Proceedings of 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS 2024)
IEEE Xplore Part Number: CFP24DJ3-ART; ISBN: 979-8-3503-7999-0

Securing IoT Healthcare Data: The Power of Blockchain and Homomorphic Encryption

Sathishkumar M
Research Scholar,
Department of Computer Science, School of Computing Sciences,
Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, Tamilnadu 600117 –India
sathishmohan355@gmail.com

Dr. V. Raghavendran
Assistant Professor,
Department of Computer Science, School of Computing Sciences,
Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, Tamilnadu 600117- India
raganand78in@gmail.com

2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS) | 979-8-3503-7999-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICSCSS60660.2024.10624820

Abstract— **The rapid progress of the Internet of Things (IoT) and the increasing use of medical software in this field have raised considerable concerns regarding the security and privacy of sensitive health data. In response to these difficulties, blockchain technology has arisen as a viable remedy, offering autonomous and unchangeable data storage as well as accessible records of transactions. Nevertheless, conventional blockchain systems continue to encounter constraints in maintaining data confidentiality. This study presents an innovative method for improving privacy protection in medical devices based on the Internet of Things (IoT). It achieves this by combining homomorphic techniques for encryption with blockchain technology. Homomorphic encryption enables the execution of computations on data that has been encrypted without the need for decryption, ensuring the data's privacy during the entire computational procedure. Authorized parties can process and evaluate the encrypted data without disclosing the real contents, thus safeguarding patient privacy. In addition, this approach integrates smart contracts into the blockchain network to enforce access control and establish data-sharing policies. The smart contracts offer precise permission settings, guaranteeing that only authorized entities can access and exploit the protected data.**

Keywords — Electronic Health Record, Ethereum, MetaMask, Blockchain, Decentralization, Cryptocurrency wallet, IoT

I. INTRODUCTION

The genesis of blockchain technology may be traced back to 2008 when Satoshi Nakamoto introduced it through the release of the Bitcoin whitepaper. Bitcoin, the initial decentralized digital money, unveiled the globe to the possibilities of blockchain as an impervious and transparent record-keeping system. Subsequently, blockchain technology has progressed beyond its initial use in bitcoin and has been implemented in many sectors, such as healthcare. Electronic Health Records (EHRs) were developed as a digital format for storing patient medical records. However, they encountered difficulties including security vulnerabilities and a lack of interoperability. As a result, blockchain technology was investigated as a means of enhancing the administration and protection of electronic health records (EHRs) [1]. Electronic Health Records, in the healthcare context, are digital representations of a patient's medical history that include crucial clinical and administrative information about their healthcare. Electronic Health Records (EHRs) have the objective of optimizing healthcare procedures, enhancing patient care, and facilitating smooth transmission of information among healthcare practitioners. Nevertheless, conventional EHR systems frequently face problems including as data security and vulnerabilities, privacy concerns, and interoperability limitations. Blockchain offers a distributed and highly secure method for handling Electronic Health Records (EHRs). Blockchain utilizes its distributed ledger capabilities to guarantee the integrity of records by employing cryptographic hashing, thereby rendering data modification without consensus from numerous network participants arduous. Public-key cryptography is employed for data security and confidentiality, where each user possesses a distinct public and private key. This cryptographic framework improves the security of data and reduces the chance of unauthorized access to patient information [2] [3].

Integrating blockchain technology with electronic health records (EHRs) provides remedies for multiple challenges encountered by conventional systems. An important issue is the absence of interoperability among various healthcare organizations and systems [3]. The decentralized structure of blockchain allows for efficient and cost-effective sharing of data across trusted parties, reducing the need for expensive and inefficient means of transmitting records. Secure and efficient sharing of data can be authorized, leading to improved continuity of care and overall efficiency in healthcare delivery. Blockchain technology enables the implementation of smart contracts, which are automated agreements that execute activities based on predefined parameters. These intelligent agreements simplify the administration of consent by enabling data access only based on defined conditions. As a result, this method tackles concerns about privacy and complies with regulatory requirements like the General Data Protection Regulation (GDPR). Integrating blockchain with Electronic Health Records (EHRs) enables healthcare systems to strengthen data security, improve privacy, facilitate interoperability, and empower individuals to have more control over their health data [1] [4].

A. Objectives

1) The goal of utilizing blockchain technology in health record management will be to resolve comparability

challenges and facilitate smooth data interchange between healthcare providers through the use of distributed ledgers, defined protocols, and safe means for sharing data.

2) The objective is to implement a homomorphic encryption method for encoding and decoding IoT Medical data within the blockchain network.
3) To achieve automation and ensure compliance with privacy policies and data access controls, the objective is to safeguard patient health records by permitting access and interactions only for authorized persons, by predetermined rules and conditions.

B. BACKGROUND

Blockchain is a decentralized network that constructs a chain of interconnected blocks. A cryptographic hash and timestamp are appended to the preceding block on the blockchain, as depicted in Figure 1.

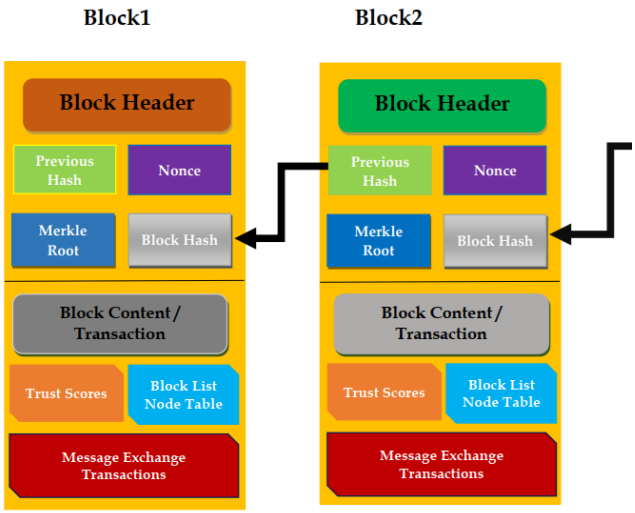

Figure 1. Blockchain Structure

.

II. LITERATURE SURVEY

The authors expanded on previous research and addressed the difficulties of achieving interoperability in the healthcare industry, as stated by the authors in [10]. The proposal suggests storing electronic medical records (EMRs) on a data lake outside of a blockchain, rather than directly on the blockchain itself. Although they offer fundamental guidelines for a prospective workflow and briefly address scalability, access security, and data privacy, they do not present a novel system or provide detailed instructions for complete implementation. The study lacks an evaluation or depiction of fault tolerance, disaster recovery, or performance factors. The study [11], provides a detailed description and implementation of BlocHIE, a Healthcare Information Exchange platform that employs blockchain technology and runs within a cloud context. This platform comprises two interconnected blockchains: EMRChain and PHD-Chain. EMRChain utilizes a combination of off-chain storage and on-chain verification mechanisms to effectively handle Electronic Medical Records (EMRs). However, PHD-Chain is specifically tailored to store personal healthcare data that is generated directly by patients. Their suggested consensus mechanism is based on Proof of Work and incorporates a modified transaction processing approach. This solution has demonstrated an impressive throughput of 46 transactions per second, exceeding the capabilities of both Ethereum and Bitcoin. Nevertheless, it is crucial to acknowledge that additional testing and assessment are still needed to assess the scalability and efficacy of the platform in high-stress and crisis scenarios [12].

The research paper referenced in [10], their collaborators, presents a framework for securely exchanging electronic medical record (EMR) data with exact access control. The researchers showcased a customized prototype designed specifically for clinical systems in cancer. The prototype focused primarily on managing consent, facilitating efficient data transmission across hospitals, and improving the management of longer treatment durations. The patient data in this system is encrypted and stored in a cloud repository outside of the main system, but the access permissions and electronic health record (EHR) metadata are stored within the main system. The prototype is developed using Hyperledger Fabric and utilizes a PBFT consensus method. Nevertheless, the system's ability to handle larger workloads has not been tested in real-life situations, and the authors recognize the necessity for more evaluation of its performance.

Furthermore, as stated by the authors in [4], the medical chain serves as a case study derived from the industry, which exhibits resemblances to other suggestions. The major objective of the medical chain is to empower users with ownership and authority over their health records, while simultaneously fostering transparency among healthcare stakeholders. The offered whitepaper mostly focuses on the business concept and lacks in-depth technical information. Significantly, the work does not directly discuss the scalability characteristics and performance evaluation. However, an important element emphasized in the medical chain is the incorporation of a contingency access system for emergencies. This approach involves the use of an emergency bracelet that caregivers can scan to retrieve vital patient information in situations where the patient is unable to give consent or is incapacitated. To summarize, blockchain technology has the potential to greatly revolutionize the administration systems of Electronic Health Records (EHR). It provides decentralized, secure, and transparent methods for exchanging Electronic Health Records (EHR) with patient control, ensuring data integrity and enabling interoperability. Several blockchain models, such as Ethereum, Hyperledger, Corda, and Tendermint, have been suggested, offering benefits such as enhanced privacy, data security, patient empowerment, and access control [13] [14]. Nevertheless, it is essential to prioritize the resolution of scalability, performance, and emergency access backup systems when it comes to the practical management of health records based on blockchain technology.

This study presents an innovative hybrid-deep learning-based homomorphic encryption (HE) model for the Industrial Internet

of Medical Things (IIoMT) to address these difficulties using a consortium blockchain. Incorporating human engineering (HE) with the proposed Industrial Internet of Medical Things (IIoMT) system is crucial to this research. Utilizing homomorphic encryption (HE) while outsourcing storage to the cloud offers a distinct capability to carry out machine learning and statistics operations on encrypted electronic medical record (EMR) data [15]. In addition, the method they used integrates smart contracts into the blockchain network to regulate access control and establish data-sharing regulations. The smart contracts offer precise and detailed permission settings, guaranteeing that restricted parties can access and exploit the protected data [16].

III. Proposed Methodology

The system's architecture conforms to certain high-level patterns and assumptions. It mostly focuses on the visible parts of the system that users communicate with and how they interact with each other. Figure 1 depicts the comprehensive structure of the system. This architecture comprises three modules, or layers.

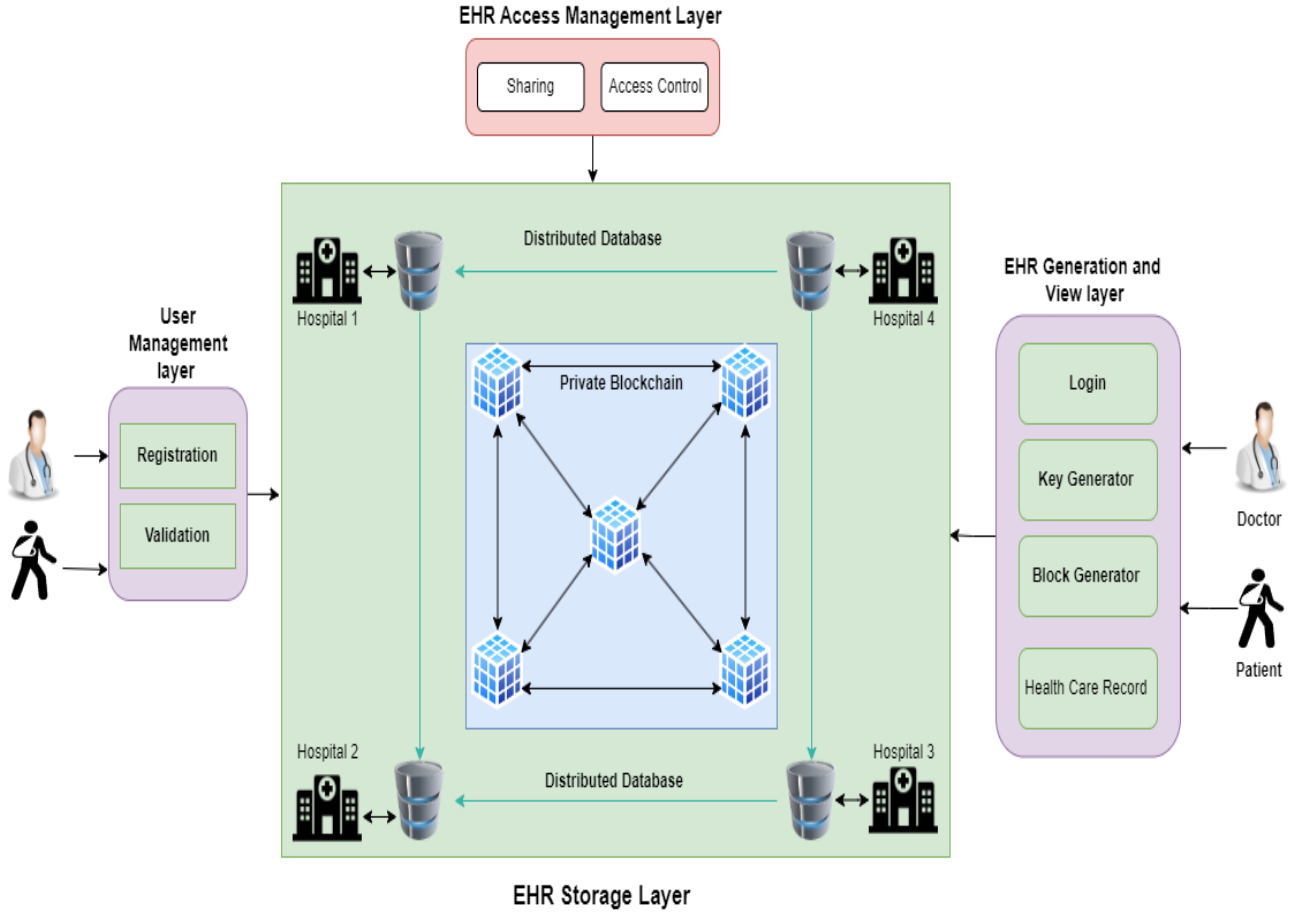

Figure 2. The Proposed System Architecture

Figure 2 depicts the proposed system architecture. The initial component is the User Acquisition Layer, which furnishes a user environment for medical professionals and patients to engage with the Electronic Health Record platform. This module allows users to create and then retrieve content which will be maintained in a distributed storage system.

The EHR Storage Layer is the second module that functions as the fundamental component of the system. Data in this module is saved on blockchains that are managed by hospitals. The databases are dispersed over the network. The module has utilized Next.js, Ganache, Truffle, and MetaMask as widely used technologies. APIs are utilized to streamline interactions between the User Management Layer and the EHR Storage Layer, where incoming requests initiate data storage procedures in the latter.

The third component is the EHR Generation and View Layer, which offers a thorough and effective method for controlling patients' medical records in a digital manner. The following module enables healthcare providers to retrieve patient data from many sources. It incorporates tools for scouring, filtration, and displaying observations and trends in the information.

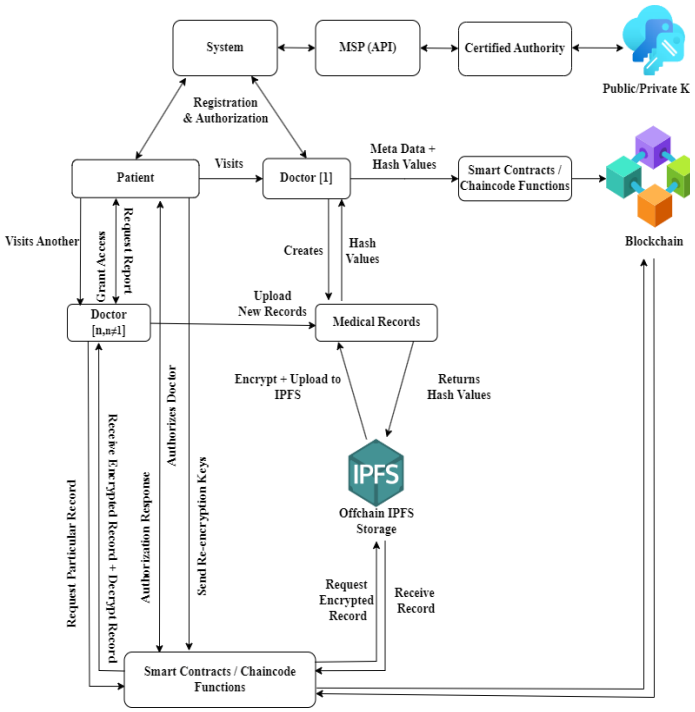

Figure 3. The Process Flow of the Proposed System

Figure 3 illustrates the operation of the Electronic Health Record Management Systems. It graphically illustrates the procedures of encryption, key creation, and access control. Upon user registration, the system generates three keys: a private key, a public key, and a symmetric key. The device being used by the user has the secret key, while the public key is saved in a database. The key that is symmetric undergoes encryption using the public key and is then saved on the server. The issuance of access requires the patient to provide their private key. The private key is thereafter used to recover and decode the symmetric key, granting access to approved medical professionals, lab personnel, or physicians.

The process of storing Electronic Health Records (EHRs) in IPFS requires the implementation of multiple procedures to ensure both security and efficiency. Initially, the medical information undergoes encryption and is thereafter transformed into a PDF document. Afterward, it undergoes additional encryption using a symmetric key and is then saved in IPFS, resulting in the creation of a Content ID (CID) or hash value. The CID is kept as a single unit in the blockchain. Users must supply their private key in order to access EHRs. The blockchain is accessed to retrieve the CID (Content Identifier) for a particular patient's Electronic Health Record (EHR). The IPFS network is subsequently employed to get the files with encryption, which are deciphered using the private key for the purpose of viewing. The system's technological stack comprises the following steps: collecting patient lists from the database, inserting encoded healthcare files, preserving them in IPFS, recording activities on the decentralized ledger, and ultimately recovering and decrypting EHR files for authorized individuals to see. The main characteristics of this initiative are its practicality, cost-effectiveness in utilizing blockchain technology, strong security through private keys, and the capacity to handle large file storage by utilizing IPFS as opposed to the blockchain.

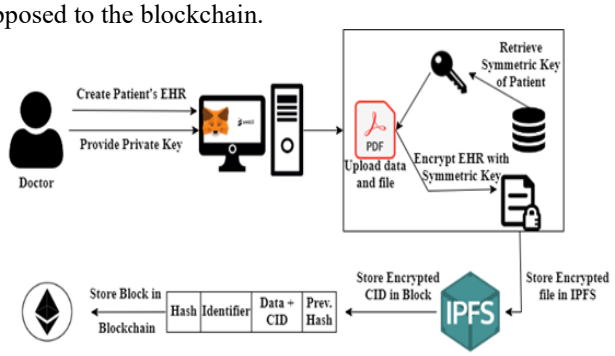

Figure 4. The Storing of Data in IPFS

After securely storing the medical record, we can now proceed with the user's procedure for retrieving the file. This is the operational process:

1. Key Authentication: The user begins the process of gaining access by supplying two crucial keys: their private key and the patient's public key.
2. System Demand: The user initiates an inquiry for the patient's Electronic Health Record (EHR) via the system's user interface.
3. Blockchain Validation: The initial request is sent to the blockchain, which then answers by furnishing the client with an authenticated Information Identify (CID) and the healthcare provider's information.
4. The CID record is essential as it functions as the method to locate the material saved on IPFS. The user employs this CID to access the encrypted Electronic Health Record (EHR) from IPFS.
5. Decryption: The process of decrypting the medical record involves retrieving the symmetrical key from the server. After decrypting, the patient's electronic health record (EHR) is effectively shown to the authorized person.

IV. Simulations Settings

The following are the prerequisites for running the system successfully.

Front End

- Python_3.8
- Django version 4.0.4
- Face recognition module
- OpenCV
- MySQL database

Back End

- Truffle v4.1.15 (development framework for Ethereum)
- Node JS version 8.9.0
- Ganache
- Meta mask extension for web browser

V. IMPLEMENTATION

A. MODULES DESCRIPTION

This section provides an overview of the procedure for gaining accessibility to the system being considered. This system is not simply a scientific attempt, but also an original and collaborative adventure. Its goal is to introduce a new solution and radically transform medical records administration. Our idea has been realized in the form of an ecosystem that effortlessly combines blockchain-based technology with the intricate healthcare industry, going beyond traditional approaches. The result is not simply a compilation of interfaces, but rather a seamless integration of data security, user-centric architecture, and streamlined record management. The development of the blockchain-based Electronic Health Record administration system has been characterized by diligent work and meticulous planning. Upon analyzing the outputs of each interface - The main page, physician, the administrator, and Customer - it is evident that they are the result of diligent effort. These pages demonstrate a cooperative effort to smoothly incorporate blockchain technology into healthcare, ensuring the protection of data, enhancing customer service, and simplifying handling records.

Figure 5 depicts the transaction-related cost and time spent computing associated with every ACC process. When contrasted with two intelligent contracts, ACC demands several system signals because it has complete control over the accessibility control of the complete operation. However, the gas value is determined by the primary duties of the intelligent contract. The functions of ACC involve overseeing several activities such as the registration procedure, the formulation of topic rules for access, and the implementation of mechanisms for controlling access.

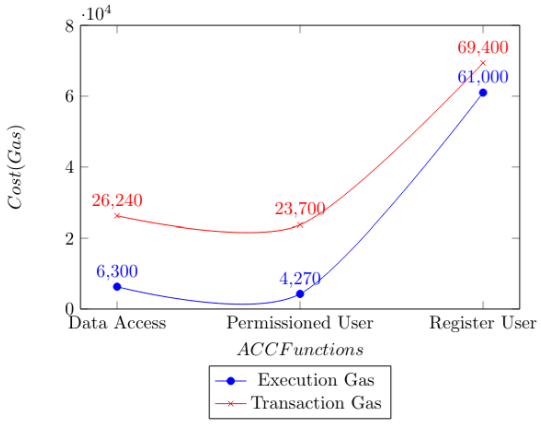

Figure 5. The Account Creation Cost

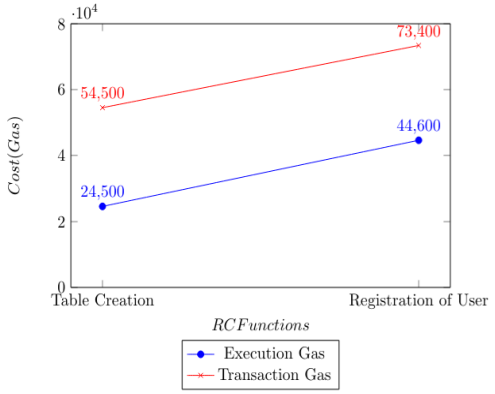

Figure 6. The Register User Cost

Figure 6 illustrates both the transaction and execution costs associated with RC activities. The purpose of RC is to oversee the setting up of accounts for users and maintain an authentication table to store user information. The main functions of RC consist of handling the registry table and facilitating the user authorization procedure.

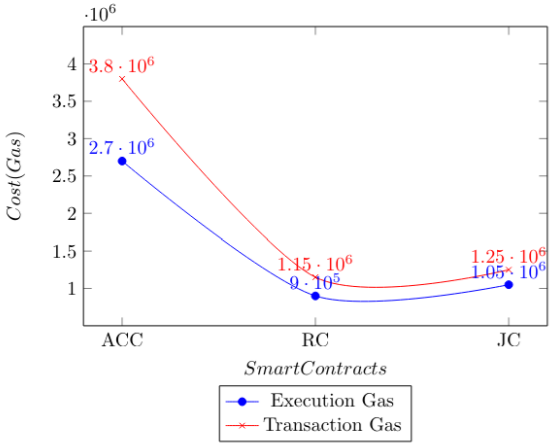

Figure 7. The Smart Contract Cost

Figure 7 displays the cost of transactions and execution costs associated with consensus mechanisms such as ACC, RC, and JC. The gas products employed by ACC exceed those of other smart contacts, such as RC and JC, as illustrated in the illustration below. The ACC serves as the main smart contract that facilitates connectivity to the network, manages expenses, and carries out sophisticated operations across two systems that are interdependent.

VI. CONCLUSION AND FUTURE WORKS

To summarize, the suggested system, the Blockchain-Based Electronic Health Record Maintenance System, signifies a substantial advancement in the field of medical technology. This solution has transformed safeguarding information and patient confidentiality by utilizing blockchain technology, effectively removing any illegal access. The technology facilitates the efficient exchange of medical records among medical facilities, improving overall coordination. The system's intelligent contracts effectively manage patient input and ensure

compliance with regulations, while minimizing organizational complications. Upon completing this article, it is clear that we are leading the way in the revolution in medical technologies. We have shown how blockchain can enhance healthcare by improving efficiency, security, and patient-centeredness.

REFERENCES

[1]. S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, [Online]. Available: https://bitcoin.org/bitcoin.pdf .

[2]. Tanwar, S., Gupta, N., Kumar, P. et al. Implementation of blockchain-based e-voting system. Multimed Tools Appl 83, 1449–1480 (2024). https://doi.org/10.1007/s11042-023-15401-1

[3]. Chinnasamy P, Albakri A, Khan M, Raja AA, Kiran A, Babu JC. Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System. Applied Sciences. 2023; 13(6):3970. https://doi.org/10.3390/app13063970

[4]. P. Chinnasamy, P. Deepalakshmi, V. Praveena, K. Rajakumari, P. Hamsagayathri, (2019) “Blockchain Technology: A Step Towards Sustainable Development” International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-2S2

[5]. Chinnasamy P., Vinothini C., Arun Kumar S., Allwyn Sundarraj A., Annlin Jeba S.V., Praveena V. (2021) Blockchain Technology in Smart-Cities. In: Panda S.K., Jena A.K., Swain S.K., Satapathy S.C. (eds) Blockchain Technology: Applications and Challenges. Intelligent Systems Reference Library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_11

[6]. A. Jain, A. Kumar Tripathi, N. Chandra and P. Chinnasamy, "Smart Contract enabled Online Examination System Based in Blockchain Network," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-7, doi: 10.1109/ICCCI50826.2021.9402420.

[7]. Hajian Berenjestanaki M, Barzegar HR, El Ioini N, Pahl C. Blockchain-Based E-Voting Systems: A Technology Review. *Electronics*. 2024; 13(1):17. https://doi.org/10.3390/electronics13010017

[8]. P Chinnasamy and B Vinodhini and V Praveena and C Vinothini and B Ben Sujitha, Blockchain based Access Control and Data Sharing Systems for Smart Devices, Journal of Physics: Conference Series, Vol.1767, No.1, pp.012056, 2021, doi.10.1088/1742-6596/1767/1/012056

[9]. Raja Rajeswari, T.S., Khajashareef, S.K., Sandhya, N., Chinnasamy, P. (2023). E-Voting System Using Blockchain. In: Mandal, J.K., Hinchey, M., Rao, K.S. (eds) Innovations in Signal Processing and Embedded Systems. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-19-1669-4_1

[10]. Alshehri A, Baza M, Srivastava G, Rajeh W, Alrowaily M, Almusali M. Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain. *Applied Sciences*. 2023; 13(2):1096. https://doi.org/10.3390/app13021096

[11]. Sallal M, de Fréin R, Malik A. PVPBC: Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain. *Future Internet*. 2023; 15(4):121. https://doi.org/10.3390/fi15040121

[12]. Malkawi, M., Yaseen, M. B., & Habeebalah, D. (2023). Ethereum blockchain based e-voting system for jordan parliament elections. Appl. Math. Inf. Sci, 17(2), 233-241.

[13]. Chentouf, F. Z., & Bouchkaren, S. (2023). Security and privacy in smart city: a secure e-voting system based on blockchain. International Journal of Electrical and Computer Engineering, 13(2), 1848.

[14]. Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. Materials Today: Proceedings, 80, 3363-3370.

[15]. A. Ali *et al*., "A Novel Homomorphic Encryption and Consortium Blockchain-Based Hybrid Deep Learning Model for Industrial Internet of Medical Things," in *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2402-2418, 1 Sept.-Oct. 2023, doi: 10.1109/TNSE.2023.3285070.

[16]. Ali A, Al-rimy BAS, Alsubaei FS, Almazroi AA, Almazroi AA. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors. 2023; 23(15):6762. https://doi.org/10.3390/s2315676