IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Analysis Of Security Concerns Privacy Issues And Interoperability In Healthcare System

Mrs.D.Kalpana[1] , Dr.R.Ramkumar[2]

Ph.D Research scholar [1] , Principal [2]

[1] Department of Computer Science, [1]Sasurie College of Arts & Science, Tirupur. Tamil Nadu, India.

Abstract: Security concerns, privacy issues, and interoperability are critical challenges facing modern healthcare systems. While the use of technologies like Internet of Things (IoT) devices, telemedicine, and Electronic Health Records (EHRs) has changed patient care, it has also brought new risks. This paper examines cyber security measures, privacy regulations, and interoperability standards essential for safeguarding patient data and ensuring seamless information exchange. Addressing these challenges is crucial to protect patient confidentiality, prevent data breaches, and enhance healthcare delivery. By promoting robust security practices, adhering to privacy laws, and fostering interoperable systems, healthcare organizations can harness the full potential of digital health technologies while maintaining patient trust and improving outcomes.

Index Terms - Security concerns, Privacy issues, Interoperability, Healthcare systems, Cyber security, Electronic Health Records (EHRs), Internet of Things (IOT).

I. INTRODUCTION

The healthcare sector has experienced a digital revolution in recent years, leveraging technology breakthroughs to optimize patient care, optimize workflow, and boost productivity. Key technologies driving this transformation include Electronic Health Records (EHRs), telemedicine, wearable health devices, and Internet of Things (IoT) applications. These innovations promise substantial benefits but also bring critical challenges in terms of security, privacy, and interoperability. The shift to digital platforms has led to the electronic storage and transmission of vast amounts of sensitive patient data, making healthcare organizations attractive targets for cyber attacks. Ensuring robust cyber security measures such as encryption, secure authentication, and access controls is essential to protect patient information. Additionally, maintaining patient privacy amid interconnected systems and diverse data sources remains a significant concern, necessitating stringent data protection policies as well as conformity to legal requirements. Furthermore, achieving interoperability between different healthcare systems and devices is crucial for seamless information exchange and coordinated patient care, requiring the adoption of standardized data formats and communication protocols. Addressing these challenges is imperative to harness the full potential of digital healthcare while safeguarding patient information and maintaining trust in healthcare systems.

Security Concerns

Security Issues Given the sensitive nature of patient data, security in healthcare systems is critical. With the adoption of EHRs and IoT devices, vast amounts of patient information, including medical history, treatments, and personal identifiers, are now stored and transmitted electronically. This digitalization introduces new security vulnerabilities, making healthcare organizations prime targets for cyber attacks. Breaches can lead to unauthorized access to patient records, identity theft, financial fraud, and even compromise patient safety by manipulating medical devices. Therefore, robust cyber security measures,

such as encryption, secure authentication, access controls, and regular security audits, are essential to safeguard patient data and maintain trust in healthcare systems.

Privacy Issues

Privacy concerns go hand-in-hand with security in healthcare systems. Patients have a right to expect that their personal health information will be kept confidential and used only for authorized purposes. However, the interconnected nature of modern healthcare environments, where data flows between healthcare providers, insurers, pharmacies, and other entities, poses significant challenges to maintaining patient privacy. Moreover, the use of health apps, wearable devices, and remote monitoring tools adds another layer of complexity, as these devices often collect sensitive health data that may not be adequately protected. Addressing privacy issues requires robust data protection policies, informed patient consent mechanisms, and adherence to regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in the European Union.

Interoperability Challenges

The capacity of various devices, applications, and information systems to communicate, share data, and use the information that has been exchanged, is crucial for delivering seamless and coordinated patient care. Despite the widespread adoption of EHR systems, healthcare organizations often struggle with interoperability challenges. Different systems may use different data formats, coding systems, or communication protocols, making it difficult to share information accurately and efficiently. Efforts to achieve interoperability include the development and adoption of health information exchange (HIE) standards, the use of Application Programming Interfaces (APIs) to facilitate data sharing, and policy initiatives aimed at promoting data exchange among healthcare providers.

II. LITERATURE SURVEY

1. M. M. Mahdy (2020) et.al proposed Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records. An Electronic Health Record (EHR) is an electronic, official health record containing a systematic collection of a patient's health information maintained by a healthcare provider. While EHRs have the potential to revolutionize healthcare, their adoption is hindered by concerns over patient privacy and data security, exacerbated by numerous hospital data breaches. Despite various proposed solutions for patient-controlled EHR data access, a secure and private system for flawless EHR sharing is still lacking. This paper proposes a hybrid distributed system architecture that addresses these issues by combining the decentralized data storage model's high reproducibility and availability with the centralized system's security through authorization and authentication. Additionally, the system leverages blockchain technology to ensure security, patient pseudonymity, usage consent requirements, and eventual data consistency among peers, while maintaining a ledger of all shared EHRs among healthcare providers.

2. J. N. Al-Karaki (2019) et.al proposed DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain. The healthcare industry is a complex system of interconnected entities, each managing patient data and records through disjoint information systems. Current IT solutions face significant challenges in sharing and accessing medical records across various stakeholders while maintaining their security and privacy. The global problem of creating, maintaining, and sharing sensitive medical records and clinical data among different stakeholders without compromising data privacy and integrity is still up for debate. The current state of healthcare records is frequently fragmented, disorganized, non-uniform, and decentralized. In response, we introduce DASS-CARE, a Blockchain-based platform that facilitates safe, scalable, decentralized access to medical records and other healthcare services. This architecture protects patient data's security, integrity, and confidentiality while enabling real-time access and modifications. Our objectives are to improve healthcare quality and lower delivery costs, enhance medical records management through EHR unification, and provide users with the ability to access their medical records without reference to their past, which is difficult to do with the current disjointed systems.

3. K. Ito (2018) et.al proposed i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data. The swift advancement of information and communication technology has led to the generation, storage, and utilization of copious amounts of personal health data in healthcare-related services. However, challenges such as data interoperability, security, and privacy still need to be addressed. Decentralized peer-to-peer digital ledgers like blockchain have gained popularity as a potential solution to these issues and privacy concerns with personal data. People can use blockchain technology to better use their own health data for better healthcare. In addition to describing blockchain-powered solutions for the use of personal health data in healthcare, this article provides a brief overview of blockchain's key components and addresses associated problems and obstacles. We introduce i-Blockchain, an individual-focused framework built on top of a permission blockchain extension. We cover its fundamental design, protocols, and many use cases.

4. C. Esposito (2017) et.al proposed Security and privacy for cloud-based data management in the health network service chain: a micro service approach. New tools facilitating the harmonization and interconnection of health data are essential for monitoring and preventing illness and sharing medical knowledge. Cloud-based solutions now support collaborative data science platforms and deliver various processing operations through network service chains. This article discusses the management and interchange of data connected to healthcare and suggests new micro services approach along with security and privacy needs. We explore the adoption of cloud computing within healthcare systems, emphasizing that interoperability of existing technologies will enhance the quality of life and efficiency of healthcare systems by making them more personalized and patient-centered while reducing operational costs and medical errors. In order to create a health network service chain that is socially acceptable, security and privacy issues must be carefully considered and resolved. We investigate these requirements and implications, discuss existing methods, and propose architecture for a secure manager for cloud-based healthcare-related data management and exchange.

5. B. Alamri (2021) et.al proposed A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain. People's health depends on having an up-to-date personal health record (PHR) system. However, in the e-Health and m-Health age, establishing a dependable PHR system is still difficult because of problems with data interoperability, patient control over data access, and data integration from various EHRs. In order to overcome these obstacles, we suggest an electronic health wallet (EHW) system that makes use of decentralized technologies such as IPFS and blockchain and embraces health data interoperability standards such as FHIR's APIs. Interoperability and data protection are guaranteed by the GDPR-compliant framework that the EHW for IoT-based PHR systems functions under. This system architecture and conceptual framework offer a complete solution for an interoperable, patient-centered IoT-based PHR system that respects data privacy. Furthermore, it permits health big data analytics by utilizing IoT data in a privacy-preserving way by promoting patients to share their data in a regulated way.

6. R. Gupta (2019) et.al proposed HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0. Telesurgery holds immense potential to provide real-time surgical services to remote locations via wireless communication, improving diagnostic precision and accuracy. However, existing telesurgery systems suffer from security, privacy, and interoperability issues, hindering their widespread adoption in healthcare centers globally. To address these challenges, we propose HaBiTs, a blockchain-based framework for secure and interoperable telesurgery. HaBiTs ensures security through block chain's immutability and interoperability via Smart Contracts (SCs), written in solidity or other blockchain-specific languages, which establish trust among all connected parties and eliminate the need for intermediaries in data sharing. This framework mitigates traditional telesurgery system issues and enhances its applicability in healthcare.

7. R. Gupta (2020) et.al proposed AaYusH: A Smart Contract-Based Telesurgery System for Healthcare 4.0. Telesurgery (TS) enabled by 5G Tactile Internet (TI) has significant potential to deliver real-time, highly accurate surgical services remotely, which could greatly benefit society with precise surgical diagnosis. However, current TS systems face challenges, including security, privacy, latency, and the high costs associated with blockchain storage, which limit their widespread adoption in surgical procedures globally. To overcome these challenges, we propose AaYusH, an innovative approach that leverages Ethereum smart contracts (ESC) and the Interplanetary File System (IPFS) for TS. ESC addresses security and privacy concerns by establishing trust through blockchain technology, while IPFS tackles storage cost issues by decentralizing data storage. We implement a real-time smart contract written in Solidity and rigorously test its security using the MyThril tool. Our evaluations demonstrate that AaYusH achieves lower

latency and reduced storage costs compared to traditional telesurgery systems. This method clears the way for wider adoption of TS in healthcare settings while also improving its security and efficiency. However, there are several obstacles to overcome, including implementation complexity, scalability issues, and regulatory compliance.

8. F. Gao (2016) et.al proposed Exploring Cloudy Collaboration in Healthcare: An Evaluation Framework of Cloud Computing Services for Hospitals. Cloud computing (CC) has the potential to enhance collaboration in hospitals, yet the adoption of cloud computing services (CCS) remains low. There is insufficient research on evaluating CCS in the hospital sector to inform adoption decisions. We suggest an evaluation framework (EF) for CCS in hospitals that is based on the human, organization, and technology fit model in order to close this gap. Our EF utilizes six dimensions to assess how CCS can facilitate collaboration. We applied this framework to evaluate 38 identified CCS for hospitals, demonstrating its effectiveness. This research contributes to both practice and research by providing a tool to screen available CCS and expedite cloud adoption processes in hospitals. By enhancing understanding of the benefits and challenges of CCS in hospital settings, our EF supports informed decision-making and promotes the integration of cloud technologies to improve healthcare collaboration.

9. A. Buzachis (2019) et.al proposed On the Design of a Blockchain-as-a-Service-Based Health Information Exchange (BaaS-HIE) System for Patient Monitoring. Health Information Exchange (HIE) activities among practitioners have expanded dramatically as a result of the digitization of health information; nevertheless, adoption of Electronic Health/Medical information (EHRs/EMRs) has been slower because of privacy, confidentiality, interoperability, and integrity concerns. We suggest a Blockchain-as-a-Service solution for HIE (BaaS-HIE) to overcome these difficulties. Our approach leverages a private Blockchain and smart contracts to manage access control to medical records. In order to ensure high application performance and economic viability, all health data are encrypted and stored in a decentralized Interplanetary File System (IPFS), while the hashes of the asset URIs are stored on the blockchain. Experimental results validate the feasibility of our approach, demonstrating its ability to provide a decentralized and finely-grained accessibility mechanism for both patients and doctors within healthcare systems. This solution enhances HIE activities, ensures data confidentiality, promotes interoperability and integrity, and utilizes blockchain and IPFS to enhance security and accessibility, despite potential challenges related to implementation complexity, scalability, initial costs, dependency on emerging technologies, and regulatory compliance.

10. A. H. Celdran (2018) et.al proposed ICE++: Improving Security, QoS, and High Availability of Medical Cyber-Physical Systems through Mobile Edge Computing. The next generation of eHealth systems is represented by the vision of Medical Cyber-Physical Systems (MCPS), which are intended to interact effectively, securely, and safely. These interconnected systems analyze patients' vital signs collected from medical devices, assess the patient's health status, and initiate treatments while providing information to doctors and medical actuators, thereby enhancing patient safety in a cost-effective manner. However, the MCPS vision also brings forth significant challenges, including security, privacy, Quality of Service (QoS), and the high availability of devices supporting the MCPS environment. The Integrated Clinical Environment (ICE) standard has made strides in promoting the open coordination of diverse medical devices, yet more effort is needed to fully address these challenges and realize the future of eHealth. In response, we identify critical limitations of ICE through scenario-based challenges related to security, QoS, and high availability. We suggest the ICE++ design as a solution to these issues and an expansion of the ICE standard. ICE++ uses SDN and NFV approaches to manage MCPS components effectively and autonomously, guaranteeing security, quality of service, and high availability. It is specifically built for the Mobile Edge Computing paradigm. Our experiments demonstrate the potential benefits of this solution in efficiently managing ICE components.

11. J. Liu (2018) et.al proposed BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. Electronic medical records (EMRs) are a critical form of healthcare data that are currently receiving significant attention. Sharing health data is essential for improving the quality of healthcare services and reducing medical costs. However, EMRs are often fragmented across decentralized hospitals, which impede data sharing and compromises patients' privacy. We suggest BPDS, a blockchain-based privacy-preserving data sharing solution for EMRs, as a solution to these problems. In BPDS, original EMRs are securely stored in the cloud, while their indexes are stored in a tamper-proof consortium blockchain. This approach significantly reduces the risk of medical data leakage, and ensures that EMRs cannot be arbitrarily modified, thanks to the blockchain indexes. Secure data sharing is facilitated

automatically based on patients' predefined access permissions through blockchain smart contracts. Additionally, the joint design of the CPABE-based access control mechanism and content extraction signature scheme ensures strong privacy preservation during data sharing. Security analysis demonstrates that BPDS is a secure and effective method for achieving EMR data sharing.

12. R. Kalaipriya (2020) et.al proposed Certain Investigations on Leveraging Blockchain Technology for Developing Electronic Health Records. This study aims to improve the state-of-the-art Electronic Health Records (EHR) frameworks by presenting a Blockchain-based design. EHRs contain sensitive patient information, necessitating robust tracking of all record events to ensure data integrity and secure transactions. To address these challenges, we propose two smart contracts: classified contracts and user record associated contracts. Classified contracts organize records in a distributed ledger format with secure interventions from doctors and healthcare providers. We evaluate this architecture using the Ethereum framework, including Remix environment, Metamask wallet, and Solidity language. Compared to conventional EHR frameworks, our proposed structure leveraging Blockchain technology improves efficiency and security in storing electronic health records.

Here's a comparison table summarizing the content

Author(s) & Year	Title	Proposed Solution	Merits	Demerits
M.M.Mahdy (2020)	Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of EHRs	Hybrid distributed system combining decentralized data storage and centralized security measures using blockchain.	Enhanced data security, improved patient privacy, high data reproducibility and availability, patient control over data access, secure and traceable EHR sharing.	High implementation costs, complexity in system integration, regulatory challenges, requires significant technological infrastructure, potential resistance from stakeholders.
J.N.AlKaraki (2019)	DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain	Blockchain-based platform for safe, scalable, decentralized access to medical records.	Improves healthcare quality, lowers costs, unifies EHRs, enhances data access and updates, ensures security, integrity, and confidentiality of patient data.	High implementation costs, technological complexity, potential integration challenges, regulatory hurdles, possible resistance from existing systems.
K. Ito (2018)	i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data	Individual-focused framework using permission blockchain for personal health data privacy and security.	Enhances data interoperability, improves security and privacy, empowers individuals with data control, facilitates better healthcare, supports diverse applications.	Complex implementation, high costs, potential scalability issues, integration challenges with existing systems, possible regulatory compliance hurdles.
C.Esposito (2017)	Security and privacy for cloud-based data management in the health network service chain	Microservices approach for secure and private cloud-based data management in healthcare.	Improves data interoperability, enhances healthcare quality, personalizes patient care, reduces costs and errors, addresses security and privacy requirements.	Complex implementation, high initial costs, potential integration challenges, ongoing security concerns, reliance on continuous cloud

				service availability.
B.Alamri (2021)	GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain	EHW system using IPFS and blockchain for interoperable, GDPR-compliant IoT-based PHR system.	Enhances data integration, ensures patient control, preserves privacy, supports interoperability, enables big data analytics, utilizes IoT data effectively.	High complexity, potential implementation costs, reliance on decentralized technologies, possible integration issues with existing systems, regulatory compliance challenges.
R.Gupta (2019)	HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0	Blockchain framework for secure, interoperable telesurgery.	Enhances precision in remote surgical procedures, improves diagnosis accuracy, ensures security and privacy via blockchain and Smart Contracts, enhances interoperability without intermediaries.	Complex implementation, potential scalability issues, high initial costs, dependency on blockchain technology, regulatory compliance challenges.
R.Gupta (2020)	AaYusH: A Smart Contract-Based Telesurgery System for Healthcare 4.0	Telesurgery system using Ethereum smart contracts and IPFS for secure, cost-effective telesurgery.	Enhances precision in remote surgical procedures, improves diagnosis accuracy, ensures security and privacy via blockchain and Smart Contracts, enhances interoperability without intermediaries.	Complex implementation, potential scalability issues, high initial costs, dependency on blockchain technology, regulatory compliance challenges.
F. Gao (2016)	Exploring Cloudy Collaboration in Healthcare: An Evaluation Framework of Cloud Computing Services for Hospitals	Evaluation framework for cloud computing services in hospitals to enhance collaboration.	Facilitates informed adoption decisions, enhances collaboration, comprehensive evaluation framework, practical application to screen and expedite cloud adoption in hospitals.	Complex implementation, potential resistance to change, resource-intensive evaluation process, adaptation to varying hospital contexts may be required.
A.Buzachis (2019)	Blockchain-as-a-Service-Based Health Information Exchange System for Patient Monitoring	BaaS solution using blockchain and IPFS for secure HIE.	Enhances HIE, ensures data confidentiality, interoperability, and integrity; uses blockchain and IPFS for security; decentralized accessibility mechanism.	Complex implementation, potential scalability issues, high initial costs, dependency on emerging technologies, regulatory compliance challenges.
A. H. Celdran (2018)	ICE++: Improving Security, QoS, and High	ICE++ design using SDN and NFV for secure,	Improves eHealth systems' efficiency and safety, enhances	Complex implementation, potential integration

	Availability of Medical Cyber-Physical Systems	high-quality, and available MCPS.	security, QoS, and availability.	challenges, reliance on emerging technologies, regulatory compliance requirements.
J. Liu (2018)	BPDS: Blockchain Based Privacy-Preserving Data Sharing for EMRs	BPDS using blockchain and CPABE-based access controls for secure EMR sharing.	Ensures secure, privacy-preserving EMR data sharing, improves healthcare service quality.	Requires robust infrastructure, careful management of smart contracts and encryption keys, potentially increasing complexity and costs.
R. Kalaipriya (2020)	Leveraging Blockchain Technology for Developing Electronic HealthRecords	Blockchain-based design for secure and efficient EHR storage using smart contracts.	Enhances security and efficiency in storing EHRs, ensures data integrity and secure transactions.	Requires expertise in blockchain technology, ongoing management of smart contracts and associated infrastructure.

III. CONCLUSION

In conclusion, addressing security concerns, privacy issues, and interoperability challenges is essential for the advancement of healthcare systems. Robust cyber security measures, strict adherence to privacy regulations, and the promotion of interoperability standards are crucial. Protecting patient data from cyber threats, ensuring confidentiality, and enabling seamless data exchange are paramount to maintaining trust and enhancing patient care. By fostering a secure and interoperable healthcare environment, healthcare providers can leverage technological advancements to improve efficiency, accuracy, and patient outcomes while safeguarding sensitive health information.

REFERENCES

[1] M. M. Mahdy, "Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records," *2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, Khartoum, Sudan, 2021, pp. 1-4, doi: 10.1109/ICCCEEE49695.2021.9429554.

[2] J. N. Al-Karaki, A. Gawanmeh, M. Ayache and A. Mashaleh, "DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco, 2019, pp. 330-335, doi: 10.1109/IWCMC.2019.8766714.

[3] K. Ito, K. Tago and Q. Jin, "i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data," *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, Hangzhou, China, 2018, pp. 829-833, doi: 10.1109/ITME.2018.00186.

[4] C. Esposito, A. Castiglione, C. -A. Tudorica and F. Pop, "Security and privacy for cloud-based data management in the health network service chain: a microservice approach," *in IEEE Communications Magazine*, vol. 55, no. 9, pp. 102-108, Sept.2017, doi: 10.1109/MCOM.2017.1700089.

[5] B. Alamri, I. T. Javed and T. Margaria, "A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain," *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, 2021, pp. 1-5, doi: 10.1109/NTMS49979.2021.9432661.

[6] R.Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat and B. Sadoun, "HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0," *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Beijing, China, 2019, pp. 1-5, doi: 10.1109/CITS.2019.8862127.

[7] R. Gupta, A. Shukla and S. Tanwar, "AaYusH: A Smart Contract-Based Telesurgery System for Healthcare 4.0," *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICCWorkshops49005.2020.9145044.

[8] F. Gao, S. Thiebes and A. Sunyaev, "Exploring Cloudy Collaboration in Healthcare: An Evaluation Framework of Cloud Computing Services for Hospitals," *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, 2016, pp. 979-988, doi: 10.1109/HICSS.2016.125.

[9] A. Buzachis, A. Celesti, M. Fazio and M. Villari, "On the Design of a Blockchain-as-a-Service-Based Health Information Exchange (BaaS-HIE) System for Patient Monitoring," *2019 IEEE Symposium on Computers and Communications (ISCC)*, Barcelona, Spain, 2019, pp. 1-6, doi: 10.1109/ISCC47284.2019.8969718.

[10] A. H. Celdran, F. J. García Clemente, J. Weimer and I. Lee, "ICE++: Improving Security, QoS, and High Availability of Medical Cyber-Physical Systems through Mobile Edge Computing," *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Ostrava, Czech Republic, 2018, pp. 1-8, doi: 10.1109/HealthCom.2018.8531185.

[11] J. Liu, X. Li, L. Ye, H. Zhang, X. Du and M. Guizani, "BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records," *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8647713.

[12] R. Kalaipriya, S. Devadharshini, R. Rajmohan, M. Pavithra and T. Ananthkumar, "Certain Investigations on Leveraging Blockchain Technology for Developing Electronic Health Records," *2020 International Conference on System,Computation Automation and Networking (ICSCAN)*, Pondicherry, India, 2020, pp. 1-5, doi: 10.1109/ICSCAN49426.2020.9262391.