CrossRef DOI of original article:

A Blockchain Technology to Secure Electronic Health Records in Healthcare System

Received: 1 January 1970 Accepted: 1 January 1970 Published: 1 January 1970

Abstract

Index terms—

1 I. INTRODUCTION

The SARS-CoV-2 virus, responsible for the greatest epidemic in millennia, has posed a serious threat to healthcare systems throughout the world. In addition to the immediate problems caused by the virus, the pandemic has revealed flaws in even the most modern healthcare systems, such as the inability to keep track of individuals with pre-existing diseases. Although industrialized nations like the United States were better equipped than others in responding to the epidemic, nearly one million Americans lost their lives as a result of the virus. Pre-pandemic research revealed flaws in the world's top healthcare systems, which impeded the most effective response to SARS-CoV-2. While wealthy countries' healthcare systems have their flaws, those in underdeveloped or underprivileged areas, such as India, are far more at risk. Long-term needs for hospital facilities, support personnel, and manpower are created by this sort of viral pandemic, all of which are often in limited supply in developing nations [1]. For us to meet this challenge, we'll need to manage our resources efficiently.

The potential effect of SARS-CoV-2 on the Indian Subcontinent, and India in particular, has been recognized ever since the breakout of the virus [2]. Big data is the capability to manage a huge volume of disparate data, at the right speed, and within the right time frame to allow real-time analysis and reaction. Big data is an evolving term that describes any amount of structured, semi-structured and unstructured data that has the potential to be mined for information [3].

2 II. LITERATURE SURVEY

With a population of close to 1.4 billion, India is one of the most populous countries on Earth. Before the epidemic, India's healthcare system already had significant challenges that were wreaking havoc on the country. Major public health issues include HIV/AIDS, malaria, and TB. As the income gap widens between the affluent and poor, another key worry is the availability and cost of decent healthcare. This problem has been exacerbated by statewide lockdowns. Recent studies have shown that the immediate effects of the lockdown would be a decrease in healthcare availability and an adverse effect on the population's physical and mental health and social well-being.

The widespread use of handwritten prescriptions especially in rural areas without computer systems and the almost complete lack of integration between healthcare and insurance systems are just a few of the widespread problems that have arisen as a result of the fragmented nature of the healthcare industry's information, communication, and tracking infrastructure [4].

Poor healthcare professional accountability is exacerbated by inadequate facilities, further straining doctor-patient ties. Paper records are more prone to human errors, such as illegibility or the loss of the physical object, which may lead to delays in treatment and perhaps preventable deaths.

Prescriptions and insurance coverage data are just two examples of the kinds of critical information that healthcare and insurance providers may share with pharmacies to expedite the delivery of pharmaceuticals to patients. It is difficult to achieve large-scale coordinated performance using paper-based information, but this is made possible by integrated healthcare system synchronization, which allows for patient-oriented monitoring capabilities and refill requests.

Any healthcare system that lacks the modern infrastructure essential to facilitating effective communication between healthcare practitioners, insurance providers, and patients would benefit greatly from implementing an Electronic Health Record (EHR) system. The influence of EHR will grow as the worldwide effort to disseminate and administer the Coronavirus vaccination continues [5].

Electronic health record systems will be crucial in managing the massive amounts of information sharing and monitoring that will be necessary to accomplish this massive task. [6].

3 Healthcare Records Security Breaches

Between 2009 and 2020, the HHS Office for Civil Rights received 3,705 allegations of healthcare data breaches involving 500 or more records. 268,189,693 healthcare records have been lost, stolen, leaked, or unlawfully released. 81.72 percent of the US population. In 2018, one breach involving 500 or more records was recorded each day. The rate doubled by 2020. In 2020, 1.76 breaches occurred daily. Figure 1 shows 500+ Healthcare Data breaches from 2009 to 2020. As our digital infrastructure develops, privacy concerns rise. Due to the sensitivity of healthcare information, a system breach might endanger a patient's identity and the providers' reputation. Statistically, scammers value patient data.

4 Electronic Health Record (HER) Benefits

Electronic Health Record (EHR) is a computerized compilation of medical information and other data that can be readily shared. EHR has numerous promises, including lowering morbidity and mortality, enhancing continuity of care, boosting efficiency, and minimizing adverse medication reactions. Electronic health records (EHR) provide real-time data that can be accessed and shared securely [7].

Transmitting information swiftly helps healthcare personnel to effectively support patients based on their individual medical requirements while dealing with the unpredictable Coronavirus, which disproportionately affects persons with underlying health concerns. EHR enabled patients and providers with major advances [8].

5 Figure 2: Typical Features of an Ideal EHR System

EHRs have been used in industrialized countries for over 50 years. Since the early 2000s, more U.S. doctors have joined HER incentive schemes. The dramatic increase of EHR utilization during this era is not surprising given EHR competitive benefits and the government's drive to strengthen EHR usage in healthcare IT infrastructure. The loss of life during the Coronavirus pandemic would have been substantially greater without EHR technologies to support healthcare services [9]. Even in industrialized countries, the need to enhance healthcare is evident. Before the epidemic, EHR implementation faced difficult hurdles.

People may complicate EHR systems; skepticism and disillusionment with technology are common, and EHR systems are no exception. Older medical workers and patients may resist change, particularly new technology. Minor EHR system glitches might demotivate hesitant participants. When we consider challenges new users may encounter while completing crucial jobs, including external communications, the situation becomes frustrating. Developed nations have several EHR service providers for offices, hospitals, clinics, and pharmacies. Without a proper referral, healthcare providers may overlook vital patient medical history information. Introducing a new workflow may be stressful for all workers, regardless of tech familiarity. HER systems must be adapted to user needs [10]. It's impractical to assume ideal efficiency in the early phases of EHR deployment, although training may boost user competency.

6 Blockchain Technology: From Centralized to Decentralized System

Blockchain technology generates a transparent, immutable, append-only record of network transactions. Digitally signed and broadcast transactions are organized and timestamp into blocks. A Block contains hashed and encoded valid transactions in a Merkle tree. The preceding block's hash is included. The Blockchain's Genesis Block may be found using the previous hash. The blockchain seeks maximal length. Changing one block's hash makes the next block invalid and reduces the blockchain's size. Due to the blockchain's purpose of maintaining the longest chain possible, it is immutable [11].

Each blockchain member has Public and Private keys. Public key is users shared identification. Only the user knows the private key. Digital signatures deterministically verify a message's origin and content. The 15 user signs the message using his private key, and others may verify it with his public key. Blockchain adds a new block using the consensus process. Consensus protocols distribute requests across nodes so each runs the identical sequence on its service instance. Popular consensus protocols include PoW and PoS. Digitalized technology has widely changed today's world. Depending upon this technology, starting from the day-to-day workings to the financial transactions, all can be controlled through the fingertip. By following the same fashion, the transition of the stock market is directly switching to the online platform and hence, the rate of the randomized investment rate in the stock is getting higher [12] .

7 Permissionless or Public Blockchain

Anyone may submit and confirm transactions on a permissionless blockchain. Transactions may be submitted by anybody who can pay fees. Anyone may be a validator by verifying transactions. This must be available to anybody who practices reasonably. Everyone who submits properly signed transactions to the network should expect it to execute them without fear of a group or firms banning them [13]. Blockchain technology is currently generating a lot of buzz among banks, businesses, and government agencies. Nearly every day, new initiatives and various collaboration agreements on Blockchain applications are announced in the economic press. This includes projects run by governments and central banks as well as banks and private enterprises [14].

8 Permissioned or private Blockchain

Permissioned or private Blockchains don't allow open involvement in submitting or verifying transactions, thus participants can't trust the network to withstand censorship. This means not all participants have a realistic assurance that their transactions won't be discriminated against.

Permissioned blockchain uses a membership structure to admit users. In permissioned Blockchains [15], nodes verify transactions using the originator's credentials. Permissioned blockchain technology's architectural design assures privacy and security. The Sybil Attack, 51% attack, and blockchain endpoint vulnerability affect public or permissionless Blockchains. We exclusively explore permissioned blockchain because we believe it can handle sensitive healthcare data [16].

9 Electronic Health Record (EHR) Is a Social Need

An electronic health record (EHR) is a collection of electronically controlled health information that many users may access. A patient's record traditionally documented their medical care. Smart care services urge doctors to consider the full patient, including wellness, sickness, and rehabilitation [17].

The main important risks and critical issues in a conventional healthcare system include a single point of failure, data modification, high chances of different malicious cyber attacks, centralized authority, high data management, keeping storage as well as cost, and databases that are not transparent. To address these issues, researchers have proposed numerous blockchain-based solutions. [18] The record must include health and illness information from multiple doctors in different locations. Data should be kept so that hospitals, pharmacies, insurance companies, and academics may get different views. EHR systems offer clinical reminders and alerts, information assets for healthcare decision support, and aggregate data analysis for care administration and research. To extract clinical information from a paper medical record, the reader must edit data mentally or on paper. EHR systems give computer-based capabilities to organize, analyze, and respond to data [19].

10 III. RESEARCH METHODOLOGIES

Health concerns that are common in India were the focus of the research. Below is a key point of the main healthcare concerns:

? The absence of a comprehensive end-to-end electronic health record (EHR) system interlinking among separate, stand-alone hospital record systems, as well as the lack of just-in-time record updating ? Because of the prevalence of handwritten prescriptions, an abundance of fake medications have entered the market.

? Unauthorized hospital administrators may access and change patients' information stored in insecure hospital databases, and caregivers aren't held accountable for any harm that may result.

? A lack of a secure, immutable, auditable, and traceable health infrastructure system

The potential of an electronic health record system built on the Blockchain to resolve these problems is also highlighted. This study suggests a Blockchain-based HER system that can reliably identify users by their national ID, allows users access to and control over their health records, prevents malicious data manipulation, and can be easily scaled. As a result of the synergy, massive data like CT scans and X-ray reports may be kept in the cloud for easy access. A patient-centric electronic health record (EHR) system will need unique identifiers in order to accurately identify patients. When it comes to government-issued IDs like Aadhar and PAN, there is presently no comprehensive EHR system (Permanent Account Number).

It is also essential that the proposed system include unique identifiers such as national IDs for patients to ensure accurate identification. Users need to be able to exercise control over their health information, such as authorizing updates, and this can only be achieved with secure identification.

Blockchain's cutting-edge safety features prevent unauthorized changes to medical records. With the suggested scalable system, previous paper-based medical records may be migrated into the new system while also benefiting from useful features such as a mobile app-based interface for translating paper prescriptions to text using Natural Language Processing (NLP) algorithms. Therefore, the purpose of this thesis is to suggest a patient-centered EHR design that can communicate with other, separate healthcare systems and parse out information from paper prescriptions. The issues addressed by the suggested architecture are as follows:

? Health records should be readily available at the point of service and updated in real time to help medical professionals make more educated choices.

? Paper prescriptions are a common source of human mistake, but digitizing them and incorporating them into an existing system has many benefits.

? Data manipulation is impossible with secure, immutable, auditable, and traceable health infrastructure solutions.

11 ? Integrated Health Record (EHR) Systems and Local Hospitals

? A patient-centered framework that protects sensitive information and gives individuals control over their own health records.

12 IV. RESULTS AND ANALYSIS

The study's goals were strictly adhered to throughout every step of the process, from framework execution through data collecting and analysis to system design. In this section, we also use benchmarks and other forms of evaluation to figure out how well the suggested architectural framework works. Hyperledger caliper is an instrument for measuring the efficiency of blockchain systems. This works with many different hyperledger frameworks. The performance of the system and its many metrics, including latency and throughput, may be tested and operated with the use of caliper.

System evaluation measures including latency, throughput, CPU utilization, memory, disc write/read, and network I/O are also checked and executed. The experiment was run with both read-and write-transaction modes, as well as with blocks of varied sizes and durations.

13 Experiment With Varying Transaction

14 Measurements with varying transaction: Write modes:

In simulation, we employed 3 firms with 3 peers each and 1 Orderer. The experiment uses 1000 writing transactions at 50, 100, 150, 200, and 250 per second. 1 Firm 1 Peer, 2 Firm 2 Peer, and 3 Firm 3 Peer are tested for transaction performance. Each round consists of 1000 transactions at different per-second speeds (tps).

Table 1 shows the time needed to perform transactions in the atypical network arrangement. 1 firm 1 peer's 5005th transaction takes 240 seconds. 2firm2peer completes 4509 transactions in 240 seconds, but 3 firm 3 peer completes just 4001. Latency in a Blockchain network is the time between submitting a transaction and receiving network confirmation. Equation (1) measures blockchain write transaction delay.

15 ??? (1)

Where W l : Write transaction latency, Ct: confirmation time, Nth: Network threshold, St: Submission Time.

Table 2 illustrates 1 and2 show that delay increased with additional firms and peers. Table 3 shows throughput for different transaction rates and the number of transactions per minute for three network types. 1 Firm and 1 Peer had the lowest average latency, fastest throughput per transaction rate, and most jobs per minute. The 3 Firm and 3 Peer network architecture had the greatest average latency, lowest throughput per transaction rate, and completed the fewest jobs per minute. The 2 Firm/2 Peer network concepts were in between. 1 firm 1 peer throughput is 190; however it decreases with more firms and peers. Table 3 showed 182 for 2 firm 2 peer and 180 for 3 firm 3 peers. Write transaction throughput on a block chain network is given by:??????.. (**2**)

Where W t : Write transaction throughput, W ct : transaction committed on the entire network, T ts : Total transaction time, N cn : committed node.

16 Measurements with varying transaction-Read modes:

Five hyperledger caliper measurements were collected. The configuration file sets read mode to 50,100,150,200,250 tps. The delay for reading from a blockchain network may be calculated using equation (3).R l = R t -S t ? ???????. (**3**)

WhereVolume 23 | Issue 1 | Compilation 1.0

17 London Journal of Research in Computer Science and Technology

A Blockchain Technology to Secure Electronic Health Records in Healthcare System R l : Read transaction latency, Rt: Response time, S t = Submission time Equation (4) measures read transaction throughput from a blockchain network.R t = R o /T t ???????(**4**)

Where R t : Read transaction throughput, R o : Total number of reading operations, T t = total time in sec. Reading or querying is quicker than writing a transaction, as seen in tables 4 and 5. Table 2 shows that 3 firm 3 peer's maximum write latency was 78.009 seconds, while its greatest read latency was 12.099 seconds. Maximum read throughput for 1 firm 1 peer was 280, while write throughput was 180. The greatest read throughput with changing transaction rate was 240 for 3 firm 3 peer, compared to 180 for writes. Experiment with Varying block time

18 Measurements with varying block time: Write modes:

This experiment tries to assess network latency and throughput. Hyperledger caliper's EHR system block formation time was modified between 250ms and 2s with variable outcomes. To reduce 3 firm 3 peer transaction latency, optimization metrics were used. Caliper defaults to block time after rising endorse policy block creation time. Switching from 250ms to 2s reduces latency by 35-50%.

Minimum latency for 50 tps is 40s, down from 80s. Table 6 shows that 250 tps has 60s latency, down from 89s. Changing hyperledger's default network setup improves performance. Latency is inversely related to throughput; changing the block time and policy increases read throughput. Table 9 shows that 50 tps transaction throughput is 49 and 250 tps is 77. Read throughput has risen 1.3 times. Experiment with Varying block size A blockchain's block size affects its performance. Changing block size improves performance. We analyzed 20 and 40-block sizes. Table 10 shows completed transactions for block sizes 20 and 40 over time. Table 10 shows those bigger blocks with a block size of 40 indicate more completed transactions, meaning a negligibly greater number of transactions per second. Our second experiment measured delay and block size as tps changed. We're using 50, 100, 150, 200, or 250 transactions per second. The assessment uses 20-by-40-blocks. Table 11 shows those 20-byte blocks have 50% less latency than 40-byte blocks. Reducing block size will reduce network latency, which may improve performance. Transaction per second for an individual node

Transactions per second measures transaction volume (TPS). It may be approximated based on the number of test transactions and then recalculated.

Transactions per Second of peer u can be calculated by the following equation (**??**) ????????? (**??**)

Where Tx: Number of transactions, t i , t j are initial and final time, respectively Average TPS of N peers, we can take the calculated by: CPU utilization CPU use is another key metric. It's the most essential OS number during tweaking. Almost all operating systems display user and system CPU use. These supplementary stats help determine CPU activity.

Caliper estimates CPU use, RAM, incoming/outgoing traffic, and disc read/write. Table 12 shows four rounds of transactions into our hypothetical blockchain network with a 1000-transaction ledger.

Table 12 shows CPU use by network model. The network models' CPU utilization varied with transaction rates.

19 V. RESULT AND DISCUSSION ABOUT EXPERIMENTAL ANALYSIS

? The simulation phase used a network model with three companies and three peers. As the number of firms, block size, and block duration rose, throughput and latency were assessed. ? Adding more firms and peers increases network latency. Read/query latency is lower than write latency.

? Increasing block time decreases latency, boosting network efficiency and throughput. When write block duration is raised from 250 ms to 2s, 250 tps throughput improves by 4x.

? Block size 20 is 50% faster than block size 40, improving network performance.

? Since the network model's CPU utilization has remained steady over time, a drop in block size and an increase in block time will lead to a considerable decrease in network latency, boosting network performance.

20 VI. CONCLUSION

Blockchain is vital in today's healthcare systems. It may lead to automated data collection and verification procedures, accurate and aggregated data from varied sources, and a lesser risk of cyberattacks. Distributed data, redundancy, and failure tolerance are also possible. Blockchain might be an alternative to documenting transactions and sending data via a trusted third party. Blockchain may ease transparency and security concerns, such as third-party trust, at every level of a transaction, eliminating intermediaries or third parties. This book addresses contemporary healthcare business challenges, focusing on the Indian subcontinent. We propose system architecture and methodology for permission EHR that communicates with local freestanding EHR systems, checks users against national citizen databases like UIDAI, and collects data from handwritten prescriptions. The suggested framework's performance findings are impressive and might transform EHR systems throughout the Indian subcontinent. [1]

1

Figure 1: Figure 1 :

4

Figure 2: © 2023 London Journals Press 4

11

Figure 3: 1 Firm 1

1

Time in min ->	1	2	3	4
1 Firm 1 Peer	801	1909	3901	5005
2 Firm 2 Peer	701	1600	3500	4509
3 Firm 3 Peer	601	1452	3303	4001

Figure 4: Table 1 :

2

TPS->	50	100	150	200	250
1 Firm 1 Peer	20.0098	34.0098	40.09	50.08	55.09
2 Firm 2 Peer	35.009	44.0087	49.009	68.09	70.1
3 Firm 3 Peer	46.1	55.1	60.009	75.09	78.009

Figure 5: Table 2 :

3

TPS->	50	100	150	200	250
1 Firm 1 Peer	40	90	150	175	190
2 Firm 2 Peer	35	82	140	170	182
3 Firm 3 Peer	33	77	135	165	180

Figure 6: Table 3 :

4

TPS->	50	100	150	200	250
1 Firm 1 Peer	2.02	3.01	3.0002	4.0008	5.129
2 Firm 2 Peer	6.0021	7.0032	8.0098	10.0087	11.021
3 Firm 3 Peer	7.0098	8.0087	10.0098	11.098	12.099

Figure 7: Table 4 :

5

TPS->	50	100	150	200	250
1 Firm 1 Peer	80	150	200	250	280
2 Firm 2 Peer	60	130	180	230	250
3 Firm 3 Peer	50	110	170	220	240

Figure 8: Table 5 :

6

TPS->	50	100	150	200	250
250ms Block time	40.001	45.02	50.02	49.03	60.05
2s Block time	80.007	90.9	85.008	90.06	89.6

Figure 9: Table 6 :

7

Figure 10: Table 7

7

TPS->	50	100	150	200	250
250ms Block time	20	25	22	25	15
2s Block time	50	70	55	60	65
Measurements with varying block time: Read modes					

Figure 11: Table 7 :

8

TPS->	50	100	150	200	250
250 ms Block time	20.09	25.02	30.03	31.01	38.1
2s Block time	9.1	14.2	20.1	25.1	30.4

Figure 12: Table 8 :

9

TPS->	50	100	150	200	250
250ms Block time	50	55	55	60	57
2s Block time	70	72	78	80	76

Figure 13: Table 9 :

10

Time->	00:15	00:30	00:45	01:00	01:15	01:30	01:45	02:00
Block Size:40	70	100	150	225	250	400	600	725
Block Size:20	60	90	140	210	245	390	590	710

Figure 14: Table 10 :

11

TPS->	50	100	150	200	250
Block Size:40	80	90	85	90	89
Block Size:20	40	45	50	49	60

Figure 15: Table 11 :

12

Round-1

Figure 16: Table 12 :

13

TPS->	50	100	150	200	250
peer0.firm1.example.com	40	32	33	38	40
peer1.firm1.example.com	35	40	39	45	42
peer2.firm1.example.com	33	35	36	40	44
orderer.example.com	18	20	19	21	22

Figure 17: Table 13 :

13

Figure 18: Table 13

[Xu et al. (2017)] ‘A taxonomy of blockchain-based systems for architecture design’. X Xu , I Weber , M Staples , L Zhu , J Bosch , L Bass . *Proceedings of 2017 IEEE International Conference on Software Architecture*, (2017 IEEE International Conference on Software ArchitectureGothenburg, Sweden) 2017 Apr 3-7. p. .

[Shaikh and Hannan (2022)] ‘An Examination of the Blockchain Technology: Challenges and Future Opportunities’. Abdul Shaikh , Hannan . *International Journal of Engineering and Computer Science* 09 November2022. 11 p. .

[Shaikh and Hannan (2016)] ‘An Overview of Big Data and Hadoop’. Abdul Shaikh , Hannan . *International Journal of Computer Application* -0975-887. November 2016. New York, USA. 154 (10) .

[Dagher et al. ()] *Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology*, G G Dagher , J Mohler , M Milojkovic , P B Marella . 2018. Sustain Cities Soc. 39 p. .

[Minoli and Occhiogrosso (2018)] *Blockchain mechanisms for IoT security. Internet of Things*, D Minoli , B Occhiogrosso . 2018 Sep. 1 p. .

[Shaikh and Hannan (2023)] ‘Challenges of Blockchain Technology using Artificial Intelligence in Healthcare System’. Abdul Shaikh , Hannan . *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)* Jan 2023. 12 p. . (Issue 01)

[Shaikh and Hannan (2023)] ‘Challenges of Blockchain Technology using Artificial Intelligence in Healthcare System’. Abdul Shaikh , Hannan . *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)* Jan 2023. 12 p. . (Issue 01)

[Neal (2011)] ‘Choosing an electronic health records system: professional liability considerations’. D Neal . *Innov Clin Neurosci* 2011 Jun. 8 (6) p. .

[Xhafa et al. (2014)] ‘Designing cloud-based electronic health record system with attribute-based encryption’. F Xhafa , J Li , G Zhao , J Li , X Chen , D S Wong . *Multimed Tools Appl* 2014 Feb 11. 74 (10) p. .

[Prasad et al.] ‘Detailed Investigation of the role of Artificial Intelligence in stock market predictions’. Arun Prasad , Shaikh Abdul Hannan , Kavita Panjwani , Muthe Ramu , Kawaender Singh Sidhu , Nagabhusanam Tida . *British Journal of Administrative Management* UK. 58. (Issue 06, 6 th Sept 2022)

[Mcmullen et al. (2014)] ‘Electronic Medical Records and Electronic Health Records: Overview for Nurse Practitioners’. P C Mcmullen , W O Howie , N Philipsen , V C Bryant , P D Setlow , M Calhoun , Z D Green . *The Journal for Nurse Practitioners* 2014 Oct. 10 (9) p. .

[Nugent et al. ()] ‘Improving data transparency in clinical trials using blockchain smart contracts’. T Nugent , D Upton , M Cimpoesu . *F1000Res* 2016. 5 p. 2541.

[Van Der Linden et al. ()] ‘Interorganizational future proof EHR systems: a review of the security and privacy related issues’. H Van Der Linden , D Kalra , A Hasman , J Talmon . *Int J Med Inform* 2009. 78 (3) p. .

[Kierkegaard (2012)] *Medical data breaches: Notification delayed is notification denied. Computer Law & Security Review*, P Kierkegaard . 2012 Apr. 28 p. .

[Dubovitskaya et al. ()] ‘Secure and Trustable Electronic Medical Records Sharing using Blockchain’. A Dubovitskaya , Z Xu , S Ryu , M Schumacher , F Wang . *AMIA Annu Symp Proc* 2017. 2017 p. .

[Dubovitskaya et al. ()] ‘Secure and trustable electronic medical records sharing using Blockchain’. A Dubovitskaya , Z Xu , S Ryu , M Schumacher , F Wang . *AMIA Annu Symp Proc* 2018. 2017 p. .

[Ichikawa et al. (2017)] *Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR Mhealth Uhealth*, D Ichikawa , M Kashiyama , T Ueno . 2017 Jul 26. 5 p. 111.

[Rifi et al. ()] ‘Towards using blockchain technology for eHealth data access management’. N Rifi , E Rachkidi , N Agoulmine , N C Taher . *Fourth International Conference on Advances in Biomedical Engineering (ICABME); October 19-21*, (Beirut, Lebanon) 2017. 2017.

[Azaria et al. ()] ‘Using Blockchain for Medical Data Access and Permission Management’. A Azaria , A Ekblaw , T Vieira , Medrec . *nd International Conference on Open and Big Data (OBD)*, (Vienna, Austria) August 22-24, 2016. 2016. p. .