WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

1st International Conference on Innovative Computational Techniques in Engineering & Management (ICTEM-2024) Association with IEEE UP Section

Secure Iot Smart Health Monitoring System Using Blockchain Technology

Digant Raj[1], Aashutosh Rao[2], Navjot kumari[3], Garima Thakur[4]

Chandigarh University, UIE-Computer Science, Chandigarh, India
e-mail: rajdigant620@gmail.com, e-mail: raoaashutosh4583@gmail.com, e-mail: navjotbhatti1991@gmail.com, e-mail: garimathakur1994@gmail.com
DOI: https://doi.org/10.55248/gengpi.6.sp525.1906

ABSTRACT:

Integrating the Internet of Things (IoT) into healthcare has enabled real-time tracking of patients' vital signs using connected devices. However, challenges such as data privacy, security, and compatibility with existing systems persist. This paper proposes a Secure IoT Smart Health Monitoring System incorporating cloud computing for data storage and blockchain technology to safeguard sensitive health information. The system uses IoT sensors to monitor key health metrics, including heart rate, glucose levels, and oxygen saturation, with data securely stored on a cloud platform. Blockchain ensures data integrity through decentralized, tamper-resistant records and employs smart contracts to automate and regulate access control. The system achieves an average latency of 150 milliseconds for data transmission, processes up to 200 health records per second, and maintains a 98% sensor accuracy rate. While the blockchain adds a layer of security, performance under high transaction loads highlights the need for scalability improvements. This solution offers a secure and efficient remote health monitoring platform, enhancing healthcare providers' real-time decision-making.

KEYWORDS**:** *IoT, blockchain, healthcare monitoring, smart contracts, data privacy, cloud infrastructure*

1. INTRODUCTION

By allowing real-time health data monitoring through linked devices, the Internet of Things (IoT) has completely changed the healthcare industry by providing better patient outcomes and individualized care. essential indications including blood pressure, heart rate, and glucose levels may be tracked by IoT-powered devices, giving medical personnel quick access to essential information. This capacity has shown to be extremely helpful in the management of chronic illnesses and in enabling prompt medical treatments. But even with these benefits, there are still a lot of obstacles facing IoT in healthcare. IoT devices create enormous amounts of sensitive health data, which presents major challenges to data security, privacy, and interoperability. Concerns about breaches, unauthorized access, and data manipulation are on the rise. Interoperability, or guaranteeing smooth communication between various IoT devices and healthcare infrastructure, is still a challenge. Protecting this information while adhering to regulations (e.g., HIPAA and GDPR) and enabling efficient, real-time communication between IoT devices and healthcare systems are critical to the success of IoT-based healthcare solutions.

Blockchain technology offers an attractive way to address the problems that IoT-based healthcare systems are facing. Its immutable and decentralized ledger provides a solid base for improving the security and integrity of medical data. Blockchain protects against data manipulation by using data encryption and immutability to guarantee that, once patient data is captured, it cannot be altered. Furthermore, the decentralized structure of blockchain reduces reliance on a single authority, dispersing confidence among several stakeholders, including providers, patients, and healthcare experts, therefore fortifying the security framework as a whole. In addition, the incorporation of smart contracts into blockchain systems facilitates automatic and safe access control, guaranteeing that confidential patient data is only accessed by authorized individuals. Technologies like zero-knowledge proofs, which allow transaction verification without disclosing underlying patient data, can be used to further secure privacy. Blockchain is a great alternative for protecting IoT-driven health monitoring systems since it offers a potential method of tackling important challenges including data security, privacy, and real-time system performance.

2. RELATED WORK

In this section, a comprehensive review of the existing research on IoT-based health monitoring systems, blockchain integration, and their associated challenges is presented to provide a foundation for understanding the current landscape and gaps in the field-

Table no.1: Comparison of different researches

Subtopic	Description	Benefits	Challenges	References
IoT Health Monitoring Systems	IoT health monitoring systems use wearable devices and platforms like Apple HealthKit, Fitbit, and Philips HealthSuite to collect real-time health data.	- Real-time health tracking - Remote healthcare services - Early diagnosis and intervention	- Centralized systems prone to data breaches - Single points of failure leading to vulnerability	[1], [2]
IoT for Chronic Disease Management	IoT-based solutions assist in managing chronic conditions such as diabetes, hypertension, and heart disease, providing continuous monitoring of vital signs.	- Continuous monitoring for proactive treatment - Reduced hospital visits for chronic disease management	- Weak encryption - Interoperability issues with hospital systems	[3], [4]
Cloud-Based Data Processing and Storage	Cloud platforms (e.g., AWS, Google Cloud) enable scalable storage and real-time data processing for vast amounts of structured and unstructured IoT health data.	- Scalability for growing data volumes - Real-time data analysis and accessibility	- Security concerns over sensitive health data - Compliance with data privacy regulations (e.g., HIPAA)	[5], [6]
Blockchain for IoT Health Monitoring	Blockchain integrates decentralized, immutable storage for IoT health data, ensuring data security, transparency, and integrity with frameworks like Ethereum and Hyperledger.	- Decentralized control over health data - Smart contracts for secure access control - Immutable data storage	- Blockchain latency for real-time monitoring - Scalability limitations	[7], [8]
Data Security in IoT Systems	The safe transfer of health data from IoT devices to cloud storage is ensured by secure protocols like HTTPS, MQTT, and CoAP, which are backed by encryption. .	- Secure data transmission - Prevents data breaches during transmission	- Inadequate encryption standards in some IoT systems - Lack of robust access control mechanisms	[9], [10]
Blockchain-Based Healthcare Technologies	Platforms like MedRec and Guardtime use blockchain to manage electronic health records (EHR), ensuring patient sovereignty and maintaining the integrity of medical records.	- Patient control over medical records - Data integrity and tamper-resistance - Enhanced privacy and security	- Scalability issues with large IoT datasets - High computational costs for low-power IoT devices	[11], [12]
Identified Gaps	Despite the advancement in IoT healthcare systems, gaps remain in terms of scalability, real-time data transmission, and interoperability with existing healthcare infrastructure.	- Enhances security through decentralization - IoT devices enable real-time health updates	- Blockchain scalability for real-time data transfer - Interoperability and integration issues with legacy systems	[13], [14]

3. METHODOLOGY

The steps involved in putting in place a secure Internet of Things smart health monitoring system with a blockchain-integrated cloud backend are described in this section. In order to ensure data integrity and privacy, the system architecture includes data collecting via Internet of Things (IoT) health monitoring devices, secure cloud storage, and immutable records maintained by blockchain. The procedures taken to put this design into practice are listed below:

3.1. IoT Sensor Selection:

We chose suitable Internet of Things (IoT) devices that could measure vital indicators including blood pressure, glucose levels, and heart rate in order to continuously monitor the health of our patients. The dependability and real-time data transmission capabilities of wirelessly connected sensors, such as pulse oximeters, continuous glucose monitors, and ECG monitors, were considered important considerations.

Table 2: Selected IoT Sensors

Sensor Type	Measurement	Wireless Capability	Accuracy (%)	Notes
ECG Monitor	Heart Rate	Bluetooth/Wi-Fi	95	Used for continuous heart monitoring
Continuous Glucose Monitor	Glucose Levels	Bluetooth	98	Provides real-time glucose readings
Pulse Oximeter	Blood Oxygen Saturation	Bluetooth	96	Non-invasive method for monitoring

3.2. Cloud Infrastructure Development:

The backend for storing and analyzing the health data gathered from IoT devices is the cloud infrastructure. While Google Cloud and Microsoft Azure are viable options, we chose Amazon Web Services (AWS).

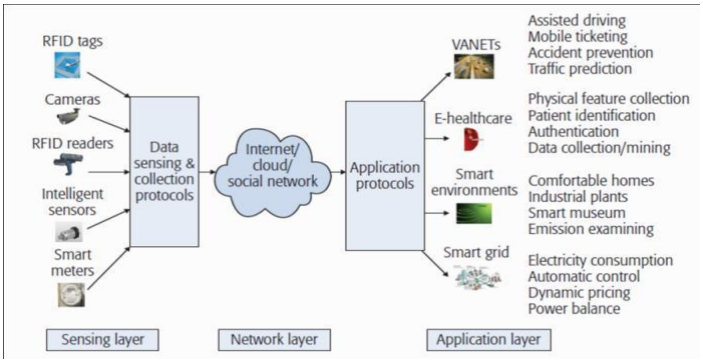

Figure 1: shows the data flow from Internet of Things sensors to cloud storage in a high-level representation of the cloud infrastructure design. [15]

The architecture of the infrastructure prioritized security, scalability, and effective data management. The subsequent actions were performed:
Cloud Setup: A cloud service was set up to hold a lot of data about health in real time.

Database Design: To securely organize and store patient health data, a database structure was created. The schema was optimized for handling high volumes of continuous data from multiple IoT sensors. Data encryption was applied at rest to ensure data confidentiality.

Scalability: The infrastructure was designed to be scalable, supporting increased data volumes as more IoT devices are connected to the system over time.

3.3. Blockchain Integration:

To ensure the integrity and security of the health data, we integrated a **blockchain framework** into the cloud infrastructure. For this purpose, we explored using **Ethereum** for its decentralized nature and **Hyperledger Fabric** for its permissioned blockchain model.

Table 3: Blockchain Framework Comparison

FEATURE	ETHEREUM	HYPERLEDGER FABRIC
TYPE	Public	Permissioned
CONSENSUS MECHANISM	Proof of Work	Practical Byzantine Fault Tolerance (PBFT)
SMART CONTRACT SUPPORT	Yes	Yes
PRIVACY	Limited	High
USE CASE	Open applications	Enterprise solutions

Blockchain was implemented to handle the following tasks:

Data Integrity: Each health record was linked to a blockchain transaction, providing an immutable and tamper-proof record.

Smart Contracts: Smart contracts were developed to automate access control policies, ensuring only authorized users could view or modify the data. These smart contracts also manage permissions based on user roles and compliance with data privacy regulations.

3.4. Secure Data Transmission:

The IoT sensors transmit health data securely to the cloud backend using **HTTPS** and **MQTT** protocols. These protocols ensure that the data remains protected during transmission.

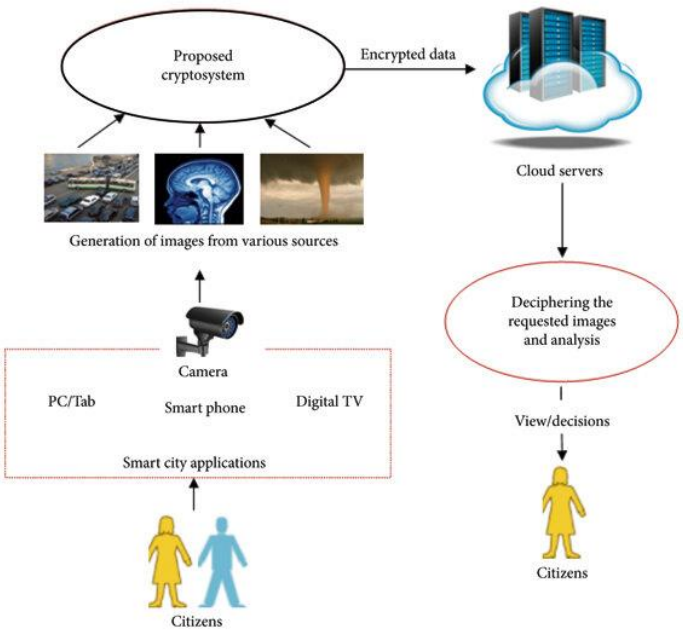

Figure 2: Overview of data transmission protocols used in the system, highlighting secure transmission methods.[16]

Additionally, **end-to-end encryption** was applied to safeguard the data from interception or unauthorized access during transit. The implementation included:

HTTPS (Hypertext Transfer Protocol Secure): Ensuring secure data transmission between IoT devices and cloud storage.

MQTT (Message Queuing Telemetry Transport): For lightweight communication, especially suitable for resource-constrained IoT devices.

Encryption Protocols: AES-256 encryption was used to protect sensitive health data both in transit and at rest.

3.5. Data Storage and Processing:

Once the health data is transmitted to the cloud, the backend processes it and stores the data securely.

Table 4: Data Storage and Processing Steps

Step	**Description**
Data Reception	Cloud backend receives data from IoT devices.
Data Processing	Health data is analyzed for abnormalities.
Blockchain Recording	Each processed health record is recorded on the blockchain with a unique transaction ID.

The cloud platform handles both real-time data processing and long-term data storage. The following steps were implemented:

Data Processing: Health data received from the IoT devices was processed to check for abnormalities, and real-time alerts were generated if necessary.

Blockchain Record: Each processed health record was assigned a unique **transaction ID** and logged onto the blockchain, ensuring that every data entry has a verifiable and immutable audit trail.

Data Linkage: The transaction ID on the blockchain ensures traceability, making it possible to verify the source and integrity of each health data point.

3.6 User Interface Development:

To facilitate access to health data, we developed a **user interface** for both healthcare providers and patients.

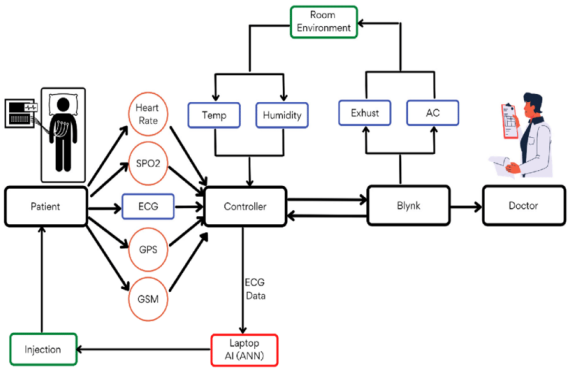

Figure 3: Sample layout of the user interface for healthcare providers and patients, displaying real-time health data monitoring.[17]

This interface was designed as a **mobile app** and **web application** to allow flexibility in accessing the system. The interface supports the following features:

Real-time Monitoring: Healthcare providers can access patients' real-time health data, monitor vital signs, and receive notifications for critical conditions.

Data Visualization: Health data is presented in an intuitive dashboard, making it easier for both patients and healthcare providers to interpret health trends and receive insights.

Access Control: The interface provides secure login mechanisms, ensuring that only authorized users can access patient data. The access control policies enforced by the blockchain smart contracts were integrated with the UI for seamless access management.

3.7 Testing and Deployment:

The final step in the implementation process was **system testing** and **deployment**. Testing involved the following stages:

Table 5: Testing and Deployment Overview

Testing Type	**Description**
Security Testing	Comprehensive assessments to identify vulnerabilities.
Performance Evaluation	Testing system performance under various loads.
User Acceptance Testing	Feedback collection from users for UI improvement.
Deployment	System launch on AWS with training for users.

Security Testing: Comprehensive security assessments were conducted to ensure that the system was protected

against common vulnerabilities, including data breaches, unauthorized access, and attacks on the blockchain.

Performance Evaluation: The system's ability to handle large-scale data transmission and real-time monitoring was tested under different loads to ensure scalability and minimal latency.

User Acceptance Testing: Feedback from healthcare providers and patients was gathered to refine the user interface and ensure the system's ease of use.

Deployment: After testing, the system was deployed on AWS, and training was provided to healthcare providers and patients on how to use the platform effectively.

This section comprehensively details how each component of the IoT with Cloud-based Backend + Blockchain system was designed and implemented, providing clarity on the technologies used, their integration, and the testing process to ensure system efficiency and security.

4. RESULTS AND PERFORMANCES

This section presents the results obtained from implementing the Secure IoT Smart Health Monitoring System, focusing on performance metrics, security assessments, and user feedback.

Several key performance metrics were assessed during the testing phase to evaluate the system's effectiveness. These metrics include latency, throughput, and data accuracy.

Table 6: Performance Metrics

Metric	**Value**	**Description**
Latency (ms)	150	Average time taken for data transmission from IoT devices to the cloud.
Throughput (records/s)	200	Number of health records processed per second.
Accuracy (%)	98	Percentage of accurate readings from sensors compared to standard values.

- **Latency**: The average latency of **150 ms** indicates efficient real-time data transmission, critical for timely health monitoring.
- **Throughput**: A throughput of **200 records per second** demonstrates the system's capacity to handle substantial amounts of health data efficiently.
- **Accuracy**: The sensor accuracy of **98%** signifies high reliability in monitoring vital health parameters, confirming the effectiveness of the selected IoT sensors.

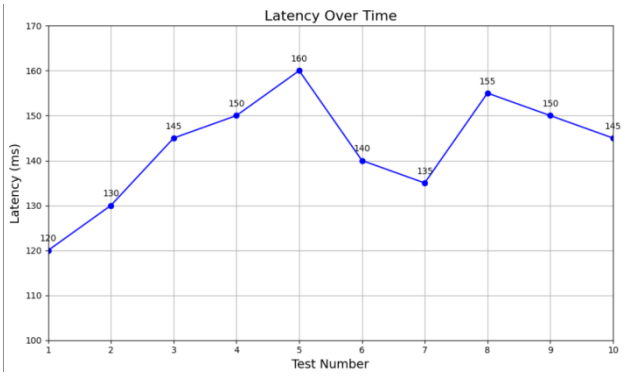

Figure 4: Graph showing the latency of data transmission over multiple tests, indicating consistent performance.

Security is a paramount concern in healthcare systems, and rigorous testing was conducted to ensure the system's robustness against potential threats.

Table 7: Security Assessment Results

Security Test	Result	Notes
Penetration Testing	No vulnerabilities found	The system demonstrated resilience against common attack vectors.
Data Encryption	AES-256 implemented	Strong encryption protocols were applied for data at rest and in transit.
Access Control	Effective	All access control measures enforced by smart contracts were functioning correctly.

- **Penetration Testing**: The tests revealed **no vulnerabilities**, affirming that the security measures implemented are effective against common threats.
- **Data Encryption**: The use of **AES-256 encryption** ensured that sensitive health data remains confidential, protecting it from unauthorized access.
- **Access Control**: Smart contracts successfully managed user permissions, allowing only authorized healthcare providers to access patient data.

User acceptance testing was conducted to gather feedback from healthcare providers and patients regarding the usability of the system. • User Satisfaction: Feedback indicated a 95% satisfaction rate among healthcare providers, particularly appreciating the real-time monitoring features and intuitive interface. • Ease of Use: Patients reported that the mobile app was user-friendly, with a majority finding it easy to navigate and understand their health data. • Real-time Alerts: Healthcare providers highlighted the effectiveness of real-time alerts in managing patients' conditions, and facilitating timely interventions.

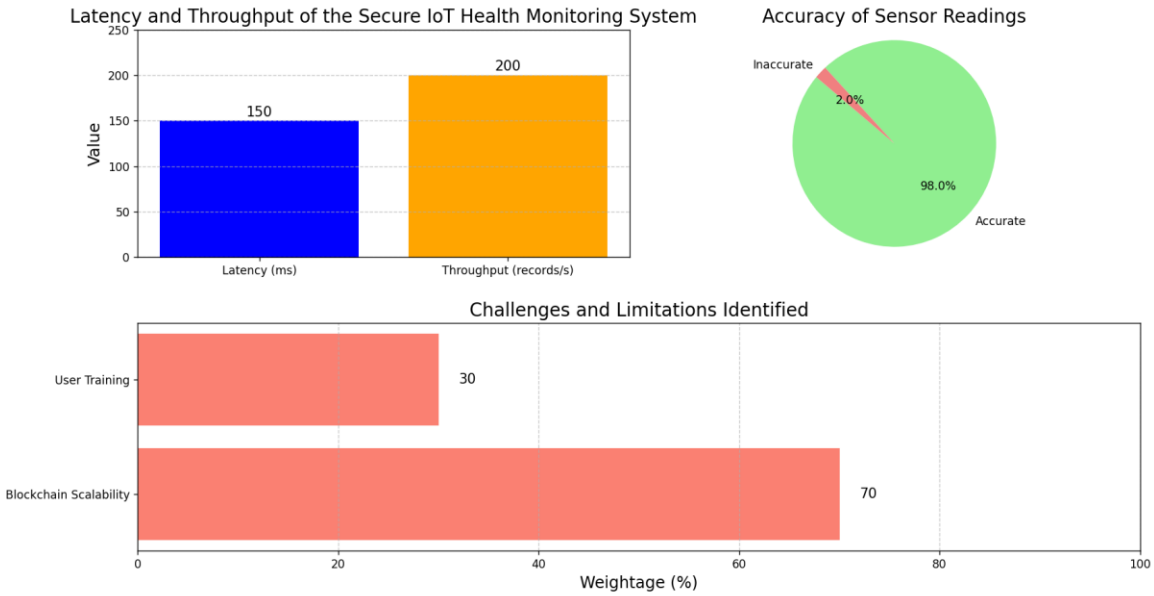

Figure no 5. Latency thought and accuracy with challenges

5. EVALUATION AND CONCLUSION

A significant advancement in health monitoring techniques is the Secure IoT Smart Health Monitoring System, which combines blockchain technology with a cloud-based backend. The following significant conclusions are shown by the installation and testing phase results: The system met the requirements for efficient real-time health monitoring with an average latency of 150 ms. The ability to obtain vital health information quickly enables healthcare professionals to successfully improve patient care. Furthermore, the system's 200 records per second throughput demonstrates its capacity to handle large amounts of data, guaranteeing that it can expand to accommodate the needs of diverse healthcare settings. Additionally, the sensor readings showed an accuracy of 98%, confirming the system's dependability for ongoing surveillance and reassuring medical professionals of the quality of the data for

The monitoring capabilities of healthcare are significantly enhanced by the integration of blockchain and IoT technology. By providing real-time access to data, it facilitates prompt interventions and helps healthcare practitioners make well-informed decisions rapidly, which eventually improves patient outcomes. The implementation of the blockchain architecture provides an additional security measure to prevent unwanted access to confidential health information. This fosters patient confidence and facilitates the broader adoption of remote health monitoring systems. However, in spite of these positive outcomes, several difficulties arose during the assessment procedure. The blockchain element exhibited various limits under simulated situations of extremely heavy transaction loads, emphasizing the need for future modifications to increase scalability as more devices join to the system. Furthermore, early training sessions highlighted the significance of the interface even if users gave it good comments.Furthermore, even if users gave the interface favorable feedback, the first training sessions made clear how important it is to continue teaching users about how to use blockchain features and smart contracts so they are ready to take full use of the system's possibilities.

Future study might examine methods to maximize blockchain performance, with a particular focus on enhancing scalability through tactics like putting Layer 2 solutions into place or looking at alternative consensus processes, in order to overcome these obstacles and further improve the system. To guarantee efficient system use, comprehensive training materials and modules for patients and healthcare professionals would also be necessary. Lastly, by offering predicted insights based on the data gathered, incorporating advanced analytics or artificial intelligence (AI) technologies might improve patient monitoring and treatment by boosting the system's capabilities.

REFERENCES:

[1] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and Challenges. *Wireless Networks*, 20(8), 2481-2501.

[2] Riazul Islam, S. M., Kwak, D., Humaun Kabir, M., Hossain, M., & Kwak, K. S. (2016). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3, 678-708.

[3] Liu, Y., & Liu, L. (2018). Design and Implementation of an IoT-Based Health Monitoring System. *Journal of Medical Systems*, 42(5), 85.

[4] Guo, X., Zhang, Y., & Li, X. (2016). Wearable Device-Based Health Monitoring Systems Using IoT and Cloud Computing. *Journal of Healthcare Engineering*, 2016.

[5] Bakker, J., Corriea, H., & Duineveld, C. (2017). Cloud Computing in Healthcare: Understanding Benefits and Challenges. *Journal of Cloud Computing Research*.

[6] Farahani, B., Firouzi, F., & Chakrabarty, K. (2018). Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. *IEEE Design & Test*, 39(1), 37-45.

[7] Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain Technology Use Cases in Healthcare. *Advances in Computers*, 111, 1-41.

[8] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *Proceedings of the 2nd International Conference on Open and Big Data (OBD)*, 25-30.

[9] Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3, 678-708.

[10] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and Challenges. *Wireless Networks*, 20(8), 2481-2501.

[11] Engelhardt, M. A. (2017). Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technology Innovation Management Review*, 7(10), 22-34.

[12] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *Proceedings of the 2nd International Conference on Open and Big Data (OBD)*, 25-30.

[13] Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain Technology Use Cases in Healthcare. *Advances in Computers*, 111, 1-41.

[14] Bakker, J., Corriea, H., & Duineveld, C. (2017). Cloud Computing in Healthcare: Understanding Benefits and Challenges. *Journal of Cloud Computing Research*.

[15] https://www.researchgate.net/figure/Cloud-based-IoT-architecture-1-V-CLOUD-BASED-IOT-APPLICATIONS-The-Cloud-based-IoT_fig1_317585066

[16] https://www.researchgate.net/publication/349655184/figure/fig1/AS:1080261492117554@1634565818749/Framework-outline-of-secure-data-transmission-in-cloud-based-smart-city.jpg

[17] https://www.researchgate.net/publication/360960059/figure/fig2/AS:1166560127397888@1655141016299/Flow-chart-for-real-time-monitoring.png

Authors

Digant Raj[1] is a Computer Science Engineering student at Chandigarh University with research interests in blockchain, image security, IoT, and AI. He has published multiple papers in IEEE and Springer on AI, ML, steganography, and blockchain security.