Health Care Data Management System Using Blockchain

Shivani S Shetty[1], Sowmya V Prabhu[2], Srushti Sogalad[3], Sushmitha[4], Mr. Shivaraj B G[5]
[1,2,3,4]*Students, Department of Computer Science & Engineering, Mangalore Institute of Technology & Engineering, Moodabidri*
[5]*Assistant Professor, Department of Computer Science & Engineering, Mangalore Institute of Technology & Engineering, Moodabidri*

***Abstract*—The paper describes a decentralized Secure Electronic Health Record (EHR) Management System leveraging Blockchain and the InterPlanetary File System (IPFS) to address the drawbacks of traditional healthcare systems that are centralized. Such systems have been known to encounter challenges that include but are not limited to data breaches, unauthorized access, interoperability gaps, and the absence of patient control over personal medical data. Blockchain in the proposed solution guarantees the aspects of data integrity, transparency, and immutability, whereas IPFS holds the encrypted medical records securely in a distributed way. The patient-to-doctor consent OTP-based method allows patients to grant or withdraw access to their health records to anyone that they want thus, ensuring that no unauthorized data disclosure takes place. Also, the use of smart contracts and MetaMask facilitated blockchain transactions promotes even more privacy, trust, and security in the system. It is a system that makes it possible for medical data to be shared in a secure way, free from tampering, and efficient, at the same time, patients are given more control than they would have with the usual centralized storage methods.**

***Index Terms*—Blockchain, Electronic Health Records (EHR), IPFS, Smart Contracts, OTP Authentication, MetaMask.**

I. INTRODUCTION

The healthcare sector over the last few years has been a victim of rapidly changing digital transformation through the embracing of technologies such as Electronic Health Records (EHRs), telemedicine, wearable devices, and cloud-based patient management systems. Altogether, these novelties have made the healthcare system more accessible and efficient but at the same time, they raised issues of data privacy, security, interoperability, and trust. For the most part, centralized healthcare data storage systems that hold healthcare data are very much exposed to risks like cyberattacks, unauthorized access, single points of failure, and data manipulation. Moreover, patients are given very little control over their health data, thus resulting in reduced transparency and increased privacy concerns in the healthcare ecosystem. On the other hand, blockchain tech is hailed as the next big thing in healthcare revolution because of the features that came with decentralization, immutability, and transparency. As a result, healthcare providers can now store large medical files in a secure off-chain manner with the help of a decentralized storage platform such as the InterPlanetary File System (IPFS) while maintaining the integrity of the files through the use of cryptographic hashing.

The paper introduces the Secure E-Health Record System that is focused on the patient and combines Ethereum-based Blockchain, IPFS, and OTP consent mechanism. The proposed framework empowers patients to have medical data ownership and control whereas doctors can access the information with the patient consent that is OTP based. Smart Contracts facilitate secure identity verification, access permission management, and also transaction log recording. The system has the aim of regaining security, privacy, and trust in the handling of healthcare data while giving the assurance that authorized users will still have easy access to the information entrusted to them. The blockchain-enabled solution is a better option to the implementation of the centralized system and this is evident given the functionalities which the former has like tamper-proof storage, better interoperability, transparency, and more privileged patient data autonomy.

II. LITERATURE REVIEW

Hüseyin Bodur et al.,[1] presented a hybrid blockchain-based framework that enables the sharing of electronic medical records (EMRs) in a secure manner. Traditional cloud and centralized systems can raise issues including uncertain data ownership, cyber-attacks, and restricted scalability. In order to address these issues, the authors decided to use blockchain for access control and integrity verification while EMR files, encrypted, were kept in a distributed database. Both sensitive and non-sensitive data were encrypted with AES-256, and metadata was protected by elliptic curve cryptography and SHA-256 hashing. Data access was regulated by smart contracts with the consent of the patient. The authors' experiment on PoW, PoS, and PoA revealed that PoW was the most efficient in terms of memory usage and scalability.

Meenavolu S. B. Kasyapa et al.,[2] explore how blockchain can improve healthcare by addressing limitations of centralized systems such as insecure EHRs, inefficient data sharing, and limited patient control. By going through more than 5,700 publications, they understand how blockchain is used in different platforms such as Ethereum and Hyperledger Fabric and different consensus mechanisms like PoW and PoS. Blockchain makes healthcare more open, traceable, and gives more power to the patient which results in secure EHR sharing, trustable clinical trial consent, supply chain provenance tracking, as well as fraud-resistant insurance claims. Even though off-chain storage helps in lowering the expenses and increasing the speed, there are still issues with scalability, privacy, storage, and smart contract complexity, thus suggesting that there is a need for solutions that can provide a compromise between security and efficiency for healthcare to be able to be used widely.

Sonkamble et al.,[3] address security, privacy, and integrity challenges in Electronic Health Records (EHRs) by proposing a decentralized, patient-centric framework using Hyperledger Fabric and IPFS. The system allows patients to retain data ownership and control access via smart contracts, with SPAKE-based key exchange ensuring secure authentication and Role-Based Access Control regulating stakeholder permissions. Tested on a hepatitis dataset, the framework demonstrated efficient upload/download for files up to 100 MB, stable block creation, and a balance between encryption strength and performance. Compared to MedChain, it achieved higher throughput through multiple certificate authorities and attribute-based access control. The study concludes that the Patient-Centered Healthcare Data Management system enhances privacy, transparency, and secure interoperability, with blockchain and IPFS providing immutability, though architectural complexity and minor access delays remain.

Adnan et al.,[4] addresses healthcare data challenges such as poor interoperability, lack of transparency, and frequent breaches by proposing a blockchain-based system connecting patients, doctors, pharmacies, and insurers through decentralized, immutable records. The system uses Ethereum's Ganache, Corda, Solidity smart contracts, and IPFS for off-chain storage to automate consent, payments, and record sharing. At the same time, it allows secure access through a ReactJS front-end and Aadhar-based identity verification. Benchmarking the system revealed that insurance processing times were cut by 40% and redundant medical tests by 30%, with Ethereum transactions taking an average of 2–3 seconds, however, scalability during peak loads is still a challenge. The paper interprets that healthcare blockchain revolutionizes the sector by enhancing security, transparency, and interoperability whereas the next steps should be tackling issues of scalability, consensus efficiency, and IoT integration to enable a wider opening.

Farahat et al.,[5] propose a blockchain-based framework to secure decentralized medical data exchange for IoMT-driven healthcare, addressing vulnerabilities in encryption and authentication of centralized systems. The model employs blocks that utilize a modified SHA-256 hashing and LZ4 compression to store medical data for a quicker and low-computation process, while a new party-authentication mechanism approves patients and doctors through wallet addresses and shared token words. The system on a modified Ethereum framework with ESP8266-based IoMT devices, smart contracts are used to authorize access, thus, achieving ~1-second block creation, low time complexity (O(n)), and energy-efficient operation. Simulation results

indicate secure authentication, storage that is efficient, and doctor-patient transactions that are reliable, however, there are limitations like bulk data handling and AI integration. The research points out the use of blockchain as a means to increase trust, data integrity, and eco-friendly performance in healthcare systems.

Guo et al.,[6] carried out an exhaustive survey of the blockchain technology that focused on the security features, vulnerabilities, and use cases of the technology. Even though blockchain is credited with decentralization, immutability, and transparency, it is still susceptible to being targeted, mostly in smart contracts and code areas, as was the case in the DAO hack and Parity wallet exploits incidents. Their work identifies risks as attack on the network, weaknesses of endpoints, deliberate misuse, coding errors, data protection issues, and human negligence and evaluates these risks in the work done on consensus algorithms, cryptographic mechanisms, and smart contract designs. By means of ZEUS, Oyente, Securify, and MAIAN tools, a massive audit was conducted, leading to the finding that seven smart contracts out of ten have in theory some kind of vulnerability that can be exploited. The article ends with a statement that the security problems mentioned above are only a fraction of the issues that still exist, such as 51% attacks, scalability limitations, and endpoint risks, and therefore the solutions required for a safe and secure large-scale deployment include post-quantum cryptography, ML-based anomaly detection, and standardized auditing frameworks.

Alrebdi et al.,[7] introduced SVBE, a decentralized EMR system that aims to overcome the drawbacks of centralized healthcare systems such as single-point failures, tampering, and limited privacy. To make medical records searchable, verifiable, and privacy-preserving, the system combines blockchain, IPFS, and cloud storage. Records are secured using Elliptic Curve Cryptography (ECC) and kept on IPFS while the hashes and metadata are stored on a mock Ethereum blockchain. In contrast, patients, providers, and verifiers communicate with each other via smart contracts and a DApp interface. The performance measurement has brought about the decision that the processes of adding, searching, and verifying files were done in a timely manner, the delay was at a reasonable level, and the confidential information was dealt with in a safe manner. SVBE is a good example of a system that is tamper-resistant, privacy-preserving, and securely interoperable, albeit there are issues of file size inflation, transaction costs, and scalability, which thus points to further research in AI integration and multi-keyword search improvements.
According to Shahin et al. [8] a decentralized blockchain-based framework is suggested to resolve issues that are frequently found in centralized EHR systems, which are unauthorized access, data breaches, and manipulation, among others. Patients become the main controllers of their data, which is ensured to be private, secure, and verifiable, the system thus maintains data confidentiality, security, and transparency. In their proposal, they have also included the stakeholders such as doctors, EHR servers, insurers, and verifiers. The transactions are executed by the use of secure hash functions, RSA-based cryptography, and bilinear maps, and all the transactions are logged in separated blockchain ledgers. The system's performance was compared with that of a centralized one by measuring the time of data retrieval. The results demonstrated improvements in the data retrieval time, authentication, and identity management, decentralization, and integrity in the case of blockchain-based systems as compared to the traditional centralized ones. Being a technology that is open, transparent, and tamper-resistant, the system is nevertheless suffering from problems with a large volume of data as well as a high demand for memory. Thus, future directions are laid out in terms of memory usage, advanced consensus mechanisms, and more comprehensive smart contract functionalities.

III. METHODOLOGY

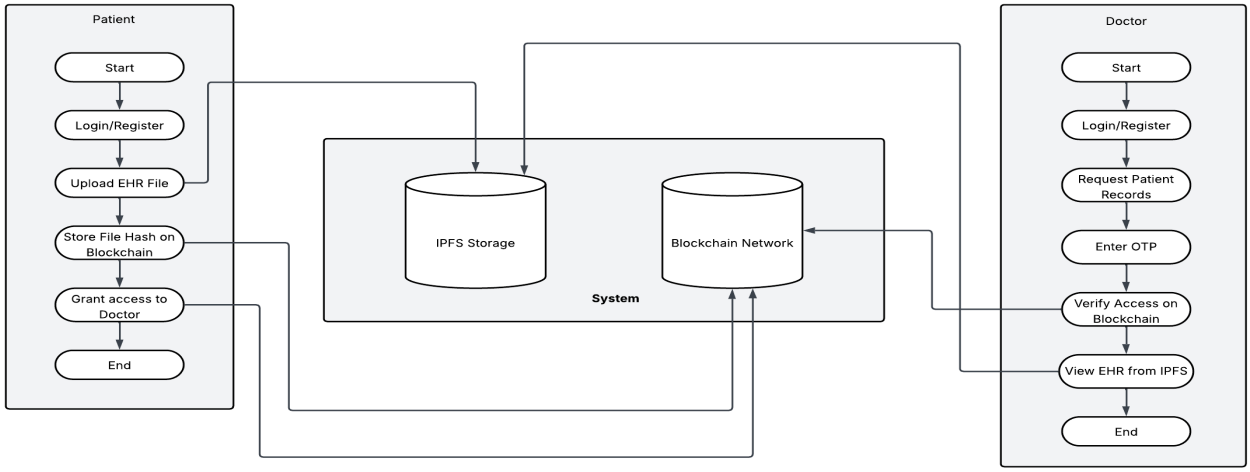
The suggested system adopts a decentralized method for safe healthcare data management with the use of Blockchain and IPFS. The approach involves launching a private Ethereum blockchain network with Ganache, where smart contracts in Solidity are deployed for user authentication, data access control, and transaction logging. MetaMask is implanted in the system in order to make patients' and doctors' blockchain interactions safe and easy. They can carry out the transactions via their wallet addresses. The system's frontend is created with React.js, which utilizes Web3.js to communicate with the blockchain,

and the frontend also communicates with backend services built with Node.js and Express.

Both patients and doctors sign up on the platform, and their data are packed on the blockchain with security measures that guarantee the data are immutable and that no unauthorized changes can take place. After registration, patients have the option of uploading their medical reports or prescriptions by means of a user-friendly application. The files are not put straight on the blockchain; the system first encrypts them and then puts them on the InterPlanetary File System (IPFS). IPFS gives each file a unique identifier (CID) which is kept on the blockchain along with the metadata such as time and description of the file. This combination of storage methods addresses issues related to file size on the blockchain and ensures that medical files are handled efficiently by IPFS while the blockchain can be used for small, critical information.

A request to access a medical record of a patient is sent by a doctor. To get the consent of a patient and to respect the privacy of a patient, the system has devised a permission mechanism, which is OTP-based. Once a patient receives the one-time password via email, he or she types it in, and thus permission is given for a doctor to see the patient's medical file. The smart contract checks the authorization and hence, if the doctor gets the go-ahead, he or she can find the IPFS hash on the blockchain and get the file through IPFS. Thus, the procedure also guarantees that files remain inaccessible in the absence of direct patient permission. All the times when access is gained, approvals, as well as file transactions, are recorded on the blockchain in a secure manner, thus constituting an unbiased and unalterable audit trail.

Protection, data correctness, and confidentiality, are the guarantees that the system provides all through the process. Security techniques take care of the files in IPFS, blockchain is used to ensure that logs of access are unchangeable, and smart contracts are employed for the purpose of making sure that permission can never be circumvented or modified by a person that has not got the authority. The procedure does not only address the necessity of decentralizing the storage and control of healthcare data but it also gives patients absolute power over their records, thus freeing their hands from the centralized healthcare systems' constraints.



IV. RESULTS AND DISCUSSION

The proposed Blockchain and IPFS-based Electronic Health Record system was successfully developed and tested. The patients are enabled by the system to upload their medical reports after encrypting them on IPFS and the blockchain stores the file hashes, permissions, and access logs in a secure manner. To get access to patient records, doctors have to wait for the approval of a request by the patient through an OTP verification, thus guaranteeing absolute data privacy and patient control.

During testing, all core functions such as patient/doctor registration, report upload, IPFS storage, access request, OTP verification, and record viewing worked accurately. Uploading a 1–5 MB file to IPFS took around 2–4 seconds, while blockchain transactions were executed in less than a second on Ganache. The implementation proved that using blockchain ensures data immutability and transparent

access history, while IPFS reduces storage cost and improves efficiency.

There are no risks of data tampering, unauthorized access, and single-point failure in the case of the proposed system, which is a decentralized one, as opposed to a conventional centralized hospital system. Patients have complete control over their medical data, and doctors are allowed to see it only if permission is given. Still, the arrangement relies on network connection and might encounter some difficulties in scaling on public blockchains.

V. CONCLUSION

The decentralized Electronic Health Record (EHR) system that was proposed is a fair solution to the major issues with the traditional, centralized healthcare data storage system that are data breaches, unauthorized access, lack of transparency, and limited patient control. The system, through the use of Blockchain technology for immutability and access control and IPFS for decentralized file storage, guarantees security, a tamper-resistant, and an efficient way of handling medical records. The use of OTP-based authentication is also a plus in terms of privacy since it allows patients to give or deny access to doctors, thus ensuring that data sharing is done only with explicit consent.

The test results indicate that the system is a secure file storage medium with transparent access logs, faster data retrieval, and trust between patients and healthcare providers built up over time. Patients are the sole owners of their medical records, and each access or transaction is recorded indefinitely on the blockchain, thus there is no need for any central authority. In short, the system is a dependable and scalable way of handling data in the healthcare sector of the future. It is a proof-of-concept that blockchain and IPFS can revolutionize medical data storage, access, and sharing.

VI. FUTURE SCOPE

In the future, this system can be improved by connecting it with real hospitals and government health platforms for real-time use. AI can be added to analyze medical data and help in early disease prediction. Biometric or Aadhaar-based login can replace OTP to make access more secure. The system can also be scaled to public blockchain networks and support more hospitals, doctors, and patients, making it a complete and practical healthcare solution.

REFERENCES

[1] H. Bodur and I. F. T. A. Yaseen, “An improved blockchain-based secure medical record sharing scheme,” *Cluster Computing*, vol. 27, no. 6, pp. 7981–8000, Apr. 2024, doi: 10.1007/s10586-024-04414-6.

[2] M. S. B. Kasyapa and C. Vanmathi, “Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies,” *Frontiers in Digital Health*, vol. 6, Apr. 2024, doi: 10.3389/fdgth.2024.1359858.

[3] R. G. Sonkamble, A. M. Bongale, S. Phansalkar, A. Sharma, and S. Rajput, “Secure data transmission of electronic health records using blockchain technology,” *Electronics*, vol. 12, no. 4, p. 1015, Feb. 2023, doi: 10.3390/electronics12041015.

[4] M. M. Adnan, “Design and development of healthcare system using blockchain,” *Journal of Smart Internet of Things (JSIoT)*, vol. 2023, no. 1, pp. 36–45, 2023, doi: 10.2478/jsiot-2023-0004.

[5] I. S. Farahat, W. Aladrousy, M. Elhoseny, S. Elmougy, and A. E. Tolba, “Secure medical blockchain model,” *Information*, vol. 14, no. 2, p. 80, Jan. 2023, doi: 10.3390/info14020080.

[6] N. Alrebdi, A. Alabdulatif, C. Iwendi, and Z. Lian, “SVBE: Searchable and verifiable blockchain-based electronic medical records system,” *Scientific Reports*, vol. 12, no. 1, Jan. 2022, doi: 10.1038/s41598-021-04124-8.

[7] H. Guo and X. Yu, “A survey on blockchain technology and its security,” *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100067, Feb. 2022, doi: 10.1016/j.bcra.2022.100067.

[8] A. I. Taloba, A. Rayan, A. Elhadad, A. Abozeid, O. R. Shahin, and R. M. A. El-Aziz, “A framework for secure healthcare data management using blockchain technology,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 12, Jan. 2021, doi: 10.14569/IJACSA.2021.0121280.