Health chain Security Using Block Chain Technology

Swathi B[1], Athira P[2], Monicka M[3], Sathiyamurthi P[4]

[1, 2, 3, 4]Dr.Mahalingam College of Engineering and Technology

Abstract- *Health chain is a paper that proposes an efficient Public Key Cryptography and Blockchain-based secure healthcare system.This technology enables secure device tracking and, in the context of this project, high availability of personal health records while protecting patients' privacy and data integrity via Blockchain Technology. With higher performance on communication cost, computation cost, and storage cost, the suggested strategy solves the security disadvantages of recent techniques. The health chain framework is secure and privacy-protected against numerous assaults, according to the privacy performance analysis.*

Keywords- Health chain , sensor , temperature , blockchain

I. INTRODUCTION

Electronics, magnetics, photonics, sensors, circuits, and algorithms can all be used to measure and change biological features. By building new circuits, devices, systems, and analyses, applications vary from basic biological science to clinical medicine, enabling new discoveries, diagnoses, and therapies. Many biometrics must be measured by medical professionals. To monitor vital indicators (heart rate, blood pressure, temperature, respiration rate, pO2) or comprehensive data such as ECG, effective sensors must be mounted to the patient. Sensors must be comfortable to wear, simple to install, and offer verifiably accurate data for the duration of their intended use.

A Key Generation Center (KGC), a HealthChain Service Provider (HSP), a patient, a doctor, and blockchain are the five entities in the proposed paradigm.HSP, which is defined as a trustworthy entity, starts the system.

The Health Chain server maintains encrypted patient health data and doctor diagnosis results and uploads transactions related to the data. For diagnosis, a patient uploads encrypted personal health data from a Health Device. If a doctor's access tree of health data stored in the Healthchain server is satisfied, the doctor can request the health data from the Healthchain server. The consortium blockchain is organized by health centers and local hospitals. The ledgers are accessible to both patients and doctors.

II. LITERATURE SURVEY

We will attempt a brief review of previous methodologies employed by researchers for the health chain. In the year 2021, there will be the EXchange: Using Ring Signature and Stealth Address, a privacy blockchain-based framework for health information exchange has been developed.The goal of this study is to design and construct a novel privacy-preserving blockchain-based system.The algorithms used here are ring signature and stealth address. Finally, the study does not take into account the various formats of health information.

The DITrust Chain will strive on Blockchain-based Trust Models for Long-Term Healthcare IoT Systems by 2020.The goal of this research is to provide a privacy-aware management framework for preserving patient sensitive data. This work uses the public key elliptic curve cryptography approach (ECC). The demand for resources rises as a result.

EdgeMediChain is a Hybrid Edge Blockchain-Based Framework for Health Data Exchange that will be launched in 2020. The purpose of this study is to propose a data management architecture that is both secure and efficient. For sharing health data, it's called "EdgeMediChain." The elliptic curve digital signature algorithm is utilized in this paper (ECDSA).

Because there is no system to validate mobile users, a DDoS can be readily started.

Designing a Secure Authentication Protocol Cloud-Assisted Telecare Medical Information System using Blockchain in the year 2020. The purpose of this research is to provide a secure authentication system for a cloud-based TMIS with access control based on blockchain. Access control for health data stored on the cloud server was established using the ciphertext-policy attribute-based encryption (CP-ABE) technology, and data integrity was ensured using blockchain. As a result, the suggested technique can be used in a TMIS environment. Lijun Xiao will publish A Secure Framework for Data Sharing in Private Blockchain-Based WBANs in the year 2020. The purpose of this article is to present the Blockchain-based architecture of WBAN. The paper's algorithm proposes a blind signature system based on

Blockchain. A blind signature is a one-of-a-kind electronic signature.

Secure and Lightweight Data Aggregation Based on FoG The purpose of this project is to develop an Efficient and Secure Data Transmission and Aggregation (ESDTA) approach that will increase the efficiency and security of data aggregation. At the Mobile Node (MN) and Fog Node (FN), the Secure Message Aggregation (SMA) and Secure Message Decryption (SMD) algorithms were used (FN). The NS simulation programme is used to test the proposed scenario.

III. PROPOSED SYSTEM

In medical service applications, the Internet of Things improves communication between specialists and remote patients who are equipped with wearable sensors. Patients' information is crucial, and any security breach might have catastrophic implications. Patient safety may be jeopardized by several current healthcare regimes. As a result, security in such systems must be appropriately implemented. Blockchain is a secure technique that has been used in a variety of IoT applications. The Blockchain's notable qualities, such as decentralization, immutability, transparency, security, and privacy, are the most obvious arguments for applying it in medical care settings.

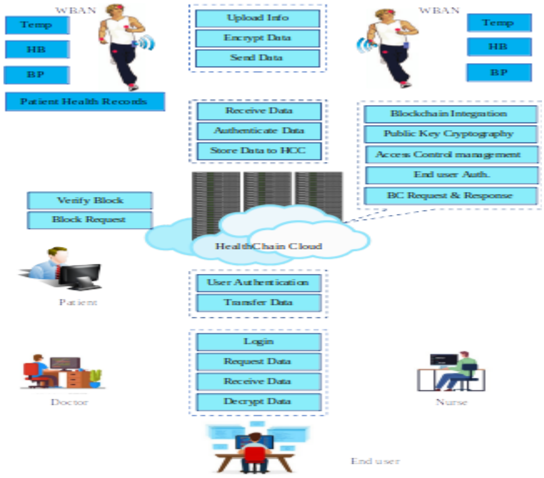
For the security of Electronic Health Records, we introduced HealthChain, a PKC and blockchain-based healthcare IoT solution (EHRs). Patients' medical records are encrypted and saved on the servers of the health-care service provider, with hash values stored in the blockchain. Identification and security in internet connections are handled by public key infrastructure (PKI). Public key cryptography is an encryption technology that uses two related keys, a public key and a private key. To encrypt and decode a transmission, these two keys are combined. When two cryptographic keys are paired in this way, it is called asymmetric cryptography.
Cryptographic techniques are used in public key cryptography to safeguard identities and data from unauthorized access or usage, hence protecting against cybercriminals and other bad actors. Rivest-Sharmir-Adleman (RSA) is a public key cryptography method for sending secure, sensitive data over an insecure network like the internet. The RSA algorithm is well-known because it encrypts messages using both public and private keys while maintaining their confidentiality and authenticity. RSA performs two functions at the same time..

The client encrypts data before transmitting it to the server with the public key, which the server decrypts with the private key. The session key is calculated by both parties using this information (a symmetric, private key that will be used to communicate). The client verifies that it holds the pre-master secret, which is the private key needed to decode the data. The session key passed between the two parties can then be used to communicate. The Internet of Medical Things (IoMT) is a group of medical equipment and software that communicate with healthcare professionals via the internet.
Machine-to-machine (M2M) communication between wireless medical equipment is the core of IoMT. Through wearable gadgets, medical care providers and authorities can obtain real-time health updates from patients in remote locations. However, in addition to the benefits of IoMT, there are also disadvantages, such as IoMT devices' vulnerability to security attacks. Not only has the need for novel medical devices expanded dramatically since the Covid-19 outbreak, but so have the security dangers associated with them.

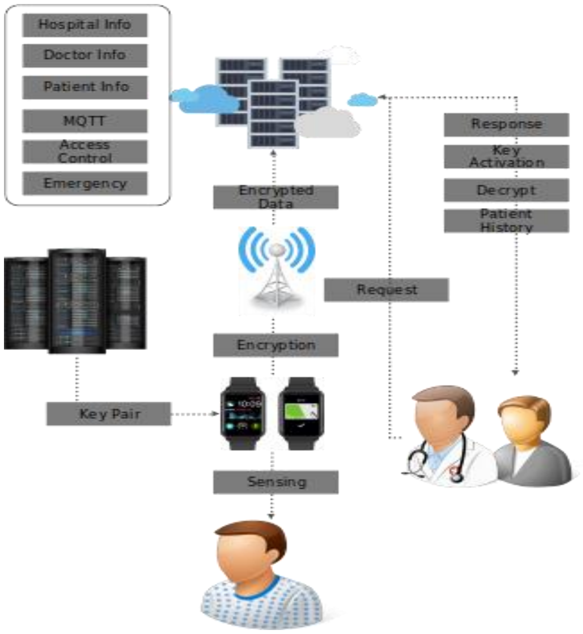
In the face of the threats posed by IoMT devices, blockchain could be a lifesaver. Blockchain's decentralized key management, inseparability, and integrity qualities can help smart medical equipment communicate safely. The system is built on smart contracts and blockchain technology. A consortium blockchain can be created by multiple hospitals working together. Instead of the power and time-consuming consensus mechanisms used in bitcoin, a faster consensus algorithm might be used to allow faster transactions. After attribute encryption, data blocks containing public parameters and digest information are recorded on the blockchain. To fulfill tasks like registration and permission, smart contracts are used. To provide a more secure environment, the blockchain can be headed by the government or a number of large hospitals.Smart Contracts

Smart contracts are written in JSON. The first smart contract is the Registration SC (SC). The Registration SC is required since only authorized participants can communicate on-chain and conduct function calls. It has capabilities that allow doctors, nurses, and cloud servers to sign up. It can also prohibit previously registered users from gaining access or calling functions. Tamper resistance and asymmetric encryption are two elements of decentralization. A secure manner to manage and keep data is one of the advantages.

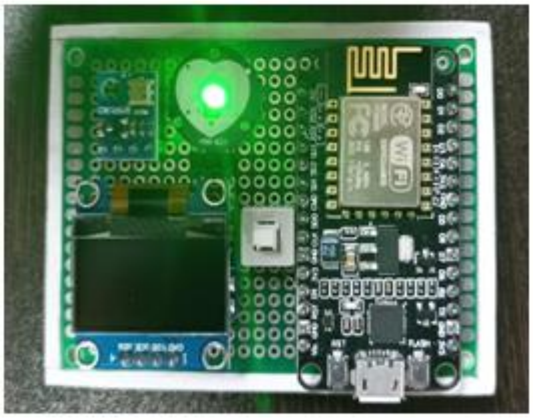
IV. FLOW DIAGRAM

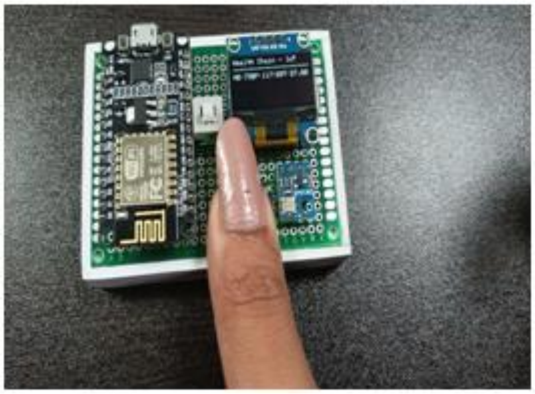


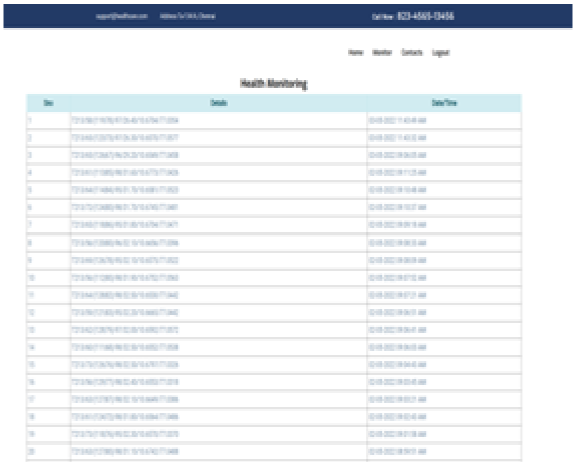
V. SYSTEM ARCHITECTURE



VI. RESULTS







Call Now: 823-4565-13456

Home Monitor Contacts Logout

Health Monitoring

Sno	Details	Date/Time
1	[illegible]	[illegible]
2	[illegible]	[illegible]
3	[illegible]	[illegible]
4	[illegible]	[illegible]
5	[illegible]	[illegible]
6	[illegible]	[illegible]
7	[illegible]	[illegible]
8	[illegible]	[illegible]
9	[illegible]	[illegible]
10	[illegible]	[illegible]
11	[illegible]	[illegible]
12	[illegible]	[illegible]
13	[illegible]	[illegible]
14	[illegible]	[illegible]
15	[illegible]	[illegible]
16	[illegible]	[illegible]
17	[illegible]	[illegible]
18	[illegible]	[illegible]
19	[illegible]	[illegible]
20	[illegible]	[illegible]

VII. ADVANTAGES

1. Decentralization, tamper resistance, and asymmetric encryption characteristics.
2. A dependable method of data management and storage.
3. Because medical data is recorded in the blockchain, it is extremely secure and cannot be readily tampered with. It is safe, dependable, and effective.Patients can use the technique to share disease information.
4. Controlling access to Electronic Health Records is essential. Smart Contracts will define and enforce access controls to EHR material, while Blockchain will contain

references to EHR data. Only authorized individuals will have access to the EHR data.

5. From birth to grave data integrity and provenance While traditional systems provide many of the benefits, such as safe, resilient, unalterable evidence, blockchain is unique in that it provides them "out of the box." There is no single point of failure in blockchain; if one node fails, other members can still access their data. This decentralized strategy increases resilience.
6. A blockchain solution functions as a "single source of truth." Immutability: Data can only be inserted; it cannot be modified or deleted afterwards. For all transactions, an in-built, tamper-proof, timestamped audit trail is available.

VIII. CONCLUSION

In telecare medicine based on WBANs, security and privacy of medical information are significant problems. This study presented the HealthChain concept for mutual authentication between patients' portable personal terminals and hospitals. The Internet of Medical Things (IoMT) employs encryption and the blockchain idea to solve concerns with centralized storage systems and offer secure patient data sharing among network participants. The blockchain technology has overcome the concerns of secrecy, privacy protection, and secure storage and handling that have been reported by healthcare service providers in previously published systems. To make patient information more accessible, the technology was connected with the online application. At any time and on any device, the patient or authorized healthcare staff can do simple and quick searches. According to the investigation, Health Chain outperforms comparable systems in terms of security and execution speed as well as communication costs. Performance and security at the highest levels. Patients and health-care providers may rest easy knowing that their medical information is only shared with authorized parties and is not maliciously altered during transmission thanks to TLAP.

REFERENCES

[1] Secure Y. Li, Y. Yu, R. Chen, X. Du, and M. Guizani, ``IntegrityChain: Provable data possession for decentralized storage," IEEE J. Sel. Areas Commun., vol. 38, no. 6, pp. 1205-1217, Jun. 2020. J.

[2] J. Li, H. Yan, and Y. Zhang, ``Identity-based privacy preserving remote data integrity checking for cloud storage," IEEE Syst. J., vol. 15, no. 1, pp. 577-585, Mar. 2021, doi: 10.1109/JSYST.2020.2978146.

[3] M. Kumar and S. Chand, ``A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability," IEEE Internet Things J., vol. 7, no. 10, pp. 10650-10659, Oct. 2020.

[4] P. Kasyoka, M. Kimwele, and S. M. Angolo, ``Certificateless pairing free authentication scheme for wireless body area network in healthcare management system," J. Med. Eng. Technol., vol. 44, no. 1, pp. 12-19, Jan. 2020:doi: 10.1080/03091902.2019.1707890.

[5] M. Monshizadeh, V. Khatri, O. Koskimies, and M. Honkanen, ``IoT use cases and implementations," in IoT Security. Hoboken, NJ, USA: Wiley, 2020, pp. 225-245, doi: 10.1002/9781119527978.ch12.

[6] X. Jia, D. He, N. Kumar, and K.-K.-R. Choo, ``Authenticated key agreement scheme for fog-driven IoT healthcare system," Wireless Netw., vol. 25, no. 8, pp. 4737-4750, Nov. 2019, doi: 10.1007/s11276-018-1759-3.Y. Xie, S. Zhang, X. Li, Y. Li, and Y. Chai, ``CasCP: Efficient and secure certificateless authentication scheme for wireless body area networks with conditional privacy-preserving," Secur. Commun. Netw., vol. 2019, pp. 1-13, Jun. 2019, doi: 10.1155/2019/5860286.

[7] S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, ``Privacy preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment," IEEE Access, vol. 7, pp. 47962-47971, 2019, doi: 10.1109/ACCESS.2019.2909556.

[8] W. Tang, K. Zhang, J. Ren, Y. Zhang, and X. Shen, ``Flexible and efficient authenticated key agreement scheme for BANs based on physiological features," IEEE Trans. Mobile Comput., vol. 18, no. 4, pp. 845-856, Apr. 2019, doi: 10.1109/TMC.2018.2848644.

[9] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, ``Cloudaided lightweight certificateless authentication protocol with anonymity for wireless body area networks," J. Netw. Comput. Appl., vol. 106, pp. 117-123, Mar. 2018, doi: 10.1016/j.jnca.2018.01.003.

[10] V. Lozupone, ``Analyze encryption and public key infrastructure (PKI)," Int. J. Inf. Manage., vol. 38, no. 1, pp. 42-44, Feb. 2018, doi: 10.1016/j.ijinfomgt.2017.08.004.

[11] H.-Y. Lin, ``A secure heterogeneous mobile authentication and key agreement scheme for e-healthcare cloud systems," PLoS ONE, vol. 13, no. 12, Dec. 2018, Art. no. e0208397, doi: 10.1371/journal.pone.0208397

[12] A. Zhang and X. Lin, ``Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain," J. Med. Syst., vol. 42, no. 8, p. 140, Aug. 2018.

[13] H. Wang and Y. Song, ``Secure cloud-based EHR system using attribute based cryptosystem and blockchain," J. Med. Syst., vol. 42, no. 8, p. 152, Jul. 2018.

[14] IEEEAccess (Volume:9) https://ieeexplore.ieee.org/document/9627166

[15] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, ``Cloudaided lightweight certificateless authentication protocol with anonymity for wireless body area networks," J. Netw. Comput. Appl., vol. 106, pp. 117-123, Mar. 2018, doi: 10.1016/j.jnca.2018.01.003.