Security aspects related Intelligent e-Health Systems

Hamza Rafik[1*], *Abdelaziz* Ettaoufik[2], and *Abderrahim* Maizate[1]

[1] RITM- ESTC/CED -ENSEM Hassan II University Casablanca, Morocco
[2] LTIM - FS Ben M'SIK Hassan II University Casablanca, Morocco

Abstract. Current health situations and crises require physicians and researchers to convert traditional healthcare services to a new generation of digital healthcare known as e-health smart systems that operate close to the end user with the objective to provide medical assistance using advanced technologies including Internet of Medical Things technology, edge computing, and cloud computing paradigms. However, this system architecture reveals limitations in terms of latency, bandwidth, power consumption as well as security and privacy of collected data. Through this paper, a presentation of different healthcare monitoring system layers has been defined, in addition to listed challenges faced by the deployment of this technology, while providing an introduction of security risks that threaten the user data safety alongside the e-health layers. Moreover, a summarized discussion of Blockchain technology came over to provide a secure decentralized architecture in sharing data across allowed entities.

1 Introduction

Today Healthcare plays a crucial role in human life, especially with the rise evolution of chronic and viral diseases that spread in worldwide level, as well as the healthcare landscape is facing the dual challenge of increased demand for hospital beds and staff shortages [1] which need continuous monitoring of medical records over time with health specialist alongside with intelligent mechanisms that provide recent smart technologies in favor of keeping control healthcare monitored in different kind of health world crises. Healthcare monitoring systems based on IoT, and edge computing technologies known as e-health smart systems become a priority in this time period, due to the various use cases that can support including Real-time health monitoring, Emergency management systems, Health-aware mobile devices, and Health care information spreading [2].

The healthcare industry is undergoing a major shift towards digitalization as new technologies and platforms emerge to create a new framework for healthcare operations. Healthcare is a fundamental human need and generates billions of dollars in revenue. In 2022, digital healthcare investment in the US and Europe exceed $22 billion [3]. The healthcare industry in the US has been growing up by 2.7% in 2021, reaching $4.3 trillion [4], which exposed the interest and importance of this sector.

* Corresponding author: hamza.rafik-etu@etu.univh2c.ma

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

Therefore, the main implementation of e-health smart systems is dependable on three major tiers including the end user layer, the edge layer, and the cloud layer as seen from **figure 1** below, where each layer has a specific role in the global system architecture, however, this technology led to significant difficulties regarding high-latency, Energy Efficiency, Quality of service (QoS), Cost, storage and computing resources, location awareness, and Low-level Security/Privacy of manipulated data [2]. However, creating reliable, adaptable, and secured healthcare system-based edge computing using recent technologies has become a priority to address these challenges.

Securing collected medical data over e-health smart systems gain considerable attention from multiple researchers due to the type and volume of gathered data by these systems, in addition, to get contacted by many external contributors such as caregivers, doctors, Emergency departments, and the target patients, which categorize the e-Health systems as a compact network of monitoring and sharing medical data and information within various conditions. While the fact of protecting this data requires the deployment of recent technologies such as the Blockchain Network which is considered as an evolutionary technology that enables secure data transactions, and efficient storage capability based on distributed databases [5], while it can improve patient care, optimize data management, increase compliance, and facilitating efficient management of healthcare-related data flow.

The objective of this paper is to provide an overview of the deployment of modern technologies to address the security challenges revealed by healthcare monitoring systems such as the blockchain with its variants applications, the paper sections uncover a presentation of different e-health system layers including different security cyber-attacks risks threaten this architecture and recommended measures related CIA triad [6] to handle occurred challenges in a different layer. Additionally, an introduction of blockchain technology and its mechanism of deployment as well as some related works exposed the benefits of this technology in a healthcare environment.

In the following sections of this paper, several key points will be discussed in detail as the following parts:

- Presentation of e-Health smart system main architecture.
- Discussion of security challenges related to the e-health system according to the CIA Triad model.
- Introduction of Blockchain Technology to address exchanging medical data security limitations.

2 E-Health Smart System Architecture

2.1 Overview of e-health smart systems

Smart systems-related e-health services refer to the use of advanced technologies and techniques, such as Artificial Intelligence (AI), Big Data analytics, the Internet of Things, and edge computing to enhance medical services delivery. These systems models are designed to make healthcare more reliable and effective for different contexts including:

- Telemedicine: enable remote healthcare monitoring by healthcare providers through different system's communication capabilities
- Predictive analytics: Using AI algorithms with the objective of analysing patient medical records and providing predicted health future consequences, particularly for patients with chronic conditions.
- EHR management: Appears as a collected digital record containing relevant patient information and diagnosis metrics accessible to healthcare providers enabling them to collaborate on patient care.

These Systems enable real-time data collection, analysis, and sharing among various stakeholders. Designed to help reduce healthcare deployment costs, enhance patients' health delivery, and improve the overall experience. In addition to empower collaboration between healthcare providers, health organizations, and patients.

2.2 Related works

The healthcare field has seen significant advancement in recent years, particularly with the introduction of e-health smart systems that aim to digitalize the whole sector for better service experiences. Leveraging advanced technologies such as IoMT, AI, edge, and cloud computing have revolutionized healthcare delivery and management. However, the authors in [7] presented a user-friendly system designed to offer health services for elderly and disabled at home. Liang et al [8] proposed an effective system model integrating physiological sensors, transmission components, and processing capabilities that provide continuous health monitoring. Pap et al in their work [9] proposed an implementation of e-health system based IoT technology offering local and remote monitoring capabilities.
Moreover, in the work [10] the authors introduced a developed wearable wireless monitoring device aims to measures patient temperature and pulse rate and enabling the communication with healthcare provider over cellular network. In the work [11], authors presented a potable IoT-based smart e-healthcare system allows secure and low-cost exchanging of critical medical data across different stakeholders.

2.3 The core layers of e-Health smart system

Healthcare monitoring system combine various type of layers that involving creating a compact system to monitor health activities in coordination with external collaborators and organizations, among the layers, there is the IoMT or end user layer, edge or gateway layer, and the Cloud layer.

2.3.1 Internet of Medical Things Layer

The integration of e-health services with Internet of Things (IoT) technology has brought about improvements in the healthcare industry, enabling low-cost deployment and intelligent development. IoT devices, including wearables, smart components, and sensors, collect and transmit useful information in real-time to the corresponding entities. This data can be analysed to identify health patterns and provide remote health assistance and medical services to patients. Although, IoT has been widely used in the healthcare sector, another specialized system leveraging medical devices and technologies known as Internet of Medical Things (IoMT) come over to facilitate remote patient monitoring, reduce healthcare costs, and increase the accessibility of medical services.
The Internet of Medical Things offers significant advantages for humankind to save their lives as well as providing healthcare assistance in case of chronic and viral diseases as occurred recently like COVID-19, also for elderly in their normal daily life. This technology brings the digitalization to the current healthcare environment by controlling intelligently all health aspects such as ECG (Electrocardiography), EEG (Electroencephalography), EMG (Electro-myography), SpO^2, pulse rate, blood pressure, pandemic tracking, , cardiovascular disease, and cancer detection and diagnosis [12].
The IoMT layer is represented as a group of medical devices and connected components as seen from the **figure 1** below that are placed near to patients for monitor and track health activities purposes in supported environment. These devices may include Wireless Body

Area Networks, smartphones, smart watches/bands, IP Motion Cameras, and healthcare assistant sensor devices.
Beside the benefits guaranteed by Internet of Medical Things, but still suffering from multiple issues that can affect the main goals of this technology, in terms of confidentiality and data protection, IoMT network layer still susceptible of various kind of Cyberattacks to control and manipulate user private data that can affect the safety of users by providing wrong data to collaborators.

2.3.2 Edge Computing Layer

Edge computing is a successor technology of cloud computing, that inherits the basic functionalities provided in cloud level to be closer to the end user including storage, Processing, bandwidth, and security.
Through this technology multiple benefits can occur such as an important low latency, storage capabilities, enhancing security of data inside the internal user network. However, related to healthcare aspect, the time is very important in emergency conditions where edge computing plays an important role processing and reacting at quick as possible which can save lives and provide better health supporting.
However, the widespread use of IoMT technology produces a large amount of data that needs to be analysed and shared with healthcare provider. This can produce a serious challenge for the edge devices in terms of computing, latency, enough storage as well as the security field. Dealing with private data always puts edge computing layer in risk of data leakage or attacking attempts and this can decrease the trust to share private data through this technology. However, several researchers focused on developing new mechanisms to handle these issues.

2.3.3 Cloud Computing Layer

The cloud infrastructure has been around for several decades, but it has become more prevalent and developed in recent years it can deliver performant resources such as storage, processing, and services over the internet by enabling users to access data from anywhere and at any time.
The cloud recently become a game-changer for businesses of all kind sizes due to the benefits. Therefore, this technology can be exploited in many forms such as Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service. However, the cloud in health sector is helpful to enhance the digitalization of remotely services by improve the quality of managing medical data over important computing units and building a sharing network of health records between different entities including doctors, hospitals, health institutions and the patients.
Deploying cloud to share medical records over the internet exposed to several challenges in terms of security and privacy due to risk presented by the internet network, however resolving these issues become priority to guaranty the confidentiality, integrity, and privacy of shared data on the cloud computing environment.

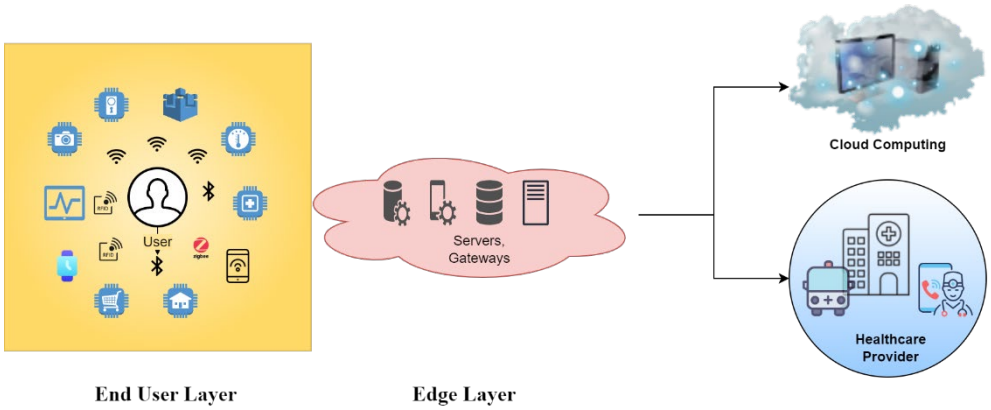

Figure 1. Conventional e-Health smart system-based edge computing

2.3.4 Key Challenges related Intelligent e-Health system

The present e-health smart systems, brings the intelligence to current traditional systems by deployment of advanced tools and mechanisms to enhance the quality of health services closer to users, however, this technology still limited due to the large amount of data generated [2], to various boundaries as seen from the **table 1** below.

Table 1. Related challenges on e-Health smart system's deployment

e-Health Limitations	Description
Latency	Healthcare applications require real time response activities particularly in emergency cases
Energy efficiency	Continuous monitoring of medical activities consumes more much power in each deployed device.
Resources	Due to the generation of large amount of data, which overloading the resources continuously.
Security/Privacy	Advanced cyber-attacks require renewal the policies and deployment of advanced protection tools.
Usability	Make deployment devices easy to manipulate by users specially for elderly.
Cost	e-health system is a distributed system with layers each layer represents an important cost to be deployed.

3 E-Health System Related Security Challenges

3.1 e-Health cyber-attacks threats-based CIA model

Making a secure healthcare system to overcome security and privacy challenges requires the deployment of cryptographic, hashing and authentication systems in addition to many recent technologies to defeat the common cyber risks.
Recently with the raise implementation of IoMT and medical tracking devices, the cyber-attacks become more aggressive and developed to manipulate user private data that is considered more valuable for advertising markets also can be exposed to the worldwide network in bad faith.
Otherwise, the current healthcare monitoring systems still struggle from various security issues that can classify the system out of scope of the CIA triad regulator model that stand for Confidentiality, Integrity, Availability [6]. However, according to the CIA model, the e-health systems can be exposed to the following types of attacks:

- Confidentiality: Phishing, Man-in-the-middle (MitM), Insider attacks, social Engineering.
- Integrity: Tampering of data, File injection, Replay attacks, Distributed Denial of Service (DDoS).
- Availability: Ransomware attacks, Advanced Persistent Threats (APTs), Botnets.

These sorts of attacks can consequently lead to disruption of normal healthcare services features, data leakage, or damage, and personal user life destabilization.

3.2 Security requirement-based CIA triad

Protecting user medical data, and system components, needs the involvement of the main three pillars of information security standards based on the e-health system architecture including confidentiality, Integrity, and Availability.
The confidentiality conducted to guarantee that the system can only be used by authorized entities in limited instructions.
Additionally, the integrity of data within e-health system layers serves to be accurate and matched the received data to the original ones to prevent any manipulation of data occurring.
In the last point, the Availability is an essential aspect, particularly for remote healthcare services to be accessible at every request. Accordingly, the **table 2** below lists different security measures defined to different e-health system layers-based CIA triad.

Table 2. e-Health system-based CIA triad security requirement **[13]**

CIA triad	Security measures
Confidentiality	- Strong Password complexity - M2FA authentication - Access control policies - Encryption
Integrity	- Encryption and signature - Certification - Hashing mechanisms - Backup policies - Non-repudiation
Availability	- Upgrading versions - Clustering - Fault Tolerance - Failover - Recovery policies

4 Toward The Blockchain and Decentralized Networks

4.1 Blockchain comprehensive Overview

Due to the limited capacity of edge and IoMT devices, remote management of a large number of medical records overloads the edge networks which redirect the user's workload to be processed in a centralized structure, such as hospitals and cloud provider storage areas [14]. This centralized architecture uncovers limitations in terms of latency, availability, security, and privacy. Meanwhile, deployment of decentralized architecture can enhance service delivery and also develop the security levels [15] as well as reduce the latency and ensure high availability of the network.

Previously, data transactions were performed within the end-user layer, where only basic encryption techniques were applied. However, the widespread use of data with external parties such as doctors, insurance companies, hospitals, and emergency departments were not a common practice, this requires a persistent technology to make this operation functional in great performance while safeguarding the important security aspects of the exchange data regulations.

Among the solutions that has been take most consideration is the Blockchain, this technology come to play important role in exchanging medical data over internet network while protecting personal data and ensuring the privacy of the patients and other entities. The Blockchain is a decentralized system that records events in the form transactions across multiple network peers in a peer-to-peer (P2P) network [16]. This technology has three main types, the public Blockchain also known as permissionless, refers to a type of blockchain

where everyone is allowed to review transactions and take part in the consensus-building process, as an example of Public blockchain, Bitcoin and Ethereum. In the other hand, the private Blockchain that is known as a permissioned technology, is the based allowing only the authorized nodes to participate on the network, as an example of this type, the Hyperledger fabric. While the consortium or hybrid blockchain is mixed type of private and public blockchain designed for a specific sort of applications [17].
Blockchain technology possesses several benefits for new smart system models, which are as follows: interoperability, immutable ledgers, crypted transactions, and high availability services [16]. The workflow process related blockchain is based on variety of algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof of Stake (DPoS) that can be used to ensure the integrity and consistency of all blockchain transactions [18]. Otherwise, deployment of smart contracts within the blockchain network enforces the application of common agreements and policies through all network entities and helps to use network administrators' instructions commonly. Deployment of Blockchain technology within healthcare monitoring systems could address many security and privacy challenges revealed by the traditional e-health systems through protecting sharing data between the edge and cloud levels as well as can guarantee remotely providing healthcare is total trust of sharing data over secure network.

4.2 Blockchain enabled healthcare monitoring systems models

The blockchain have a big advantage in current e-health systems, by providing an extra layer of security in sharing process of data while guaranty the confidentiality as well as the integrity of private patients' data, for the same reason the authors through the work [19] exposed the benefits of implementing the blockchain as a solution for sharing medical data across diverse organizations. As well as for the contribution [20] that describe a medical architecture database based on Ethereum Blockchain named as Gem Health network. However, the authors in [21] presented a solution to search for medical records in a protected and encrypted method based on blockchain technology. While a contribution introduces the use of smart contract within blockchain network under the name of MedShare to ensure a certified link between the edge layer and cloud layer [22]. Additionally, in [23] a solution known as BlocHIE, focuses on deployment of two chain networks related blockchain technology to provide storing and sharing functionalities of Electronic Healthcare Records.
Alongside with different contribution based on the Blockchain, revealed the importance of this technology on the e-Health smart system process life and how can improve the security of sharing medical data with various entities including doctors, emergency departments, insurance companies, and Health government institutions.

5 Conclusion

Healthcare monitoring systems-based edge computing technology made a huge difference in bring health assistance close to the end user by multiple mechanisms revealed in three main layers define the basic architecture of the healthcare monitoring smart system or known as e-health smart system, the layers appear as IoMT network layer, edge computing layer, and the cloud computing layer where medical data collected and processed in two levels on edge and cloud stages. Meanwhile, the workflow process exposed several challenges to benefit all features provided by this system, including latency for emergency cases, bandwidth limitation, and security of circulated data. Related to the security aspect, the current technologies can involve solving some limitations by deployment of mechanisms and measures to prevent bad consequences to patient life safety.

Therefore, sharing data from end user layer to cloud layer for computing and consulting purposes put big charge in securing the data flow over the system's architecture where the introduction of the blockchain solution to overcome the confidentiality, integrity as well as the availability through a decentralized infrastructure.

References

1. P. J. Pronovost, M. D. Cole, and R. M. Hughes, JAMA **327**, 1125 (2022)
2. M. Hartmann, U. S. Hashmi, and A. Imran, Trans Emerging Tel Tech **33**, (2022)
3. https://www.svb.com/trends-insights/reports/healthcare-investments-and-exits
4. A. B. Martin, M. Hartman, J. Benson, A. Catlin, and The National Health Expenditure Accounts Team, Health Affairs **42**, 6 (2023)
5. M. Laroui, B. Nour, H. Moungla, M. A. Cherif, H. Afifi, and M. Guizani, Computer Communications **180**, 210 (2021)
6. S. Nasiri, F. Sadoughi, M. Tadayon, and A. Dehnad, Acta Inform Med **27**, 253 (2019)
7. M. W. Raad and L. T. Yang, Inf Syst Front **11**, 529 (2009)
8. T. Liang and Y. J. Yuan, IEEE Sensors Journal **16**, 8186 (2016)
9. I. A. Pap, S. Oniga, I. Orha, and A. Alexan, in *2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)* (2018), pp. 1–5
10. M. Omoogun, V. Ramsurrun, S. Guness, P. Seeam, X. Bellekens, and A. Seeam, in *2017 1st International Conference on Next Generation Computing Applications (NextComp)* (2017), pp. 169–174
11. N. Semwal, M. Mukherjee, C. Raj, and W. Arif, Journal of Information and Optimization Sciences **40**, 1787 (2019)
12. Z. Ghias and A. Avokh, Biomedical Signal Processing and Control **73**, 103403 (2022)
13. Sinchan Banerjee "https://www.linkedin.com/pulse/cia-triad-heath-care-standards-sinchan-banerjee/"
14. J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, IEEE Internet of Things Journal **6**, 8770 (2019)
15. E. Bonnah and J. Shiguang, Future Generation Computer Systems **113**, 363 (2020)
16. S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, Applied Sciences **9**, 1736 (2019)
17. A. Z. Al-Marridi, A. Mohamed, and A. Erbad, Computer Networks **197**, 108279 (2021)
18. L. M. Bach, B. Mihaljevic, and M. Zagar, in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (2018), pp. 1545–1550
19. S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F.-Y. Wang, IEEE Transactions on Computational Social Systems **5**, 942 (2018)
20. M. Mettler, in *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)* (2016), pp. 1–3
21. L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, Future Generation Computer Systems **95**, 420 (2019)
22. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, IEEE Access **5**, 14757 (2017)
23. S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)* (2018), pp. 49–56