Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 21 No. 5 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v21i05.52991

PAPER

Proposed Architecture for Hospital 4.0: Integrating IoT, Edge AI, and Blockchain for Secure and Efficient Healthcare Systems

Azzedine El Mrabet[1](✉), Imam Alihamidi[1], Ayoub Tber[1], Mohamed Benaly[2], Laamari Hlou[2], Rachid El Gouri[1]

[1]Laboratory of Advanced Systems Engineering, Ibn Tofail University, Kenitra, Morocco

[2]Faculty of Sciences, Laboratory of Electronic Systems, Information Processing, Mechanics and Energetics, Ibn Tofail University, Kenitra, Morocco

azzedine.elmrabet@uit.ac.ma

ABSTRACT

The rapid development of various healthcare technologies results in an innovative context known as Hospital 4.0, which integrates Internet of Things (IoT), AI, and blockchain to enhance patient care, optimize operational efficiency, and guarantee robust data security. This paper proposes an innovative layered architecture that can solve some critical problems of healthcare systems: patient identification, real-time data processing, security, scalability, and interoperability. The architecture ensures that it is highly adaptable and accurate by incorporating three IoT-enabled methods of identification, including facial recognition, fingerprint scanning, and NFC/RFID. Advanced AI algorithms process biometric data, enabling real-time insight with privacy guarantees. Blockchain technology enhances security, offering an immutable, decentralized ledger for managing interactions with electronic health records (EHRs). The interoperability of the proposed framework also rests on standards like HL7 FHIR and protocols like MQTT that ensure seamless exchange of data amongst diverse systems. It further explores scalability and regulatory compliance through practical applications, including patient-centric engagement tools and predictive analytics. The architecture puts together dispersed technological innovations in an effort to provide a robust foundation for safe, efficient, patient-centered healthcare delivery and sets the stage for further research into its widespread adoption.

KEYWORDS

Hospital 4.0, Internet of Things (IoT) in healthcare, Edge AI, blockchain in healthcare, AI in healthcare, Hospital 4.0 architecture

1 INTRODUCTION

The most dramatic transformation in modern times is happening in the healthcare sector, which is amalgamating advanced technologies such as Internet of Things (IoT), AI, and blockchain. These are the building blocks of Hospital 4.0, a new

El Mrabet, A., Alihamidi, I., Tber, A., Benaly, M., Hlou, L., El Gouri, R. (2025). Proposed Architecture for Hospital 4.0: Integrating IoT, Edge AI, and Blockchain for Secure and Efficient Healthcare Systems. *International Journal of Online and Biomedical Engineering (iJOE)*, 21(5), pp. 87–102. https://doi.org/10.3991/ijoe.v21i05.52991

Article submitted 2024-10-21. Revision uploaded 2025-01-30. Final acceptance 2025-02-02.

paradigm in transforming healthcare delivery with improved operational efficiency and enhanced patient outcomes. Hospital 4.0 is designed to inspire the principles of Industry 4.0: it is centred on intelligent technologies for improving efficiency and quality across diverse sectors by enabling real-time, data-driven decision-making, automation, and secure communication [1]. Hospital 4.0 is based on the ideas of Industry 4.0, which prioritizes the use of intelligent technologies to improve efficiency and quality across several sectors.

IoT lies at the centre of this transformation, supporting continuous data acquisition through wearables, medical devices, and environmental sensors. Indeed, these devices churn out inordinate quantities of real-time data that let health professionals monitor patients, identify warning signs, and accelerate clinical decision-making. Such a rampant inflow of data brings potential challenges related to processing speed, latency, and security. Technologies such as edge computing and AI provide solutions through the processing of data closer to its source, reducing latency and allowing for real-time insights [2], [3].

Blockchain technology is equally crucial for ensuring data confidentiality, integrity, and transparency in healthcare systems. Its decentralized ledger provides a secure framework for handling sensitive healthcare data, mitigating unauthorized access, and fostering trust among stakeholders. By leveraging blockchain, Hospital 4.0 enhances data security and facilitates compliance with stringent data protection regulations [4], [5], [6].

Despite these advancements, significant hurdles remain in realizing the full potential of Hospital 4.0. A key challenge is achieving interoperability, the seamless communication between diverse systems and devices. Many healthcare facilities continue to operate with a mix of legacy systems and modern technologies, complicating efforts to implement integrated, real-time data processing. Additionally, while IoT and AI exhibit considerable promise, their integration into a unified, scalable, and secure system remains a pressing issue [7]. Guaranteeing secure and effective data handling across IoT devices and platforms continues to be a substantial challenge.

This paper introduces a novel architecture designed to address these challenges by integrating IoT, AI, and blockchain technologies into a cohesive framework. The proposed architecture prioritizes interoperability, enhances data security, and enables real-time, data-driven decision-making, thereby advancing the vision of Hospital 4.0. By presenting a layered, scalable, and secure solution, this work aims to establish a new standard for healthcare delivery, bridging technological gaps and paving the way for more efficient and patient-centred systems.

2 BACKGROUND AND RELATED WORK

The integration of IoT, Edge AI, and blockchain technologies in healthcare has garnered considerable interest in recent years, as it presents viable answers to numerous critical concerns within the industry, including real-time data monitoring, privacy, security, and system interoperability. This section offers a comprehensive examination of these technologies and investigates pertinent research that has established the foundation for the suggested architecture.

2.1 Background

The IoT denotes a network of interlinked devices capable of gathering and exchanging data. In healthcare, IoT technologies like wearables, sensors, and intelligent

medical apparatus have become indispensable for real-time patient health monitoring. These gadgets incessantly produce substantial quantities of health-related data, necessitating quick processing and analysis to facilitate prompt medical actions [8]. The transmission of data from IoT devices across insecure networks poses considerable privacy and security risks, particularly in the healthcare industry.

Edge computing mitigates certain difficulties by relocating data processing nearer to the data-collecting source, hence decreasing latency and alleviating the load on centralized cloud systems [9]. This method facilitates real-time data processing at the network's periphery, which is especially advantageous in healthcare applications where rapid response times are essential. When integrated with AI models, edge computing may execute sophisticated data analytics, including anomaly detection and predictive analytics, directly at the source, therefore improving the system's responsiveness [10].

Blockchain technology has become an essential instrument for safeguarding healthcare data by offering a decentralized, immutable ledger capable of securely storing and validating data transactions. In IoT-based healthcare systems, blockchain fortifies security by obstructing illegal access to sensitive patient information and preserving data integrity across decentralized networks. Moreover, blockchain smart contracts enable secure, automated data sharing, guaranteeing that only authorized individuals can access or alter the information [11].

2.2 Related work

The integration of IoT, Edge AI, and Blockchain technologies in healthcare has garnered considerable interest owing to its capacity to address pivotal difficulties, including real-time data monitoring, security, privacy, and system interoperability. This section offers a thematic summary of current study on these technologies and identifies the deficiencies that the suggested design seeks to rectify.

Edge computing in healthcare. Edge computing has arisen as a remedy to address the constraints of cloud-based architectures, especially in applications where minimal latency and real-time data processing are essential. In healthcare, edge computing facilitates data processing in proximity to the data source (e.g., IoT devices), hence diminishing response time and alleviating the bandwidth strain on centralized systems. Previous research, like the study by [9], has illustrated the advantages of edge intelligence in real-time decision-making in healthcare settings, emphasizing its function in reducing latency and enhancing patient outcomes.

Furthermore, edge computing has demonstrated a reduction in reliance on centralized cloud services, rendering it suitable for healthcare applications that necessitate continuous monitoring and rapid decision-making support. For instance, [12] proposed an edge computing architecture for clinical decision support systems, demonstrating that it can reduce latency by approximately 87 times compared to traditional cloud-based systems, making it highly effective for time-sensitive healthcare scenarios. Nonetheless, as highlighted by [13], numerous edge computing solutions are deficient in strong methods to guarantee data security and privacy, which are essential for managing sensitive patient information in real-time healthcare contexts.

Blockchain for data security and privacy. Blockchain technology has garnered substantial attention in safeguarding healthcare data owing to its decentralized, immutable ledger that guarantees data integrity and confidentiality. In healthcare, where data security is critical, blockchain offers a safe framework for handling

sensitive patient information across IoT networks. For instance, [14] demonstrated how blockchain-enabled privacy-preserving systems can enhance data integrity and protect sensitive healthcare information in IoT networks through distributed applications and smart contracts. Research such as that conducted in [15] extensively examined the possibilities of blockchain in healthcare, highlighting its capacity for traceability, immutability, and improved privacy through smart contracts. These studies demonstrate how blockchain can inhibit unauthorized access and guarantee adherence to regulatory mandates, such as HIPAA.

Notwithstanding its benefits, the scalability of blockchain continues to be an issue, particularly when combined with extensive IoT networks. Researchers such as Samala and [16] have investigated the amalgamation of blockchain technology with cloud infrastructure in EHR systems, showcasing enhanced data security. Nonetheless, they highlighted that blockchain systems frequently encounter issues pertaining to computational inefficiencies and elevated energy usage, especially in extensive healthcare implementations. Subsequent research ought to concentrate on lightweight consensus algorithms, including proof of stake or proof of authority, to mitigate these limitations and enhance the scalability of blockchain-based healthcare systems.

Explainable AI for healthcare decision-making. The use of AI in healthcare, especially Explainable AI (XAI), has been thoroughly investigated to augment decision-making transparency and bolster trust in automated systems. XAI offers healthcare practitioners comprehensible insights into AI-generated judgments, which is particularly vital in emergencies where prompt and precise patient prioritizing is crucial. [17] suggested an architecture that integrates IoT and XAI to enhance triage processes through real-time contextual recommendations. Their research demonstrated that XAI could enhance the interpretability of AI models, enabling healthcare providers to comprehend the rationale behind AI-generated predictions.

Although XAI enhances decision-making openness, it does not comprehensively resolve the overarching issues with data security, privacy, and real-time processing in extensive healthcare systems. Consequently, the integration of XAI with other technologies, such as Edge computing and blockchain, may offer a more holistic solution to the security and performance concerns in healthcare IoT settings.

Middleware for system interoperability. A primary difficulty in healthcare is attaining interoperability among diverse systems and platforms. Middleware solutions are essential for enabling seamless data flow between IoT devices, edge nodes, and healthcare information systems. Research highlights the role of blockchain frameworks in addressing EHR interoperability issues, with standards like HL7 FHIR ensuring the secure exchange of patient data. For instance, [18] proposed a blockchain-based framework for interoperable EHRs that aligns with international standards such as HL7 and HIPAA to enhance data security and usability. Similarly, [19] underscored the potential of blockchain and FHIR to revolutionize EHR interoperability by improving data sharing efficiency and security. Their research underscores the capability of middleware to eliminate data silos, enhance inter-institutional collaboration, and facilitate real-time communication among healthcare practitioners.

Current middleware solutions frequently prioritize data flow and integration while overlooking vital elements such as data security and scalability, which are crucial for extensive healthcare ecosystems. [13] underscored the necessity of middleware protocols like MQTT and HTTP to facilitate efficient and secure data transmission in real-time healthcare applications. Integrating middleware with blockchain and edge AI enables healthcare systems to attain interoperability and security while maintaining scalability.

3 PROPOSED ARCHITECTURE

This section provides a comprehensive description of the planned architecture for Hospital 4.0. This design incorporates advanced technologies including IoT, edge AI, and blockchain to establish a safe, efficient, and scalable healthcare system that tackles the principal difficulties faced by contemporary hospitals. The design comprises five separate layers: IoT data collection, Edge AI for processing, middleware and interoperability, advanced analytics for personalized healthcare, and blockchain-based security. Each layer is engineered to execute a distinct function, facilitating the uninterrupted transmission of data from patient devices to healthcare practitioners while upholding elevated standards of data security, integrity, and real-time processing.

3.1 Overview of the architecture

The architecture is structured as a multi-tiered framework, with each tier accountable for certain facets of data gathering, processing, integration, and security. The framework guarantees the seamless integration of IoT devices utilized in healthcare, including wearables, medical apparatus, and sensors, with AI algorithms for real-time analysis and decision-making support. Simultaneously, the implementation of blockchain technology ensures data integrity and safe access.

The suggested architecture framework for Hospital 4.0 consists of five essential layers: IoT Data Collection, Edge AI for Processing, Middleware & Interoperability, Advanced Analytics & Personalized Healthcare, and Blockchain-Based Security. Every layer is essential for guaranteeing secure, effective, and real-time healthcare administration. Figure 1 illustrates the architectural framework, with a detailed description of each layer provided below.

3.2 IoT data collection layer

The IoT data collection layer constitutes the architectural base, facilitating data acquisition from various medical devices, wearables, and ambient sensors. These devices constitute the initial point of interface with patients, recording real-time health data and other essential indicators. This layer comprises the following essential components:

- Biomedical devices: These encompass wearables, including smartwatches and fitness trackers, that incessantly monitor patient vital parameters (e.g., heart rate, oxygen saturation, and glucose concentrations). These gadgets deliver continuous, real-time data, crucial for monitoring patient health beyond hospital environments.
- Medical equipment: By being seamlessly connected into the IoT framework, hospital-based medical equipment, like MRI machines, ultrasound machines, and CT scanners, can gather and transmit diagnostic data with ease. These machines can produce substantial quantities of data that are promptly analysed at the edge for expedited decision-making.
- Environmental sensors: Sensors utilized in medical environments can assess environmental parameters including temperature, humidity, and air quality. This information is essential for maintaining a safe and supportive environment for patient recovery, especially for those with respiratory ailments.

The data collected by these devices is relayed instantaneously to the subsequent layer of the architecture using secure and encrypted communication protocols. These IoT devices must comply with interoperability standards to provide successful communication with other systems and devices within the hospital.

3.3 Edge AI for processing layer

The edge AI for the processing layer is tasked with processing data gathered from IoT devices at the network's periphery instead of transmitting all raw data to centralized cloud services. This markedly diminishes latency, enhances response speeds, and facilitates real-time decision-making.

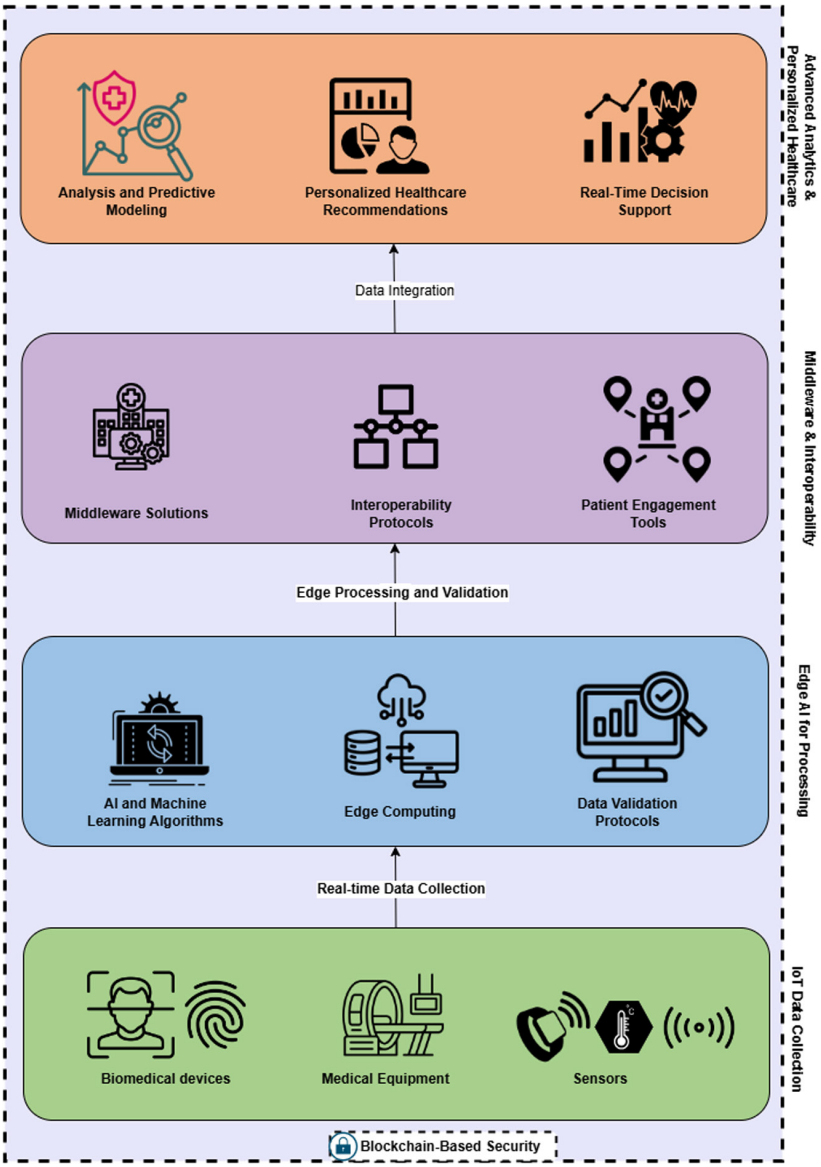

Fig. 1. Proposed architecture for Hospital 4.0 using IoT, Edge AI, Middleware, Advanced Analytics, and blockchain to enhance security and efficiency in healthcare systems

- Edge computing: By processing data nearer to its origin, Edge computing diminishes the necessity of transmitting substantial data volumes to a central cloud,

thereby reducing latency. This is especially critical in time-sensitive healthcare situations, such as intensive care units or emergency departments, where real-time data might be vital for patient survival.

- AI and machine learning algorithms: AI algorithms implemented at the Edge assess incoming data in real time, facilitating the rapid detection of significant health concerns such as irregular heartbeats or abrupt decreases in oxygen levels. These AI models are trained on extensive datasets to guarantee precise predictions and are perpetually updated as further data is acquired.
- Data validation protocols: Prior to processing or transmitting data to subsequent layers, it must be validated to confirm its accuracy and completeness. These protocols ensure data integrity and inhibit the incorporation of erroneous or incomplete data that may impact patient outcomes. A corrupted or incomplete set of patient vitals would be identified and not forwarded for additional processing.

This layer guarantees local data processing, offering healthcare providers prompt insights into patient status while alleviating large computational burdens from centralized systems.

3.4 Middleware and interoperability layer

Middleware is a link between IoT devices, edge computing platforms, and hospital information systems. Middleware facilitates smooth data exchange between systems despite differences in hardware, software, or communication protocols. Middleware standardizes heterogeneous data formats and protocols to provide consistent, accurate data to healthcare professionals. For instance, middleware converts device-specific data into formats that EHR systems can use, making it consistent and reliable.

Middleware solutions. Middleware bridges IoT devices, edge computing platforms, and hospital information systems, ensuring seamless data transfer in systems even with heterogeneous hardware, software, and communication protocols. This layer standardizes diverse data formats and protocols so that healthcare providers can access consistent, accurate information. For example, device-specific data is converted into EHR-friendly formats by middleware for uniformity and reliability.

Interoperability protocols. To ensure secure and efficient data transmission across platforms, this layer employs well-defined interoperability protocols such as HTTP, MQTT, and HL7 FHIR (Fast Healthcare Interoperability Resources). These protocols are crucial for integrating data produced by IoT devices and edge systems into hospital EHRs, enabling real-time access for healthcare providers.

- HL7 and FHIR: This healthcare-specific data standard is widely used for organizing, conveying, and interpreting medical information across various healthcare systems. FHIR ensures that data from different sources (e.g., wearables, medical devices, EHRs) can be seamlessly integrated, promoting uniformity and interoperability.
- MQTT for real-time communication: Message queuing telemetry transport (MQTT) is a lightweight messaging protocol that facilitates real-time communication between IoT devices and hospital systems. It is particularly effective in scenarios where low latency and high reliability are required, such as in emergency care or intensive care units.
- Blockchain Integration: Interoperability protocols like MQTT and HTTP are also integrated with blockchain frameworks to ensure secure data exchange. For example, MQTT can be used to transmit encrypted data from IoT devices

to a blockchain network, where it is stored in an immutable ledger. This combination of protocols and blockchain technology enhances both security and interoperability.

Patient engagement tools. This layer enhances patient-centric care by empowering patients to interact directly with the healthcare system through dedicated tools, such as mobile applications and web portals. These tools enable patients to:

- Access health information: Patients can view their medical records, lab results, and treatment plans in real-time.
- Receive notifications: Patients can receive alerts and reminders for medication schedules, upcoming appointments, or critical health updates.
- Communicate with healthcare providers: Patients can directly communicate with their healthcare providers through secure messaging platforms, reducing the need for in-person visits and improving convenience.
- Data exchange with patients: The middleware layer ensures that patient-generated data (e.g., from wearables or mobile apps) is securely transmitted to hospital systems. This data is then integrated into the patient's EHR, providing healthcare providers with a comprehensive view of the patient's health status.
- Patient-centric care: By enabling patients to access and manage their health information, the middleware layer promotes a more patient-centric approach to healthcare. This not only improves patient satisfaction but also encourages proactive health management.

Interoperability and data integration. The interoperability provided by this layer ensures that data from diverse sources such as IoT devices, edge computing platforms, and external healthcare providers can be integrated into a cohesive system. This allows healthcare providers to make informed decisions based on a holistic view of the patient's health. For example:

- Cross-system data sharing: Data from external healthcare providers (e.g., specialists, labs) can be seamlessly integrated into the hospital's EHR system, ensuring that all relevant information is available to the care team.
- Real-time updates: The middleware layer enables real-time updates to patient records, ensuring that healthcare providers always have access to the most current information. This is particularly important in emergency situations where timely decision-making is critical.

3.5 Advanced analytics and personalized healthcare layer

The advanced Analytics and personalized healthcare layer, positioned at the apex of the data processing hierarchy, transforms raw patient data into actionable insights with sophisticated data analytics and AI models.

- Predictive analytics and machine learning: Using historical and real-time data, predictive analytics algorithms can forecast potential health risks or outcomes. For example, these models can predict the likelihood of a patient being readmitted based on their current health data and past medical history.
- Personalized healthcare recommendations: By utilizing historical and real-time data, predictive analytics algorithms can anticipate prospective health risks

or consequences. These models can forecast the probability of a patient's readmission based on their current health data and historical medical records.
- Real-time decision support: This layer assists healthcare professionals by delivering immediate decision support, facilitating expedited, data-informed decisions. For instance, if a patient's vital signs suggest a possible cardiac arrest, the system can promptly notify the healthcare team and propose emergency measures.

This layer is essential for facilitating proactive and personalized healthcare by utilizing data-driven insights to enhance patient outcomes and optimize resource utilization in hospitals.

3.6 Blockchain-based security layer

The blockchain-based security layer guarantees the integrity, confidentiality, and protection of any data produced and handled by the system. The protection of healthcare data, which is very sensitive, is a paramount concern in the suggested design.

- Data integrity and security: Blockchain technology guarantees the secure storage of patient data in a tamper-proof format. Every transaction or alteration to patient records is recorded in the blockchain, ensuring an unalterable and verifiable account of all data interactions.
- Decentralized trust: By distributing control over data access, blockchain eliminates the necessity for a singular centralized authority, thereby mitigating the danger of data breaches or illegal access. The decentralized architecture of blockchain guarantees data accessibility despite the failure of any one component of the system.
- Privacy and compliance: Blockchain facilitate adherence to regulatory standards like HIPAA and GDPR by offering comprehensive audit trails and guaranteeing that only authorized personnel can access sensitive health information.

This layer ensures optimal security, trust, and transparency in the management of healthcare data, rendering it suitable for protecting patient information within a highly networked framework such as Hospital 4.0.

4 HYPOTHETICAL SCENARIO: APPLICATION OF THE PROPOSED ARCHITECTURE

The section highlights the hypothetical use case for the application of the Hospital 4.0 architecture: granting secure and real-time access to patients' EHRs with the help of IoT, AI, and blockchain.

4.1 Scenario overview

In a health centre that implements the proposed framework, patient identification is among the most critical processes in offering secure access to patients' medical records. Patients can choose facial recognition, fingerprint scanning, or NFC/RFID tapping for identification. These processes are convenient, flexible, error-minimizing, administrative process-streamlining, and patient safety-improving. The workflow (see Figure 2), IoT devices, AI-powered authentication, and blockchain-based data management enable seamless healthcare processes.

4.2 Patient identification through IoT devices

Patients authenticate their identity using IoT-enabled devices, such as facial recognition cameras, fingerprint scanners, or NFC/RFID devices. The collected data is securely transmitted to the hospital's system via encrypted protocols (e.g., MQTT, HTTPS). These devices ensure continuous, automatic, and precise data collection and validation.

4.3 AI-based processing and authentication

AI algorithms validate the patient's biometric or NFC/RFID data by cross-referencing it with existing records in the hospital's EHR system. In case of discrepancies, additional verification methods, such as multi-factor authentication, are employed. This step enhances security and minimizes unauthorized access.

4.4 Secure data access and management with blockchain

Once authenticated, all data interactions, including access, updates, and modifications to EHRs, are recorded on an immutable blockchain ledger. This ensures transparency, accountability, and data integrity while empowering patients to control who accesses their information.

4.5 Real-time data access and updates

Healthcare providers can access real-time updates, such as vital signs from IoT devices (e.g., heart rate or glucose levels), enabling timely and informed clinical decisions. The middleware layer ensures interoperability, integrating data from various sources across departments and external systems.

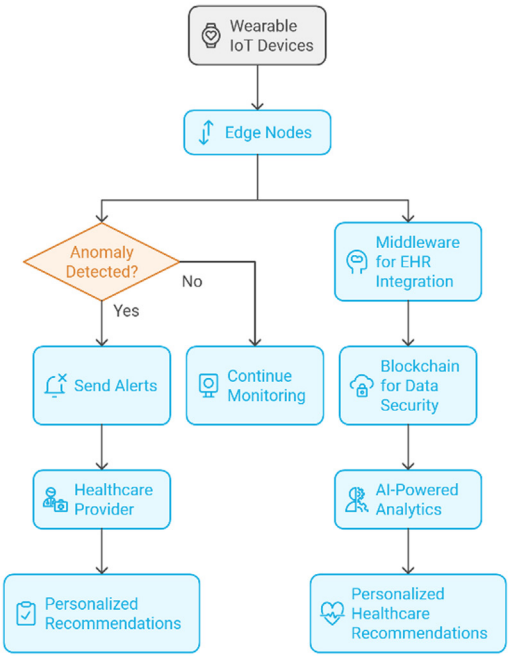

Fig. 2. Workflow for secure patient identification and EHR management

4.6 Outcome of the scenario

- Enhanced security: Secure patient identification and blockchain-ledgered data management reduce the risk of data breaches.
- Improved patient safety: Accurate, real-time identification minimizes errors and optimizes care.
- Efficient data management: Integrated IoT systems provide healthcare providers with immediate access to comprehensive patient records.

This streamlined scenario highlights how the Hospital 4.0 architecture effectively addresses key challenges like data security, scalability, and interoperability while advancing patient-centric care.

5 DISCUSSION

The Hospital 4.0 architecture proposed that combines the use of IoT, AI, and blockchain technologies addresses some of the major healthcare problems of real-time data access, security, scalability, and interoperability. Its contributions, practicability, challenges, and future impact are discussed in detail in this section.

5.1 Enhancing patient identification and data security

A key underlying aspect of this architecture is its patient identification system, which is dynamic and robust. IoT sensors like facial recognition, fingerprint scanners, and NFC/RFID systems offer many secure means of identity verification, thereby minimizing errors and maximizing security measures. These mechanisms allow for smooth fallback methods, which are required to safeguard patients. Studies indicate that biometric verification systems using IoT and AI greatly enhance real-time accuracy and minimize human errors [20].

The application of blockchain technology complements this system with data integrity and transparency in the form of unalterable ledgers that maintain all interactions with EHRs. This creates trust between stakeholders and prohibits unauthorized modifications, which is a key element in the healthcare industry [21], [22].

5.2 Real-time data processing and decision-making

The combination of Edge computing and AI enhances the system's capacity for real-time data processing, a key requirement in time-sensitive applications like emergency care. Edge computing pushes data processing closer to the origin, minimizing latency and facilitating prompt decision-making. AI algorithms provide precise data analysis, leading to improved patient outcomes through timely interventions [9].

However, with the increase in IoT devices within healthcare networks, performance becomes difficult to maintain. Scalability of blockchain in IoT environments necessitates lightweight mechanisms like Proof of Stake consensus or hybrid mechanisms, which allow for stable and efficient performance [16].

5.3 Interoperability with existing systems

Interoperability is a significant hurdle in healthcare technology adoption. Many hospitals operate legacy systems alongside modern platforms, creating barriers to seamless data exchange. The proposed middleware leverages interoperability standards like HL7 FHIR and MQTT to address this issue, ensuring secure and efficient data sharing between heterogeneous systems [23].

Real-world implementations validate the architecture's potential. For instance, the ACTION-EHR system at Stony Brook University Hospital integrates blockchain and HL7 FHIR to enable secure and interoperable EHR sharing [24]. Similarly, HealthChain has demonstrated a 50% reduction in data breaches and a 40% improvement in interoperability [25]. Moreover, IoT and AI-driven systems, such as those used in remote patient monitoring, have reduced hospitalization rates and improved patient outcomes by enabling early interventions through real-time analytics [26].

5.4 Challenges and limitations

Despite its advantages, the architecture faces challenges:

- Regulatory compliance: Adhering to regulations like HIPAA and GDPR is essential. Blockchain supports compliance by providing transparent audit trails and restricting data access to authorized personnel [27].
- Implementation costs: The integration of IoT, AI, and blockchain technologies requires significant investment in infrastructure, training, and maintenance, which may deter smaller providers. For example, while the financial costs of blockchain and IoT implementation in healthcare are often broadly acknowledged, detailed and specific cost analysis remains scarce in the literature. Broader studies highlight the general resource-intensive nature of these technologies, including high initial setup costs for blockchain deployment and ongoing operational expenses for IoT maintenance [27], [28].
- Scalability: The volume of IoT-generated data increases as hospital networks grows, complicating real-time processing. Solutions such as off-chain processing and hybrid architectures mitigate these issues [28].

5.5 Future research and development

The subsequent phase of this study will concentrate on the execution of the proposed architecture, particularly in the context of patient identification for accessing EHRs. The implementation will showcase the comprehensive integration of IoT, AI, and blockchain technologies inside a practical hospital environment, evaluating the architecture's scalability, security, and interoperability.

This phase will yield critical data on the architecture's performance under realistic restrictions, serving as a framework for broader implementation in hospital environments and establishing a basis for future investigations into further applications of IoT, AI, and blockchain in healthcare.

6 CONCLUSION

The proposed Hospital 4.0 architecture integrates IoT, AI, and blockchain technologies to address key challenges in healthcare, including real-time data access, patient identification, data security, scalability, and interoperability. This multi-layered approach enables secure and efficient data transmission, enhances patient safety, and supports real-time clinical decision-making by utilizing cutting-edge technologies.

The architecture's adaptability in patient identification methods such as facial recognition, fingerprint scanning, and NFC/RFID ensures reliability across diverse healthcare environments. AI and edge computing facilitate swift data processing at the source, reducing latency and enabling immediate decision-making in critical scenarios. Blockchain technology further strengthens data security by creating an immutable, decentralized ledger that safeguards patient records and ensures transparency and accountability.

While this architecture demonstrates significant potential, challenges such as scalability, integration with legacy systems, and regulatory compliance remain. Addressing these barriers requires focused efforts, such as exploring lightweight blockchain consensus mechanisms, developing middleware solutions to enhance interoperability, and collaborating with regulatory bodies to ensure adherence to standards like HIPAA and GDPR. Pilot studies and prototype implementations can serve as critical steps to evaluate the architecture's performance and adaptability in real-world healthcare environments.

Future research should prioritize optimizing blockchain scalability and improving middleware integration to enable seamless data exchange among heterogeneous systems. Cost-effective deployment strategies must also be explored to make this architecture accessible to smaller healthcare providers, fostering widespread adoption.

In conclusion, the Hospital 4.0 architecture offers a transformative approach to addressing the increasing demands of modern healthcare systems. By leveraging IoT, AI, and blockchain technologies, this framework lays the foundation for secure, efficient, and patient-centric care. The forthcoming implementation phase will provide valuable insights, enabling broader applications of these technologies and advancing the future of healthcare globally.

7 REFERENCES

[1] A. Abatal, M. Mzili, T. Mzili, K. Cherrat, A. Yassine, and L. Abualigah, "Intelligent interconnected healthcare system: Integrating IoT and Big Data for personalized patient care," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 11, pp. 46–65, 2024. https://doi.org/10.3991/ijoe.v20i11.49893

[2] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A novel smart healthcare design, simulation, and implementation using Healthcare 4.0 processes," *IEEE Access*, vol. 8, pp. 118433–118471, 2020. https://doi.org/10.1109/ACCESS.2020.3004790

[3] I. Alihamidi, A. Deroussi, A. Addaim, and A. A. Madi, "Revolutionizing healthcare: Convergence of IoT and open-source ERP systems in health information management," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 9, pp. 83–98, 2024. https://doi.org/10.3991/ijoe.v20i09.48805

[4] T. Alam and M. Benaida, "Internet of Things and blockchain-based framework for coronavirus (COVID-19) disease," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 6, pp. 82–94, 2022. https://doi.org/10.3991/ijoe.v18i06.29919

[5] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, emerging technologies, and case studies," *IETE Technical Review*, vol. 39, no. 4, pp. 775–788, 2022. https://doi.org/10.1080/02564602.2021.1927863

[6] F. Xie, D. Chen, B. Qin, C. Fu, and S. Chen, "The complete mitochondrial genome of white-tailed mole (Parascaptor leucura)," *Mitochondrial DNA Part B*, vol. 6, no. 3, pp. 1112–1113, 2021. https://doi.org/10.1080/23802359.2021.1899871

[7] A. F. Abbas, N. A. Qureshi, N. Khan, R. Chandio, and J. Ali, "The blockchain technologies in healthcare: Prospects, obstacles, and future recommendations; lessons learned from digitalization," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 9, pp. 144–159, 2022. https://doi.org/10.3991/ijoe.v18i09.32253

[8] P. P. Ray, Di. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases," *IEEE Syst. J.*, vol. 15, no. 1, pp. 85–94, 2021. https://doi.org/10.1109/JSYST.2020.2963840

[9] V. Hayyolalam, M. Aloqaily, O. Ozkasap, and M. Guizani, "Edge intelligence for empowering IoT-based healthcare systems," *IEEE Wirel. Commun.*, vol. 28, no. 3, pp. 6–14, 2021. https://doi.org/10.1109/MWC.001.2000345

[10] S. H. Akundi, R. Soujanya, and P. M. Madhuri, "Big data analytics in healthcare using machine learning algorithms: A comparative study," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 16, no. 13, pp. 19–32, 2020. https://doi.org/10.3991/ijoe.v16i13.18609

[11] B. Ren, L. T. Yang, Q. Zhang, J. Feng, and X. Nie, "Blockchain-powered tensor meta-learning-driven intelligent healthcare system with IoT assistance," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2503–2513, 2023. https://doi.org/10.1109/TNSE.2022.3227317

[12] R. H. Kumar and B. Rajaram, "Design and simulation of an edge compute architecture for IoT-based clinical decision support system," *IEEE Access*, vol. 12, pp. 45456–45474, 2024. https://doi.org/10.1109/ACCESS.2024.3380906

[13] L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, and M. Vento, "Trends in IoT based solutions for health care: Moving AI to the edge," *Pattern Recognit. Lett.*, vol. 135, pp. 346–353, 2020. https://doi.org/10.1016/j.patrec.2020.05.016

[14] P. Sharma, S. Namasudra, N. Chilamkurti, B. G. Kim, and R. Gonzalez Crespo, "Blockchain-based privacy preservation for IoT-enabled healthcare system," *ACM Trans. Sens. Netw.*, vol. 19, no. 3, pp. 1–7, 2023. https://doi.org/10.1145/3577926

[15] V. Rattanawiboomsom, M. S. Korejo, J. Ali, and U. Thatsaringkharnsakun, "Blockchain-enabled Internet of Things (IoT) applications in healthcare: A systematic review of current trends and future opportunities," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 19, no. 10, pp. 99–117, 2023. https://doi.org/10.3991/ijoe.v19i10.41399

[16] A. D. Samala and S. Rawas, "Transforming healthcare data management: A blockchain-based Cloud EHR system for enhanced security and interoperability," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 2, pp. 46–60, 2024. https://doi.org/10.3991/ijoe.v20i02.45693

[17] O. Stitini, F. Ouakasse, S. Rakrak, S. Kaloun, and O. Bencharef, "Combining IoMT and XAI for enhanced triage optimization: An MQTT broker approach with contextual recommendations for improved patient priority management in healthcare," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 7, pp. 145–162, 2024. https://doi.org/10.3991/ijoe.v20i07.47483

[18] F. A. Reegu *et al.*, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability*, vol. 15, no. 8, p. 6337, 2023. https://doi.org/10.3390/su15086337

[19] G. Anand and D. Sadhna, "Electronic health record interoperability using FHIR and blockchain: A bibliometric analysis and future perspective," *Perspect. Clin. Res.*, vol. 14, no. 4, pp. 161–166, 2023. https://doi.org/10.4103/picr.picr_272_22

[20] M. Elhoseny, K. Haseeb, A. A. Shah, I. Ahmad, Z. Jan, and M. I. Alghamdi, "IoT solution for AI-enabled privacy-preserving with Big Data transferring: An application for healthcare using blockchain," *Energies*, vol. 14, no. 17, p. 5364, 2021. https://doi.org/10.3390/en14175364

[21] V. Bidve, K. Kakade, P. Sarasu, S. Kediya, P. Tamkhade, and S. S. Nair, "Patient data management using blockchain technology," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 3, pp. 1746–1754, 2023. https://doi.org/10.11591/ijeecs.v32.i3.pp1746-1754

[22] A. Adavoudi Jolfaei, S. F. Aghili, and D. Singelee, "A survey on blockchain-based IoMT systems: Towards scalability," *IEEE Access*, vol. 9, pp. 148948–148975, 2021. https://doi.org/10.1109/ACCESS.2021.3117662

[23] D. Mauricio *et al.*, "Electronic health record interoperability system in peru using blockchain," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 3, pp. 136–153, 2024. https://doi.org/10.3991/ijoe.v20i03.44507

[24] A. Dubovitskaya *et al.*, "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *J. Med. Internet Res.*, vol. 22, no. 8, p. e13598, 2020. https://doi.org/10.2196/13598

[25] G. Husnain *et al.*, "HealthChain: A blockchain-based framework for secure and interoperable electronic health records (EHRs)," *IET Communications*, vol. 18, no. 19, pp. 1451–1473, 2024. https://doi.org/10.1049/cmu2.12839

[26] S. Chintala, "Iot and Ai Synergy: Remote patient monitoring for improved healthcare," in *4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 2024, pp. 1–6. https://doi.org/10.1109/ICIPTM59628.2024.10563530

[27] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," *Sustainability*, vol. 12, no. 17, p. 6960, 2020. https://doi.org/10.3390/su12176960

[28] A. H. Mayer, V. F. Rodrigues, C. A. Da Costa, R. Da Rosa Righi, A. Roehrs, and R. S. Antunes, "FogChain: A fog computing architecture integrating blockchain and internet of things for personal health records," *IEEE Access*, vol. 9, pp. 122723–122737, 2021. https://doi.org/10.1109/ACCESS.2021.3109822

8 AUTHORS

Azzedine El Mrabet is a PhD student and an associate member of the Advanced Systems Engineering Laboratory at ENSA, Ibn Tofail University, Morocco. His research explores the intersection of AI, IoT, and blockchain in healthcare, with a strong focus on improving quality of life through ICT. He is particularly interested in TinyML and IoT for embedded systems, driving innovation in healthcare, security, and advanced systems engineering (E-mail: azzedine.elmrabet@uit.ac.ma).

Imam Alihamidi holds a Ph.D. in Computer Science and Telecommunications and is a Research Professor at EMSI. As a member of the Advanced Systems Engineering Laboratory and SMARTiLab, he actively contributes to research on emerging technologies. He is also a consultant specializing in IoT, cyber-physical systems, and AI, with a focus on applying ICT to healthcare, particularly IoT and

blockchain integration in smart hospitals. He graduated as a State Engineer in Networks and Telecommunications (ENSA Kenitra, 2018) and earned his Ph.D. at Ibn Tofail University, where he also lectured. He has held leadership roles in scientific associations and helped organize international conferences. Beyond academia, he consults on Industry 4.0 and cloud infrastructure, with expertise in cybersecurity, IoT architectures, and healthcare information systems (E-mail: i.alihamidi@emsi.ma).

Ayoub Tber is a PhD student and associate member of the Advanced Systems Engineering Laboratory ENSA, Ibn Tofail University, Morocco. Throughout my career, I have developed solid expertise in the information systems engineering. Specifically, on various projects that focused on machine and deep learning models, building and deploying ML models to solve complex problems. My interests include AI, IoT(Internet of Things), embedded and Blockchain, especially in the context of intelligent systems, healthcare, and security (E-mail: ayoub.tber@uit.ac.ma).

Mohamed Benaly is a PhD student specializing in exploiting high-performance embedded systems in Unmanned Aerial Vehicles (UAVs) at the Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco. With a strong academic foundation that includes a Master of Science in Embedded Systems and a Bachelor of Science in Electronics and Telecommunications Systems, their research focuses on optimizing embedded architectures to enhance UAV performance (E-mail: mohamed.benaly@uit.ac.ma).

Laamari Hlou is a Professor at the Faculty of Science, Ibn Tofail University, Kenitra Morocco. His research interests in Electrical Engineering and renewable energy include the modelling and design optimization of renewable energy systems, the development of microelectronic energy management systems and power electronic converters for renewable energy sources applications, and the development of sensors and electronic measurement systems and information security (E-mail: hloul@yahoo.com).

Rachid El Gouri serves as Professor in the National School of Applied Sciences at Ibn Tofail University in Kenitra – Morocco (ENSAK), Director of the Doctoral Studies Center at ENSA in Kenitra. His research interests in Electrical Engineering and Renewable Energy include the modelling and design optimization of Renewable Energy systems, the development of microelectronic Energy Management Systems and power electronic converters for Renewable Energy Sources applications and the development of sensors and electronic measurement systems and information security (E-mail: elgouri.rachid@yahoo.fr).