Data Security Mechanisms, Approaches, and Challenges for e-Health Smart Systems

https://doi.org/10.3991/ijoe.v19i02.37069

Hamza Rafik[1](✉), Abderrahim Maizate[1], Abdelaziz Ettaoufik[2]
[1]RITM – ESTC/CED – ENSEM Hassan II University, Casablanca, Morocco
[2]LTIM – FS Ben M'SIK Hassan II University, Casablanca, Morocco
hamza.rafik-etu@etu.univh2c.ma

Abstract—In the new era, the trend of using wearable devices and smart accessories gained considerable popularity and become a necessity utility for human life due to their major role to keep monitoring health conditions and providing healthcare services. The combination of IoT networks with edge computing paradigms develops an intelligent e-health system that aims to monitor different real-time scenarios. The deployment of an e-health system exposes several challenges regarding the security and privacy aspects, particularly in the case of dealing with an enormous quantity of medical data and the risk presented by exchanging operations with external entities. In this paper a comprehensive presentation covered the basic topics of e-health system layers thus the advantages and limitations in terms of existing challenges has been mentioned, subsequently, adapted to the exposed cyber risk through the traditional systems in exchanging medical data, a discussion of the blockchain technology come over for new application opportunities, where this approach efficiently ensure the security of data transactions over the network, in addition, an overview outlined the main research works related to this technology. Therefore, a presentation study of diverse works reveals different security framework solutions related to e-health system's layers, furthermore, uncovering the benefits of integrating intelligent technologies such as Machine Learning (supervised, and unsupervised types), Deep Learning, and Reinforcement Learning as well as introducing a comparison analysis of multiple AI algorithm models based on their efficiency for future deployment related security purposes to provide a smart healthcare monitoring system that meets patient needs. The end of this review highlighted further research directions and the actual open challenges regarding the e-Health system's limitations.

Keywords—Internet of Things (IoT), edge computing, blockchain network, Internet of Medical Things (IoMT), Artificial Intelligence (AI), healthcare data, Machine Learning (ML), Reinforcement Learning (RL), cloud computing, security

1 Introduction

IoT technologies-based Healthcare is the main component of human life and becomes a priority, specifically since the largest increase of viral and chronic diseases that spread rapidly where the need for a monitoring system to control and supervise the health

status of patients through specialists such as doctors, caregivers, and emergency departments. However, the biggest use of this technology with traditional architecture-based cloud computing led to serious challenges in terms of latency, quality of service (QoS), storage efficiency, energy consumption, and security. In the projection of the current pandemics, the pervasive deployment of IoT paradigm requires an interested resources such as processing units, storage spaces and managing data tools due the important volume of data generated. The development of a smart, dependable, flexible, and secure edge computing-based healthcare system has become a priority to oversee these challenges.

The health industry is going through a total digitalization in the next few years as numerous crossing platforms evolve to form a new operational framework for the health and healthcare sector. One of the main fundamental human needs today is healthcare, this business generates several billion dollars in revenue in the near future. Related to this subject, with the exceptional spread of contagious diseases such as COVID-19, according to the Organization for Economic Co-operation and Development (OECD) health spending as a share of GDP jumped to 9.7% in 2020, up from 8.8% in 2019. While with estimates that health spending still growing exponentially by years [1]. the digitalization of the health monitoring process gains important benefits to address the revealed lack of resilience of traditional health systems, according to precedence research the global smart healthcare market size in 2020 was 44.65 billion USD while expected to grow by 9.2% approximately 85.37 billion USD from 2021 to 2030 [2].

Although intelligent e-health systems based on IoT networks serve real-time healthcare applications, while still need a big effort to define innovative techniques to secure the collected data from the sensor layers which is considered sensitive personal data and allowed to be checked only by authorized healthcare professionals. In the recent literatures, most of IoT based healthcare systems try to focus on managing data in the edge-to-cloud layers with the special deployment of recent adaptive technologies, otherwise, the security and privacy of Medical data enable a development direction path for most of the authors by using recent techniques including the blockchain network that is considered as an evolutional technology cover the basic data transactions, exchange and storage processes without any centralized control based on a distributed database [3], also the encryption algorithms that aim to preserve the anonymity and the integrity of health parameter records.

Over the past few years, Blockchain technology takes great attention from the industry field along with the academic perspective [4], due to the potential impact of this technology to overcome security, storing, and data exchange challenges. However, this emergent technology influence directly the business process of healthcare results of organizations and external collaborators, also enhancing the health services of patients, optimizing the management of data, acquiescence improvement, and empowering efficient use of healthcare-related data flow [5].

Therefore, this paper aim to provide a summary of some contributions in objective to build next generation of e-health systems based on recent technologies such the blockchain networks, Artificial intelligence models, and traditional security mechanisms, to address revealed security and privacy challenges. Through this paper a structured

summary of different layers of this innovative system has been introduced as well as outlined many contributions related security aspect of each layer based on recent framework solutions along with an analytic comparison of different AI algorithms serving to enforce patient data protection over using this system model. Indeed, affording efficient data analytics with a combined edge-based healthcare system fulfil the recent requirement for an embedded healthcare ecosystem in term of latency, energy efficiency, real-time prediction activities, and secure transactions between all the professional stakeholders.

In the remaining parts of this work, multiple aspects focus on the security of data in the e-health system will be discussed as the following main points:

- A summary of different technologies contributing to the e-Health smart system building.
- Representation of decentralized architecture system model with projection on the blockchain technology-related smart health care system.
- Taxonomy of different security frameworks and measures proposed for securing Medical Data in addition to exposing the benefit of integrating intelligent technologies while illustrating a comparison analysis disclosed different AI algorithms for serving security purposes.
- Future directions and open challenges.

2 Background

This part of the paper highlighted different elements of the healthcare monitoring ecosystem, such as IoT technologies, edge computing, and cloud computing, which are used to provide a well-consolidating system for monitoring health conditions and improve the response time in emergency cases, in addition to providing a higher accuracy of medical activities, especially for senior cases and in pandemic situations.

2.1 Internet of Things-based healthcare services

Currently, the Internet of Things (IoT) brings interesting benefits to several fields, including industries, vehicles, smart homes, hospitals, logistics, and more, for their efficiency and flexibility. However, the digital transformation aspect in the healthcare sector has a big impact from the advantages and facilities that will be provided to the patients. Combining Internet of Things with Healthcare services created a new paradigm named IoMT, which stands for Internet of Medical Things. It is essentially made up of a collection of medical devices and components attached or located close to the patients that aim to monitor health parameters and activities within an intelligently supported environment, such as WBAN (Wireless Body Area Network), Smartphones, smart watches/bands, IP Motion Cameras, and healthcare assistant sensor devices [6]. Although the obvious operational and practical benefits of IoMT technology, it plays a crucial role in deploying core functions of healthcare services to patients.

In fact, these smart health devices have a fundamental role in collecting bio-signals such as ECG (Electrocardiography), EEG (Electroencephalography), EMG (Electromyography), SpO^2, pulse rate, blood pressure, pandemic tracking, assistant management of diabetes parameters, cardiovascular disease, and cancer detection and diagnosis [7].

IoMT technology allows the combination of recent communication technologies with medical devices, to serve as a practical remote healthcare monitoring and treatment tracking service. This technology is based on three essential layers, for instance, perception, network, and application layers [8]. Each layer defines several types of protocols used for exchanging data workflow as detailed in Table 1.

In order to keep remotely monitoring patients' activities, ensure daily health assistance and emergency aid, especially for elderly people, and to construct a global health management infrastructure to keep updating health status with other stakeholders. However, this technology reveal security difficulties can be an objective of various type of attacks related controlling data management of end user such as passive/active attacks, virtual/physical attacks, hardware/software attacks, and even human manipulation attacks [9] which can be a subject for developing safety measures to preserve security directives illustrated in integrity, Reliability, availability, and non-repudiation of the system.

In view of the critical and private data communicated through IoMT network, the security and high availability of the interconnected devices must be ensured [8]. Besides the benefits offered by this technology, it still has limitations in terms of reliability, interoperability, energy consumption, and security of medical data.

2.2 Edge computing paradigm-based healthcare functionalities

Edge Computing is an emergent technology that aims to allocate resources and services regarding storage, processing, and security to end users to resolve IoMT layer limitations. However, the Edge Computing paradigm is a new computing architecture focused on bringing the cloud's services close to the end user layer to benefit the cloud advantages [10]. In fact, this nascent technology provides several advantages over cloud computing, such as providing lowest latency, increasing security, and efficient energy consumption. These features make edge computing convenient for different scenarios, including healthcare, real time traffic management, industry, and education. According to [11], the edge computing model consists of a multiple heterogenous devices that communicate with each other and provide computing services, including storage and processing of data.

Table 1. A Summary of main IoT layers with their communication technologies and protocols

IoT Layers	Description	Communication Protocols and Technologies		
		Name	Acronym	Type
Perception Layer	Considered as the physical layer, collects medical data, and discover the physical environment, it is the first layer where execute identification and sensing operations.	IrDA	Infrared	Protocol
		RFID	Radio Frequency Identification	Technology
		NFC	Near Field Communication	Technology
		Bluetooth/BLE	Bluetooth Low Energy	Technology
		Z-wave	N/A	Protocol
		UWB	Ultra-Wideband	Technology
Network Layer	Particularly the layer is the middle layer which charged for ensuring communication and transport of data between interconnected devices of the network.	Wi-Fi	Wireless Fidelity	Protocol
		NFC	Near Field Communication	Technology
		ZigBee	N/A	Protocol
		6LoWPAN	IPv6 Low power Wireless Personal Area Networks	Technology
		Bluetooth/BLE	Bluetooth Low Energy	Technology
		LoRaWAN	Long Range Wide Area Network	Protocol
		Z-wave	N/A	Protocol
Application Layer	From this layer, the IoT network deliver applications to specific users, however it transforms the collected data in a processed form.	HL7	N/A	Standard
		COAP	Constrained Application Protocol	Protocol
		MQTT	Message Queue Telemetry Transport	Protocol
		HTTP	Hypertext Transfer Protocol	Protocol

Moreover, several papers addressed this technology from multiple angles in terms of optimizing response time of critical applications, saving energy consumption, and securing data coming from the sensor layers by multiple known mechanisms. Additionally, there are multiple forms of the gateway layer such as fog computing, Edge computing and Cloudlet which all perform the same role while bringing the resources and services near to the patient.

Edge devices are an extension of the cloud computing global network that aims to offload tasks to the edge layer resources to achieve the target of minimizing latency and increasing the efficiency of the data analytics process. However, the pervasive deployment of IoMT networks generates an important volume of data that needs to be analyzed and exchanged with third party organizations.

Otherwise, collected data related security and privacy outlines a big challenge, especially while utilizing the internet network to transport and manage remotely private data through the cloud computing layer and then to medical organizations and collaborative institutions. Even in this case, users still hesitate to share their private medical data among healthcare collaborator entities due to the internet's essential risks [12]. Hence, deploying advanced security technologies can efficiently decrease the security threats and encourage patients to trust the system to share their medical data over the network.

On the other hand, the deployment of edge computing highlights several limitations regarding the quality of services, the latency especially in dealing with healthcare emergency situations where the time is crucial, the scalability of the system, and the protection of transferred data.

2.3 Overview on cloud computing technology

Basically, cloud computing is a centralized approach based on the traditional Client-Server architecture. The Cloud provides on-demand services such as Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service, which can be ensured through the main three layers including Application layer, Platform layer, and Resource layer that help to build a compact Cloud system [13]. The key points of this technology are providing computing services for different kinds of applications based on sharing resources with multiple users at the same time. Hence, related to the healthcare field, cloud computing is helpful for digitalization of medical services including hospitals, patient records, and emergency diagnosis [14], hence enhancing the clinical results and quality of patients' life.

Actually, cloud computing-based healthcare systems interact in a positive manner by helping patients' treatment, including facilitate medical assistant and virtual health checking in the most remote environments [15]. However, with all these advantages, the cloud-related healthcare industry struggles from multiple difficulties, in particular high latency, confidentiality, and security of patients' data, also the dependency of the internet network. While regarding health monitoring sector, the cloud computing contributes to enhance the resource sharing and provide an effective remote healthcare monitoring, hence manage system with reduced costs. The security aspects open new research paths and challenges in medical research-based Cloud infrastructure in the case of dealing with the interesting amount of medical data generated from the IoT layer.

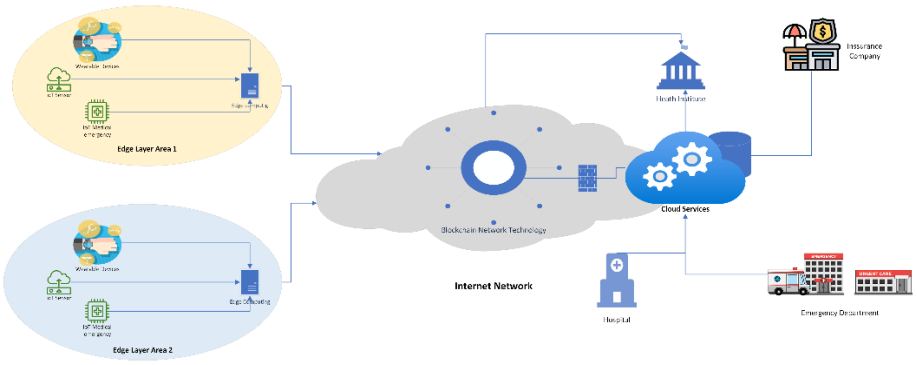

Fig. 1. Blockchain technology-based e-health smart system architecture

3 Security mechanisms for exchanging medical data over e-Health systems

In this section from the review, regarding the integration of a healthcare monitoring system, an analysis study of different literature demonstrates several methods of securing the medical data exchange process by the deployment of recent techniques, especially the blockchain technology related hash techniques and cryptography algorithms.

3.1 e-Health system architecture

Remote monitoring and management of an intensive number of vital signs put an overload on the edge networks due to the limited resources of edge and IoMT devices, commonly user's health data collected and processed in a centralized environment such as the hospitals and the clouds storing areas [16] where sufficient resources are available, this transition still struggles from issues in terms of data exchange security and privacy.

Otherwise, healthcare data generally reflects the patient's health status that is collected as Electronic Healthcare Records (EHR) form. Usually, medical parameters are collected through sensors and WBAN devices in the form of data streams that appear as time series records. The information extracted from Medical records can be classified into immutable information characterized by maintaining protection, integrity, and authenticity of data, whereas the other type of information is mutable data, which includes tags, raw data and descriptions [17]. Hence, the data is transmitted to the next layer composed of an edge computing device acting as a gateway device to execute basic processing and storing functions. Meanwhile, the edge device has an always-on connection function with the cloud services for extra processing services and improved storage capabilities in case of additional needs of resources.

During epidemics an urgent demand of an intelligent healthcare system become a necessity to avoid spread of pandemics, thanks to the edge computing, IoMT network and the Cloud infrastructure combined with security technologies and mechanisms, such as blockchain mechanism. Designing a secure, collaborative health model to integrate multiple entities is now more realizable than ever before [6].

The architecture model e-Health system is based on three main layers composed of the typical system model: end user layer, Edge layer and Cloud Layer as seen from the Figure 1 that illustrates the main components of the next generation e-Health System. Meanwhile, this architecture represents promising alternatives that complement the traditional system-based cloud architecture [18]. However, the centralized architectures produce delays and low performance, as well as security issues for connected devices and data that might affect human lives.

The current concerns in this system model architecture are to ensure total protection of personal medical data among all layers while guaranteeing the anonymity and integrity of data. That can be achieved through deploying a decentralized approach based on the Blockchain concept and combinations of cryptography techniques and hashing algorithms over data exchanging processes.

3.2 Development toward decentralized architecture

Previously, data transactions were based on a centralized structure as mentioned in the subsection above by forwarding data from original source nodes to a central server for processing functionalities. The central sever node has the larger capacity in terms of resources and mechanisms. This topology shows multiple drawbacks, mainly latency for critical time response applications, data delivery, availability, third party application involvements, and security issues.

Therefore, edge computing is based on a distributed model in contrast to the Cloud Computing that operate on the traditional structure client-server interconnection [10]. While to achieve Cloud services is certainly slower and risky compared to edge computing architecture due to multiple hop transactions that separate end user devices and the service cloud provider through internet network. The healthcare sector is a critical field when it comes to monitoring patients remotely in real time, where the needs for total securing environment and availability resources.

A huge part of the benefits has been adopted by decentralization of the network. This structure help to improve service delivery also enhance the security levels [19].

3.3 Exchange medical data based blockchain technology mechanisms

Sharing vital signs is a challenge for the edge computing-based healthcare system deployment. Before, data transactions were done internally into the end user layer, where only simple cryptography technologies were used. Otherwise, communicating the data with external stakeholders including doctors, insurance companies, regional hospitals, emergency departments, and health government organizations as displayed from the following Figure 2 puts a high risk of leakage of personal patients' data on the internet network.

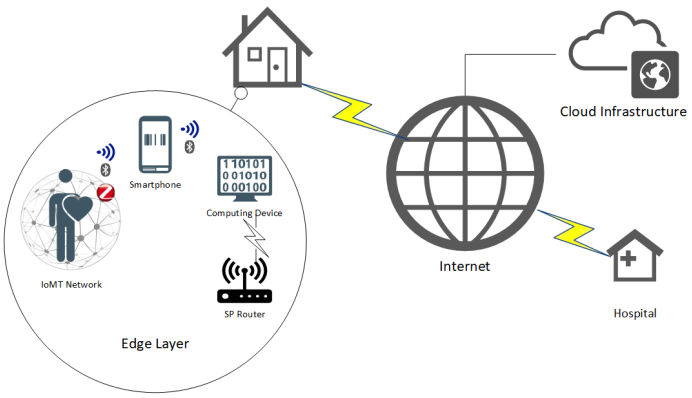

Fig. 2. Edge computing based healthcare conventional system

Basically, the edge computing architecture is based on a centralized approach. This model is still insufficient to integrate users in the healthcare global system due to its weakness in terms of security. However, the research community leverages the decentralized architecture by deployment of the recent technologies, including Artificial intelligence algorithms with its variants (ML, DL, RL) and the Blockchain technology.

Among the decentralized technologies used to secure data transactions, the blockchain technology, is an innovative solution that was launched in 2008 as a decentralized ledger recording the events in the form of information transactions over multiple network peers into a peer-to-peer network. This technology has Three main types named as public known also as permissionless, private named as permissioned Blockchain and consortium or Hybrid blockchain [20]. Actually, Blockchain technology is a substantive rapid development worldwide [21], due to strong encryption mechanisms along with all data transactions processes and also the complexity provided by the blockchain structure, this technology has become a main topic for secure data exchange in several domains, while The blockchain is characterized by multiple advantages for newer smart scheme systems outlined as below:

- Interoperability with different nodes without any commitment of a third party's policies.
- Depending on immutable distributed databases.
- Enforced protection by utilization of cryptography and hashing algorithms.
- High availability of access data, according to the decentralization and duplication of databases amongst all blockchain nodes.
- Ensuring high level security, resilience, integrity, and decentralized process flow of data.

Recently, the rapid evolution of Cyberattacks threats and privacy issues reveal serious challenges to preserve data from evolutive leakage risks and gaining the patients' trust to share their data over the network. Meanwhile, the blockchain will play an important role in facilitating sharing of medical data and providing a distributed immutable database to store data, hence the blockchain system is based on two fundamental components in the blockchain's design, such as the consensus blockchain algorithm and smart contract structure. Firstly, the blockchain is formed on a particular consensus algorithm that ensures the integrity and coherency of all blockchain components based on a variety of algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Delegated PoS (DPoS) [22]. On the other hand, smart contracts are defined as contractual programs composed of instructions and policies agreed upon by all network entities by fulfilling their obligations and following the automatic execution of the workflow [23].

The blockchain model is made up of multiple nodes that form a secure distributed network. Furthermore, among the blockchain network nodes, the miners, these computing entities have the responsibility to validate the exchange process to added data into a verified blocks as represented in the Figure 3 which display the different process chain for validating a transaction of data inside the Blockchain Network, the miners are considered as contributors of the blockchain system while they guarantee the consistency and enforcement of the smart contract [24]. Blockchain technology get better comprehensible by illustrating different features describing this technology as shown from the Table 2.

Table 2. Blockchain network main functionalities

Functionality	Description
Decentralized	The blockchain operations doesn't have any control from any governing authority or a node, it can be accessed from any entity connected to the network which offer less Failure, User control, no third-party involvement, zero scams transparency, less prone to breakdown and have an authentic nature.
Enhanced Security	The records in the network become immutable once have been stored in the blocks, no one can change the network characteristics due to using encryption layer.
Faster Settlement	Making the transactions faster due to the distributed characteristics of the system architecture which save much time specially for healthcare purposes.
Hashing	Due to its complex structure and difficulty to break and alter the key, Blockchain network based on hashing as a best solution for securing transactions of data.
Distributed Ledgers	A blockchain shared database private or public and record all transactions, the ledger normally maintained by all nodes of the network, hence it offers managership, no extra favors, require ownership of verification, Quick response, and total security.
Consensus	The blockchain architecture based on consensus algorithms which reveal the decision-making process for the nodes on the network this result the system to run smoothly and being a trust network.

Therefore, to address security issues of sharing medical data, this part of the paper introduces related works dealing with the blockchain network integrating e-health systems. The authors in [25] displayed the empower of blockchain technology to ensure overall medical data exchange within diverse organizations, including patients, different healthcare communities, private clinics, and hospitals. While the IoT, especially in the medical sector named as IoMT, carries highly critical patients' medical data where the priority is to offer the best level of security in IoMT [26], [27]. Healthcare applications require the integration of the blockchain to maintain high confidentiality while exchange medical data, in the work [28] a description of a decentralized medical database based on the Ethereum Blockchain named Gem Health Network, beside the advantages offered by this solution, is still struggle from obstacles such as weakness in the patient identification and scalability. Additionally, the authors in [29] suggested a new healthcare system based on blockchain technology aims to enable searching of medical records in an encrypted manner, while as a consequence, this system suffers from scalability issues. From the literature [30] the authors introduce a solution named MeDShare for sharing patient's medical data with external organizations linked to cloud datacenters based on smart contract solution that enables audit, analyze and control over sharing health records while offer total control over data exchange activities and guarantee high level of authenticity and minimize security risks on data. Otherwise, in [31] a new platform named BlocHIE based on two chain networks derived from Blockchain came to offer separately storing and exchanging Electronic Healthcare Records (EHR) in an objective to improve the system throughput and fairness through entities. However, this solution has an issue with scalability and flexibility. Indeed, expand smart healthcare system capabilities and improving the health quality

of services is an important aspect, an emergent solution referenced as Healthcare Data Gateway (HGD) comes to empower the patient's ability to control, personalize, and manage their private data in a total secure environment based on blockchain technology introduced by Yue et al. [32]. Therefore, the emergent use of advanced technologies such as Artificial Intelligence, Deep Learning, and others, allows the authors in [25] to define a new Parallel Healthcare Systems Framework (PHS) based on the blockchain technology to enhance healthcare accuracy analysis and quality treatment delivery in secured environment by adopting artificial systems, computational experiments, and parallel execution approaches.

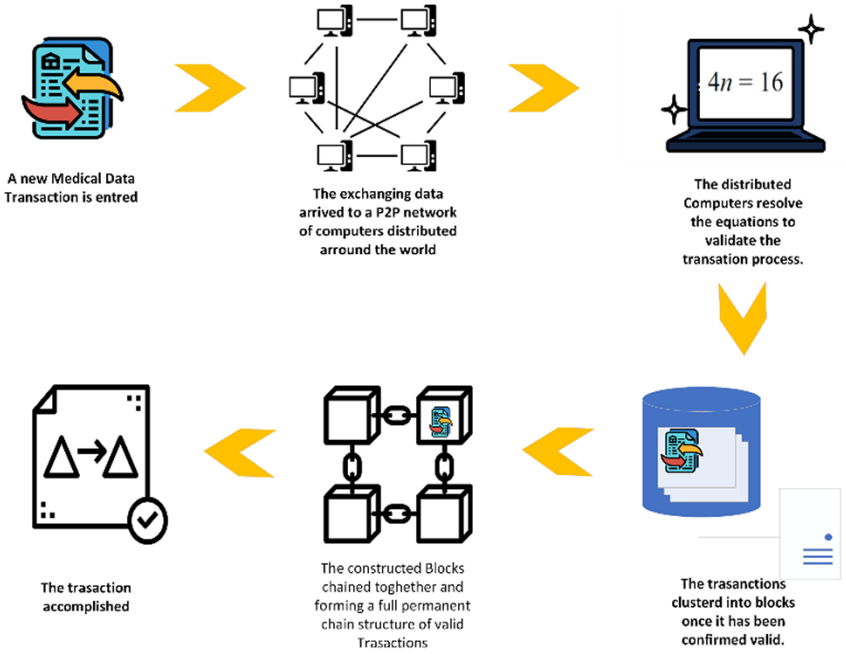

Fig. 3. Blockchain data transactions process flow

Once an increase occurs in feeding computing systems with data, the systems become smarter and more efficient thanks to the advanced AI technologies that are coupled with security mechanisms like the blockchain that lead to increased performance and gain the trustworthiness of users. With the same vision, Kuo and Ohno-Machado [33], represent a framework solution for a private blockchain network that aims to train machine learning model systems through the contribution of health data from all entities to improve the self-security development and management of data.

4 e-Health system structure-based security measures related works

Protection of a user's medical data is a serious challenge for healthcare monitoring systems due to the valuable generated information. However, next-generation systems try to provide an embedded system with security tools and algorithms able to deal with data safety problems in addition to providing optimal healthcare applications, which is still limited in terms of several factors. In this remaining section, this review introduced multiple security methods and frameworks deployed by researchers to enforce the system architecture in the projection of different layers, in addition to a discussion of the benefits of integrating AI technologies to maintain security within an e-health system.

4.1 Security mechanisms for IoMT network layer

The end user layer is considered as a sensitive part of the e-health ecosystem architecture due to the essential presence of IoMT and sensor devices attached directly to the human body. However, this layer faced potential security threats, consequently this affects the creation steps of an efficient and secure healthcare monitoring system to ensure total protection of the private user's medical data.

The IoMT network is currently exposed to a variety of security attack risks including Jamming Attacks, DDoS, Intrusions, Side Channel, Buffer Overflow, Impersonation, and Spoofing attacks [34]. Integration of practical countermeasures could bring a positive impact on safeguarding this layer from critical menaces.

Otherwise, the majority of the literature focuses on the security branch of the IoMT network in the end user layer [35]. According to the work presented in [36], the authors listed the most important communication protocols used by IoMT as well as their security characteristics. Nevertheless, with the evolution of cyber mechanisms to exploit vulnerabilities due to protocols' weaknesses, the authors in [37], presented a solution to reinforce authentication for Radio Frequency Identification (RFID) Technology to preserve location privacy, hence, ensure protection against DoS and replay attacks. While, in the literature [38] the authors introduced an emergent encryption solution using identity-based encryption algorithms named as VLFSR, which is useful for mitigating most of the attacks against RFID Tags. Additionally, the contribution of Eun et al. [39] helps to mitigate the security limitations that occur in NFC's architecture by proposing two security mechanisms, SSE and SCH solutions, the Shared Secret Service (SSE) secures the communication between NFC devices through generation of secret key, while the Secure Channel Service (SCH) ensure the propre confidentiality and the integrity of target data. However, using Bluetooth or BLE connectivity within end user area may exposed network devices to critical security problems, thus the authors in [40] guided for a solution based on the AES coprocessor for encryption and decryption mechanisms applied on collected data, as well as Minh Dang et Jalil [41] the presented a solution to prevent leakage of data in transmission section based on frequency hopping techniques. Meanwhile, the frequent use of devices with Wi-Fi communication

protocol requires high level protection by deployment of encryption access techniques for wireless connectivity such as WEP, WPA (Personal/Enterprise), WPA2, and WPA3. To prevent forwarding attacks, according to the authors in [42] introduced a sequential counter of frames where it can be reset it each time sending or receiving a frame for communication-based ZigBee protocol. Lastly, from the work [8] the authors conducted to use a combination of encryption mechanisms and tools such as Datagram Transport Layer Security (DTLS) and a host identification technology in addition with Internet Key Exchange (IKE) technology, this association of two technologies aims to establish secure communication channel for data transmission while using 6LowPAN protocol.

Besides all the advanced security techniques developed for the IoMT network layer, the risk increases continuously when it comes to protecting health data, in addition with lack of an organization charter to standardize the use of security utilities to enforce the end user layer.

4.2 Edge computing layer-based security feature techniques

Leveraging edge computing technology within the healthcare domain represents a significant challenge in terms of security for incoming end users' data. From the edge layer, multiple activities launched such as processing, storing, data analytics, and forwarding operations to the cloud layer. All these procedures faced serious security threats.

Actually, to enforce this mid-layer in terms of security, the authors in [43] suggested a solution based on constant message expansion that helps to mitigate gateway attacks such as eavesdropping attacks, the robustness of this solution fulfills the security and privacy users' needs. Furthermore, a proposed solution basically provides protection to systems and safeguards medical data. In case of device-edge communication based on IPv4 and IPv6, this solution used a lightweight version of IPsec Standards [44]. Therefore, in the work [45] the authors introduced a security model based on a two-stage Markov algorithm, Intrusion Detection System (IDS) and a Virtual Honeypot Device (VHD) to detect harmful gateway devices located on the edge layer. However, due to the sophisticated features provided by edge technology, cyberattacks are still evolute with advanced techniques. Such as the case for end users' requests based on HTTP protocol suggested in the work [8] should be encapsulated over SSL/TLS to construct an HTTPS exchange protocol to secure data transactions in the edge environment. Moreover, in the work [46] there is a proposition of an Intrusion Detection System as a detection layer of any malicious or threats. In fact, the heterogenous nature of edge computing systems integrating IoMT devices reveals the essential role to preserve collected data safety as well as ensuring the privacy of patients information [10], which motivates patients to adopt this kind of systems with full trust.

Meanwhile, the authentication process is an important factor to affirm the privacy and preventing leakage of data. For this reason, Donald et al. [47] presented a technique based on a trusted third-party entity assigned to ensure the authentication process, even this strategy is still limited due to the dependency on an authentication server acting as

a gateway device. Additionally, in the work [48], the authors proposed a system-based user authentication while users' credentials are stored on all edge devices belonging to the workflow network to ensure authenticated users at any edge node of the network. Therefore, the access control mechanism takes more attention in the deployment of a secure edge computing ecosystem. Hence, using Attribute-Based Encryption (ABE), that is considered as a cryptographic primitive attribute, to realize an access control attribute based on defined policies and rules introduced in [49].

Edge computing is an innovative technology that serves in a variety of domains. While recently this technology has taken a big interest on the healthcare sector by bringing health services to end users, this paradigm requires more development and improvement in terms of enhancing real time response in the same way as ensuring security of managed data.

4.3 Cloud computing related security approaches

The explosive growth of unstructured data mostly forwarded to be treated on cloud-based technology [10], due to the insufficient capacity of storage neither of the processing of the edge layer devices. Thus, cloud computing provides important capacity in regards of storage and computing resources, while following the combination with advanced technologies and big data analytics will be able to offer acceptable quality for healthcare remote assisting and expanding the healthcare services delivery.

Besides, the benefits of cloud technology, it presents limitations in terms of ensuring the security of data exchanged with the edge network and high latency for critical health applications. Therefore, some researchers proposed solutions that aim to minimize the security issues impact while basing on diverse mechanisms. According to the authors in the Work [50] proposed using a decoy information technology by deploying disinformation attacks to track the threats inside the system for securing the cloud. Additionally, as mentioned in the sections above, ensuring the security of exchanging medical data is guaranteed through the use of blockchain technology and other encryption algorithms.

Security and privacy are two fundamental approaches to building an efficient monitoring health system and enabling the confidentiality and integrity model of circulated data into the cloud computing model, where it becomes an active topic for the research community. However, according to the cloud-on-demand-service models including SaaS, PaaS and IaaS the security countermeasures separate from one service to another depending on the threats impact form, as for instance the authors in [51] introduced a methodology called MetaMORP(h)OSY used to reduce the Cross-VM Side-channel attack impact based on thermal behaviors tool that analyze the real time thermal status. Additionally, an approach based on creating an XML signature, named XML signature and encryption used against XML attacks [52]. Moreover, in the literature [53], a smart framework called Trusted Computing Base (TCB) is proposed to deal with the lack of interoperability with devices, it is considered as a sort of secure layer over the OS. Furthermore, Hashizume et al. [54] listed an approach based on the RSA algorithm that aimed at dealing with forwarded data in terms of preserving the authentication

and confidentiality. This cryptographic method mitigates data breach threats. Additionally, a new framework proposed in [55] addresses the scanning of HTTP requests and responses to avoid data vulnerability issues through the use of a Web Application Scanner. Even, for the Distributed Denial of Service (DDoS) attacks the Cloud Computing researchers proposed a set of solutions against this type of cyberattacks, as well as for [56] introduce utilizing Ingress filtering to ensure the address IP match the domain instead it will be drop. Otherwise, to avoid Hijacking attacks on the cloud, a deleting code technique that is applied on the network-based IDS to detect the vulnerabilities and correct them in real time to avoid any intrusion inside the cloud and leakage of the sensitive data [57].

Cloud computing technology provides multiple advantages to individuals in several domains, such as industry, education, media, health, and others. Otherwise, the important resources and services provided by this technology raise challenges to be addressed in terms of security and latency for real-time applications in further research work.

4.4 Security aspects related emergent technologies

Recently, Artificial Intelligence technologies (AI) and their subcategories, including Deep Learning (RL), Reinforcement Learning (RL), and Machine Learning (ML) have played a crucial role in deploying and managing smart systems in terms of optimizing processing activities. Basically, AI technologies are used in diverse fields such as smart cities, healthcare sector, industry, robotics, education, and web applications, which require a variety of intelligent algorithms adapted for different scenarios depending on deployment cost, latency, and flexibility constraints, as elaborated in Table 3 that enables a comparative study of diverse AI algorithms based on their marked efficiency in several domain applications across research contributions. Consequently, the parameters noticed in the table have been concluded through different research contributions result. Accordingly, the table makes a solid analytics basis for further deployment, particularly in security fields. The application of AI algorithms in the healthcare industry in terms of security improves the efficiency and reliability of health applications services, which leads to uncover the following contributions addressed the security and privacy aspects of the system.

The scope of this section discusses research contributions performed the integration of emergent AI techniques in securing e-health system environments. Therefore, in projection with the healthcare sector, the advantages of deploying these technologies enhance the quality of health services delivery as well as reinforce the security in an intelligent technique. As more data is fed into the systems, more systems become intelligent and self-sufficient in their ability to predict and classify data [58]. Otherwise, Chen et al. [59] listed the recent countermeasure security against adversarial attacks-based Reinforcement Learning (RL) techniques. Additionally, in the work [60] the authors presented a review summarized the utilization of Machine Learning techniques to detect and identify multiple malicious attacks in the interconnected devices to enhance the security in IoT network devices. Furthermore, an authentication system based on a Machine Learning (ML) algorithm applied to extract bio-features as tokens forms, even

executes verifications of the block simultaneously in real-time without notifying users, as introduced in [61]. While, in the work [62] a new developed authentication scheme using naïve bayes ML algorithm named Risk-based Adaptive Authentication to analyze different authentication risks, this mechanism continuously monitors the channel characteristics variation to optimize the authentication process for the users and devices for an e-health system. In [63] the authors introduced a Deep Learning solution based on Recurrent Neural Network (RNN) to detect the condition status of nodes within a WSN network to prevent network peers from cyber-attacks such as botnet attacks. Moreover, the authors in [20] proposed approaches of RL techniques such as Deep Q-Network, Double Deep Q-Network, and Dueling Double Deep Q-Network associated to an intelligent Blockchain Manager toward achieve improvement in latency, security, and cost qualities. While, in [64] the authors introduced an approach based on the RL techniques such as the Dueling Double Deep Q-Network (D3QN) that able to select the most efficient Blockchain network depending on several constraints. The authors in [65] presented new mechanisms to discover DDoS attacks, which stand for Distributed Denial of Service within IoT Network based on Machine Learning and Deep Learning models while providing a comparison analysis of accuracy rate achieved by each algorithm. Apparently dealing with collected medical data put an overload on the e-health systems in terms of security due to frequent use of different end user devices that may exposed to serious threats, which drives the authors in [66] to introduce an approach based on Deep-Q-Network to minimize the cyber-attack impacts.

Today, the IoMT network represents the next generation of life assistance devices for tracking personal activities and instant medical records. This technology in association with edge computing and AI algorithms, builds a smart system with the embedded abilities to enable self-decision for critical situations before an actual event occurs, especially in the case of protecting private data as well as the whole system. The authors through the work [67] introduced a scheme of three Intrusion Detection System (IDS) with embedded Supervised Learning algorithms to build a performant detection layer on the network to determine malicious activities and attacks actions for instance DDoS, IoT framework weakness, Spoofing, Man-in-the-middle and Botnets. While over the work [68] Mahmood Naser et al. develops a combined security model based on AI Technology including deep and machine learning to protect the Wireless Sensor Network inside an IoT network layer with highest accuracy compared to others. Additionally, the work [69] presented a robust framework known as fog-based attack detection, proposed as an efficient solution related to the fog computing technology and an ELM-based Semi-supervised Fuzzy C-Means (ESFCM) approach, the framework serves performant data analysis and enhances the speed of detection of malicious activities. Moreover, through the contribution [70] a detailed comparison study of different machine learning models was deployed to predict attacks such as DoS, spyware, malwares, misfunction of structures, and malicious on the IoMT layer. Accordingly, Table 4 listed a summary of the above contribution works, outlined different frameworks proposed by authors-based AI algorithms to address Security problems among

health monitoring systems' layers. We took into account the problems addressed and which techniques are considered to have the best accuracy in resolving the issue, along with the referring application domain and limitations of each listed framework.

Recently, the emergent AI Algorithms are the most deployed technologies in several system architectures due to the intelligence activities that can bring to systems to enable the ability to be more independent in decision-making operations, especially in critical domains such as the healthcare domain where patients' data safety is the priority, as well as the urgent need to increase the security of systems in parallel with global technological evolutions.

5 Open research challenges and future directions

The continuous development of the new e-health smart systems generation enables the intention for the research community to work in resolving most of addressed security issues related classical systems.

The vast use of IoMT devices reveal serious risks on healthcare monitoring systems in term of data privacy and security, however, deployment of a robust e-health system requires resolving the addressed issues regarding deployment of artificial algorithms and recent technologies. Additionally, the complexity of E-health systems has caused a variety of technical difficulties on different system's layer where the need for a deep study and analysis for novel protocols ensuring the protected communication through multiple IoMT devices.

Considering optimization aspect of exchanging data over the network that opens new research directions as for instance deployment of lightweight security protocols especially for limited resource devices. In the same angle, the blockchain network implementation raise multiple challenges in sharing personal data with external stakeholders due to the evolution of cyberattack threats, as for instance, working on optimize and enforce data transaction while guarantee the privacy and security by avoiding involvement of third party applications, in addition, implementing next generation access control systems for connected blockchain entities while preserving a reasonable latency and deployment costs.

Finally, the Use of AI models particularly Deep Learning, Reinforcement Learning and Machine Learning will speed up system digitalization and independency for future systems deployment, as well as the combination of Blockchain-AI technologies will mark an important enhancement in security field of healthcare systems.

Table 3. Comparison analysis of multiple AI algorithms-based security purposes [71], [72]

AI Model	Algorithm Type	Issue Type	Category	Power	Interpretability	Prediction Speed	Training Speed	Accuracy Rate
Machine Learning	Linear Regression	Regression	Supervised ML	Low	Yes	Fast	Fast	Lower
	Logistic Regression	Classification	Supervised ML	Low	Yes	Fast	Fast	Lower
	Decision Tree	Classification/Regression	Supervised ML	High	Yes	Fast	Fast	Lower
	Linear Discriminant Analysis	Classification for more than two classes	Supervised ML	Low	Medium	Fast	Fast	Higher
	Naïve Bayes	Classification	Supervised ML	Medium	Yes	Fast	Fast	Lower
	Support Vector Machines	Classification	Supervised ML	High	Medium	Fast	Fast	Higher
	K-Nearest Neighbors (KNN)	Classification/Regression	Supervised ML	Medium	Yes	Fast	Fast	Lower
	Random Forest	Classification/Regression	Supervised ML	High	Yes	Medium	Slow	Higher
	Regression tree	Regression	Supervised ML	High	Yes	Good	Fast	Medium
	K-Means	Clustering	Unsupervised ML	Medium	Yes	–	–	Lower
	Fuzzy Clustering (Fuzzy c-means)	Clustering	Unsupervised ML	Medium	Yes	–	–	Lower
	Q-Learning	Decision Making	Reinforcement Learning	High	Yes	Fast	Fast	Higher
	SARSA algorithm	Decision Making	Reinforcement Learning	High	Yes	Fast	Medium	Medium
Deep Learning	MLP (Multilayer Perception)	Classification/Regression Data Recognition	Artificial Neural Network	Medium	No	Slow	Slow	Higher
	CNN	Classification/Regression Data Recognition	Artificial Neural Network	Higher	No	Fast	Fast	Higher
	RNN	Classification/Regression Data Recognition	Artificial Neural Network	Higher	No	Fast	Fast	Higher
	LSTM (Long Short-Term Memory)	Classification/Regression Data Recognition	Artificial Neural Network	Low	No	Fast	Slow	Medium
	GAN (Generative Adversarial Networks)	Classification/Regression Data Recognition	Artificial Neural Network	Medium	No	Fast	Slow	Higher

Table 4. A summary of papers addressed security purposes regarding AI technologies-based e-Health monitoring systems

Ref	Contribution	Addressed Threats	AI Technique	Type	Category	Strength	Limitations
[63]	Detecting Malicious the node on a WSN network	Botnets, Distributed Denial of Service	RNN	Deep Learning	Security	Accurate	Scalability Interoperability
[65]	Prevent DDoS attacks on the IoT network	Distributed Denial of Service	MLP LSTM CNN LSTM Naïve Bayes Random Forest	Machine Learning Deep Learning	Security	Accurate	High time of Data Training High computation resources
[66]	Framework to deal with malware attacks in a healthcare environment	Malicious attacks	Deep-Q-Network	Reinforcement Learning	Security Privacy	–	Task offloading Lower accuracy
[62]	Analyze potential risks and enhance the authentication process	Man in the middle Attacks, Eavesdropping Attacks, Brute Force Attacks	Naïve Bayes	Machine Learning	Privacy	–	–
[20]	Secure data exchange based on an intelligent version of blockchain technology	Data leakage, Eavesdropping, replay attacks, Sniffing Data Data Tampering	DQN DDQN D3QN	Reinforcement Learning	Privacy	Transparency Immutability	High computation resources
[64]	Selecting the optimized Blockchain network	Man-in-the-middle	Dueling Double Deep Q Network	Reinforcement Learning	Security	Adaptative	Complexity High computation resources
[67]	Powerful detection of data to prevent suspicious attacks on the IoT Layer	DDoS, IoT framework weakness, Spoofing, Man-in-the-middle, and Botnets	Supervised ML Classifier	Machine Learning	Security Privacy	Accurate	Scalability
[68]	Improves Cyber risks Detection speed on WSN	Malicious Traffic	PCA, SVD, SGD, CNB	Machine Learning Deep Learning	Security	Accurate Reliable	Scalability Complexity
[69]	Data analysis from malicious attacks and improved speed of detection	Malicious emails, collusion attacks, and denial of service attacks	ELM-based Semi-supervised Fuzzy C-Means (ESFCM)	Machine Learning	Security	Accurate	High computation resources
[61]	Transparent Authentication system based on real-time entities verification through extracting user bio-features as tokens	Potential threats	Support Vector Machine with Gaussian radial basis function (SVM-GF)	Machine Learning	Security	Scalable	Lower Accuracy High computation resources

6 Conclusion

Remote Healthcare systems become necessary due to the pandemic spread and the need for providing health assistance to the elderly, thanks to the edge computing based IoMT technology that brings resources such as computing, and storage services close to the end user. However, dealing and managing sensitive patient's data introduces an important challenge in different stages of an e-health smart system. From the above sections of this paper, a brief introduction represents the main components of the e-health system. Furthermore, a detailed study revealed the benefits of incorporating Blockchain technology, as well as listing some research works adopted for e-health systems based on a decentralized structure to secure sharing medical records across different stakeholders such as hospitals, Doctors, caregivers, emergency departments and others, while the followed sections discussed multiple security mechanisms introduced by some authors deployed to secure different layers of healthcare monitoring system, which led to address the existing security issues, additionally, an analyze study of different contributions to implement the intelligent technologies algorithms based security aspect provided as countermeasures against multiple e-health Threats.

Besides the exciting role represented by AI algorithms shown as enabling system protection-driven decisions, adaptative to several situations, and high accuracy coverage, they are still causing significant challenges in the healthcare industry, for instance, missteps and serious false results with serious impact to be addressed for future deployment of this technology. The paper concludes by identifying future and open challenges to attaining the desired objectives in terms of security and privacy for the e-health smart system and its related medical data.

This paper disclosed the security and privacy drawbacks represented by e-health conventional systems due to the crucial challenges enduring to be addressed. Thus, perfect usage of intelligent algorithms and recent technologies can fulfill the remaining requirement for providing a suitable healthcare monitoring system. Furthermore, this study serves as an important basic structure for future contributions research to address unresolved security issues, particularly with the exponential deployment of connected medical devices, IoMT, where there is a need for a smart, robust, and secure architectures for further research.

7 References

[1] "Health Expenditure – OECD." https://www.oecd.org/health/health-expenditure.htm (accessed Oct. 31, 2022).

[2] "Smart Healthcare Products Market Size US$ 85.37 Bn by 2030." https://www.precedenceresearch.com/smart-healthcare-products-market (accessed Oct. 31, 2022).

[3] M. Laroui, B. Nour, H. Moungla, M. A. Cherif, H. Afifi, and M. Guizani, "Edge and fog computing for IoT: A survey on current research activities & future directions," *Computer Communications*, vol. 180, pp. 210–231, Dec. 2021, https://doi.org/10.1016/j.comcom.2021.09.003

[4] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Applied Sciences*, vol. 9, no. 9, p. 1736, Apr. 2019, https://doi.org/10.3390/app9091736

[5] T. K. Mackey et al., "'Fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare," *BMC Med*, vol. 17, no. 1, pp. 68, s12916-019-1296–7, Dec. 2019, https://doi.org/10.1186/s12916-019-1296-7

[6] A. Awad Abdellatif et al., "MEdge-chain: Leveraging edge computing and blockchain for efficient medical data exchange," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15762–15775, Nov. 2021, https://doi.org/10.1109/JIOT.2021.3052910

[7] Z. Ghias and A. Avokh, "Towards energy- and interference-aware health monitoring by using WBANs in medicine services," *Biomedical Signal Processing and Control*, vol. 73, p. 103403, Mar. 2022, https://doi.org/10.1016/j.bspc.2021.103403

[8] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT communications: A survey," *Sensors*, vol. 20, no. 17, Art. no. 17, Jan. 2020, https://doi.org/10.3390/s20174828

[9] Y. Zou and J. Lv, "Information security transmission technology in Internet of Things control system," *Int. J. Onl. Eng.*, vol. 14, no. 06, p. 177, Jun. 2018, https://doi.org/10.3991/ijoe.v14i06.8707

[10] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, Aug. 2019, https://doi.org/10.1016/j.future.2019.02.050

[11] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014, https://doi.org/10.1145/2677046.2677052

[12] H. Abrar et al., "Risk analysis of cloud sourcing in healthcare and public health industry," *IEEE Access*, vol. 6, pp. 19140–19150, 2018, https://doi.org/10.1109/ACCESS.2018.2805919

[13] Q. Wan and Y. Wang, "Exploration of wireless sensor network based on cloud computing," *Int. J. Onl. Eng.*, vol. 14, no. 11, p. 16, Nov. 2018, https://doi.org/10.3991/ijoe.v14i11.9501

[14] M. Javaid, A. Haleem, R. P. Singh, S. Rab, R. Suman, and I. H. Khan, "Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers," *International Journal of Cognitive Computing in Engineering*, vol. 3, pp. 124–135, Jun. 2022, https://doi.org/10.1016/j.ijcce.2022.06.001

[15] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems," *J Ambient Intell Human Comput*, vol. 10, no. 10, pp. 4151–4166, Oct. 2019, https://doi.org/10.1007/s12652-017-0659-1

[16] J. Xu et al., "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019, https://doi.org/10.1109/JIOT.2019.2923525

[17] B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," *Applied Sciences*, vol. 9, no. 6, Art. no. 6, Jan. 2019, https://doi.org/10.3390/app9061207

[18] C. Martín, D. Garrido, L. Llopis, B. Rubio, and M. Díaz, "Facilitating the monitoring and management of structural health in civil infrastructures with an Edge/Fog/Cloud architecture," *Computer Standards & Interfaces*, vol. 81, p. 103600, Apr. 2022, https://doi.org/10.1016/j.csi.2021.103600

[19] E. Bonnah and J. Shiguang, "DecChain: A decentralized security approach in Edge computing based on Blockchain," *Future Generation Computer Systems*, vol. 113, pp. 363–379, Dec. 2020, https://doi.org/10.1016/j.future.2020.07.009

[20] A. Z. Al-Marridi, A. Mohamed, and A. Erbad, "Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems," *Computer Networks*, vol. 197, p. 108279, Oct. 2021, https://doi.org/10.1016/j.comnet.2021.108279

[21] G. Li, Y. Dong, J. Li, and X. Song, "Strategy for dynamic blockchain construction and transmission in novel edge computing networks," *Future Generation Computer Systems*, vol. 130, pp. 19–32, May 2022, https://doi.org/10.1016/j.future.2021.12.005

[22] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2018, pp. 1545–1550. https://doi.org/10.23919/MIPRO.2018.8400278

[23] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics and Informatics*, vol. 35, no. 8, pp. 2337–2354, Dec. 2018, https://doi.org/10.1016/j.tele.2018.10.004

[24] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, https://doi.org/10.1109/ACCESS.2016.2566339

[25] S. Wang et al., "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 942–950, Dec. 2018, https://doi.org/10.1109/TCSS.2018.2865526

[26] S. R. Moosavi et al., "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Generation Computer Systems*, vol. 64, pp. 108–124, Nov. 2016, https://doi.org/10.1016/j.future.2016.02.020

[27] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, Jun. 2017, https://doi.org/10.1016/j.jnca.2017.04.002

[28] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Sep. 2016, pp. 1–3. https://doi.org/10.1109/HealthCom.2016.7749510

[29] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, Jun. 2019, https://doi.org/10.1016/j.future.2019.01.018

[30] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trustless medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017, https://doi.org/10.1109/ACCESS.2017.2730843

[31] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, Jun. 2018, pp. 49–56. https://doi.org/10.1109/SMARTCOMP.2018.00073

[32] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J Med Syst*, vol. 40, no. 10, p. 218, Aug. 2016, https://doi.org/10.1007/s10916-016-0574-6

[33] T.-T. Kuo and L. Ohno-Machado, "ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks." arXiv, Feb. 05, 2018. https://doi.org/10.48550/arXiv.1802.01746

[34] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, Sep. 2020, https://doi.org/10.1016/j.iot.2020.100227

[35] M. Sain, Y. J. Kang, and H. J. Lee, "Survey on security in Internet of Things: State of the art and challenges," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Feb. 2017, pp. 699–704. https://doi.org/10.23919/ICACT.2017.7890183

[36] H. Fotouhi, A. Čaušević, M. Vahabi, and M. Björkman, "Interoperability in heterogeneous Low-Power Wireless Networks for Health Monitoring Systems," in *2016 IEEE International Conference on Communications Workshops (ICC)*, May 2016, pp. 393–398. https://doi.org/10.1109/ICCW.2016.7503819

[37] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," in *Proceedings of the First ACM Conference on Wireless Network Security*, New York, NY, USA, Mar. 2008, pp. 140–147. https://doi.org/10.1145/1352533.1352556

[38] C. Ivan, M. Vujic, and S. Husnjak, "Classification of Security Risks in the IoT Environment," in *DAAAM Proceedings*, 1st ed., vol. 1, B. Katalinic, Ed. DAAAM International Vienna, 2016, pp. 0731–0740. https://doi.org/10.2507/26th.daaam.proceedings.102

[39] H. Eun, H. Lee, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," *IEEE Transactions on Consumer Electronics*, vol. 59, no. 1, pp. 153–160, Feb. 2013, https://doi.org/10.1109/TCE.2013.6490254

[40] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019, https://doi.org/10.1109/JIOT.2019.2935189

[41] L. M. Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on Internet of Things and cloud computing for healthcare," *Electronics*, vol. 8, no. 7, Art. no. 7, Jul. 2019, https://doi.org/10.3390/electronics8070768

[42] S. Khanji, F. Iqbal, and P. Hung, "ZigBee Security Vulnerabilities: Exploration and Evaluating," in *2019 10th International Conference on Information and Communication Systems (ICICS)*, Jun. 2019, pp. 52–57. https://doi.org/10.1109/IACS.2019.8809115

[43] L. Zhang and J. Li, "Enabling robust and privacy-preserving resource allocation in fog computing," *IEEE Access*, vol. 6, pp. 50384–50393, 2018, https://doi.org/10.1109/ACCESS.2018.2868920

[44] G. Glissa and A. Meddeb, "6LowPSec: An end-to-end security protocol for 6LoWPAN," *Ad Hoc Networks*, vol. 82, pp. 100–112, Jan. 2019, https://doi.org/10.1016/j.adhoc.2018.01.013

[45] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," *Computers & Security*, vol. 74, pp. 340–354, May 2018, https://doi.org/10.1016/j.cose.2017.08.016

[46] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Feb. 2017, pp. 477–480. https://doi.org/10.1109/I-SMAC.2017.8058395

[47] A. C. Donald and L. Arockiam, "A secure authentication scheme for MobiCloud," in *2015 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, Jan. 2015, pp. 1–6. https://doi.org/10.1109/ICCCI.2015.7218101

[48] M. Ibrahim, "Octopus: An edge-fog mutual authentication scheme," *International Journal of Network Security*, vol. 18, pp. 1089–1101, Jan. 2016.

[49] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991–3005, 2016, https://doi.org/10.1002/cpe.3485

[50] S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," in *2012 IEEE Symposium on Security and Privacy Workshops*, San Francisco, CA, USA, May 2012, pp. 125–128. https://doi.org/10.1109/SPW.2012.19

[51] F. Amato, F. Moscato, V. Moscato, and F. Colace, "Improving security in cloud by formal modeling of IaaS resources," *Future Generation Computer Systems*, vol. 87, pp. 754–764, Oct. 2018, https://doi.org/10.1016/j.future.2017.08.016

[52] P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, "Cloud computing security issues in infrastructure as a service," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 1, 2012.

[53] M. T. Sandikkaya and A. E. Harmanci, "Security Problems of Platform-as-a-Service (PaaS) Clouds and Practical Solutions to the Problems," in *2012 IEEE 31st Symposium on Reliable Distributed Systems*, Irvine, CA, USA, Oct. 2012, pp. 463–468. https://doi.org/10.1109/SRDS.2012.84

[54] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J Internet Serv Appl*, vol. 4, no. 1, p. 5, 2013, https://doi.org/10.1186/1869-0238-4-5

[55] D. Freet, R. Agrawal, S. John, and J. J. Walker, "Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS," in *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems*, Caraguatatuba Brazil, Oct. 2015, pp. 148–155. https://doi.org/10.1145/2857218.2857253

[56] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "Cloud security: Emerging threats and current solutions," *Computers & Electrical Engineering*, vol. 59, pp. 126–140, Apr. 2017, https://doi.org/10.1016/j.compeleceng.2016.03.004

[57] E. B. Chawki, A. Ahmed, and T. Zakariae, "IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors," *Procedia Computer Science*, vol. 134, pp. 328–333, 2018, https://doi.org/10.1016/j.procs.2018.07.180

[58] P. Mamoshina et al., "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, Nov. 2017, https://doi.org/10.18632/oncotarget.22345

[59] T. Chen, J. Liu, Y. Xiang, W. Niu, E. Tong, and Z. Han, "Adversarial attack and defense in reinforcement learning-from AI security view," *Cybersecur*, vol. 2, no. 1, p. 11, Mar. 2019, https://doi.org/10.1186/s42400-019-0027-x

[60] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges," *Arch Computat Methods Eng*, vol. 28, no. 4, pp. 3211–3243, Jun. 2021, https://doi.org/10.1007/s11831-020-09496-0

[61] K.-H. Yeh, C. Su, C.-L. Hsu, W. Chiu, and Y.-F. Hsueh, "Transparent authentication scheme with adaptive biometrie features for IoT networks," in *2016 IEEE 5th Global Conference on Consumer Electronics*, Oct. 2016, pp. 1–2. https://doi.org/10.1109/GCCE.2016.7800550

[62] M. T. Gebrie and H. Abie, "Risk-based adaptive authentication for Internet of Things in smart home eHealth," in *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*, New York, NY, USA, Sep. 2017, pp. 102–108. https://doi.org/10.1145/3129790.3129801

[63] J. Atiga, N. E. Mbarki, R. Ejbali, and M. Zaied, "Faulty node detection in wireless sensor networks using a recurrent neural network," in *Tenth International Conference on Machine Vision (ICMV 2017)*, Apr. 2018, vol. 10696, pp. 711–716. https://doi.org/10.1117/12.2314837

[64] T. T. Anh, N. C. Luong, Z. Xiong, D. Niyato, and D. I. Kim, "Joint Time Scheduling and Transaction Fee Selection in Blockchain-based RF-Powered Backscatter Cognitive Radio Network." arXiv, Jan. 10, 2020. https://doi.org/10.48550/arXiv.2001.03336

[65] M. Roopak, G. Yun Tian, and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2019, pp. 0452–0457. https://doi.org/10.1109/CCWC.2019.8666588

[66] A. Thakkar and R. Lohiya, "A review of the advancement in intrusion detection datasets," *Procedia Computer Science*, vol. 167, pp. 636–645, Jan. 2020, https://doi.org/10.1016/j.procs.2020.03.330

[67] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, Oct. 2019, https://doi.org/10.1109/JIOT.2019.2926365

[68] S. Mahmood Naser, Y. Hussain Ali, and D. Al-Jumeily OBE, "Hybrid cyber-security model for attacks detection based on deep and machine learning," *Int. J. Onl. Eng.*, vol. 18, no. 11, pp. 17–30, Aug. 2022, https://doi.org/10.3991/ijoe.v18i11.33563

[69] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Applied Soft Computing*, vol. 72, pp. 79–89, Nov. 2018, https://doi.org/10.1016/j.asoc.2018.05.049

[70] M. Hasan, Md. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, Sep. 2019, https://doi.org/10.1016/j.iot.2019.100059

[71] F. Malik, "Machine Learning Algorithms Comparison," *FinTechExplained*, Oct. 01, 2018. https://medium.com/fintechexplained/machine-learning-algorithm-comparison-f14ce372b855 (accessed Oct. 31, 2022).

[72] "Comparing supervised learning algorithms," *Data School*, Feb. 27, 2015. https://www.dataschool.io/comparing-supervised-learning-algorithms/ (accessed Oct. 31, 2022).

8 Authors

Hamza Rafik is PhD student at RITM – ESTC/CED – ENSEM Hassan II University in Casablanca, Morocco. His current research interest turns around security, and privacy measures and methodologies, as well as data analytics features for a Healthcare monitoring smart systems-based edge computing systems (email: hamza.rafik-etu@etu.univh2c.ma).

Abderrahim Maizate an Associate Professor works at the Department of Computing Science, Hassan II University of Casablanca. His research interests include fields such as Wireless communications, WSN, smart cities, NDN, AI, Virtualization, cloud computing and security (email: abderrahim.maizate@univh2c.ma).

Abdelaziz Ettaoufik an Associate Professor at the Department of Mathematics and Computer Science, FS Ben M'SIK Hassan II University Casablanca. His research fields interest includes big data, cloud et security, IoT, blockchain, and IA (email: abdelaziz.ettaoufik@etu.univh2c.ma).

Article submitted 2022-11-28. Resubmitted 2023-01-15. Final acceptance 2023-01-15. Final version published as submitted by the authors.