International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

Blockchain-Secured Telemedicine and Remote Patient Monitoring System

Bazif Ahmed Syed, Arunendra Mani Tripathi, Yuvraj Kumar

School of Computer Science & Engineering, Galgotias University, Greater Noida, India

bazif.23SCSE1010711@galgotiasuniversity.ac.in, arunendra.tripathi@galgotiasuniversity.edu.in, yuvraj.22scse1012318@galgotiasuniversity.edu.in

ABSTRACT

In this paper, the author introduced a blockchain-protected telemedicine system to improve data privacy, integrity, and access control in remote patient monitoring settings. Combining IoT-based health data with blockchain and smart contracts provides security, transparency, and the impossibility of changing medical records. The experimental validation results using an IoT healthcare dataset demonstrated the effectiveness and practicality of the proposed solution. The next step in work will be the integration of AI, Blockchain, remote patient monitoring (RPM) and telemedicine, which has revolutionized health care delivery. Still, data integrity and privacy are among the significant issues because of centralized architectures. The paper suggests using IoT, AES encryption, SHA-256 hashing, and smart contracts as components of the Blockchain-Secured Telemedicine and RPM System to guarantee the security of decentralized data management. It is based on a four-layer architecture, including an IoT layer, vital signs collection, an Edge layer, encryption and hashing, a Blockchain layer, immutable storage and access control, and an application layer for secure telemedicine interaction. The system was coded in Python, Ethereum (Solidity), IPFS, and Flask/Streamlit and tested on a real IoT Healthcare Patient Monitoring dataset. Experimental results show low latency, high throughput, and strong access control, demonstrating that it should be used in real-time telemedicine. Confidentiality, integrity, and tamper resistance were checked through security analysis. In the future, AI, Federated Learning, Layer-2 scaling (Polygon), and Edge Computing will be integrated to improve performance and intelligence, providing intelligent, scalable, and real-time solutions in healthcare.

Keywords: *Blockchain, Telemedicine, Remote Patient Monitoring, IoT, Data Security, Smart Contracts, Healthcare 4.0.*

1. Introduction

With the advent of telemedicine and remote patient monitoring (RPM) systems, healthcare delivery has been transformed by the ability to monitor and assess patients remotely and in real-time beyond the traditional clinical setting. Especially in the post-COVID-19 era, these technologies are essential to chronic disease management, elderly care, and rural health accessibility [1]. Relying on wearable sensors and Internet of Things (IoT) devices, RPM systems capture key parameters such as heart rate, blood pressure, and oxygen saturation, and transmit them to healthcare providers for prompt diagnosis and treatment [2]. Despite the progress, traditional telemedicine systems are primarily based on centralized cloud infrastructures, which are highly risky from the point of view of data security and privacy. Centralized storage has a single point of failure, risk of unauthorized access, and data tampering, which results in a lack of transparency and trust among stakeholders [3]. The sensitivity of medical data calls for a robust mechanism to ensure confidentiality, integrity, and accountability while maintaining real-time accessibility.

To overcome these challenges, blockchain technology provides a decentralized and immutable ledger that can capture and validate transactions related to medical data without the need for a

trusted third party [4]. Its inherent properties, transparency, auditability, and tamper resistance, have established it as a promising technology to secure telemedicine environments. Furthermore, smart contracts can facilitate access control policies and consent management and ensure that only authorized organizations (e.g., doctors, patients) can access or update patient records [5]. Integrating IoT-based health monitoring with Blockchain enables secure, end-to-end data management, where IoT devices collect patient vitals, encrypt them, and store the corresponding hashes on the Blockchain. This combination ensures that any unauthorized modification will be immediately recognized and can be traced [6]. This research aims to design and implement a blockchain-secured telemedicine and Remote Patient Monitoring System that ensures data confidentiality, authenticity, and controlled data accessibility.

2. Literature Review

Telemedicine, IoT, and blockchain have been extensively integrated to enhance access to healthcare and data security. This section discusses the current literature on three prominent topics: telemedicine models, IoT-based remote patient monitoring systems, and blockchain-based healthcare security models.

2.1 Current Telemedicine Models.

The latest innovations in telemedicine solutions have helped to ensure constant patient care and distance consultation, minimizing the reliance on physical hospital visits. Conventionally, data storage and processing use cloud-based architecture [7]. An example of this is the suggestion by Kaur et al. [8] proposing a cloud-centric telemedicine system enabling the sharing of remote diagnosis and prescription. Nonetheless, such systems are not free of centralization problems, which form the single point of vulnerability and leave sensitive data vulnerable to cyberattacks. Correspondingly, Singh et al. [9] designed a mobile telehealth system in chronic disease management. Despite its efficiency in communication, the deficiency of data provenance and integrity checks renders it inappropriate for critical healthcare use cases. Such constraints demonstrate that a decentralized security system, such as blockchain, is required to instill confidence in the remote healthcare system.

2.2 Remote Patient Monitoring Systems using IoT.

IoT is a critical component in facilitating the implementation of real-time Remote Patient Monitoring (RPM) by wearables and embedded devices. RPM systems based on IoT can collect continuous health data, including heart rate, blood pressure, and oxygen saturation [10]. For example, Zhao et al. [11] designed an IoT-based healthcare monitoring system with Raspberry Pi and the MQTT protocol to exchange real-time data. Nonetheless, information stored on public networks is prone to decryption unless it is strongly encrypted or stored.

Additionally, IoT-cloud systems in most healthcare applications are prone to latency and scaling problems when data is centrally managed [12]. Therefore, effective monitoring is possible with the help of IoT, but its security and interoperability issues require integration with a decentralized blockchain.

2.3. Healthcare data security via blockchain.

Blockchain technology offers decentralized, immutable, and transparent data handling, essential to healthcare systems. Wang et al. [13] proposed an electronic health record (EHR) framework that leverages blockchain technology to protect patient data and enable selective data sharing. Similarly, Ahmed et al. [14] adopted a role-based access control system that leverages smart contracts for medical data exchange. These techniques enhanced data integrity and traceability but could not easily synchronize real-time data with IoT sources.
Moreover, hybrid schemes combining blockchain and off-chain storage (e.g., IPFS or cloud storage) have been proposed to achieve optimal performance [15]. Nevertheless, the problem of IoT-blockchain interoperability is a significant challenge [16].

2.4. Research gaps

The gaps are as follows:

- Slow processing of blockchain transactions requires real-time monitoring.
- Low interoperability between the blockchain and IoT devices.
- The lack of fine-grained access control mechanisms.
- The absence of end-to-end encryption when transmitting data.
- Minimal prototyping based on actual IoT medical data.

To address these lapses, this paper proposes a Blockchain-Secured Telemedicine and RPM System that combines IoT data capture, AES-based encryption, SHA-256 hashing, and smart contracts for decentralized access control.

3. Proposed System

The section has introduced the proposed Blockchain-Secured Telemedicine and Remote Patient Monitoring (RPM) System, which will ensure data privacy, integrity, and controlled access at multiple levels. The architecture incorporates IoT-enabled health data collection, edge encryption, blockchain-based integrity verification, and access control via smart contracts.

3.1. System Overview

- The proposed system will have four major layers as depicted in Fig. 1. A layer is charged with a set of operations, delivering secure, transparent, and real-time telemedicine services together.
- IoT Layer: This layer records essential health measurements, including Heart Rate (HR), Blood Pressure (BP), and Oxygen Saturation (SpO_2), with the help of the connected sensors or simulated dataset [17]. Information is constantly flowing to the edge layer for pre-processing.
- Edge Layer: The edge node (e.g., Raspberry Pi or cloud gateway) will encrypt (AES) and hash (SHA-256) data collected and send it to the blockchain. This ensures that the original data will remain confidential and intact in the event of communication interception.
- Blockchain Layer: This is implemented with Ethereum, and it contains the hash values of the data and ensures access control through smart contracts. The data can be accessed only by authorised entities (i.e., doctors and patients) based on the public ledger provided by

the blockchain [18].

- Application Layer: Doctors and patients can access data through a web-based dashboard (written in Flask or Streamlit) to visualise health trends, grant or revoke access to data based on executing smart contracts.
- This multi-layer architecture provides secure data transfer, storage that cannot be tampered with, and access control at a fine-grained level, eliminating the problems highlighted in Section 2.

3.2. Architecture Diagram

Figure 1 depicts the end-to-end data flow and interactions among the layers of the proposed system's conceptual architecture.

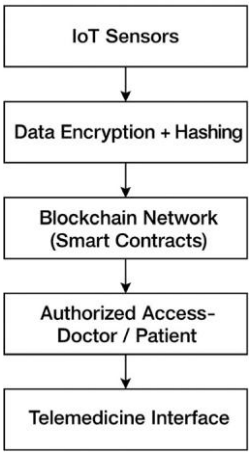

Figure.1. Blockchain-Secured Architecture of Telemedicine and RPM System Proposed.

The data flow begins with IoT sensors that gather health data. The Edge Layer uses encryption (AES) and hashing (SHA-256). The resulting hash is accessible to the Blockchain Network, which validates access requests via smart contracts. Lastly, authorized people handle the Real-Time monitoring, Consultation and Records through the Telemedicine Interface.

3.3. Component description

All the elements in the proposed system are crucial to end-to-end security and efficiency. Each layer is described in detail below:

a) IoT Layer - The IoT Layer is the data collection hub for gathering real-time patient vitals using wearable or embedded devices. Simulation environments can emulate real patient conditions using open datasets or Raspberry Pi sensor emulators [19]. The data obtained is time-stamped and sent to the edge node.

b) Edge Layer- The Edge Layer provides a means to guarantee the confidentiality of data prior to transmission using AES-256 encryption and data integrity using SHA-256 hashing. Off-chain storage (IPFS or a safe local database) can store encrypted data, and the hash values are transmitted to the blockchain. This semi-centralised solution saves blockchain load without sacrificing immutability.

c) Blockchain Layer

This layer keeps track of and is implemented on Ethereum or Hyperledger.

- Hash Storage: It stores hash values to validate the integrity.
- Smart Contracts: Solidity-based, stating access controls, consent regulations and audit

trails.

- Consensus Protocol: Assuring distributed trust between the nodes involved. Ganache enables local testing, allowing transactions to be valid without the high gas fees. A blockchain transaction is initiated by every new piece of data that is stored irreversibly [20] [21].

d) Smart Contracts- Smart contracts are independent access controllers. They encode access, revocation, and authorization rules of data. For example, decrypted data can be accessed only by a doctor whose address is listed in the contract. Any change request is recorded in a non-mutable way.

e) Off-Chain Storage- The storage capacity of blockchain is limited, so raw encrypted data is stored in IPFS (InterPlanetary File System) or a local database, and file hashes are stored in blockchain. This architecture is a tradeoff between security and scalability.

g) Frontend (Application Layer)

The Frontend Layer will include user-friendly interfaces to:

- Doctors: See health trends, check integrity and consult notes.
- Patients: Check their vitals, provide/ deny access to data and get notifications.

Dashboard creation is made with Flask or Streamlit frameworks and includes web3.py interaction with the blockchain and IPFS API retrieval.

4. Mathematical Formulation

This part provides the mathematical basis for the proposed Telemedicine and Remote Patient Monitoring System based on the Blockchain, which is secured to guarantee data confidentiality, integrity, and trust through encryption, hashing, access validation, and transaction verification.

4.1. Encryption model

The collected data D of patient health provided by IoT sensors is encrypted with the help of the symmetric key encryption algorithm (AES-256). Encryption can be defined as follows:

$$C=EK(D)$$

Where: C=Cipher Text, D= Original patient data, K= Secret encryption key, E=Encryption function.

This will guarantee data security because unauthorized agencies cannot access plaintext data without the key.

4.2. Hash Generation

To ensure the integrity of the data and to identify any manipulation, the cryptographic hash is created with the help of the SHA-256 function:

$$H=SHA256(C)$$

where: H refers to the hash of the cypher text C.

Every hash is put on the Blockchain, a verifiable integrity vehicle. Any difference between re-

computed and stored hash values shows that the data has been tampered with.

4.3. Access validation function

Role-based authorisation imposed by smart contracts governs access to patient data. The mechanism of validation is as follows:

$A_{valid}=f(Role,Permission,SmartContract)$

Where:

$Role \in \{Doctor,Patient\}$

$Permission \in \{Read,Write\}$

SmartContract=Blockchain-based access control logic

if $A_{valid}=1$, access is granted; otherwise, it is denied.

4.4. Transaction verification

Every Blockchain transaction must be verified, authenticated, and registered in the ledger. A valid transaction should meet two conditions: a digital signature and a hash satisfying the conditions:

$Tx_{valid}=(Sig \wedge H_{match})$

Where:

Sig=valid digital signature of the sender

H_{match}=Integrity check passed ($Hn_{ew}=Hs_{tored}$)

Thus, $Tx_{valid}=1$ ensures that transactions on the blockchain are trusted and verifiable.

Combining these mathematical models provides a safe computational environment in which data is encrypted, hashed, and verified, with transparent verification on the blockchain, ensuring confidentiality, integrity, and non-repudiation.

5. Algorithm

The end-to-end workflow of the proposed Blockchain-Secured Telemedicine System is described in the following pseudocode.

Algorithm 1: Telemedicine Secured Data Flow with blockchains.

- Input: IoT sensor PatientData.
- Output: Confirmed, checked, and encrypted data that is available within the smart contract.

Algorithm Blockchain_Secured_Telemedicine()

Step 1: Collect patient vitals → {heart_rate, bp, spo2, temp}

Step 2: Encrypt Data using AES key → CipherData

CipherData = E_K(PatientData)

Step 3: Generate Hash = SHA256(CipherData)

Step 4: Store (Hash, patient_id, timestamp) on Blockchain

Step 5: Deploy SmartContract with Access Rules:

Roles = {Doctor, Patient}
Permissions = {Read, Write}
Step 6: On Access Request:
If Verify(Signature, Role, Consent) == TRUE:
Fetch CipherData
Decrypt with Key → PlainData
Display PlainData to Authorized User
Else:
Deny
Access Step 7: End
Algorithm

6. Dataset

6.1 Dataset Used

The IoT Healthcare Patient Monitoring Dataset was applied to assess the suggested Blockchain-Secured Telemedicine and Remote Patient Monitoring (RPM) System. This publicly available data can be found on Kaggle (IOT-healthcare-patient-monitoring) and is intended to simulate real-time patient data streams generated by IoT-enabled sensors. It includes simulated health data of several virtual patients and contains more than 10,000 timestamped observations in CSV format. The records consist of longitudinal readings of vital parameters related to the patient, such as heart rate, blood pressure, oxygen saturation (SpO2), and body temperature, recorded at predetermined intervals. The main goal of dataset utilization is to recreate continuous patient monitoring-related scenarios, permitting testing and verifying the main system elements, including data encryption, creating a hash (SHA-256), blockchain storage, and access control based on smart contracts. Using this dataset, it is possible to test the proposed framework in a real-world setting in the context of IoT telemedicine while retaining the reproducibility and scalability of the study at the research level, as shown in Table 1.

Table 1. Dataset Attributes and Description

Features	**Description**
Patient_ID	Unique identifier for each patient
Heart_Rate	Heart rate in beats per minute (bpm)
Blood_Pressure	Blood pressure measured in mmHg
SpO_2	Oxygen saturation level in percentage (%)
Temperature	Body temperature in degrees Celsius (^0C)
Timestamp	Time when the reading was recorded

Each record represents a snapshot of a patient's health at a given timestamp, suitable for real-time monitoring, edge encryption, and on-chain validation.

6.2 Preprocessing Steps

To guarantee quality, consistency, and readiness to be integrated in blockchain, the following preprocessing tasks have been used:

1. Handle Missing Values:

- There were cases where the entries were missing or null, which were corrected through mean imputation in case of numerical fields and forward fill in case of timestamps to ensure continuity of time.
- It provides secure encryption and hash elements with no data corruption.

2. Normalized Numerical Data:

- Min-max normalization was used to put the continuous variables (e.g., heart rate, temperature) on a standard scale (01).
- This helps minimize the effect of outliers and ensure even data distribution.

3. Compute Encrypted + Hashed Values:

- Each patient record D was coded using AES-256 and a secret key. K, producing ciphertext C=EK(D).
- Corresponding hash values H=SHA256(C) were calculated and fixed on the blockchain to ensure data integrity.

4. Blockchain Data to Map Transactions:

A blockchain transaction was formed with each encrypted record that contained:

- Patient-ID (unique identifier)
- Timestamp
- H (amount to verify integrity)
- Role Permission Access control parameters (Role, Permission) Smart contracts deal with access controls and consent-based access to data.

7. Implementation Details

The suggested Blockchain-Secured Telemedicine and Remote Patient Monitoring System is deployed as a multi-layered architecture combining data generation via an IoT-based system, blockchain-based security, and a user-friendly visualizing interface. All layers utilize technology expertise to ensure complete data flow, integrity, and access control, as shown in Table 2.

Table 2: Implementation Layers, Technologies, and Functions

Layer	Technology	Function
IoT Layer	Python (Simulation)	Generates patient vitals such as Heart Rate, BP, SpO_2, and Temperature
Blockchain Layer	Ethereum + Solidity	Deploys smart contracts for access control and stores hashed data transactions
Off-chain Storage	IPFS / MongoDB	Stored encryption patient data securely off chain
Frontend	Flask / Streamlit	Provides interactive dashboards for doctor and patients

The Python simulation scripts implement the IoT Layer, simulating continuous vital sign

readings. AES encryption is followed by SHA-256 hashing for each data record.

- The Ethereum network (tested on Ganache) is used in the Blockchain Layer, in which Solidity smart contracts handle user roles and access control on data and data integrity. The blockchain ledger captures all transactions to allow auditability.
- The Off-Chain Storage module (IPFS or MongoDB) provides a scalable and secure storage of encrypted medical data and keeps hash records on-chain to validate them.
- The Frontend Interface, built with Flask or Streamlit, allows authorized users (deauthorizations) to see real-time vital data, confirm data validity and dynamically grant or revoke access control permissions.

Development Tools:

- MetaMask - to integrate wallets and to sign transactions.
- Ganache- Ethereum blockchain to test.
- Remix IDE- to develop and deploy Solidity contracts.
- Python 3.10 backend logic, encryption, and simulation of data.
- Web3.py- Python backend and Ethereum blockchain connection.

8. Results And Evaluation

This section presents the results of evaluating the proposed Blockchain-Secured Telemedicine and Remote Patient Monitoring (RPM) System with respect to performance, scalability, and security. The model was tested using simulated IoT healthcare data to determine latency, throughput, encryption efficiency, and execution delay for a smart contract.

8.1. Performance Metrics

Several quantitative measures were employed to thoroughly examine the system, which are presented in Table 3.

Table 3: Performance Evaluation Metrics

Metric	**Description**
Latency	Average time taken to execute a blockchain transaction
Throughput	Number of transactions processed per second
Encryption Time	Time required to perform AES Encryption on patient data
Access Delay	Delay incurred during smart contract-based access validation

All these metrics can be used to measure the responsiveness and efficiency of the blockchain layer, encryption module, and access control mechanisms.

8.2 Graphical Evaluation

The performance graphs of the system at different workloads and configurations were plotted as follows:

- **Transaction Time vs Number of Requests:** Shows the system scalability and blockchain transaction latency as the number of requests grows, as shown in Figure 2.

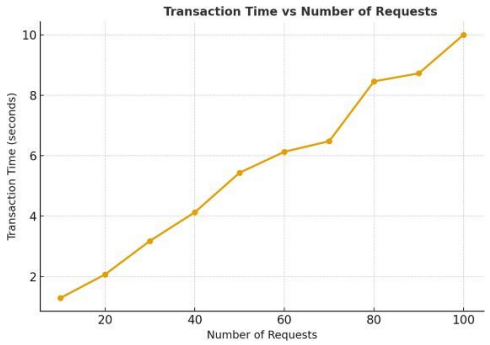

Figure 2: Transaction Time vs Number of Requests

- **Encryption Time vs Data Size:** Illustrates the calculation cost of AES encryption as the dataset size grows, as shown in Figure 3.

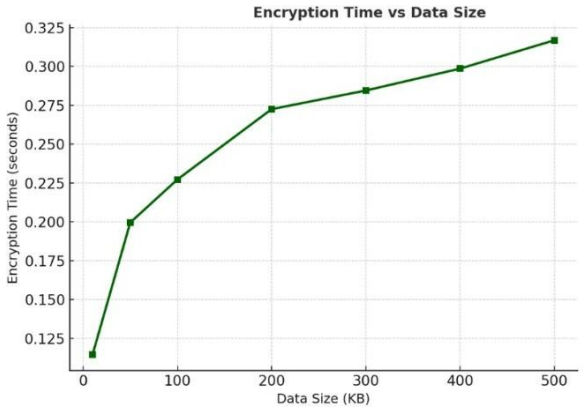

Figure 3: Encryption Time vs Data Size

- **Access Latency vs Number of Nodes** - Measures the smart contract verification delay as the number of network participants (nodes) increases, as shown in Figure 4.

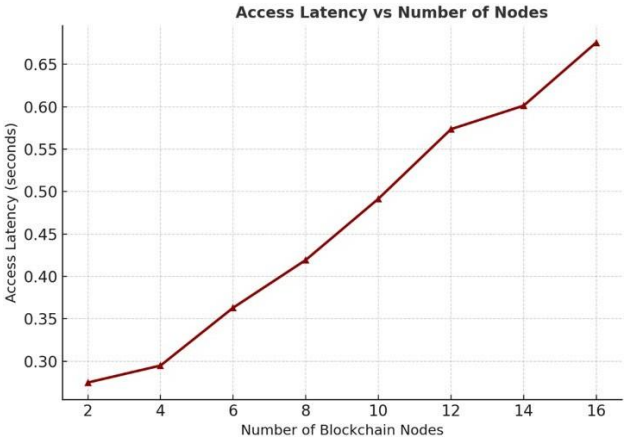

Figure 4: Access Latency vs Number of Nodes

8.3 Security Analysis

The proposed system was evaluated against the main security properties that were very important to the data transmission and storage in healthcare:

- **Integrity:** Maintained with the help of the SHA-256 hash, which means the mismatch

of hashes can easily detect any changes in encrypted data.

- **Confidentiality:** This is ensured through the AES symmetric encryption before off-chain storage, which secures sensitive patient information.
- **Access Control:** Implemented with the help of Solidity-based smart contracts, which provide roles (Doctor, Patient) and permissions (Read, Write).
- **Tamper Resistance:** It is obtained with the help of the immutability feature of blockchain, which discourages illegal changes in the transactions stored.

It is confirmed that a combination of blockchain and IoT-based telemedicine systems has a strong positive effect on data trustworthiness, privacy, and accountability.

9. Discussion

9.1 Advantages

The proposed telemedicine framework will be blockchain-secured, guaranteeing decentralization, the absence of single points of failure, and fostering transparency and auditability given by the immutable ledgers. It also improves data safety through AES encryption and automated access control through smart contracts, so the authorized users can only access sensitive medical data.

9.2 Limitations

The system has some limitations, even though it is strong, such as the high transaction costs and inability to scale, especially in a public blockchain setting. Large-scale deployments may be subject to these factors and disrupt real-time performance.

10. Conclusion & Future Work

In this paper, the author introduced a blockchain-protected telemedicine system to improve data privacy, integrity, and access control in remote patient monitoring settings. Combining IoT-based health data with blockchain and smart contracts will provide security, transparency, and the impossibility of changing medical records. The experimental validation results based on an IoT healthcare dataset showed the effectiveness and practicability of the proposed solution. The next step in work will be the integration of AI, Blockchain, and Edge Computing to provide intelligent, scalable, and real-time solutions in the healthcare field.

References

[1] Olorunsogo, T. O., Balogun, O. D., Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., & Onwumere, C. (2024). Reviewing the evolution of US telemedicine post-pandemic by analyzing its growth, acceptability, and challenges in remote healthcare delivery during Global Health Crises. *World Journal of Biology Pharmacy and Health Sciences*, *17*(1), 075-090.

[2] Kumar, Y., Verma, S. K., Singh, A., Kumar, K., & Gupta, M. (Eds.). (2024). *IoT-Enabled Healthcare Systems: Applications, Benefits, and Challenges*. CRC Press.

[3] Azeez, N. A., & Van der Vyver, C, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Informatics Journal* 20, no. 2 (2019): 97-108.

[4] U. Sugandh, M. Khari, and S. Nigam, "How Blockchain Technology Can Transfigure the Indian Agriculture Sector: A Review," Handbook of Green Computing and Blockchain Technologies (2021): 69-88.

[5] Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal*, *8*(7), 5914-5925.

[6] Sugandh, U., S. Nigam, M. Khari, S. Misra. "An approach for risk traceability using blockchain technology for tracking, tracing, and authenticating food products." Information 14, no. 11 (2023): 613.

[7] Hu, P. J. H., Chau, P. Y., & Sheng, O. R. L. (2002). Adoption of telemedicine technology by health care organizations: An exploratory study. *Journal of organizational computing and electronic commerce*, *12*(3), 197-221.

[8] M. Khari, M. Kumar. "Secure data transference architecture for cloud computing using cryptography algorithms." In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 2141-2146. IEEE, 2016.

[9] B. Mallikarjuna, G. Shrivastava, and M. Sharma. "Blockchain technology: A DNN token-based approach in healthcare and COVID-19 to generate extracted data." Expert Systems 39, no. 3 (2022): e12778.

[10] H. Sharma, P. Kumar, G. Shrivastava, K. Sharma, A. Bhola. "Using Machine Learning for Protecting the Security and Privacy of Internet of Medical Things (IoMT) Systems." In *Integrating Cloud, Fog, and Edge Computing in Healthcare: Federated Learning and Blockchain Approaches: Harnessing Distributed Technologies for Enhanced Healthcare Delivery*, pp. 123-138. Cham: Springer Nature Switzerland, 2026.

[11] X. Zhao, L. Chen, and H. Wu, "An IoT-enabled real-time patient health monitoring system using Raspberry Pi," *Sensors*, vol. 23, no. 15, p. 6762, 2023.

[12] D. Roy and K. Banerjee, "Performance analysis of cloud-based IoT healthcare systems," *Future Generation Computer Systems*, vol. 144, pp. 620–632, 2024.

[13] Y. Wang, Z. Liu, and C. Sun, "Blockchain-based electronic health record management for data integrity and privacy," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 4555–4568, 2023.

[14] M. Ahmed, J. Rahman, and S. Das, "Smart contract-based secure medical data sharing using blockchain," *Computers in Biology and Medicine*, vol. 174, p. 107513, 2024.

[15] A. Bansal and P. Jain, "Hybrid blockchain-IPFS framework for healthcare data sharing," *IEEE Access*, vol. 12, pp. 76589–76603, 2024.

[16] R. Das and V. Goyal, "Interoperability challenges in IoT-blockchain healthcare integration," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 2, pp. 1505–1516, 2024.

[17] P. Sharma and K. Bhatia, "IoT-driven healthcare systems: Design and deployment challenges," *IEEE Sensors Journal*, vol. 25, no. 4, pp. 5678–5690, 2024.

[18] R. Li and D. Xu, "Blockchain-based decentralized access control for telehealth systems," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 1852–1866, 2024.

[19] L. Thomas and J. Zhang, "Simulation of IoT-based health data using Raspberry Pi and Python," *Journal of Biomedical Informatics*, vol. 146, p. 105872, 2024.

[20] M. Kumar, A. Jain, and S. Bhosale, "Smart contract-based consent management in healthcare blockchain," *Computers in Biology and Medicine*, vol. 176, pp. 107624, 2025.

[21] V. Maurya, I. Kumar, & N. Kumar, "Developing Verifiable Computations and Homomorphic Encryption to Promote Federated Learning," In 2024 Second International Conference on Advances in Information Technology (ICAIT), 1, pp. 1-7 (2024, July) IEEE.