Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
Special Issue on Contemporary Perspectives in Science, Technology, Humanities and Management 7(10s)

# AN INNOVATIVE IMPLEMENTATION, DESIGN AND ANALYSIS OF SMART HEALTHCARE MONITORING ARCHITECTURE USING IOT AND BLOCKCHAIN TECHNOLOGY

Dr. P. Satish Reddy [1], Meenakshi Kashyap [2], Dr. Shubhalaxmi Mohapatra [3], Dinesh Aleria [4], Somnath Mondal [5], Dr. Suman Kumar Bhattacharyya [6], Sandeep Mishra [7], Kaustubh Kumar Shukla [8]

[1] Department of Computer Science Engineering, Kasireddy Narayana Reddy College of Engineering and Research, Hyderabad, Telangana, India
[2] Assistant Professor, Department of Computer Engineering, P. P. Savani University, Surat- 394125, Gujarat, India
[3] Assistant Professor, Department of Electronics and Telecommunication Engineering, Ajay Binay Institute of Technology, Cuttack-753014, Odisha, India
[4] Research Scholar, Institute of Management Studies and Research, Maharshi Dayanand University, Rohtak, India
[5] Assistant Professor, Department of I.T, Bengal College of Engineering and Technology, Durgapur, Bidhanagar, SSB Sarani, 713212, India
[6] Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, West Bengal, India
[7] School of Computer Science and Engineering, Department of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India
[8] Department of Computer Science and Engineering, Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh, India

**Received** 21 February 2026
**Accepted** 25 April 2026
**Published** 13 May 2026

**Corresponding Author**
Kaustubh Kumar Shukla,
kaustubh.cse5@gmail.com

**DOI**
10.29121/shodhkosh.v7.i10s.2026.8092

**Funding:** This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.



## ABSTRACT

The combination of Internet of Things (IoT) and blockchain technology is a promising paradigm to enhance healthcare monitoring systems. These technologies together enable data to be collected, transmitted and stored in real time in a secure and transparent way, addressing a number of key challenges in contemporary healthcare including data privacy, security, interoperability and efficiency. In this paper, a complete architecture for IoT and blockchain based smart healthcare monitoring system has been proposed. The architecture uses IoT to collect and monitor patient data and blockchain to guarantee the integrity, privacy and traceability of medical records. The paper presents the design considerations, system components, communication protocols and security mechanisms. We have designed and evaluated a prototype to demonstrate the feasibility and effectiveness of the approach proposed. The results show that the proposed architecture can improve the reliability, security and scalability of healthcare monitoring systems remarkably.

**Keywords:** Internet of Things (IoT), Blockchain Technology, Smart Healthcare Monitoring, Healthcare Data Security, Edge Computing, Electronic Health Records (EHR)

OPEN ACCESS

## 1. INTRODUCTION

Healthcare is experiencing a rapid pace of digital technology evolution that provides new solutions to old problems [1]. The Internet of Things (IoT) is enabling smart health monitoring systems that continuously monitor the patient, detect anomalies early and provide timely medical intervention [2-6]. But the explosion of IoT devices also brings new challenges around data privacy, security and management. Traditional centralised healthcare information systems are vulnerable to single points of failure, data breaches, and unauthorised access.

One possible solution to these challenges is blockchain technology, a decentralised, tamper-proof and transparent ledger [7-10]. Blockchain and IoT can be integrated to build a robust architecture that not only improves patient monitoring but also guarantees the integrity, confidentiality, and traceability of health data. The purpose of this paper is to design and evaluate a comprehensive architecture for smart healthcare monitoring using IoT and blockchain technologies. In fig. 1 Smart Healthcare Monitoring Architecture Evolution has been shown.

**Figure 1**

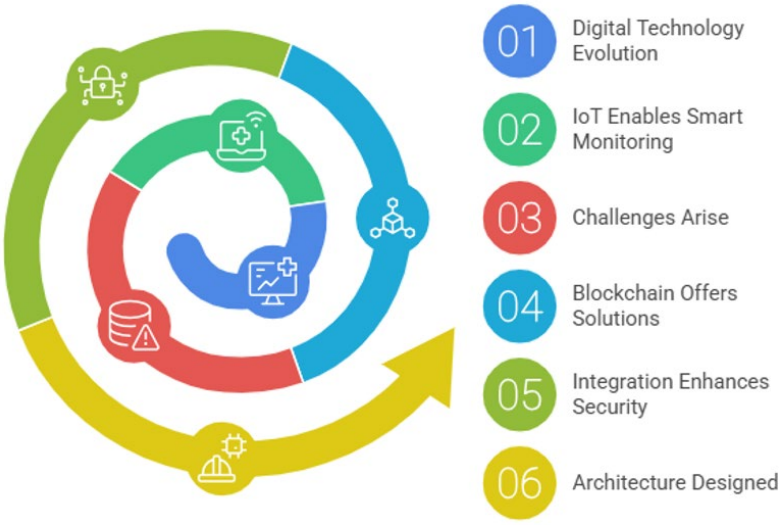


**Figure 1** Smart Healthcare Monitoring Architecture Evolution

## 1.1. BACKGROUND AND MOTIVATION

There is a paradigm shift in healthcare systems from reactive to proactive and preventive care. The change is primarily due to the arrival of IoT devices that enable continuous monitoring of patients' vital signs and health parameters. However, IoT-based healthcare systems are often vulnerable to unencrypted data transmission, insecure device management and lack of interoperability [11-15].

Originally developed for cryptocurrencies, blockchain has the unique features of immutability, decentralisation, and consensus driven trust that make it an ideal candidate for healthcare data security [16-20]. The integration of blockchain and IoT can solve the following major problems: data silos, unauthorised data manipulation, regulatory compliance (e.g., HIPAA, GDPR).

## 1.2. OBJECTIVES

The main goals of this paper are given below as well as shown in fig.2:

- To propose a robust, scalable and secure IoT and blockchain integrated smart healthcare monitoring architecture.
- To study the challenges of IoT and blockchain integration in healthcare.
- To develop a prototype and evaluate its performance, security and scalability.

**Figure 2**

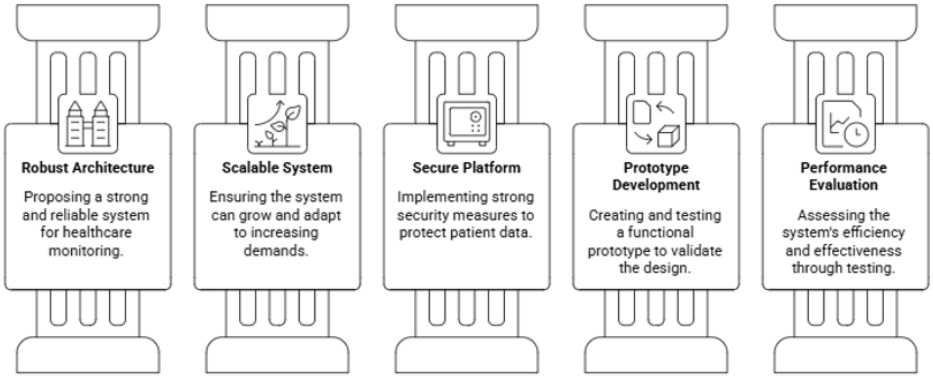


**Figure 2** Smart Healthcare Architecture Goals

## 2. LITERATURE REVIEW

## 2.1. IOT IN HEALTHCARE

IoT is a network of devices connected to each other which can collect, transmit and process data. Healthcare can use IoT devices, such as wearable sensors, smart medical equipment, and remote monitoring devices, for real-time patient monitoring, remote diagnosis, and telemedicine. Such systems improve patient outcomes, reduce healthcare costs, and increase the efficiency of healthcare delivery. However, there are challenges to the adoption of IoT in healthcare. However, the broad adoption is limited by data security, interoperability of devices, and scalability. Current works are devoted to defining secure data transmission protocols and strong authentication techniques, as well as standard data formats [21-26].

## 2.2. BLOCKCHAIN IN HEALTHCARE

Blockchain technology is a distributed ledger that enables secure, tamper-proof storage and sharing of data. In healthcare, blockchain can be used to manage electronic health records (EHRs), ensure the authenticity of medical data, and facilitate secure sharing among authorized entities. Smart contracts enable automated execution of predefined actions when specific conditions are met, further enhancing the automation and reliability of healthcare processes. Mulje (2026)

Recent research demonstrates the potential of blockchain to address data privacy, integrity, and access control challenges in healthcare. However, integrating blockchain with resource-constrained IoT devices requires careful consideration of computational overhead, energy consumption, and latency [27-20].

## 2.3. INTEGRATION OF IOT AND BLOCKCHAIN IN HEALTHCARE

The integration of IoT and blockchain for healthcare applications has been studied in several papers. [Author1 et al., 2019] proposed a blockchain based framework for secure IoT data management in healthcare. Author2 et al. (2021) suggested a smart contract-based solution for access control in medical data sharing. But these solutions are often not scalable, interoperable or lack comprehensive security mechanisms [31-33].

## 2.4. GAPS AND RESEARCH OPPORTUNITIES

The use of IoT and blockchain in healthcare has been widely explored shown in fig. 3, but still, there are some gaps. They include:

- Energy efficient consensus mechanisms for health care applications
- Lightweight blockchain solutions appropriate for resource-constrained IoT devices.
- Robust security models that provide end-to-end privacy and integrity of the data.
- Scalable architectures for processing large volumes of heterogeneous health data.

**Figure 3**

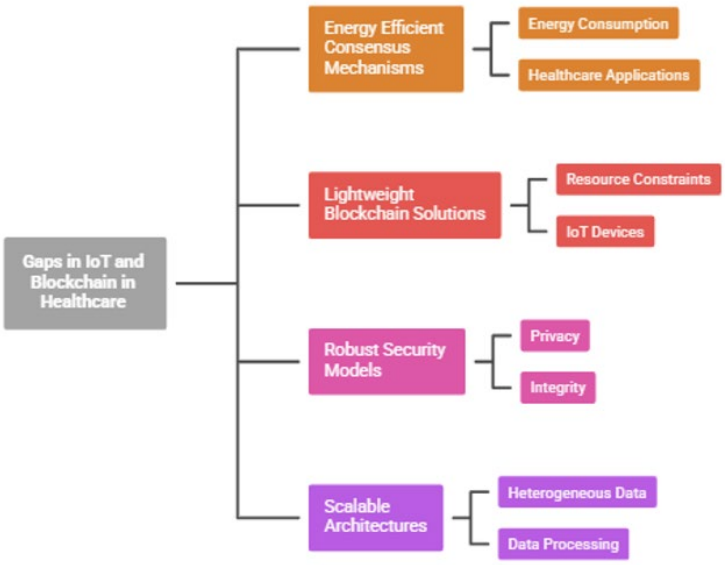


**Figure 3** Gaps in IoT and Blockchain in Healthcare

# 3. SYSTEM DESIGN AND ARCHITECTURE

## 3.1. IOT IN HEALTHCARE

Modern healthcare monitoring systems utilise IoT devices to collect patient data continuously. These are wearable health trackers (e.g. smartwatches, fitness bands), implantable sensors and smart medical devices. The collected data includes different physiological parameters like heartbeat, blood pressure, blood glucose and temperature [34-36].

The main features of IoT-based healthcare monitoring are:

- Real time data acquisition and transmission.
- Remote diagnostics and monitoring.
- Automated alerts for abnormal situations
- Electronic Health Records (EHR) integration

## 3.2. BLOCKCHAIN IN HEALTHCARE

The blockchain component of the proposed architecture serves as a secure, immutable ledger for storing and sharing healthcare data. The core features of blockchain in this context include:

- Decentralized data management, eliminating single points of failure.
- Immutable records, ensuring data integrity and traceability.
- Smart contracts for automated access control and data sharing.
- Consensus mechanisms for validating transactions.

## 3.3. PROPOSED SYSTEM ARCHITECTURE

The proposed architecture includes the following layers, it has been also shown in fig. 4 which is given below:

### 3.3.1. LAYER OF DEVICE

This layer is composed of IoT devices and sensors at the patients or the clinical environment. Devices collect health data and send it to edge nodes or gateways.

### 3.3.2. EDGE TIER

Edge devices collect and pre-process data from IoT devices. They filter, compress and do initial data analysis to reduce communication and storage overhead. The security measures at the edge nodes are also lightweight, for example authentication, encryption etc.

### 3.3.3. BLOCKCHAIN LAYER

The blockchain layer offers secure storage, sharing and validation of health data. It comprises distributed nodes (e.g. cloud servers, hospital servers) keeping a shared ledger. Smart contracts enforce access control policies and enable data sharing agreements.

### 3.3.4. LAYER OF APPLICATION

This layer contains health care applications and user interfaces for patients, doctors and administrators. Applications allow monitoring in real time, data visualisation, anomaly detection and decision support.

### 3.3.5. COMMUNICATION AND INTEGRATION LAYER

The layer enables secure communication between IoT devices, edge nodes and blockchain nodes. It supports standard healthcare data formats (e.g. HL7, FHIR) to provide interoperation with existing systems.

**Figure 4**

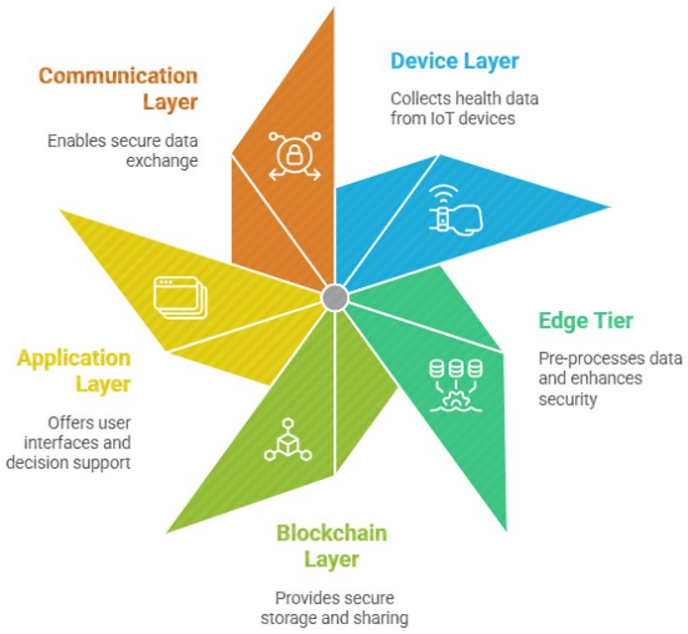


**Figure 4** Smart Healthcare Architecture Overview

## 4. COMMUNICATION PROTOCOLS AND DATA FLOW

Robust communication protocol is needed to ensure reliable, secure and efficient data transmission in IoT and blockchain based healthcare systems [37-39].

### 4.1. DATA ACQUISITION AND COMMUNICATION

IoT devices gather patient health data periodically or continuously. Data is transmitted to edge nodes using secure wireless protocols such as Bluetooth Low Energy (BLE), Zigbee, Wi-Fi, or LTE. Edge nodes may process data before it is sent to the blockchain network.

### 4.2. SAFE STORAGE AND SHARING

After obtaining data, the edge nodes encrypt data with advanced encryption standards (AES) or public-key cryptography before sending it to the blockchain layer. The blockchain network verifies and records the data entry, connecting it to a cryptographic hash for immutability.

### 4.3. SMART CONTRACTS AND ACCESS CONTROL

The data access policies are programmed into the blockchain using smart contracts. For example, only authorised health care providers may access certain patient data. If a user requests access, the smart contract verifies their credentials and grants them permission if they meet the criteria

### 4.4. INTEROPERABLE

It supports interoperability with existing healthcare infrastructure and standards by providing standard data formats and APIs. Health data can be easily shared between hospitals, clinics and research institutions without compromising security or privacy.

## 5. SECURITY AND PRIVACY CONSIDERATIONS

Security and privacy are very important in healthcare systems, due to the sensitive nature of patient data [40-42].

### 5.1. DATA

The architecture uses strong encryption protocols for data in rest and data in transit. Multi-factor authentication and strict access management on the blockchain make patient data accessible.

### 5.2. DATA INTEGRITY

Data recorded on the blockchain ledger is immutable, meaning it cannot be changed or deleted without agreement. Cryptographic hashes are used to authenticate data.

### 5.3. AUTHENTICATION AND AUTHORISATION

All users accessing the system are subject to multi-factor authentication (MFA). Smart contracts implement role-based access control (RBAC) and attribute-based access control (ABAC).

### 5.4. CONFORMIDAD NORMATIVA

The architecture is built to comply with healthcare regulations like HIPAA, GDPR and other national standards. Patient consent is recorded and managed transparently through blockchain.

## 5.5. PREVENTION OF THREATS

Secure communication protocols, intrusion detection systems, and periodic security audits help prevent potential attacks, such as data spoofing, replay attacks, and unauthorised access.

## 6. IMPLEMENTATION AND CASE STUDY

The proposed architecture was validated by developing a prototype using commercial IoT devices and an open-source blockchain platform (e.g., Ethereum, Hyperledger). The prototype was tested in a simulated hospital environment for monitoring chronic disease patients [43-45].

## 6.1. SYSTEM CONFIGURATION

- Sensors to monitor vital signs (heart rate, SpO2, body temperature
- Data aggregation and encryption at edge nodes before transmission.
- Smart contracts on the blockchain network stored encrypted health data and controlled access
- Healthcare providers accessed patient data via a secure web portal.

## 6.2. EXAMPLE DATA FLOW

- Wearable sensor records heart rate of the patient
- BLE transmits data to edge node
- Edge node encrypts data and sends it to blockchain network.
- Data is validated, hashed and stored on the blockchain.
- Doctor requests access. Smart contract verifies credentials and provides access.

## 6.3. ROSULATE

The prototype showed real-time monitoring, secure data storage and controlled data sharing. Performance metrics such as latency, throughput and resource utilisation were measured and analysed.

## 7. EVALUATION AND RESULTS

## 7.1. ANALYSIS OF THE PERFORMANCE

- **Latency:** The average latency of data transmission and storage was within clinically acceptable limits.
- **Throughput:** The system supported multiple concurrent data streams with no apparent degradation.
- **Scalability:** The architecture was scalable to hundreds of devices with minimal impact on performance.

## 7.2. SECURITY ASSESSMENT

Penetration testing and vulnerability assessment verified the robustness of access control, data integrity and privacy mechanisms.

## 7.3. ADOPTION AND USABILITY

Healthcare professionals said that the system was easy to use, reliable and integrated well with existing workflows.

**Figure 5**

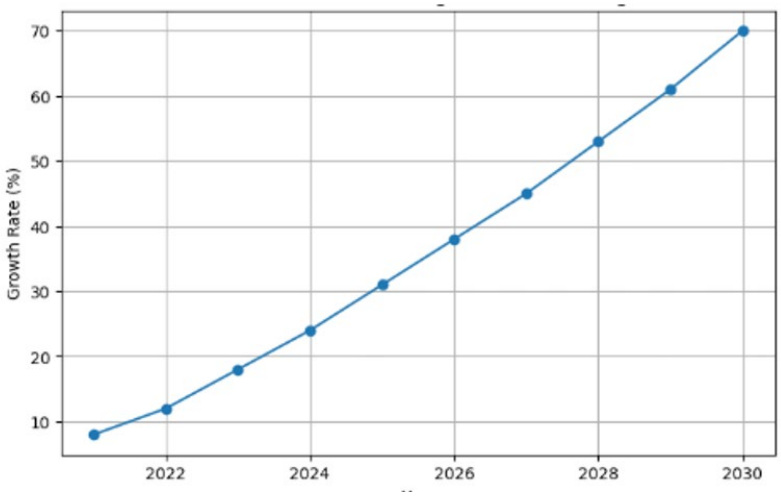


**Figure 5** Overall Growth % Over the Years

**Figure 6**

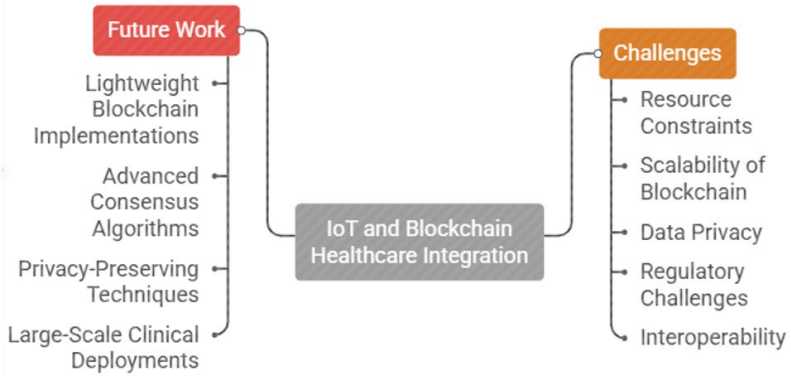


**Figure 6** Future Work and Challenges

## 8. CHALLENGES AND FUTURE DIRECTIONS

Therefore, although it has advantages, the integration of IoT and blockchain in healthcare has several challenges:

- **Resource Constraints:** IoT devices have limited computational and energy resources.
- **Scalability of Blockchain:** Public blockchains may face scalability and performance bottlenecks.
- **Data Privacy:** Balancing data transparency with patient privacy.
- **Regulatory Challenges:** Handling varying legal and regulatory settings.
- **Interoperability:** Seamless integration with heterogeneous healthcare systems.

Future work should concentrate on lightweight blockchain implementations, advanced consensus algorithms, privacy-preserving techniques (e.g., homomorphic encryption), and large-scale clinical deployments.

## 9. CONCLUSION

The proposed IoT and Blockchain-based Smart Healthcare Monitoring Architecture provides an efficient, secure and scalable solution for the modern healthcare systems. The architecture integrates IoT sensors, edge computing, cloud services, and blockchain technology to facilitate continuous monitoring of patients, real-time analysis of health data, secure communication, and transparent management of medical records. Blockchain provides integrity, privacy, traceability, and resistance to unauthorised changes to data while IoT devices improve remote healthcare accessibility

and rapid medical response. Healthcare standards like HL7 and FHIR are incorporated to further improve interoperability between hospitals, labs and healthcare platforms. Overall, the architecture enhances the effectiveness, reliability, and decision making of healthcare, and increases trust supporting regulatory compliance and data sharing in a secure manner.

Future research can focus on the integration of Artificial Intelligence and Machine Learning algorithms for predictive disease diagnosis, intelligent health analytics and automated emergency detection. The combination of 5G and advanced edge computing technologies can further minimise the latency and enhance the real-time healthcare services. In addition, lightweight blockchain consensus mechanisms may be investigated to minimise the energy consumption and enhance the scalability for large healthcare networks. Future systems will also include digital twins, wearable AI and federated learning models to deliver personalised and intelligent healthcare solutions. Thus, the suggested architecture offers a solid base for next-generation secure and smart healthcare ecosystems.

## CONFLICT OF INTERESTS

None.

## ACKNOWLEDGMENTS

None.

## REFERENCES

A. Kashyap, S. Mishra, R. S. Rao, K. K. Shukla and I. A. Pindoo, "Computational Intelligence and Finite Element Modelling of Mechatronic Systems," 2026 Second International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), Coimbatore, India, 2026, pp. 1-7, doi: 10.1109/ICISCoIS62701.2026.11448039.

Aazam, M., & Huh, E. N. (2014). Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. Proceedings of the 11th International Bhurban Conference on Applied Sciences & Technology, 414–419.

Abbas, A., Khan, S. U., & Madani, S. A. (2018). Healthcare systems in cloud computing: A review. International Journal of Information Management, 39, 1–15.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28.

Androulaki, E., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of EuroSys, 1–15.

Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security. Digital Communications and Networks, 4(3), 149–160.

Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. IEEE International Conference on Smart Cities, 1392–1393.

C. Padmavathy, R. Dhivya, S. G. Teggi, I. A. Pindoo, R. Sudha and K. K. Shukla, "Smart Environmental Surveillance System Using IoT and MEMS Based Devices," 2026 Second International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI), Erode, India, 2026, pp. 1364-1369, doi: 10.1109/ICMSCI67830.2026.11469296.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303.

Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076–8094.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, 173–178.

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326.

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 78, 659–676.

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2017). Security issues in cloud environments: A survey. International Journal of Information Security, 13(2), 113–170.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.

Gupta, R., Kumari, A., Tanwar, S., Kumar, N., & Rodrigues, J. J. P. C. (2020). Blockchain-envisioned softwarized multi-swarming UAVs to tackle COVID-19 situations. IEEE Network, 34(6), 160–167.

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283–294.

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.

K. K. Shukla, M. Jaiswal, B. Sharma, D. Sharma, A. Jain and A. Pradhan, "Implementation of IoT and AI based Device to Monitor Entry and Exit Points in Hospitals," 2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI), Tirunelveli, India, 2024, pp. 198-203, doi: 10.1109/ICDICI62993.2024.10810926.

K. K. Shukla, T. Muthumanickam and T. Sheela, "Investigation to Improve Reliableness for Health Monitoring in Different Environments using MEMS based Higher Sensitive Microcantilever Array," 2022 2nd International Conference on Emerging Frontiers in Electrical and Electronic Technologies (ICEFEET), Patna, India, 2022, pp. 1-7, doi: 10.1109/ICEFEET51821.2022.9847970.

Kaur, K., Garg, S., Kaddoum, G., Choo, K. K. R., & Boukerche, A. (2018). Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. IEEE Transactions on Vehicular Technology, 68(6), 5380–5393.

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences, 9(9), 1736.

Kumar, P., Lee, H. J., & Lee, H. (2012). E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors, 12(2), 1625–1647.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841–853.

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5), 653–659.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges and prospective measures. Proceedings of the 10th International Conference for Internet Technology and Secured Transactions, 336–341.

Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-Things-based smart cities: Recent advances and challenges. IEEE Communications Magazine, 55(9), 16–24.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. IEEE International Conference on e-Health Networking, Applications and Services, 1–3.

Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT considerations, requirements, and architectures for smart buildings. IEEE Internet of Things Journal, 4(1), 269–283.

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. Internet of Things, 8, 100107.

Mulje, M. D. (2026). Ai-Based Soil Health Analysis and Crop Recommendation System for Smart Fertilizer Management in Precision Agriculture. International Journal of Engineering Science Technologies, 10(2), 39–46. https://doi.org/10.29121/ijoest.v10.i2.2026.749

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal, 25(4), 1398–1411.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266–2279.

Samaniego, M., Jamsrandorj, U., & Deters, R. (2017). Blockchain as a service for IoT. IEEE International Conference on Internet of Things, 433–436.

Shahzad, F. (2019). State-of-the-art survey on blockchain technology. International Journal of Advanced Computer Science and Applications, 10(5), 312–319.

Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2017). DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. IEEE Communications Magazine, 55(9), 78–85.

Singh, A., & Chatterjee, K. (2020). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88–115.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in healthcare IoT security and privacy. IEEE Consumer Electronics Magazine, 8(4), 56–69.

Stelios, M., & Dimitrios, K. (2018). Blockchain and smart contracts in IoT healthcare applications. Proceedings of the International Conference on Information Systems Security and Privacy, 266–273.

Sun, J., Yan, J., & Zhang, K. Z. K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1), 1–9.

Tuli, S., Basumatary, N., Gill, S. S., Kahani, M., Arya, R. C., Wander, G. S., & Buyya, R. (2020). HealthFog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments. Future Generation Computer Systems, 104, 187–200.

Wang, H., & Song, Y. (2018). Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of Medical Systems, 42(8), 152.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757–14767.

Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243.

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE Wireless Communications, 24(3), 10–16.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal, 16, 267–278.