Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2025, 12(5):29-40**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Blockchain-Based Patient Data Collection: A Case Study in Intensive Care

Djiwa N'tèla OGA[1], *, Pélagie HOUNGUE[1], Cheikh SARR[2]

*[1]Institut de Mathématiques et de Sciences Physiques, Université d'Abomey-Calavi, Dangbo, Bénin
[2]Université Iba Der THIAM, Thiès, Sénégal
*Corresponding Author: djiwa.oga@imsp-uac.org

Abstract: The Internet of Things (IoT) has significantly transformed the healthcare domain, particularly through the development of remote patient monitoring systems. These advances have empowered healthcare professionals to diagnose, monitor, and manage a wide range of health conditions with greater efficiency and precision. However, alongside these innovations, ensuring the security and integrity of sensitive patient data remains a major challenge. In this paper, we propose a secure patient monitoring system specifically designed for intensive care units (ICUs). The proposed architecture integrates blockchain technology to guarantee data security and integrity throughout the monitoring process. The system is structured into three main layers: the data acquisition layer (including sensors and blockchain nodes), the connectivity layer (with a RESTful API), and the mobile application layer. Physicians can securely access the system through multi-factor authentication, monitor patient status in real-time, and receive automated alerts when critical physiological thresholds are reached. This approach provides a reliable and secure framework for remote patient monitoring in highly sensitive healthcare environments.

Keywords: Blockchain, API Rest, Mobile Application, Alerts, Sensors.

1. Introduction

In recent years, the Internet of Things (IoT) has become increasingly integrated into smart healthcare solutions, a trend confirmed by the bibliometric analysis of Djiwa N'tela OGA et al. [1], which highlights the rapid expansion of IoT applications in this sector. This technological integration reached a significant milestone during the COVID-19 pandemic, when remote patient monitoring emerged as a critical necessity in response to global mobility restrictions. In this context, Antonio Iyda Paganelli et al. [2] successfully implemented a system for remotely monitoring COVID-19 patients, both in hospital settings and at home. Similarly, Dev Gupta et al. [3] proposed a health monitoring solution for obese adults, underlining the crucial role of secure data storage and transmission in such systems.

Despite these advances, challenges remain-particularly in Intensive Care Units (ICUs), where inaccuracies or failures in data transmission can have severe, even fatal, consequences. Ensuring the integrity, availability, and confidentiality of patient data is therefore a fundamental requirement in the design of reliable healthcare monitoring systems.

In this study, we address these challenges by proposing a blockchain-based patient monitoring system specifically designed for ICUs. The proposed system ensures the secure storage and exchange of patient data, while maintaining high standards of data integrity, confidentiality, and availability to support critical clinical decision-making.

The main objectives of this research are:

1. to guarantee the confidentiality of patient information,

2. to ensure data integrity for accurate medical assessment,
3. to maintain continuous data availability for healthcare providers.

The remainder of this paper is structured as follows: Section 2 reviews related works, Section 3 outlines the principles and mechanisms of blockchain technology, Section 4 presents the proposed system architecture and its implementation, Section 5 highlights the contributions of the study and its limitations, and Section 6 concludes with perspectives for future research.

2. Related Works

Remote patient monitoring has significantly contributed to reducing mortality rates worldwide, especially in developing countries that face a shortage of healthcare professionals [4]. In remote areas where patients lack access to modern healthcare services, real-time monitoring of their well-being, environment, and treatment is essential [5].

After reviewing several articles, it is evident that the research on blockchain-based embedded patient data collection systems can be classified into several categories, including data security and privacy, system integration with existing healthcare infrastructure, real-time data processing, and the challenges of scalability and interoperability.

B. Swapna et al. [6] conducted a study that demonstrated the effectiveness of continuous patient monitoring, both in clinical settings and at home, using specialized sensors. Similarly, Antonio Iyda Paganelli et al. have implemented a system for remotely monitoring COVID-19 patients, both in hospitals and at home.

A. V. Shaha et al. [7] proposed a system to monitor key health parameters, such as body temperature, blood pressure, and pulse rate. Jabirullah et al. [8] focused on addressing basic healthcare challenges by developing a cost-effective IoT (Internet of Things) architecture to monitor essential medical parameters like heart rate, blood pressure, and body temperature.

P. Rakesh et al [9] presented an IoT- based health system that allows for flexible, remote monitoring of patients using sensors for heart rate, temperature, and vibration, integrated into a microprocessor. While these authors have proposed IoT-based solutions for patient monitoring, many have not fully addressed the critical issue of data security. In contrast, Rupa Ch et al. [3] developed a real-time diagnostic device using blockchain technology to secure and maintain confidentiality of medical data. Further, authors [10] employed blockchain-based deep neural networks for real-time patient health monitoring, using predictive models to assess the risk of brain diseases like Alzheimer's, mild cognitive impairment, and other cognitive disorders.

Nowadays, several innovative applications enable remote medical monitoring of patients, supervised either by doctors or by artificial intelligence platforms. However, these solutions struggle to manage the sharing of medical records between patients and medical centers. Hence the need to propose an approach based on blockchain, smart contracts and Non-Fungible Tokens, NFT, technologies [11]. Research by Bassant Nabil Mohamed et al. enables doctors and the medical sector to make early diagnoses of illnesses in order to improve the overall quality of the healthcare system [12]. Mohammed K. Elghoul et al. [13], for their part, have proposed hyperledger private blockchain technology within Amazon Web Services for secure patient management in the cloud. Md. Shohidul Islam et al. [14], Arijit Saha et al. [15], and Peng Xi et al. [16] have conducted blockchain-based research to solve the problems of risk, leakage and data confidentiality that make it difficult to share medical records while preserving privacy.

The authors [17] have proposed an intelligent and secure healthcare system (ssHealth) based on edge computing and blockchain, enabling the exchange of large quantities of medical data while guaranteeing the confidentiality of patient information. For their part, the authors [18] carried out a study to analyze the application of blockchain technology in the healthcare sector, focusing on its potential to improve the sector's overall performance. They also explored the various challenges and concerns associated with integrating blockchain into the healthcare system.

A blockchain-based electronic health warning system for both critical and non-critical patients has been proposed by [19]. In addition, [20] introduced an attribute-based access control system to enable secure and rapid access to medical data through Next-Generation Access Control technologies (NGAC), blockchain, and smart contracts. Several studies have also explored the use of blockchain for secure, confidential data storage and sharing in smart healthcare environments. Authors [21], [22] argue that the security of a blockchain-based

system can be compromised if malicious actors control more than 51% of the network nodes. To mitigate this, A. E. Guerrero-Sanchez et al. [23] proposed a methodology to enhance data integrity and availability by combining blockchain and cryptographic technics. S. J. Hsiao et al. [24] suggested using blockchain technology to improve data security in wireless sensor networks. Their system, which uses microcontrollers to connect various detection devices, was experimentally validated with over 1,600 data records, showing that the probability of data modification is nearly zero. N. Chendeb et al. [25] proposed a multi-layered architecture combining IoT and blockchain specifically for the healthcare sector. This architecture facilitates interaction between various stakeholders, including physicians, healthcare providers, insurance companies, and pharmacies. R. Thakore et al. [26] discussed how the integration of IoT and blockchain can address the limitations of both technologies, making better use of their combined advantages. However, they also highlighted the issue of blockchain's high energy consumption. Finally, N. Pavlovic' and M. Šarac [27] introduced a method to enhance the security of smart devices by preventing direct internet requests, thus safeguarding them against potential cyber threats. So far, the security of health data collection systems in environments as sensitive as intensive care units is a major challenge.

Although the existing literature has been widely interested in blockchain as a solution to secure health data, few studies have focused on integrating this technology into embedded systems to collect real-time data, particularly in critical settings such as intensive care. Our research work makes a unique contribution by introducing a blockchain-based data collection system for patients admitted to Intensive Care Units (ICUs). This system incorporates enhanced security mechanisms that go beyond traditional solutions. In particular, the combination of blockchain with embedded devices not only ensures the integrity of the data collected by ensuring that it has not been altered, but also preserves the confidentiality of sensitive patient information. Thus, this research not only enriches existing literature by providing an innovative security solution for blockchain-based health data collection systems, but also offers a more robust approach, reliable and adaptable to the specifics of intensive care.

3. Design and Development of the Blockchain-Based Data Security System

Blockchain Technology and its Role in Securing Health Data

Blockchain is a decentralized and distributed digital ledger technology that ensures secure, transparent, and immutable data recording across multiple nodes within a network. Each block contains a set of transactions or data entries, cryptographically linked to the previous block through its hash value, thus forming a tamper-evident chain.

Any attempt to modify a block disrupts the hash sequence, making unauthorized alterations immediately detectable. This intrinsic property of blockchain provides a high level of data integrity and traceability.

In healthcare, blockchain offers significant potential for addressing data security challenges, particularly in environments where the protection of sensitive patient information is paramount. By encrypting medical records and associating them with unique cryptographic identifiers, blockchain-based systems enable controlled access to health data, limited exclusively to authorized entities such as healthcare professionals and patients. This approach promotes a patient-centric model where data ownership and access permissions remain under patient control, while providing a transparent audit trail for any data modifications.

Moreover, blockchain's decentralized nature removes the dependency on centralized authorities, reducing the risks associated with data breaches and single points of failure. These features make blockchain an attractive solution for securing patient data in critical healthcare environments such as Intensive Care Units (ICUs), where data accuracy and availability directly impact clinical outcomes.

Custom Blockchain Development for Real-Time Medical Data Collection

To address the specific needs of real-time patient monitoring in ICUs, we developed a custom blockchain solution tailored to the constraints of embedded systems and medical sensor networks. Unlike general-purpose blockchain platforms (e.g., Ethereum or Hyperledger), which may involve heavy consensus mechanisms and significant computational overhead, our approach focuses on providing a lightweight, efficient, and secure blockchain adapted to healthcare monitoring scenarios.

The blockchain was implemented in Java using the Spring Boot framework and IntelliJ IDE. Its design ensures that patient data collected from embedded medical devices is directly secured through blockchain-based storage, providing immediate data integrity verification.

The core functionalities of the blockchain include:

- Initialization of the blockchain with configurable difficulty settings.
- Creation of the genesis block (the first block in the chain).
- Addition of new blocks containing encrypted patient data.
- Integrity verification across the entire chain to detect any tampering attempts.

The developed blockchain system is based on a sequence of four key operational procedures that ensure the proper initialization, functioning, and integrity of the chain.

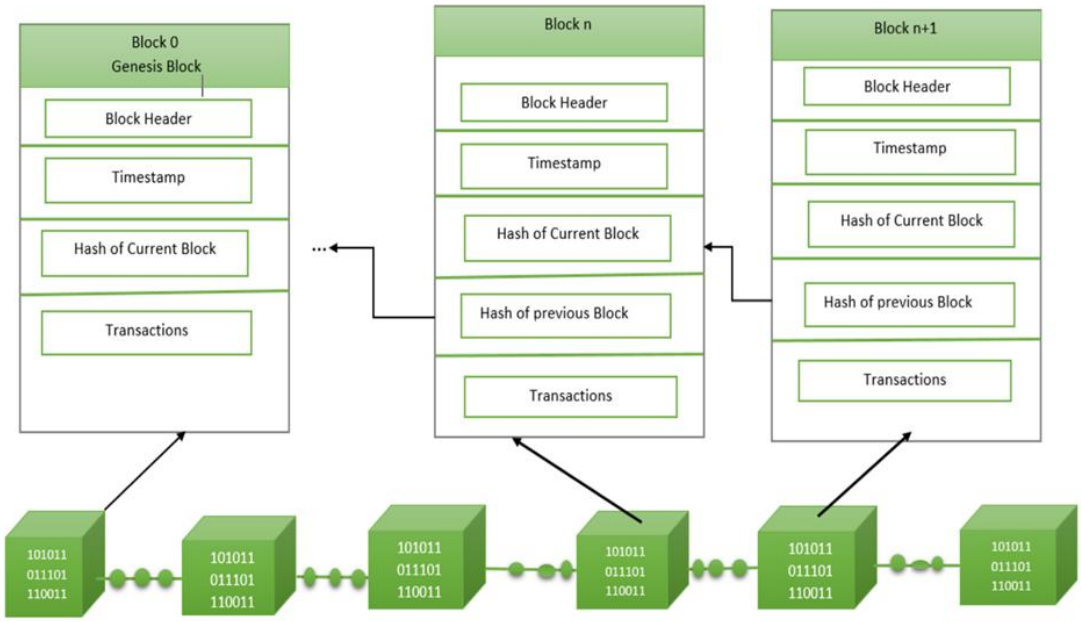

Figure 1: The architecture of a data chain in a blockchain network

The first step, InitializeBlockchain, sets up a new blockchain instance by defining the difficulty level for the mining process and preparing an empty list of blocks. This initialization process immediately triggers the creation of the initial block, known as the genesis block.

The second procedure, CreateInitialBlock, generates this genesis block by assigning it an index of 0, recording the current timestamp, and setting an empty hash since it does not reference any previous block. To ensure its validity, the genesis block undergoes a mining process that respects the defined difficulty constraints, producing a hash that meets the required conditions.

The third operation, AddNewBlock, enables the addition of subsequent blocks containing encrypted patient data. Each new block is assigned an incremented index, a current timestamp, and the hash of the previous block, thereby maintaining the cryptographic link between consecutive blocks. The mining process is again applied to validate each block before its insertion into the chain.

Finally, the VerifyChain procedure ensures the integrity of the entire blockchain by systematically checking each block's hash and verifying that the stored reference to the previous block's hash accurately matches the computed hash of that preceding block. This mechanism detects any attempt to tamper with the data and guarantees the immutability and consistency of the blockchain.

Through these operations, the blockchain system provides a reliable, transparent, and tamper-proof environment for securing patient data collected in real-time from embedded medical devices. The overall architecture of the data chain implemented in this blockchain network is illustrated in Figure 1. This diagram represents the structure of the chain, where each block securely links to the previous one through cryptographic hashes, ensuring data integrity and traceability across the entire system.

This blockchain implementation constitutes the core mechanism for securing patient data. In the next section, we present the proposed architecture that integrates this blockchain system into a comprehensive framework for real-time patient monitoring.

4. Architecture proposal

This section presents the architecture of the embedded system designed for the secure collection of patient data in Intensive Care Units (ICUs) using blockchain technology. The objective of this system is to ensure the confidentiality, integrity, and availability of sensitive medical data from the point of acquisition to the final stage of data consultation by healthcare professionals. The system has been successfully implemented, allowing encrypted patient data to be transmitted to the blockchain and accessed securely by physicians via a mobile application for real-time patient monitoring.

System designs and architecture

The proposed architecture, illustrated in Figure 2, leverages blockchain technology to secure the end-to-end process of data acquisition, transmission, and storage in ICU environments. The architecture is organized around a set of nodes representing individual patient rooms within a healthcare facility. Each room is equipped with a Cluster Head, acting as the local data aggregator and monitoring point for patient physiological signals through embedded sensors.

The Cluster Head integrates various sensors to continuously collect real-time data, including:

• MLX 90614: body temperature sensor.
• XD 58-C: pulse sensor for heart rate monitoring.
• DHT11: ambient temperature and humidity sensor for environmental monitoring.

The data collected from these sensors are aggregated by sink nodes, which function as intermediate units for gathering and forwarding information from multiple patient beds within the ICU. Before transmission, the aggregated data are encrypted using the Advanced Encryption Standard (AES) algorithm to ensure both confidentiality and integrity.

The encrypted data are then transmitted to the blockchain network, where each data entry is securely recorded on an immutable ledger. The use of blockchain guarantees that once the data are registered, they cannot be modified or deleted without detection, thereby providing a transparent and tamper-proof audit trail.

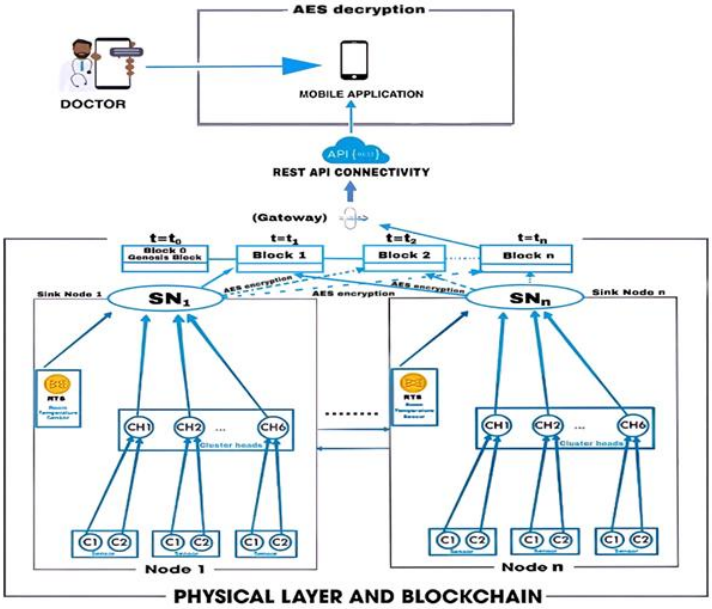

Figure 2: Proposed architecture on blockchain-based healthcare monitoring system

To facilitate access to the collected data, the system employs a RESTful API to transmit the encrypted information to a mobile application developed with Flutter. This mobile interface allows authorized healthcare

professionals to access and visualize patient data securely and conveniently. To reinforce security, the application integrates multi-factor authentication (MFA), ensuring that only verified users can access sensitive health information. Figure 3 illustrates the patient management process.

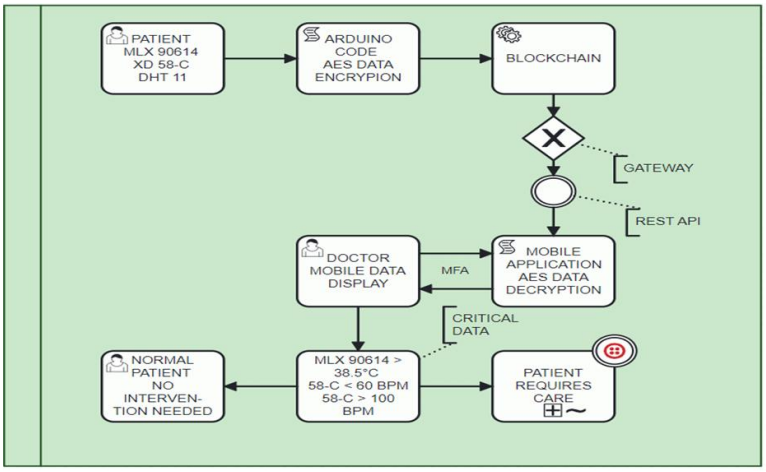

Figure 3: Patient management process schematic

This architecture combines the strengths of blockchain technology, embedded sensor networks, and mobile health applications to offer a comprehensive and secure solution for real-time patient monitoring in critical care settings.

Results & Discussion

The proposed system architecture operates across three key phases:

1. Real-time data acquisition: Patient physiological data, including body temperature, heart rate, ambient temperature, and humidity, are collected directly from the ICU environment using an Arduino-based microcontroller system.

2. Secure data encryption and transmission: Given the resource constraints of IoT medical devices, selecting an efficient encryption algorithm is critical. A comparative analysis of various encryption algorithms was conducted (see Table 1). Based on this evaluation, AES-128 was selected for its optimal balance between high security, low computational overhead, and energy efficiency, making it well-suited for embedded healthcare devices.

3. Data storage and access: Encrypted data are stored on the custom-developed blockchain (backend implemented in Java), where hash integrity is continuously verified. The data are then transmitted to the mobile application (frontend developed in Flutter), decrypted, and made available for consultation by physicians.

Table 1: Comparison of data encryption algorithms

Algorithmes	**RSA**	**DES**	**3DES**	**AES**	**BLOWFISH**
Created by	Ron Rivest, Adi Shamir and Leonard Adleman in 1978	IBM in 1975	IBM in 1977	Vincent Rijmen, Joan Daemen in 2001	Bruce Schneier , 1993
Key Length	Depend on the number of bits in the modulus n where n=p*q	56 bits	56, 112 or 168 bits	128, 192 or 256 bits	32 bits up to 448 bits
Number of Rounds	1	16	48	10-128 bit key, 12-192 bit key, 14- 256 bit key	16

Block size	Variable	64 bits	64 bits	128 bits	64 bits
Cipher type	Asymmetric Block Cipher	Symmetric Block cipher	Symmetric Block cipher	Symmetric Block cipher	Symmetric Block cipher
Speed	Slower Encryption Decryption	Less than AES	Medium	Fast Encryption Decryption less time than DES	Fastest encryption when changing key
Security	Least Secure	Not secure enough	Not secure	Excellent Security	Secure
Power comsumption	Very hight	Low	Very low	Low	Hight

The system also integrates an automated alert mechanism to support clinical decision-making. When patient data reach critical thresholds such as a body temperature above 38.5°C or a heart rate below 60 BPM or above 100 BPM, in accordance with the World Health Organization (WHO) guidelines, the system triggers an immediate notification on the physician's mobile device.

Figure 4: On-board system assembly, data retrieval and display

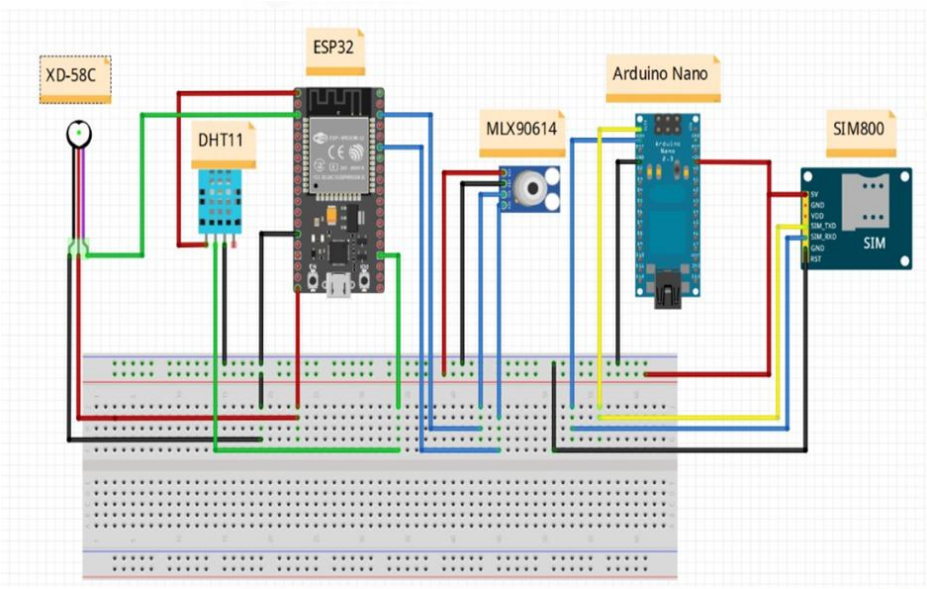

Figure 5: Electronic circuit' wiring

Upon receiving the alert, the physician can access the application directly through the notification to view patient data and take appropriate action. Additionally, the system provides an alert history feature, allowing healthcare providers to review past alerts for enhanced patient follow-up. Alerts can be filtered and displayed by date, with options to view the last five, ten, fifteen, or twenty critical events. Figures 4, 5 and 6 illustrate the on-board system assembly, the electronic circuit' wiring where all the used components are directly connected to the main element, the ESP 32, and the mobile application interface with MFA, respectively.

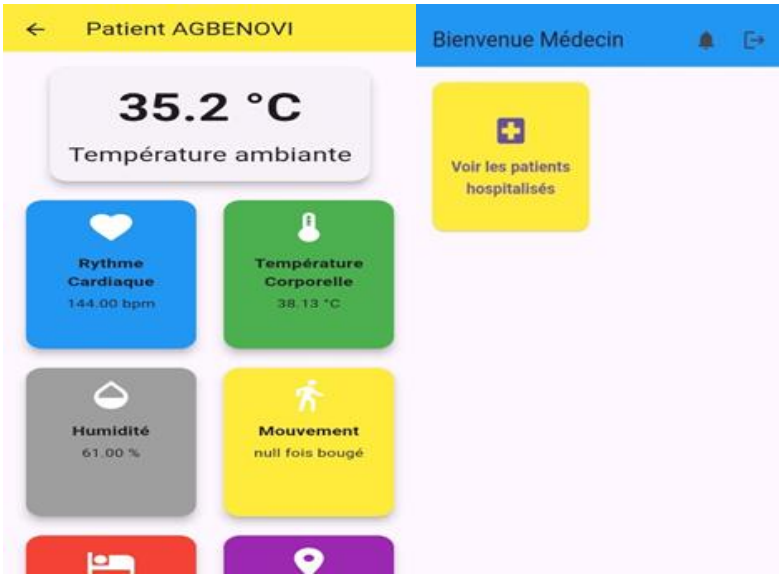

Figure 6: Connection interface with MFA and patient data displays

This system has been tested on embedded models designed for one and two patients, successfully demonstrating the secure collection, encryption, and blockchain-based storage of vital signs data. The custom backend and mobile frontend work seamlessly to provide physicians with real-time access to reliable patient health information.

A comparative analysis with existing blockchain-based healthcare monitoring solutions is presented in Table 2. This comparison highlights the novelty and robustness of the proposed system, particularly its combination of AES-128 encryption, real-time notifications, multi-factor authentication, alert history management, and scalability through microservices architecture, supported by a Byzantine Fault Tolerance (BFT) consensus mechanism and decentralized storage via IPFS.

Table 2: Comparison of Blockchain for Medical Data Management

Paper	Blockchain	AES-128 encryption	Real-time notification	Multi-factor authentification	Alert history	Scalability (Microservices)	Consensus	IPFS (decentralized IPFS storage)	Mining
Dragos Daniel Taralunga et.al [28]	Private Ethereum	✗	✗	✗	✗	✓	✓ PoW/PoS	✓	✗
Oumaima Attia et al [29]	Hyperled-ger Fabric	✗	✓	✗	✓	✓	✓ PBFT	✓	✗
Hafiza Syeda Zainab	Public Ethereum	✗	✓	✗	✓	✗	✓ PoW/PoS	✓	✓

Kazmi and Nadeem Javaid [30]									
MD. ASHRAF UDDIN et al [31]	Customized	✗	✓	✗	✓	✓	✓ PoW	✓	✓
Kusum Yadav et al. [32]	BC-XORECC	✗	✗	✓	✗	✓	✓	✓	✗
Arun Sekar Rajasekaran et al. [33]	Permission-ned	✗	✓	✗	✓	✓	✓ PoV	✓	✗
Ganesan Subramanian And Anand Sreekantan Thampy [34]	diabetes blockchain consortium	✗	✓	✗	✓	✓	✓ PoC	✓	✗
This paper	Hybride (Custom)	✓	✓	✓	✓ (last 5-20 critical events)	✓	✓ BFT	✓	✓

5. Contributions And Limitations

This research has led to the design and implementation of a comprehensive architecture for a blockchain-based healthcare monitoring system, specifically adapted to Intensive Care Units (ICUs). The system integrates biomedical sensors for real-time measurement of vital signs, including body temperature and heart rate, as well as environmental parameters such as humidity and ambient temperature.

A key innovation of this system lies in the early-stage encryption of patient data using the AES-128 algorithm, implemented directly within the Arduino firmware. This approach ensures data confidentiality and integrity from the point of acquisition without overloading the embedded devices. The encrypted data are then transmitted to a custom blockchain-based backend, developed in Java with Spring Boot, which guarantees data immutability and traceability while reducing the risk of fraudulent manipulation.

Access to the collected data is secured through multi-factor authentication (MFA) within a mobile application developed in Flutter. Authorized healthcare professionals can view decrypted patient data in real-time and receive instant notifications when physiological thresholds are exceeded (such as a body temperature above 38.5°C or a heart rate outside the normal range). The application also features an alert history, allowing doctors to review the last five to twenty critical events.

The originality of this work lies in its end-to-end integration of IoT, encryption, blockchain, and mobile technologies, providing a robust, scalable, and secure system for real-time patient monitoring. Table 3 summarizes the main innovations and their impacts.

Table 3: Summary of key innovations

Aspect	Contribution	Impact	Stack Exacte
IoT + AES-128	Secure encryption right from collection, without overloading devices	Protection of sensitive data in compliance with RGPD requirements	Arduino Nano/ESP 32 + lightweight crypto libraries
Blockchain custom	Immutable, transparent backend for a reliable medical history	Preventing data falsification	Intellij, Spring Boot, Immutable storage
Flutter + Notifications	Responsive doctor interface with real-time alerts	Improved response times in emergencies	Flutter Dart, Hive/SQLite for local caching
Scalable modeling	Proof of concept for 1+ patients, adaptable on a larger scale	Potential for extension to entire hospital departments	Micro-services, Docker

Despite these contributions, the system presents several limitations that open avenues for future improvement:

- The current implementation operates locally within a single healthcare facility and does not support inter-hospital collaboration or continuous patient monitoring across different care sites.
- The system focuses on physiological data collection and alerting but does not offer disease detection or diagnosis functionalities. For example, fever may result from various conditions (infectious diseases, inflammatory disorders, autoimmune diseases, endocrine issues, or cancers), and the system does not differentiate between these causes.
- Finally, once the patient is discharged, the system does not allow for continued remote monitoring, limiting its use to in-hospital contexts.

These limitations highlight the need for extending the system's capabilities toward more predictive and collaborative healthcare applications, which are discussed in the following section.

6. Conclusion and Future Work

The system developed in this research represents an innovative approach to real-time patient monitoring in critical care environments such as Intensive Care Units (ICUs). By integrating biomedical sensors, blockchain technology, and secure mobile applications, this architecture enables the continuous collection, encryption, transmission, and visualization of patient data. One of the major strengths of this system is its ability to automatically generate alerts when a patient's physiological parameters exceed critical thresholds, allowing healthcare professionals to respond rapidly and proactively to emergency situations.

The use of AES-128 encryption at the data acquisition level, combined with a custom blockchain-based backend, guarantees the integrity, confidentiality, and traceability of sensitive patient information throughout the data lifecycle. The implementation of multi-factor authentication (MFA) reinforces access control, ensuring that only authorized medical staff can interact with the data. These contributions lay the groundwork for a secure and reliable monitoring framework that could be adapted to various healthcare contexts.

However, as highlighted in the previous section, the current system operates locally and does not support inter-hospital collaboration or post-discharge monitoring. Additionally, while the system effectively detects abnormal physiological conditions, it does not provide diagnostic capabilities to identify the underlying causes of these abnormalities.

In future research, we plan to enhance the system by integrating artificial intelligence (AI) models capable of predicting the onset and progression of metabolic diseases, such as diabetes. This predictive functionality will support early detection of high-risk cases, allowing for individualized treatment plans and improving overall patient outcomes.

Our approach will focus on developing adaptive machine learning algorithms capable of dynamically analyzing patient data streams and refining predictions in real-time. Particular attention will be given to ensuring that these models remain compatible with real-world clinical environments and comply with data privacy regulations.

Additionally, we aim to scale the architecture beyond individual healthcare facilities, facilitating inter-hospital data sharing and collaborative patient monitoring. This will be particularly valuable in regions with limited medical resources, where continuous monitoring can play a crucial role in managing public health challenges and epidemic responses.

Ultimately, this research represents a significant step toward optimizing patient care in intensive care settings through the secure integration of IoT, blockchain, and AI technologies. Our long-term vision is to incorporate these intelligent systems into routine clinical practice, transforming how health data are collected, secured, analyzed, and utilized for better-informed medical decision-making.

References

[1]. D. N. Oga, P. Houngue, et C. Sarr, « IoT-Based Data Security and Protection for Hospital Information Systems: A Knowledge Graph Analysis », in Intelligent Sustainable Systems, A. K. Nagar, D. Singh Jat, D. K. Mishra, et A. Joshi, Éd., Singapore: Springer Nature, 2023, p. 85-95. doi: 10.1007/978-981-19-7663-6_9.

[2]. A. I. Paganelli et al., A conceptual IoT-based early-warning architecture for remote monitoring of COVID-19 patients in wards and at home, Internet Things, vol. 18, p. 100399, 2022.

[3]. R. Ch, G. Srivastava, Y. L. V. Nagasree, A. Ponugumati, et S. Ramachandran, Robust cyber-physical system enabled smart healthcare unit using blockchain technology, Electronics, vol. 11, no 19, p. 3070, 2022.

[4]. M. A. Uddin, A. Stranieri, I. Gondal, et V. Balasubramanian, Continuous patient monitoring with a patient centric agent: A block architecture, IEEE Access, vol. 6, p. 32700-32726, 2018.

[5]. E. Barka, S. Dahmane, C. A. Kerrache, M. Khayat, et F. Sallabi, STHM: A secured and trusted healthcare monitoring architecture using SDN and Blockchain, Electronics, vol. 10, no 15, p. 1787, 2021.

[6]. B. Swapna, S. Gayathri, M. Kamalahasan, H. Hemasundari, M. SiraasGanth, et S. Ranjith, E-healthcare monitoring using internet of things, in IOP Conference Series: Materials Science and Engineering, IOP Publishing, 2020, p. 012024.

[7]. A. V. Shah et P. P. Bhandari, Patient Monitoring using Internet of Things, Int. J. Eng. Res. Technol., vol. 9, no 7, juill. 2020, doi: 10.17577/IJERTV9IS070043.

[8]. M. Jabirullah, R. Ranjan, M. N. A. Baig, et A. K. Vishwakarma, Development of e-health monitoring system for remote rural community of India, in 2020 7th International conference on signal processing and integrated networks (SPIN), IEEE, 2020, p. 767-771.

[9]. P. Rakesh et I. M. Prakash, Raspberry Pi based E–Health System over Internet of Things, in IOP Conference Series: Materials Science and Engineering, IOP Publishing, 2020 p. 042008.

[10]. S. Hannah et al., [Retracted] Blockchain-Based Deep Learning to Process IoT Data Acquisition in Cognitive Data, BioMed Res. Int., vol. 2022, no 1, p. 5038851, janv. 2022, doi: 10.1155/2022/5038851.

[11]. T. L. Quy et al., Decentralized Management of Medical Test Results Utilizing Blockchain, Smart Contracts, and NFTs, Int. J. Adv. Comput. Sci. Appl., vol. 14, no 8, 2023.

[12]. B. N. Mohamed et H. Abdelkader, The Effect of Blockchain using Big data and the Internet of Things in Healthcare, Int. J. Adv. Comput. Sci. Appl., vol. 13, no 12, 2022, Consulté le: 10 mai 2025.

[13]. M. K. Elghoul, S. F. Bahgat, A. S. Hussein, et S. H. Hamad, Securing Patient Medical Records with Blockchain Technology in Cloud-based Healthcare Systems., Int. J. Adv. Comput. Sci. Appl., vol. 14, no 11, 2023.

[14]. M. S. Islam, M. A. B. Ameedeen, H. Ajra, et Z. B. Ismail, Blockchain-enabled Secure Privacy-preserving System for Public Health-center Data », Int. J. Adv. Comput. Sci. Appl., vol. 14, no 5, 2023.

[15]. A. Saha, R. Amin, S. Kunal, S. Vollala, et S. K. Dwivedi, Review on “Blockchain technology based medical healthcare system with privacy issues”, Secur. Priv., vol. 2, no 5, p. e83, sept. 2019, doi: 10.1002/spy2.83.
[16]. P. Xi, X. Zhang, L. Wang, W. Liu, et S. Peng, A review of Blockchain-based secure sharing of healthcare data, Appl. Sci., vol. 12, no 15, p. 7912, 2022.
[17]. A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, et A. Refaey, ssHealth: toward secure, blockchain-enabled healthcare systems », IEEE Netw., vol. 34, no 4, p. 312-319, 2020.
[18]. A. Odeh, I. Keshta, et Q. A. Al-Haija, Analysis of blockchain in the healthcare sector: application and issues, Symmetry, vol. 14, no 9, p. 1760, 2022.
[19]. I. Ahmad, S. Abdullah, et A. Ahmed, IoT-fog-based healthcare 4.0 system using blockchain technology, J. Supercomput., vol. 79, no 4, p. 3999-4020, mars 2023, doi: 10.1007/s11227-022-047887.
[20]. S. Salonikias, M. Khair, T. Mastoras, et I. Mavridis, Blockchain-based access control in a globalized healthcare provisioning ecosystem, Electronics, vol. 11, no 17, p. 2652, 2022.
[21]. P. Bai, S. Kumar, K. Kumar, O. Kaiwartya, M. Mahmud, et J. Lloret, GDPR compliant data storage and sharing in smart healthcare system: a blockchain-based solution, Electronics, vol. 11, no 20, p. 3311, 2022.
[22]. S.-J. Hsiao et W.-T. Sung, Employing blockchain technology to strengthen security of wireless sensor networks, IEEE Access, vol. 9, p. 72326-72341, 2021.
[23]. N. Chendeb, N. Khaled, et N. Agoulmine, Integrating blockchain with iot for a secure healthcare digital system, in 8th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2020), 2020, p. 1-8.
[24]. S.-J. Hsiao et W.-T. Sung, Utilizing blockchain technology to improve WSN security for sensor data transmission, Comput. Mater. Contin., vol. 68, no 2, p. 1899-1918, 2021.
[25]. A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, et A. Takacs, Blockchain mechanism and symmetric encryption in a wireless sensor network, Sensors, vol. 20, no 10, p. 2798, 2020.
[26]. R. Thakore, R. Vaghashiya, C. Patel, et N. Doshi, Blockchain-based IoT: A survey, Procedia Comput. Sci., vol. 155, p. 704-709, 2019.
[27]. N. Pavlović et M. Šarac, Blockchain implementation for IoT devices, Blockchain of Things, 2021.
[28]. D. D. Taralunga et B. C. Florea, A blockchain-enabled framework for mhealth systems, Sensors, vol. 21, no 8, p. 2828, 2021.
[29]. O. Attia, I. Khoufi, A. Laouiti, et C. Adjih, An IoT-blockchain architecture based on hyperledger framework for health care monitoring application, in NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security, IEEE Computer Society, 2019, p. 1-5.
[30]. H. S. Z. Kazmi et N. Javaid, Trusted Remote Patient Monitoring and IoT Devices Authorization using Blockchain-based Smart Contracts.
[31]. M. A. Uddin, A. Stranieri, I. Gondal, et V. Balasubramanian, Continuous patient monitoring with a patient centric agent: A block architecture, IEEE Access, vol. 6, p. 32700-32726, 2018.
[32]. K. Yadav, A. Alharbi, A. Jain, et R. A. Ramadan, An IoT based secure patient health monitoring system, Comput. Mater. Contin., vol. 70, no 2, p. 3637-3652, 2022.
[33]. A. S. Rajasekaran, A. Maria, M. Rajagopal, et J. Lorincz, Blockchain enabled anonymous privacy-preserving authentication scheme for internet of health things, Sensors, vol. 23, no 1, p. 240, 2022.
[34]. G. Subramanian et A. S. Thampy, Implementation of blockchain consortium to prioritize diabetes patients’ healthcare in pandemic situations, Ieee Access, vol. 9, p. 162459-162475, 2021.