International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

BLOCKCHAIN-BASED PROTOCOL FOR SAFEGUARDING HEALTH RECORDS

[1]KODAMANCHILI SANTHOSH KUMAR, [2]K.RAJA RAJESWARI

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor, Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

With the rapid digitization of healthcare systems, managing sensitive patient data securely has become a critical challenge. Traditional centralized systems are vulnerable to data breaches, unauthorized access, and tampering. This project proposes a Blockchain-based protocol, SEC-HEALTH, for secure and decentralized management of Electronic Health Records (EHR). The system leverages Blockchain technology to ensure tamper-proof, transparent, and decentralized data storage. Patient records are stored securely using cryptographic hashing, while large medical files are stored in the InterPlanetary File System (IPFS), with their hash references maintained on the Blockchain. Smart contracts are used to manage patient, doctor, and prescription data securely. The system supports multiple users including patients and doctors, enabling functionalities such as registration, appointment booking, and prescription management. Experimental results demonstrate improved security, data integrity, and accessibility compared to traditional systems. The proposed solution provides a scalable and secure framework for healthcare data management.

Keywords: Blockchain, Healthcare, Electronic Health Records, IPFS, Data Security, Smart Contracts, Decentralized Systems

I.INTRODUCTION

The healthcare industry has increasingly adopted digital systems for managing patient data, including Electronic Health Records (EHR). While digitalization improves efficiency and accessibility, it also introduces significant challenges related to data security and privacy. Traditional healthcare systems rely on centralized databases, which are vulnerable to unauthorized access, data tampering, and cyber-attacks. Sensitive patient information such as medical history, prescriptions, and personal details can be compromised, leading to serious privacy concerns.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Blockchain technology offers a promising solution to these challenges by providing a decentralized and tamper-proof data storage mechanism. In a Blockchain network, data is stored in blocks that are linked using cryptographic hash values. Any modification in the data results in a mismatch in hash values, making tampering easily detectable. Additionally, Blockchain eliminates the need for a central authority, reducing the risk of single-point failures and unauthorized access.

This project proposes SEC-HEALTH, a Blockchain-based protocol for safeguarding healthcare records. The system integrates Blockchain with IPFS for efficient storage of large medical files, while smart contracts manage interactions between patients and doctors. The application includes modules for user registration, appointment booking, and prescription management. By combining Blockchain and decentralized storage, the system ensures secure, transparent, and efficient management of healthcare data, making it suitable for modern healthcare environments.

II SURVEY OF RESEARCH

[1] The study by Satoshi Nakamoto (2008) introduced Blockchain technology as a decentralized and tamper-proof digital ledger. The methodology uses cryptographic hashing and distributed consensus to maintain data integrity. Results showed that Blockchain ensures secure and transparent data storage. However, scalability and transaction speed remain challenges. This research forms the foundation for using Blockchain in healthcare data security.

[2] The research by Juan Benet (2014) introduced the InterPlanetary File System (IPFS), a decentralized storage system. The methodology stores files across distributed nodes and retrieves them using unique hash addresses. Results demonstrated improved data availability and reduced dependency on centralized servers. However, retrieval latency may occur in large networks. In the proposed system, IPFS is used to store large medical records securely.

[3] The study by Vitalik Buterin (2015) introduced Ethereum, a Blockchain platform supporting smart contracts. The methodology allows programmable contracts to automate transactions and data management. Results showed improved automation and security in decentralized applications. However, smart contract vulnerabilities can pose risks. In the

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

proposed system, Ethereum is used to deploy smart contracts for managing patient records.

[4] The research by Whitfield Diffie and Martin Hellman (1976) introduced cryptographic techniques for secure communication. The methodology ensures data confidentiality and integrity through encryption. Results demonstrated strong data protection mechanisms. However, key management can be complex. This research supports the security features implemented in Blockchain systems.

[5] The study by Ian Goodfellow et al. (2016) highlighted the importance of secure data handling in modern applications. The methodology involves applying advanced algorithms to process sensitive data. Results showed improved performance in data-driven systems. However, data privacy concerns remain. This research emphasizes the need for secure healthcare data management systems.

[6] The research by Abraham Silberschatz et al. (2011) introduced efficient database management techniques. The methodology focuses on structured storage, indexing, and retrieval of large datasets. Results demonstrated improved efficiency in handling complex data. However, centralized systems remain vulnerable to attacks. This research highlights the advantages of decentralized systems like Blockchain for secure data storage.

III. WORKING METHODOLOGY

The proposed SEC-HEALTH system integrates Blockchain and IPFS technologies to provide a secure and decentralized healthcare data management solution. Initially, users such as patients and doctors register in the system through the sign-up module. During registration, user details are securely stored in the Blockchain using smart contracts. These smart contracts are developed using Solidity and deployed on the Ethereum Blockchain. Each transaction is recorded as a block containing a unique hash value, ensuring that the stored data is tamper-proof and verifiable.

In the next phase, patients log in to the system and can view a list of available doctors, book appointments, and upload medical reports. Since Blockchain is not suitable for storing large files, the uploaded medical reports are stored in the InterPlanetary File System (IPFS), a decentralized storage network. Each file stored in IPFS generates a unique hash address, which is then saved in the Blockchain. This ensures efficient storage while maintaining a secure link between Blockchain and patient records. Doctors can log in to the system, view

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

appointment details, access patient reports using IPFS hash addresses, and generate prescriptions.

Finally, the system ensures secure access and data integrity through role-based access control and cryptographic verification. Patients can view their prescriptions and download reports, while doctors can update patient records through smart contracts. Each interaction is recorded as a Blockchain transaction, providing transparency and traceability. The integration of Blockchain ensures data immutability and security, while IPFS provides scalable storage for large medical files. The system is implemented using Python for backend processing, Ethereum for Blockchain operations, IPFS for storage, and web technologies for user interaction, resulting in a secure and efficient healthcare management system.

IV RESULTS EXPLANATIONS

Growing technologies converting all manual data management to digital data which get saved inside some centralized server. This digital data includes user sensitive information while opening bank account, patient registration details and many more. All the existing applications were using centralized server to save user sensitive data which can be easily tamper or access by centralized server database administrator employees and make user sensitive data at risk.

This data can also hack by malicious users making leakage of user's sensitive medical data. To protect user sensitive data many encryption algorithms were introduced but it required heavy computation for keys generation, management and encryption. This encryption process also reduces data transparency and interoperability.

To overcome from above issue we are employing Blockchain technology which has inbuilt support for tamper proof, decentralized and secured data storage. Blockchain can manage patient health record more secured compare to any other technologies.

Decentralized Storage: data saved in Blockchain will be replicated to multiple connected nodes instead of single centralized server. If one node down then Blockchain can access data from other working nodes. This process is known as Decentralized storage.

Tamper Proof: Blockchain store each record as block/transaction and associate each block with unique hashcode and this hashcode will get verified for subsequent block storage, if data modify in any block then hashcode mismatch will occur and data tamper will get

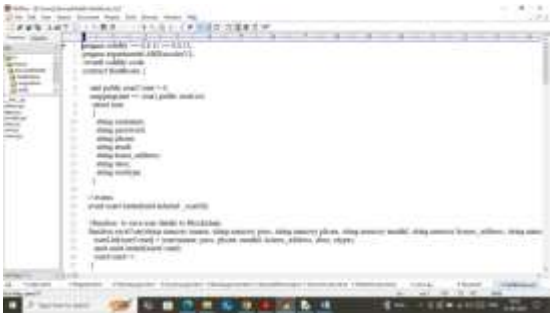
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

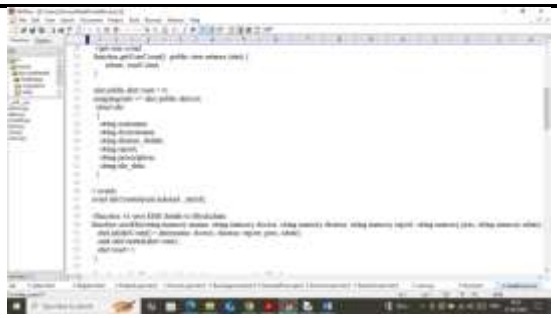
detected. This verification process make Blockchain tamper proof.

Secured Storage: all data saved in blocks will be encrypted using internal algorithms

IPFS storage: interplanetary file system (IPFS) is known as decentralized file storage, Blockchain designed to store small transaction data and cannot store patient EHR reports so all patients reports will get saved in IPFS and its storage hashcode address will get saved in Blockchain. IPFS can retrieve file by obtaining hashcode address from Blockchain

Blockchain can store and retrieve data using Smart Contracts which can be designed using Solidity programming and this contract contains which can be called to save and get data. To manage patient data we have designed following contract





In above smart contract screen we have defined functions to manage patient, doctor and prescription details. Now we need to deploy above contract in Blockchain Ethereum using below steps

First go inside 'hello-eth/node-modules/bin' folder and then look and double click on 'runBlockchain.bat' file to get below page



In above screen Ethereum started with default account and private keys and now type command as 'migrate' and then press enter key to deploy contract and then will get below page

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



In above screen in white colour text can see 'Healthcare' contract deployed and got contract address also. This address can be specify in python program to call above contract. In below screen showing python code calling above contract using address



In above screen read red colour comments to know about contract calling. In above screens we saw contract deployed and running successfully and let it run till you execute code.

Modules Information

To implement this project we have designed following modules

1) New User Sign up: using this module patients and doctor can sign up with the application and all details will get saved in Blockchain
2) Patient Login: patient can login to system
3) View Doctor List: after login patient can view list of available doctors and can make appointment with desired doctor
4) View Prescriptions: patient can view generated prescription by doctor
5) Doctor Login: doctor can login to system
6) View Appointments: after login doctor can view list of appointments and can generate prescription for each pending appointments.



In above screen patient can view list of available doctors and can click on 'Click Here for Appointment' link to book appointment with desired doctor and then will get below page

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



In above screen while booking appointment patient will enter disease details and can upload associated reports for doctor reference and now click on buttons to get below page



In above screen can see appointment is confirmed with doctor along with Blockchain log details. All booking data saved in Blockchain and uploaded report will get saved in IPFS server. Now click on 'View Prescription' link to get below page



In above screen patient can view prescription which is in pending state and now logout and login as doctor to generate prescription

V. CONCLUSION

The proposed SEC-HEALTH system provides a secure, decentralized, and efficient solution for managing healthcare records using Blockchain and IPFS technologies. By eliminating dependence on centralized servers, the system ensures data integrity, transparency, and resistance to tampering. The use of smart contracts enables automated and secure management of patient, doctor, and prescription data. IPFS enhances the system by allowing scalable storage of large medical files, while Blockchain maintains secure references through hash addresses.

The system successfully supports patient–doctor interactions such as appointment booking, report sharing, and prescription management while ensuring strict data privacy and access control. Experimental implementation demonstrates improved security, reliability, and accessibility compared to traditional healthcare systems. Overall, the proposed approach offers a robust framework for safeguarding sensitive medical data and can

be extended to large-scale healthcare applications in the future.

RE.FERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2015.

[3] J. Benet, "IPFS—Content addressed, versioned, P2P file system," 2014.

[4] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[5] A. Silberschatz, H. F. Korth, and S. Sudarshan, *Database System Concepts*, 6th ed. New York, NY, USA: McGraw-Hill, 2011.

[6] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[7] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.

[8] K. P. Murphy, *Machine Learning: A Probabilistic Perspective*. Cambridge, MA, USA: MIT Press, 2012.

[9] F. Chollet, *Deep Learning with Python*. Shelter Island, NY, USA: Manning Publications, 2017.

[10] A. Géron, *Hands-On Machine Learning with Scikit-Learn and TensorFlow*. Sebastopol, CA, USA: O'Reilly Media, 2017.

[11] S. Raschka and V. Mirjalili, *Python Machine Learning*, 2nd ed. Birmingham, U.K.: Packt Publishing, 2017.

[12] J. Brownlee, *Machine Learning Mastery with Python*. 2016.

[13] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, 2nd ed. New York, NY, USA: Springer, 2009.

[14] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed. Burlington, MA, USA: Morgan Kaufmann, 2011.

[15] R. Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection," in *Proc. IJCAI*, 1995, pp. 1137–1145.

[16] L. Rokach, "Ensemble-based classifiers," *Artificial Intelligence Review*, vol. 33, no. 1–2, pp. 1–39, 2010.

[17] H. Liu and H. Motoda, *Feature Selection for Knowledge Discovery and Data Mining*. Boston, MA, USA: Springer, 1998.

[18] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[19] A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet classification with deep convolutional neural networks," in *Advances in Neural Information Processing Systems*, 2012, pp. 1097–1105.

[20] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE CVPR*, 2016, pp. 770–778.

[21] O. Ronneberger, P. Fischer, and T. Brox, "U-Net: Convolutional networks for biomedical image segmentation," in *Proc. MICCAI*, 2015, pp. 234–241.

[22] M. Abadi et al., "TensorFlow: Large-scale machine learning on heterogeneous systems," 2016.

[23] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," in *Proc. ICLR*, 2015.

[24] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[25] A. Ekblaw et al., "A case study for blockchain in healthcare: 'MedRec' prototype," in *Proc. IEEE Open & Big Data Conf.*, 2016.