Section: Research Paper

Comparative Study of Proposed Blockchain and IPFS integrated Patient Electronic Health record System

Vishal Sharma[1], Anand Sharma[2], Niranjan Lal[3]

[1,2]Department of Computer Science and Engineering, Mody University of Science and Technology, Lakshmangarh

[3]Department of Computer Science and Engineering, SRM IST, Ghaziabad, UP

Abstract: Many patient records are included in medical data, and these records are useful for both future study and treatment. Therefore security of storage and privacy preservation during the sharing of patient's health record system (PEHR) is very essential. Blockchain appears to be establishing a foundation for a breakthrough in the established healthcare sector, which stands to gain from its special properties including data privacy and transparency. As a result, numerous studies on Blockchain-enabled PEHRs have been explored. Nevertheless, current solutions that rely on a central database are vulnerable to well-known security issues including single points of failure and various threats, which both conventional database systems share. Performance and scalability problems were not resolved by previous solutions. In this research, we present a comparison study for assessing the performance based on different performance measures, such as transaction latency, throughput, and uploading and downloading different sizes of PEHR to and from the IPFS between our proposed model and existing alternatives. We have found that our proposed system is performing well as compared to existing solutions.

Keywords: Blockchain, IPFS, Patient Electronic Health Record, Throughput, Latency

1. INTRODUCTION

Technology advancements over the past century have led to changes in the processes involved in maintaining, monitoring, exchanging, and evaluating patient health records. Instead of manually recording a patient's diagnosis and treatment on paper, the maintenance of patient medical histories is now done digitally. Doctors, Hospitals, health insurance providers, pharmacists, medical data researchers, patients, and the patients' caretakers are anticipated to often share digital medical records, also referred to as electronic health records (EHRs). Traditional patient electronic health record (PEHR) systems are reliable and easy to use, but they come with a number of privacy and security problems [1]. Electronic health records (EHR) are known as the most sensitive data collecting method since they contain a lot of private information about patients and their medical procedures. With the growth of the electronic healthcare records and the internet, EHR data has grown increasingly vulnerable to hackers [20]. The traditional healthcare records management system, in which every healthcare institution has a separate database of the patients' medical information, places a major risk on the lives of patients [2, 22]. On the other hand, a central cloud server may raise serious issues with regard to misuse and data leaking. The security and privacy of data while it is being exchanged are therefore a major concern. A central cloud server, however, could result in serious issues with data loss and misuse. Decentralization of the system has been suggested as a solution to the problems with the current PEHR sharing mechanism. A popular technology that can be utilised for this is blockchain. A distributed ledger with the decentralization's characteristics, trustworthiness, and tamper resistance is called blockchain. Blockchain thus presents a potential substitute for centralised cloud storage.

Although blockchain technology can be applied in both public and private domains [3], patient health data cannot be made accessible to the broader public due to its sensitivity. Using IPFS (InterPlanetary File System) and Hyperledger Faric, we have proposed a patient-centric, secure, and private digital healthcare system [4] in this paper. A permissioned consortium blockchain solution is built for the field of digital healthcare using Hyperledger Fabric. In IPFS [5], a peer-to-peer decentralized file system in which each file is assigned a unique hash value that users can use to find the associated file. Comparing the consortium blockchain to the public blockchain, secure storage is an advantage. The consortium blockchain has faster throughput and efficiency because it doesn't require network-wide confirmation. The consortium blockchain has also been updated to include a system for identity authentication. The consortium based network of blockchain [6] can deliver more privacy protection because only authorised users are allowed to benefit from it. Smart contracts are also supported by the consortium based blockchain, and because running smart contracts doesn't incur any costs, user access control mechanisms can be easily created using smart contracts. PEHR commonly includes larger media like images and videos, which can't currently be stored directly in the blockchain. If large files are kept in local databases, sharing and storage problems will arise on traditional systems. The usage of cloud storage increases the risk of third-party data misuse and privacy issues [7]. We have therefore introduced the IPFS here. Our method uses IPFS to store encrypted PEHR while the consortium blockchain is used to keep metadata. Only a file's metadata, which is maintained on the blockchain ledger and only accessed by the file's owner or authorised users, can be retrieved using the blockchain by users. So as to further secure the confidentiality of patient health records, Moreover, we make use of proxy re-encryption technology that focuses on security to encrypt PEHR. A patient-centric access control technology, CP-ABAC [8] (Common Policy – At.tribute Based Access Control) is also implemented in our proposed system. This technology gives doctors and patients the ability to choose who has the right to access PEHR in order to achieve more secure management of information and prevent data forgery. The main benchmarking tool used in our experimental performance investigation was Hyperledger Caliper. Our research takes average throughput and latency into account. Our experimental configuration changes the quantity of nodes and the volume of transactions (workload).

The remaining sections are arranged as follows: Section 2, we go over the literature that already exists on performance evaluation of blockchain and PEHR sharing. Section number 3 introduces our suggested system. In section 4, we assess and contrast the effectiveness of the current system with our suggested approach. In part 5, we come to a conclusion for the paper.

2. RELATED WORKS

K. Shuaib et al. in [9] presented a permissioned Blockchain-based method for sharing health-related information, and the Hyperledger Besu enterprise Ethereum blockchain is being used to implement it. Based on the Interplanetary File System and the Istanbul Byzantine Fault Tolerant (IBFT) consensus process, the proposed system (IPFS). A variety of performance indicators, including transaction latency as well as throughput of the network, have been used to analyse and compare the performance of the proposed system. The investigations were conducted with varied network sizes and transaction volumes. A. Roehrs et al. introduced the OpenPHR architecture concept in [10], leveraging combining scattered health records using blockchain-based methods and the openEHR interoperability standard. The effectiveness of integrating medical records from several production databases was assessed together with the proposed prototype. The criteria they used for evaluation also took into account non-functional performance requirements such response time, CPU utilisation, memory occupancy, disc efficiencies, and network bandwidth. Y. Chen et al. in [11] suggested a consortium blockchain (Hyperledger Fabric) based healthcare based data sharing system with keyword searchable

encryption, K-anonymity, and characteristics based access control. By modelling different rates of medical data access and different numbers of healthcare facilities, they have investigated the computational costs related to encryption procedures, the efficacy of the proposed chaincodes, and the scalability of the suggested system. According to N. R. Pradhan et al. in [12], A Google Cloud Platform-based multi-organizational, multi-host, off-chain and on-chain framework for keeping track of patient medical information as well as various peer-based plans for a hyperledger fabric-enabled medical system that addresses the issues of data privacy, data availability, and data security have been proposed. They used tcpdump to generate realistic network traffic for their performance analysis, orderer for RAFT, and Kafka for their performance research to examine the system's performance. Furthermore, they contrasted the orderer services offered by Kafka and RAFT, finding that RAFT was more appropriate for open, query, and client-side transfer operations. D. C. Nguyen et al. in [13] recommended a blockchain-based mobile cloud platform, decentralised Interplanetary File System (IPFS) framework for exchanging electronic health records. They have produced a smart contract for access management. They were able to evaluate how well the suggested approach functioned by establishing an Ethereum blockchain on the Amazon cloud. They studied secure data sharing and minimal network delay. T. B. da Silva Costa et al. in [14] have proposed a blockchain-based architecture design using Hyperledger Fabric. By increasing the network bandwidth for various nodes and examining the workload for various ranges of concurrent record submissions, they are studying the system performance. The important factors for their examination have been determined to be throughput and average latency. To achieve data security and privacy-preserving among multiple healthcare entities, A patient-centric blockchain enabled system has been proposed by I. Abunadi et al. in [15] for the securely sharing of medical data between various users. For the effectiveness of protecting health data, they have simulated and compared the suggested approach to a centralised system. Md. A. Uddin et al. in [16] developed a 2 tier Patient-Centered Agent based model based on numerous layers of interfacing for storing the required and non-required medical data architecture. For the purpose of choosing a miner- and patient-originating security protocol, they have examined the system's performance. A. Yazdinejad et al. in [17] suggested a blockchain-based solution for patient health information. They explored methods to increase network throughput while reducing overhead, accelerating response times, and consuming less energy. They compared their study to two different solutions. K. Yu et al. in [18] suggested a system based on blockchain integrated healthcare based system on research for COVID -19. They have discussed the solution for privacy issues of confidential data. They have also compared the throughput and querying transactions with existing database system. Electronic healthcare records (EHR) can be effectively stored and distributed using a system that Lei Li et al. introduced in [19] that is built on IPFS and the hyperledger fabric blockchain for onchain and offchain storage of EHR and health data files, respectively. In order to safeguard privacy and promote efficient EHR exchange, they have also used an access control mechanism that incorporates chaincode and certificate authority components. They examined the currently in use standard systems and assessed how well the suggested solution would function.

3. PROPOSED SYSTEM

The process flow for our proposed PEHR system, which is based on IPFS and Hyperledger Fabric, is described in the stages below. The suggested PEHR system's system model is shown in Figure 1:

1: Patients and doctors send their credentials to Hyperledger Fabric's certificate authority to get registered. For instance: name, age, gender, etc. Based on these credentials, the Certificate Authority generates a User’s ID and sends him/her along with the certificate.

2: When a doctor requests to access the patient's electronic health record, in that the patient has the option of accepting or rejecting the request. The healthcare provider can input the patient's diagnosis information, including any relevant images, videos, and other contents, into a PEHR after the patient has been diagnosed and treated.

3: The doctor uses the patient's public key to encrypt the PEHR before uploading it to IPFS to ensure a trustworthy user experience.

4: The file's contents are used by IPFS to generate a unique hash value, which is then sent back to the healthcare professional.

5: Using the client application we used to communicate with the hyperledger fabric and run the chaincode to add data or to get file details, through a transaction, the relevant patient record's metadata must be created and added to the hyperledger fabric, this will be subsequently validated and added to the block.

6: A doctor who needs access to the PEHR sends a request through the client, and once it is verified through attribute-based access control using the chaincode, the patient either agrees or disagrees.

7: When the doctor or insurance provider needs the PEHR, it sends a request for the key of re-encryption to the patient. The re-encryption key function generates it from the private key of the patient and the public key of the insurance provider or doctor.

8: As a way to Re-encrypt the previously encrypted PEHR with the re-encryption key (RENK) and to the individual who has requested it (doctor or insurance provider).

9: User (doctor or insurance provider) sends request through transaction to hyperledger to retrieve metadata after that retrieve hash value from metadata and sends it to IPFS to retrieve PEHR.

10: IPFS collects file blocks from across the whole network and, after assembly, distributes them to the client based on the received file hash value index.

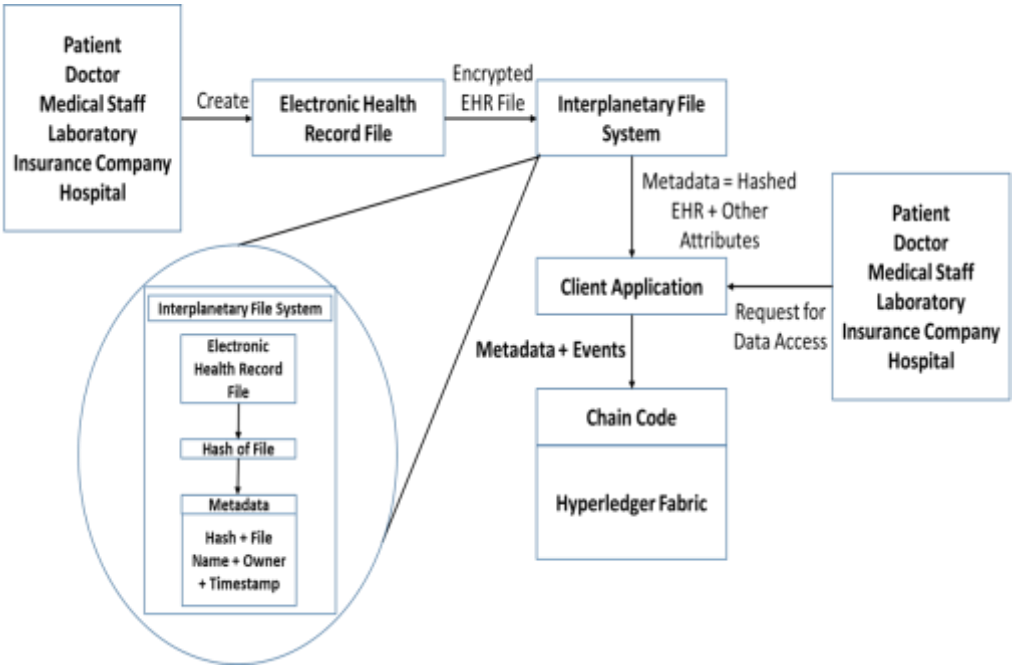

Figure 1: Patient electronic health record system concept proposed using IPFS and blockchain

4. COMPARATIVE STUDY WITH EXISTING SYSTEM

This section gives a comparison of findings that show how well the proposed PEHR system performs against the current system.

We evaluated our suggested system with an Ethereum-based system [2] for the comparative study to assess the performance of our proposed system. We compared the throughput, latency [23], and upload and download speeds of our suggested system to the PEHR on IPFS.

4.1 Transaction Throughput

It is defined as the amount of successfully completed transactions per second. Let's take Trans refer for the total number of transactions the system processed, and let's take **δ**trans be the amount of time that passed between the last confirmed time and the initial submission's time. So, the following formula can be used to get the transaction throughput (TrPt):

$$TrPt = Trans / \delta trans \quad (1)$$

The unit for measuring the Transaction throughput (TrPt) is Transactions per second (TPS) or Transaction per minute (TPM).

4.2 Average latency

It is described as the amount of time, on average, that passes between a transaction's initialization and its execution. Let's take num represent the overall number of transactions that the system has processed, and let Ltint and Ltex represent the initialization and execution of the transaction, respectively. The Average Latency (AvLt) can then be determined as shown below:

$$AvLt = (1/num) * \sum (Ltex - Ltint) \quad (2)$$

The unit for measuring the Average Latency (AvLt) is seconds or milliseconds.

For 2, 20 and 40 peer nodes, the throughput comparisons for the adding and query functions were examined. Our performance measure is configured to run a workload with steps of 150, ranging from 50 to 1000 simultaneous transactions of health metadata.

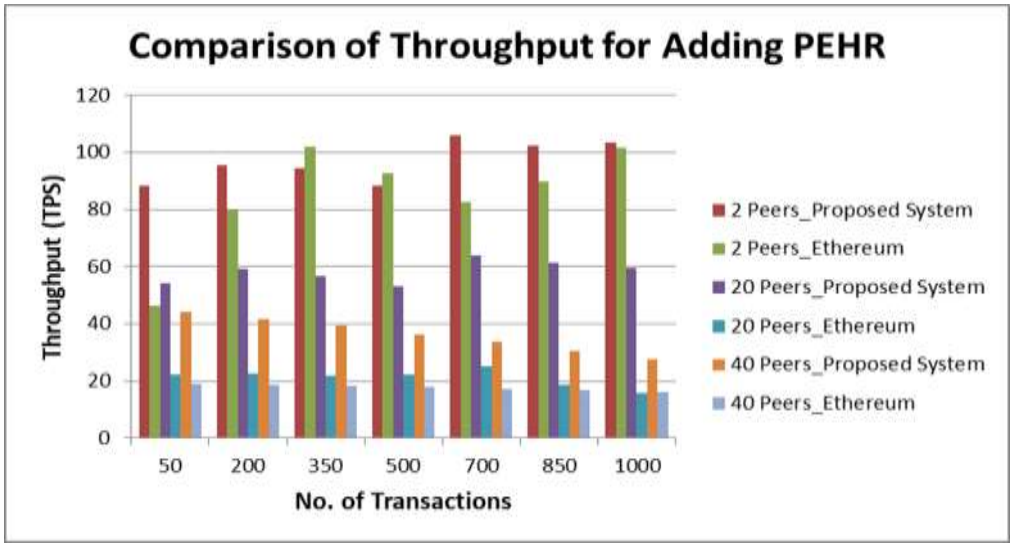

Figure 2: Comparison of different nodes throughput for adding PEHR

Figure 2 shows that, for the different number of peer nodes throughput of adding PEHR is higher than the ethereum based system. The throughput for the two peer nodes is also slightly higher than the ethereum-based system as shown by the figure 2 as the number of transactions increased.

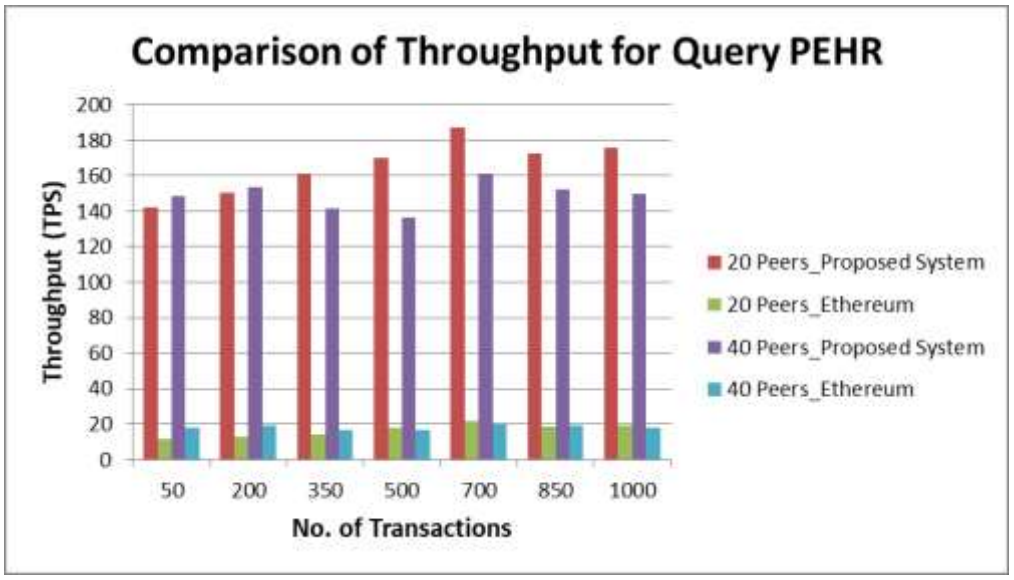

Figure 3: Comparison of different nodes throughput for query PEHR

Figure 3 shows that, for the 20 and 40 peer nodes throughput of query PEHR are higher than the system based on Ethereum. As the number of transactions rises, throughput decreases.

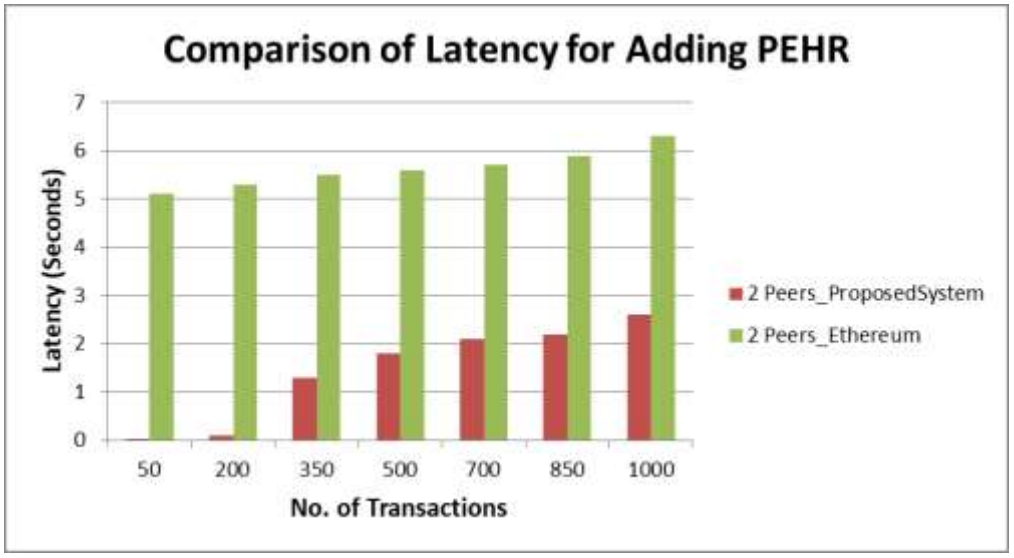

Figure 4: Comparison of two nodes latency for adding PEHR

Figure 4 demonstrates that for the two peer nodes, query PEHR latency is lower than the system based on Ethereum. As the number of transactions increases, the latency also increases.

The amount of time it took to upload the PEHR to IPFS and record the received hash value of the PEHR to the blockchain was called the execution time of the PEHR upload process. Users' download times for the PEHR over IPFS were determined by the execution time of the PEHR download procedure.

The simulation was carried out using a variety of data, ranging from 1 MB to 1 GB, in order to simulate the characteristics of a PEHR that supports different forms of data.

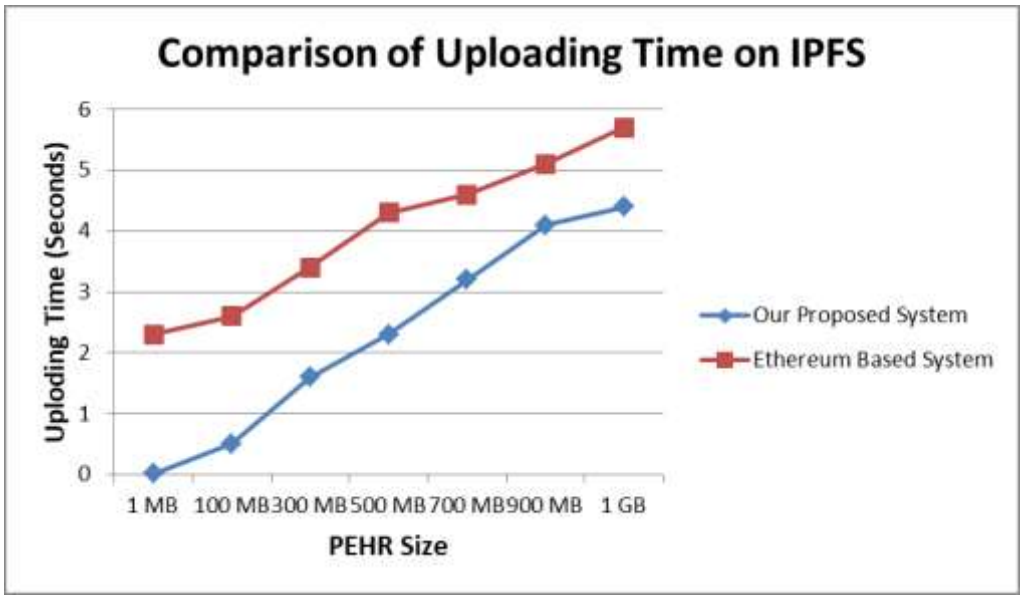

Figure 5: Comparison of uploading speed of PEHR on IPFS

Figure 5 shows that, the time of uploading the PEHR was increased as the size of the PEHR was increased. The upload time of our proposed system is slightly less when we compare with it with Ethereum and IPFS integrated system.

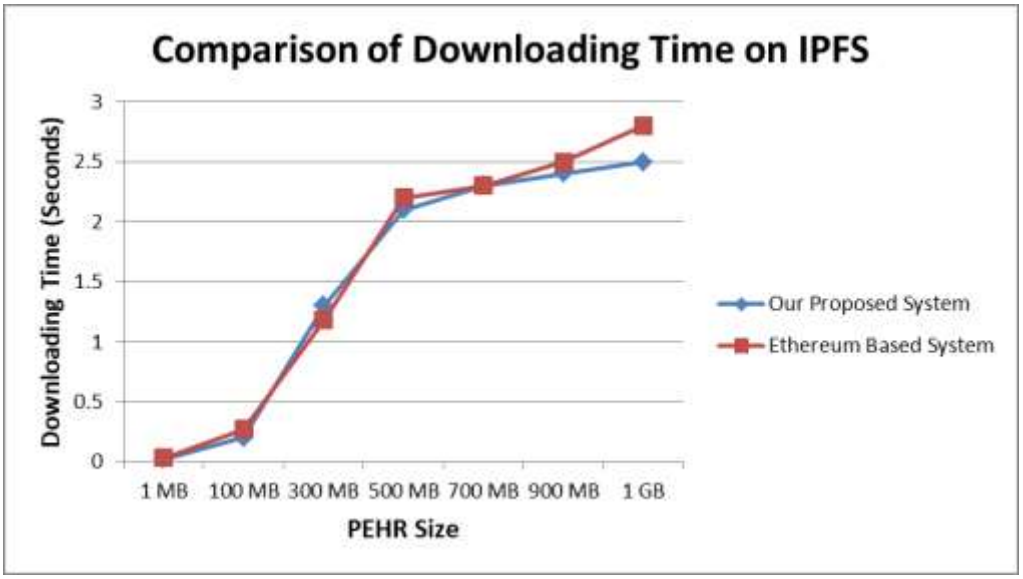

Figure 6: Comparison of downloading speed of PEHR from IPFS

Figure 6 shows that, the time of downloading the PEHR was increased as the size of the PEHR was increased. The upload time of our proposed system is almost the same as when we compare with it with Ethereum and IPFS integrated system.

5. CONCLUSION

In this research, we provide a PEHR system that integrates IPFS and the hyperledger fabric for efficient PEHR sharing and storage. To provide storage security and system scalability, the collaboration of hyperledger and IPFS is employed for online and offline storage of PEHR, respectively. In order to achieve privacy and efficient sharing of PEHR, our system also utilised proxy re-encryption and access control measures. Finally, we evaluate the performance of our system in relation to metrics like throughput, latency, and uploading and downloading of PEHR over IPFS. We accomplish this by comparing it to systems that are already in use. In comparison to the current ethereum and IPFS integrated system, we have demonstrated that our system performs well for the metrics mentioned above. In the future, we would be enhancing the performance of our proposed system for the large scale network.

REFERENCES

[1] Mamun, Azam and Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," IEEE Access, vol. 10, pp. 5768-5789, 2022.

[2] Shahnaz, Qamar and Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, vol. 7, pp. 147782 147795, 2019.

[3] Erikson, Bruno S. F., Krishnamachari B., and Jó Ueyama, "A Survey of Blockchain-Based Strategies for Healthcare," ACM Comp. Sur. 53, 2, Article 27, 27 pages, 2021.

[4] Sharma, Biradar, Sarma, and Rana, "Blockchain-based Internet of Things (IoT) for healthcare systems: COVID-19 perspective," Healthcare Monitoring and Data Analysis Using IoT: Technologies and Applications', 38, 355, 2022.

[5] Nyaletey, Parizi, Zhang and Choo, "BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability," IEEE ICB, USA, pp. 18-25, 2019.

[6] Liu, Liang, Sun, Du and Guizani, "A Privacy-Preserving Medical Data Sharing Scheme Based on Consortium Blockchain," GLOBECOM, Taiwan, pp. 1-6, 2020.

[7] Verma and Sharma, "Analysis and Classification of Security Mechanisms on the Cloud for Digital Healthcare," ICSMART, Moradabad, India, pp. 1596-1601, 2022.

[8] Zhang, Wei, Cao, Ning, Ying and Zheng D., "Blockchain-Enabled decentralized Attribute-Based access control with policy hiding for smart healthcare," JKSU - CIS, Vol. 34, Issue 10, Part A, pp. 8350-8361, ISSN 1319-1578, 2022.

[9] Shuaib, Abdella, Sallabi and Serhani, "Secure decentralized electronic health records sharing system based on blockchains," JKSU - CIS, Vol. 34, Issue 8, Part A, pp. 5045-5058, ISSN No: 1319-1578, 2022.

[10] Roehrs, André, Righi, da Silva, Goldim and Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," JBI, Vol. 92, ISSN No. 1532-0464, 2022.

[11] Chen, Yingwen & Meng, Linghang & Zhou, Huan & Xue, Guangtao,"A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection," WCMC, pp. 1-12, 2021.

[12] Pradhan, Singh, Verma, Kavita, Kaur, Roy, Shafi, Wozniak and Ijaz, "A Novel Blockchain-Based Healthcare System Design and Performance Benchmarking on a Multi-Hosted Testbed," Sensors, 2022.

[13] Nguyen, Pathirana, Ding and Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," IEEE Access, Vol. 7, pp. 66792-66806, 2019.

[14] Costa, Shinoda, Moreno, Krieger and Gutierrez "Blockchain-Based Architecture Design for Personal Health Record: Development and Usability Study," JMIR 2022.

[15] Abunadi, Ibrahim, and Kumar, "BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients," Sensors 2021.

[16] Uddin, Stranieri, Gondal and Balasubramanian , "Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture," IEEE Access, vol. 6, pp. 32700-32726, 2018.

[17] Yazdinejad, Srivastava, Parizi, Dehghantanha, Choo and Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain,"IEEE JBHI, Vol. 24, no. 8, pp. 2146-2156, 2020.

[18] Yu, Tan, Shang, Huang, Srivastava and Chatterjee, "Efficient and Privacy-Preserving Medical Research Support Platform Against COVID-19: A Blockchain-Based Approach," IEEE Cons. Elect. Mag., vol. 10, pp. 111-120, 2021.

[19] Lei, Yue, and Wu, "Electronic Medical Record Sharing System Based on Hyperledger Fabric and InterPlanetary File System," ICCDA, ACM, USA, pp. 149–154, 2021.

[20] Walia, Madaan, Agrawal, Mohan, Gupta, Sharma and Agrawal, "Blockchain in IoT and Limitations," Trust Based Communication Systems for Internet of Things Applications, pp.17-27, 2022.

[21] Venkatesan, Sahai, Shukla and Singh, "Secure and Decentralized Management of Health Records," In: Namasudra, S., Deka, G.C. (eds) Applications of Blockchain in Healthcare. Studies in Big Data, vol 83. Springer, Singapore, 2021.

[22] Babulal and Sharma, "Modified Des Cryptosystem with Steganography for Healthcare Systems in Iot," Design Engineering, pp.5530-5538, 2021.

[23] Shahnaz, Qamar and Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, vol. 7, pp. 147782-147795, 2019.