is assigned to the dimension of safe contact or consent between caregivers and patients, it is separated from privacy. Specialists who typically have relations with the patient's history have a legal or moral obligation to preserve trust in the data [23].

(d) Access control: Access to medical information can also be approved only through accredited healthcare specialists and patients. Appropriate alert protocols informed approval, and explicit permission should enable patients to receive their data and provide oversight over who will use it. Regulation is key (CCF) [24].

(e) Data Sharing: the distribution of medical records is an essential requirement when the patient's supervision is dispersed through various health care facilities. It will encourage most physicians to study the patient's medical history for optimum diagnosis and minimise duplication of diagnostic and radiology tests. The exchange of community data is broken into three separate categories depending on the members. The data is shared within the corresponding medical organisation. And the specifics are given to the patient, the patient's friends, and relatives. Lastly, the data were shared with other medical organisations and with the government [25].

(f) Data Integrity and availability: Fairness ensures the results' efficacy and accuracy are preserved. In EHR, this points to the assumption that unapproved usage of the records has not been tainted. The data must be ready for every EHR to serve its function. Moreover, this suggests that the database structures used to maintain and process EHR data, the security measures used to secure them, and the communication networks used to access them must operate properly [26][27].

EHR is a growing technology that should be implemented by fulfilling the above requirements so that the errors and issues of using it can be reduced.

C. *EHR Standards*

Different organisations and agencies have tried to standardise the EHR requirements. However, few of them have been summarised in Table1 while a comparative study between EHR standardrs, prose, cons and limitations are provided in Table 2.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6486 - 6495
Received 16 February 2021; Accepted 08 March 2021.

TABLE 1: EHR STANDARDS

EHR Standard	Description
HL7	The HL7 is the "EHR System Functional Model (EHR-S FM)". It summaries the significant functions and applications that must be regulated in an EHR system. This model delivers a standard description and understanding of operations easily in medical-care settings through the formation of practical profiles. It provides a framework for driving the necessities and requests of high standards and a standard-based methodology for applying functions related to care settings, priorities, and used by every state [28].
HITECH	The HITECH Act aims to advance the technique through which services are provided to the patients by spending on advancing medical information technology. It promotes healthcare professionals by providing financial incentives to use EHRs to maintain the privacy and security of the patient data. Additionally, there will be penalties for violating the security and privacy set rules [29].
HIPAA	Health Insurance Portability and Accountability Act of 1996 (HIPAA) certify that the patients have rights to their personal health information of any type. According to [12], the HIPAA Security Rule was also created to necessitate explicit defenses to protect the patients' electronic health information. Under the Security Rule, providers must implement specific measures to be compliant and keep protected health information secure [30].
C-CDA	The HL7 Consolidated CDA (C-CDA) is an execution guideline that particularises the library of templates and suggests their usage for collecting specific types of documents [31].
OPEN- EHR	The open standard specification defines management, collection, recovery and sharing of health data in electronic health reports (EHRs). It is the name of a new tool used for e-health, comprising exposed particularisations, clinical software, and models that could be utilised for building standards and information production with the solutions of interoperability for medical-care [32].
THE OWL	The OWL is used to address the numerous informatics challenges and terminologies associated with the description and origin of variables for reporting qualitatively from healthcare data in EHR. It is precise in meaning, reusable, and supports dispersed web-based processing of discrete healthcare data [33].
SNOMED CT	It is a standard clinical term with particular support for "multilingual translation". It is implemented in approximately more than fifty states. SNOMED-CT aims to add substantial meaning to EHR by permitting operative, significant depiction of healthcare data. It shows an essential role in world-wide activities to provide economical and high-quality healthcare to patients [34].

TABLE 2: COMPARATIVE STUDY OF EHR STANDARDS

Standard	Advantages	Disadvantages	Limitation
CEN/ISO EN13606	Ensures increased privacy of patients' data	There is a digital rights management problem	It mainly focuses on centralised data repository
Health Level7 (HL7)	Enhance care delivery,	There is a problem of	It does not handle

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6486 - 6495
Received 16 February 2021; Accepted 08 March 2021.

	decrease ambiguity, maximise workflow,	syntax complexity which leads to poor implementation	image digitisation
Digital imaging and communications in medicine (DICOM)	Ensures effective integration of medical images from various manufacturers' machines	It has too many field options to be filled with data which is time-consuming	Requires state-of-the-art sensor systems to manage digital images.
Systematized Nomenclature of medicine—clinical terms (SNOMED CT)	Ensures that clinical data is multilingual, accurate.	It is hard to adapt it natively because of many principles.	Data inconsistency and reduced integrity
The Health Insurance Portability and Accountability (HIPAA)	Protects patients' data from unauthorised users	Providers tend to pay fines in case of violations. It only provided crucial record information to patients.	More human resources required to maintain the requirements of HIPAA
Health Information Technology for Economic and Clinical Health Act (HITECH)	Improves healthcare quality, safety, efficiency	It does not increase healthcare personnel's concerns regarding liability	Deception by using false data

D. *Issues in EHR*

EHR technology resolves some issues on one side but further creates some issues on another side. It becomes easy to hack the data if prior precautions have not been taken. As it is a new way of storing data, staff need proper training to use it. Electronic health records contain highly crucial and critical patient-related medical data, requiring safe storage, sharing, retrieval, and scope. To encourage and enhance healthcare facilities' condition, medical knowledge must be preserved and exchanged routinely by several different shareholders, including physicians, healthcare professionals, pharmacies, insurance agencies, and researchers. Overall, individual key data exchange styles require rigorous confidentiality and ac-accountability requirements during data transfers. [33], it the EHR has a poorly designed interface, the workflow would become slow [35]. Inconsistency and inaccuracy are common issues in EHR technology [36].

Communicating information in an EHR might be delayed because interoperability is insufficient within the present EHR mechanisms in use or from EHR to any other systems. Therefore, in a few situations, it has been observed that physicians are unable to access labs for a patient present in a hospital from records present in a diverse portion of the hospital. Moreover, healthcare professionals may discover it challenging to interpret data because displays in EHR can be cluttering, confusing, or inaccurate. For instance, a healthcare professional strived to order 4.5 mg of medicine. Still, the EHR registered only a 7.5 mg medication, with a 4.7 mg dosage recorded in minor print that can confuse the healthcare professionals.

II. BLOCKCHAIN IN EHR

Blockchain will renovate the process through which electronic health records are shared and processed by protecting them via a distributed peer-to-peer connection through pro- viding a safe solution for medical data exchanging medical data in healthcare efficiency. According to[12], the Blockchain approach is suggested to provide sustenance and comfort to the procedure for understanding the dispersed technologies of ledger [27]. According to [19], blockchain was mainly submitted to include digital

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6486 - 6495
Received 16 February 2021; Accepted 08 March 2021.

archives of cash-related transactions autonomous of central authorities or monetary alliances [37]. Table 3 provides some existing blockchain-based EHR frameworks along with their issues.

TABLE 3: REVIEW OF EXISTING BLOCKCHAIN-BASED EHR FRAMEWORKS AND ISSUES

Ref	Year	Title	Issues
[38]	2019	BinDaaS: Blockchain-based deep learning as a Service in healthcare 4.0 applications.	Privacy, data ownership, collusion attacks, scalability of mined transactions, cost and storage issues
[39]	2018	Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology.	A collusion of 51% of mining, mitigates the ability of, high storage cost external actors to gain access to PHI
[40]	2018	BHEEM: A blockchain-based framework for securing electronic health records.	Interoperability
[41]	2018	Multi-tier blockchain framework for IoT-EHRs systems	Securing IoT devices
[42]	2020	ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care	Scalability, Interoperability
[43]	2017	MediBchain: A Blockchain-based Privacy Preserving Platform for Healthcare Data	Scalability
[44]	2018	EMRShare: A cross-organizational medical data sharing and management framework using permissioned blockchain	Interoperability
[45]	2019	DASS-CARE: a decentralised, accessible, scalable, and secure healthcare framework using blockchain.	Maintaining the privacy of data, interoperability
[46]	2019	Clinicappchain: A low-cost blockchain Hyperledger solution for healthcare.	Integration of two disruptive technologies, i.e., IoT and Blockchain
[47]	2019	Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform	interoperability, Scalability

Innovations have powered this innovative blockchain technology to provide better transactions, including insurance billing, health records, and smart contracts. Along with having a disseminated transaction record, it allows for permanent data entry and authentication. The blockchain substructure spanning a product's entire life cycle will include data interoperability, improved access to medical information, and framework monitoring. Blockchain will be used for more robust EHR solutions, among other emerging developments such as the Internet of Things (IoT) and Cloud Computing [48][49]. IoT devices may collect various health-related details such as BP, blood sugar level, temperature, ECG etc., and cloud storage can be used to store records for better resource scalability and utilisation [50]. Blockchain will discuss the security, longevity, immutability and inter-operability functionality[51]. Entry to patient health information is necessary to administer drugs, with blockchain appropriate. It will quickly boost the system of patient care services dramatically. Via previous experiments, multiple options for

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6486 - 6495
Received 16 February 2021; Accepted 08 March 2021.

refining the current vulnerabilities in medical systems can be obtained by exploiting blockchain technology. In Table 3, several of these recent Blockchain-based EHR deployments have been examined, and relevant issues have been summarised.

III. BLOCKCHAIN-BASED EHR FRAMEWORK

The proposed framework is primarily divided into three main layers. Layer 1 has different healthcare organisations having their own EHR storage. Level 2 is a blockchain layer that connects with organisation layers with the help of a transformation API and further connects with the database layer with the help of a file share application—the last layer of storage stores the records using the Interplanetary File System (IPFS). The detailed architecture of the proposed EHR framework is given in Figure 1. This framework allows different healthcare organisations such as hospitals, pathology labs, doctors and patients a platform for interconnection.

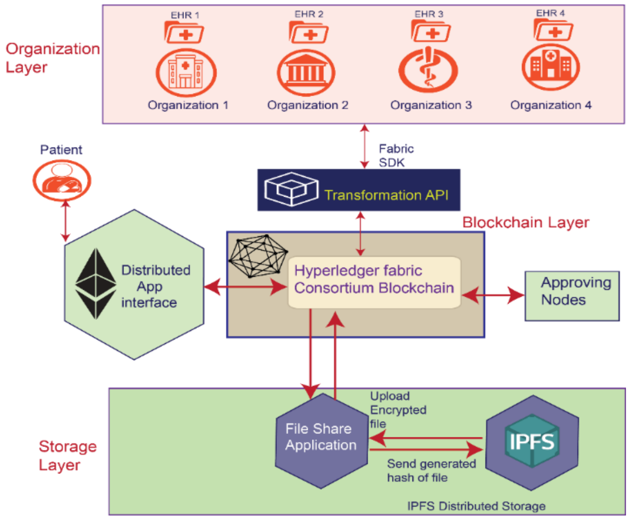

FIGURE 1: PROPOSED FRAMEWORK FOR INTEROPERABLE EHR

Through the assistance of a distributed app interface, patients are linked to the blockchain layer, and patients may be able to monitor their respective health information and authorise access to a separate group of people. It allows the personal data access. The blockchain layer would be a blockchain alliance composed of Hyper ledger fabric. A collection of pre-defined approval nodes responsible for approving every new block will be open. Once a new block is formed, all participating nodes will then be shared with it. Interaction with the Fabric blockchain network can take place with the assistance of the SDK fabric transition API. The development of a new blockchain-based EHR database for current organisations does not need this structure. The internal EHR database will be interconnected and the system-connected transition API will be used.

IV. CONCLUSION

EHR is the digital record of the medical history of the patient. It has solved many issues related to data handling and its security. For implementing this technology, a detailed study is required under modern technology and standards so that errors can be minimised in integration. It must be kept in mind that before its implementation, makes sure that it is well-designed and updated to avoid any sort of security issue related to consistency and accuracy. This paper has reviewed the various EHR requirements, issues with EHR systems, and the use of blockchain to resolve these issues. We have further examined the different EHR standards and existing blockchain-based EHR frameworks highlighting the problems. Last, we have proposed a blockchain-based interoperable EHR framework that will provide essential security and reliability requirements. It will enable different organisations following different internal structures to interact with each other without replacing the existing EHR infrastructure of organisations. Although the proposed framework has not been implemented, it provides a general framework that can be further analysed and implemented in the future.

REFERENCES

[1] B. Blobel, "Interoperable EHR systems–challenges, standards and solutions," *Eur. J. Biomed. Informatics*, vol. 14, no. 2, pp. 10–19, 2018.

[2] S. Bhartiya, D. Mehrotra, and A. Girdhar, "Issues in achieving complete interoperability while sharing electronic health records," *Procedia Comput. Sci.*, vol. 78, pp. 192–198, 2016.

[3] F. Reegu, W. Z. Khan, S. M. Daud, Q. Arshad, and N. Armi, "A Reliable Public Safety Framework for Industrial Internet of Things (IIoT)," in *2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*, 2020, pp. 189–193, doi: 10.1109/ICRAMET51080.2020.9298690.

[4] F. Masoodi, S. Alam, and S. T. Siddiqui, "Security and privacy threats, attacks and countermeasures in Internet of Things," *Int. J. Netw. Secur. Appl*, pp. 67–77, 2019.

[5] M. L. Braunstein, "Healthcare in the age of interoperability: the promise of fast healthcare interoperability resources," *IEEE Pulse*, vol. 9, no. 6, pp. 24–27, 2018.

[6] T. Hardin and D. Kotz, "Blockchain in health data systems: A survey," in *2019 sixth international conference on internet of things: Systems, management and security (IOTSMS)*, 2019, pp. 490–497.

[7] S. T. Siddiqui, R. Ahmad, M. Shuaib, and S. Alam, "Blockchain Security Threats, Attacks and Countermeasures," in *Advances in Intelligent Systems and Computing*, 2020, vol. 1097, pp. 51–62, doi: 10.1007/978-981-15-1518-7_5.

[8] M. Shuaib, S. M. Daud, S. Alam, and W. Z. Khan, "Blockchain-based framework for secure and reliable land registry system," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 5, pp. 2560–2571, Oct. 2020, doi: 10.12928/TELKOMNIKA.v18i5.15787.

[9] S. Tabrez Siddiqui, M. Shuaib, A. Kumar Gupta, and S. Alam, "Implementing Blockchain Technology: Way to Avoid Evasive Threats to Information Security on Cloud," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, Sep. 2020, no. October, pp. 1–5, doi: 10.1109/ICCIT-144147971.2020.9213798.

[10] M. Shuaib, S. Alam, S. Mohd, and S. Ahmad, "Blockchain-Based Initiatives in Social Security Sector," in *EAI 2nd International Conference on ICT for Digital, Smart, and Sustainable Development (ICIDSSD)*, 2020, p. 8.

[11] S. T. Siddiqui, S. Alam, M. Shuaib, and A. Gupta, "Cloud Computing Security using Blockchain," *J. Emerg. Technol. Innov. Res.*, vol. 6, no. 6, pp. 791–794, 2019.

[12] S. Abdus, A. Shadab, S. Mohammed, and B. Mohammad.Ubaidullah, "Internet of Vehicles (IoV) Requirements, Attacks and Countermeasures," *5 Int. Conf. "Co mputing Sustain. Glob. Dev.*, no. March, pp. 4037–4040, 2018.

[13] M. M. M. Pai, R. Ganiga, R. M. Pai, and R. K. Sinha, "Standard electronic health record (EHR) framework for Indian healthcare system," *Heal. Serv. Outcomes Res. Methodol.*, pp. 1–24, 2021.

[14] R. S. Evans, "Electronic health records: then, now, and in the future," *Yearb. Med. Inform.*, no. Suppl 1, p. S48, 2016.

[15] M. R. Cowie *et al.*, "Electronic health records to facilitate clinical research," *Clin. Res. Cardiol.*, vol. 106, no. 1, pp. 1–9, 2017.

[16] C. S. Kruse, A. Stein, H. Thomas, and H. Kaur, "The use of electronic health records to support population health: a systematic review of the literature," *J. Med. Syst.*, vol. 42, no. 11, pp. 1–16, 2018.

[17] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Informatics J.*, 2020.

[18] E. Adel, S. El-Sappagh, S. Barakat, and M. Elmogy, "Distributed electronic health record based on semantic interoperability using fuzzy ontology: a survey," *Int. J. Comput. Appl.*, vol. 40, no. 4, pp. 223–241, 2018, doi: 10.1080/1206212X.2017.1418237.

[19] U. Shrivastava, J. Song, and B. Han, "The implications of patient data security considerations for EHR

interoperability and downtime recovery," 2019.
[20] M. U. Bokhari, S. Alam, and S. H. Hasan, "A Detailed Analysis of Grain family of Stream Ciphers.," *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 6, 2014.
[21] M. U. Bokhari and S. Alam, "BSF-128: a new synchronous stream cipher design," in *Proceeding of international conference on emerging trends in engineering and technology*, 2013, pp. 541–545.
[22] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security Techniques for the Electronic Health Records," *J. Med. Syst.*, vol. 41, no. 8, 2017, doi: 10.1007/s10916-017-0778-4.
[23] B. A. Pandow, A. M. Bamhdi, and F. Masoodi, "Internet of Things: Financial Perspective and Associated Security Concerns," *Int. J. Comput. Theory Eng.*, vol. 12, no. 5, 2020.
[24] C. A. Ardagna, S. De Capitani Di Vimercati, S. Foresti, T. W. Grandison, S. Jajodia, and P. Samarati, "Access control for smarter healthcare using policy spaces," *Comput. Secur.*, vol. 29, no. 8, pp. 848–858, 2010, doi: 10.1016/j.cose.2010.07.001.
[25] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y.-C. Tu, "MedBloc: A Blockchain-Based Secure EHR System for Sharing and Accessing Medical Data," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019, pp. 594–601.
[26] M. U. Bokhari, S. Alam, and F. S. Masoodi, "Cryptanalysis techniques for stream cipher: a survey," *Int. J. Comput. Appl.*, vol. 60, no. 9, 2012.
[27] A. H. Mayer, C. A. da Costa, and R. da R. Righi, "Electronic health records in a blockchain: a systematic review," *Health Informatics J.*, vol. 26, no. 2, pp. 1273–1288, 2020.
[28] R. Saripalle, C. Runyan, and M. Russell, "Using HL7 FHIR to achieve interoperability in patient health record," *J. Biomed. Inform.*, vol. 94, p. 103188, 2019.
[29] S. T. Mennemeyer, N. Menachemi, S. Rahurkar, and E. W. Ford, "Impact of the HITECH act on physicians' adoption of electronic health records," *J. Am. Med. Informatics Assoc.*, vol. 23, no. 2, pp. 375–379, 2016.
[30] B. B. Frey, "Health Insurance Portability and Accountability Act," in *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*, 2455 Teller Road, Thousand Oaks, California 91320, Thousand Oaks, California 91320: SAGE Publications, Inc., 2018.
[31] P. Wang, L. Zhou, D. Mu, D. Zhang, and Q. Shao, "What makes clinical documents helpful and engaging? An empirical investigation of experience sharing in an online medical community," *Int. J. Med. Inform.*, vol. 143, p. 104273, 2020.
[32] L. Min, Q. Tian, X. Lu, and H. Duan, "Modeling EHR with the openEHR approach: an exploratory study in China," *BMC Med. Inform. Decis. Mak.*, vol. 18, no. 1, pp. 1–15, 2018.
[33] C. Tao *et al.*, "Phenotyping on EHR data using OWL and semantic web technologies," in *International Conference on Smart Health*, 2013, pp. 31–32.
[34] D. Lee, N. de Keizer, F. Lau, and R. Cornet, "Literature review of SNOMED CT use," *J. Am. Med. Informatics Assoc.*, vol. 21, no. e1, pp. e11–e19, 2014.
[35] P. Palvia, T. Jacks, and W. Brown, "Critical issues in EHR implementation: provider and vendor perspectives," *Commun. Assoc. Inf. Syst.*, vol. 36, no. 1, p. 36, 2015.
[36] F. Girardi, G. De Gennaro, L. Colizzi, and N. Convertini, "Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain," *Electronics*, vol. 9, no. 6, p. 884, 2020.
[37] A. Farouk *et al.*, "Blockchain platform for industrial healthcare: Vision and future opportunities," *Comput. Commun.*, vol. 154, no. February, pp. 223–235, 2020, doi: 10.1016/j.comcom.2020.02.058.
[38] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar, "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications," *IEEE Trans. Netw. Sci. Eng.*, 2019, doi: 10.1109/TNSE.2019.2961932.
[39] G. G. Dagher, J. Mohler, M. Milojkovic, and P. Babu, "Ancile : Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, no. August 2017, pp. 283–297, 2018, doi: 10.1016/j.scs.2018.02.014.
[40] J. Vora *et al.*, "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," in

2018 IEEE Globecom Workshops (GC Wkshps), Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOMW.2018.8644088.

[41] S. Badr, I. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," in *Procedia Computer Science*, Jan. 2018, vol. 141, pp. 159–166, doi: 10.1016/j.procs.2018.10.162.

[42] A. Dubovitskaya *et al.*, "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *J. Med. Internet Res.*, vol. 22, no. 8, Aug. 2020, doi: 10.2196/13598.

[43] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A blockchain based privacy preserving platform for healthcare data," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10658 LNCS, pp. 534–543, doi: 10.1007/978-3-319-72395-2_49.

[44] Z. Xiao *et al.*, "EMRShare: A Cross-Organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain," in *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, Feb. 2019, vol. 2018-Decem, pp. 998–1003, doi: 10.1109/PADSW.2018.8645049.

[45] J. N. Al-Karaki, A. Gawanmeh, M. Ayache, and A. Mashaleh, "DASS-CARE: A decentralised, accessible, scalable, and secure healthcare framework using blockchain," in *2019 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019*, Jun. 2019, pp. 330–335, doi: 10.1109/IWCMC.2019.8766714.

[46] D. J. Munoz, D. A. Constantinescu, R. Asenjo, and L. Fuentes, "Clinicappchain: A low-cost blockchain hyperledger solution for healthcare," in *Advances in Intelligent Systems and Computing*, 2020, vol. 1010, pp. 36–44, doi: 10.1007/978-3-030-23813-1_5.

[47] L. Xu, A. Bagula, O. Isafiade, K. Ma, and T. Chiwewe, "Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform," *11th Acad. Conf. ITU Kaleidosc. ICT Heal. Networks, Stand. Innov. ITU K 2019*, 2019, doi: 10.23919/ITUK48006.2019.8995905.

[48] S. Alam, S. T. Siddiqui, A. Ahmad, R. Ahmad, and M. Shuaib, "Internet of things (IoT) enabling technologies, requirements, and security challenges," in *Lecture Notes in Networks and Systems*, vol. 94, 2020, pp. 119–126.

[49] M. Shuaib, A. Samad, S. Alam, and S. T. Siddiqui, "Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challenges for Cloud Migration in Organisations," in *Advances in Intelligent Systems and Computing*, vol. 904, 2019, pp. 387–399.

[50] M. A. Khan, M. T. Quasim, F. Algarni, and A. Alharthi, *Decentralised Internet of Things: A blockchain perspective*, vol. 71. Springer Nature, 2020.

[51] M. T. Quasim, M. A. Khan, F. Algarni, A. Alharthy, and G. M. M. Alshmrani, "Blockchain Frameworks," in *Decentralised Internet of Things*, Springer, 2020, pp. 75–89.