Towards a Smart Healthcare System:
An Architecture Based on IoT, Blockchain, and Fog Computing

Laila Fetjah, University Hassan II of Casablanca, Morocco

Kebira Azbeg, University Hassan II of Casablanca, Morocco

https://orcid.org/0000-0003-3014-6281

Ouail Ouchetto, University Hassan II of Casablanca, Morocco

https://orcid.org/0000-0001-8287-215X

Said Jai Andaloussi, University Hassan II of Casablanca, Morocco

ABSTRACT

With the rapid development in smart medical devices, internet of things has a large applicability in the healthcare sector. The current system is based on a centralized communication with cloud servers. However, this architecture increases security and privacy risks. This paper describes an architecture of a smart healthcare system for remote patient monitoring. To ensure security and privacy, the architecture uses blockchain technology. For data analysis, smart contracts and artificial intelligence are used. The architecture is divided into three layers: smart medical devices layer, fog layer, and cloud layer. To validate the proposed approach, a scenario based on diabetes management system is described. The architecture is applied to provide remote diabetic patient monitoring. The system could suggest treatments, generate proactive predictions, and predict future complications as well as alerting physicians in case of emergency.

KEYWORDS

Artificial Intelligence, Blockchain, Fog Computing, Healthcare, Internet of Things, Remote Patient Monitoring, Smart Contracts

1. INTRODUCTION

Recently, there has been a steady increase in the use and applications of smart objects. Today, we are embracing the world of connected things with the number of Internet of things (IoT) devices growing exponentially. In Gartner's predictions, the number of Internet-connected devices will soon reach 20 billion this year (Hung, s. d.). In 1999, Kevin Ashton coined the IoT expression, referring it to a set of devices that can interact via the Internet (Ashton, s. d.). These interconnected devices range from smart phones, autonomous vehicles, wearables and many other electronic devices with embedded processors to be operated via network connectivity and sensors to collect, store, process and exchange massive amounts of data. The IoT architecture often segments into different layers, including sensor (smart device), network, management service and application layer (Patel, Patel & Scholar, 2016).

Beyond the general business sectors, IoT devices are now increasingly being used in the health care sector (Catarinucci et al., 2015). IoT capabilities may, in fact, be embedded in almost all types

DOI: 10.4018/IJHISI.20211001.oa16

of healthcare applications to facilitate patient care and achieve real-time patient monitoring, while collecting meaningful health data. Further, these data can be transferred remotely to a physician to execute a diagnosis. In this way, remote monitoring to all patients can be provided 24/7 by the medical team (Rahman et al., 2019). Every year, thousands of such devices join the Internet connection, enabling data to be exchanged via centralized servers in the cloud. Existing architecture raises several challenges in security risks, privacy preservation as well as bandwidth limitation and high latency. Importantly, emerging technologies such as fog computing (FC) and Blockchain can enhance IoT capabilities to overcome multiple privacy-security and other challenges (Tariq et al., 2019; Dorri et al., 2017).

In this paper, smart healthcare system architecture for remote patient monitoring is being studied. Drawing on emerging technologies such as Blockchain, FC and artificial intelligence (AI), the system will assess the individual patient health situation to respond. Such architecture will help provide medical data via advanced smart medical devices to share needed information with the medical team. Blockchain thus ensures data security via smart contract (SC), FC and AI while performing data analysis. With such architecture, patients will be able to check their health regularly via real-time medical data collection while safely sharing the information with their physicians. Purportedly, the system gives patients total control and the right to limit access to these sensitive data. Physicians can also monitor their patients regularly and perform real-time analysis. The system can also accelerate the diagnosis process and help in the disease treatment while alerting the physician in emergencies.

We organize the rest of this paper as follows. Section 2 provides the research background, emphasizing related works on the use of IoT, FC, blockchain and AI in the healthcare sector. Next, the proposed novel approach towards building smart healthcare systems architecture is described in Section 3. Following this, Section 4 illustrates a use case via applying the proposed architecture for diabetes management. Finally, Section 5 concludes the paper with insights on research limitations, practical implications and future works.

2. RELATED WORKS

With technological advances such as IoT, FC, blockchain and AI being widely integrated into the healthcare industry to improve patient care services and promote healthy lifestyles, we review here the key relevant works that engulfed the thinking of current research.

2.1 Health Care, IoT & FC

Recent IoT developments and related advances have considerably increased the number of IoT devices that could better connect patients into the different domains of health and human life.

Owing to the proliferation of medical devices, sensors and electronic wearables, the healthcare industry is experiencing phenomenal growth. Nowadays, IoT is embedded in different healthcare applications, such as clinical care, context-awareness and remote monitoring (Dhanvijay & Patil, 2019). Over the past decade, many healthcare systems have been designed to monitor various health parameters. Some of these systems highlighted by Kumar (2017) include blood glucose, temperature, and heart rate monitoring systems for elderly people.

IoT devices collect, store and process data automatically via sensors. The amount of such data is increasing rapidly; even then, some key limitations exist with the capabilities of IoT devices, for example, limited storage capacity and low-power computation. Despite such limitations, the combination of IoT and cloud will work to overcome many of these challenges by providing enormous additional storage capabilities, computing power and data analytics. Notwithstanding, many issues regarding security, privacy, latency and response time remain to be resolved. This is why FC can play an important role as an intermediate layer between IoT devices and cloud computing or CC (Atlam, Walters & Wills, 2018).

Created by Cisco, FC is a decentralized computing infrastructure (Bonomi et al., s. d.) with the underlying idea of extending the cloud to where things may be by bringing CC capabilities to the edge of IoT devices. FC enables instant data processing and real-time analysis via local handling of the data collected by IoT devices and sensors. It also allows data filtering to reduce the amount of data sent to the cloud. The coupling of IoT-FC has been applied across various sectors, including smart city and home (Kanyilmaz & Cetin, 2019), renewal energy, smart manufacturing, transportation, logistics and health care (Atlam, et al., 2018). In healthcare IoTs, FC has been widely adopted, especially for applications requiring low latency and real-time processing. In systematically reviewing the literature, Mutlag et al. (2019) note the performance of integrating FC in healthcare IoTs and discuss different systems, architecture and models that have been proposed for integrated FC infrastructure.

For securing distributed cloud architecture, Sharma et al. (2018) propose combining CC with FC, Software Defined Networking (SDN) and Blockchain. In contrast, Kumari et al. (2018) propose the building of e-health architecture via three layers: (a) medical device layer; (b) fog layer and (c) cloud layer. Using illustrative examples of possible attacks, Ni et al. (2018) survey different security threats in FC, aside from reviewing solutions to secure FC, and identify some ways of enhancing security-privacy in FC such as via the Blockchain as a secure layer between the cloud and IoT devices. In short, the fog layer could be more secured and efficient by storing, for example, log files in the Blockchain, which will be used to detect a misbehaving fog node. Finally, Rahman & Wen (2018) overview FC architecture and offer some examples of real-time FC applications apart from identifying various challenges that are still facing FC architecture implementation in respect to security-privacy and authentication of data.

2.2 Healthcare and Blockchain

Bitcoin, the first cryptocurrency created by Satochi Nakamoto (Nakamoto, 2008), is the underlying conceptualization for Blockchain. This technology embodies a decentralized ledger or a distributed database that allows both the storage and transmission of transactions. Blockchain has four major characteristics: it is secure, immutable, transparent and does not need a third party to ensure communication and/or store data. Allowing in-between node interactions via a peer-to-peer transmission, Blockchain is essentially a succession of blocks with chronologically recorded transactions. Each block is linked to the previous one via a cryptographic hash. The hash value is unique, identifies one block, and is calculated by hashing the block's entire content.

Additionally, Blockchain uses other security elements such as block creation and validation via a process called "mining" that prevents the tampering of the Blockchain's immutability, thereby supporting the replication of data on all several nodes that are linked via the Blockchain network. In the process, a full history of all transactions, which ensures the data's traceability, can be preserved.

Three types of Blockchain may be distinguished:

- **Public:** A public Blockchain, where everyone in the world may have access to the ledger, sends transactions and check them; this type of blockchain is used in cryptocurrencies such as Bitcoin and Ethereum (Buterin et al., 2014). Here, all nodes can participate freely in the consensus process.
- **Private:** No one can participate in this type of Blockchain without permission; specifically, the consensus process here is controlled by a restricted and selected number of nodes belonging to a single organization.
- **Consortium:** Access to data in this type of Blockchain may be public or private as it is partially decentralized; that is, it is a hybrid. Here, just as with a hyperledger (Cachin, s. d.), several actors, instead of a single organization, control the consensus process.

Many works have been performed to secure medical records via the Blockchain. Azaria et al. (2016) propose an architecture in which smart contracts are employed for permission managing and for medical data access. These researchers advocate using the Ethereum Blockchain to deploy specific smart contracts that will allow patients to manage access to their own medical data. Liang et al. (2017) propose using a mobile application that allows the collection of health data to be shared with healthcare providers and insurance companies. These researchers advocate storing access control policies via a permissioned blockchain based on Hyperledger Fabric (HF) to ensure both privacy and integrity in the recorded transactions.

McGhin et al. (2019) highlight the challenges and opportunities of using Blockchain in health care. These researchers survey different applications that used Blockchain in the healthcare sector and argue the benefits of applying Blockchain, given that it has features that meet the multifaceted health care requirements. Key benefits include (a) the storage and sharing of health data via a decentralized network, which is secure and scalable; and (b) it may be fully authenticated, preserving data integrity and access security. The most common challenges alluded to include attacks specific to Blockchain, scalability, the urge or incentive to mine Blockchain, and key leakage. Aside from healthcare applications, Blockchain may be applied in several other sectors such as supply chain (Wang et al., 2020; Venkatesh et al., 2020), electronic vote (Noizat, 2015), education (Liu et al., 2018), and insurance (Roriz & Pereira, 2019).

Finally, Ancile has been proposed as another framework to manage access control and increase the interoperability for electronic health records (EHR). Whereas patient data will continue to be stored in the providers' databases, this framework functions like a permissioned Ethereum Blockchain, which is used to store access permission and references to data. The framework provides six types of smart contracts to define permissions and execute other operations (Dagher et al., 2018). Rifi et al. (2017) propose using a gateway to handle data generated by sensors, an off-chain database to store the data and smart contracts deployed in an Ethereum Blockchain so as to manage access to the data.

2.3 Healthcare and AI

AI, a branch of computer science aiming to create systems and machines that can work and behave independently and intelligently, combines methods, techniques and algorithms to enable machines to emulate human intelligence. One key AI approach is Machine learning (ML), a subset of AI that enables machines to learn from examples just as humans learn from experiences. Here, machines are purposely programmed to analyze a set of predetermined behaviors and/or supervised (trained) patterns via predefined models to enable the embedded software to become smarter over time.

AI can aid physicians in diagnosing medical problems more efficiently and make more effective clinical decisions so as to impact positively on clinical best practices (Jiang et al., 2017). Today, AI technology is becoming ubiquitous, showcasing its potential in almost every aspect of human living. In health care, AI has been applied for clinical diagnosis, prognosis, health-related discovery and assistive servicing, medical records management and assistive surgery via robots (Murali1 & Sivakumaran, 2018; Rajabi Shishvan et al., 2018). Specifically, recent works have proposed the use of novel approaches based on ML algorithms to analyze and interpret medical data. These interpretations can then be used to identify and manage diseases, and in some cases, even generate proactive predictions, for example, a recent study has demonstrated the efficiency of using deep learning for image recognition to analyze 2D X-ray images in order to identify suspicious lesions and nodules in lung cancer patients (Gordienko et al., 2019).

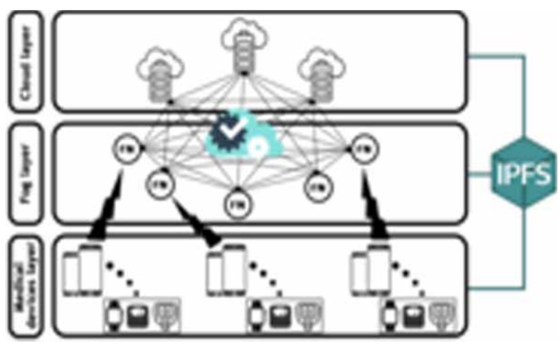
As noted, in changing the healthcare industry, IoT has become a significant source of medical data. The nature of these data requires fast and intelligent processing; indeed, a 2018 survey has provided a detailed classification of algorithms for IoT data analysis (Mahdavinejad et al., 2018). Separately, Shah et al. (2018) propose a solution to detect the freezing of gait in patients with Parkinson disease via body-mounted sensors set on the leg and hip of the patient. Ara & Ara (2017) treat a case study based on a diabetes management solution developed by Zion China, a startup venture focusing on IoT in health care. Their work highlights the modifications done by Zion China to improve the intelligence of their system. Today, Zion China[1] has evolved the Ara-Ara solution by integrating IoT, streaming analytics and Azure ML to generate a proactive prediction on glucose patient data.

Most recently, Rajan et al. (2020) have proposed a method for oral cancer identification in a novel system based on FC and IoT. Their method uses deep convolutional neural network (CNN) to detect cancer region from data and improve the classification accuracy. A modified vesselness measurement is used for filtering and noise handling.

3. RESEARCH METHODOLOGY

The Health Insurance Portability and Accountability Act (HIPPA) defines a set of rules to protect the patients' privacy so as to ensure the confidentiality, integrity and the security of their health data (HIPAA Compliance: 2019). HIPAA is part of the United States (US) legislation governing the use of health data worldwide; indeed, other regulatory standards of countries such as the European union Directive on Data Protection (1998) and Canada's PIPEDA also exist to guide the handling of patient information in order to preserve the privacy and security of such information transmission. This paper proposes the architecture for remote patient monitoring. As shown in **Figure 1**, by combining a set of technologies, including IoT devices, Blockchain, FC and CC, our proposed architecture, that will be HIPAA-compliant, may be compartmentalized into three layers: (a) medical devices layer; (b) fog layer; and (c) cloud layer.

Figure 1. A general overview of our architecture



- *Medical Devices Layer*

This layer captures the patient's data, encrypts them, and sends them to be stored in the IPFS. A decentralized application (Dapp) is used to interact with the Blockchain in the next layer. With Dapp, one can interact with one's physician, grant and/or revoke access, add and/or delete devices while having total control over one's data and devices.

More specifically, a set of medical devices first acts to collect different health measurements such as blood pressure, glucose level, sleep patterns, heart rate and patient's weight, which are necessary to track one's health and wellness. Smart medical devices such as electronic wearable(s) and smart sensors are then employed to automatically capture one's health data and track one's physical activity prior to forwarding these data to one's smart-phone. The smart-phone will then encrypt the data before sending them to the IPFS for storage.

- *Fog Layer*

An intermediate layer sandwiched between medical devices and the cloud nodes, the fog layer comprises a set of interconnected nodes called fog nodes. These nodes are used to process data and provide real-time analysis to the patient. A Blockchain network assures the connection among these nodes and the analysis is assured by the smart contracts deployed in the Blockchain network.

- *Cloud layer*

Supporting a high computing capacity and distributed storage, this layer comprises a set of nodes connected to the previous layer by the same Blockchain network. All participating nodes belonging to hospitals, pharmacies, clinics and public health organizations in this layer will constitute a distributed cloud. Notably, these nodes are used as mining nodes for our Blockchain.

The cloud layer also provides the ability to physicians to follow their patients' health and supports other organizations with the ability to extract information for statistical and research purposes. Here, the linked entities can use AI to analyze and interpret patient data to suggest treatments, identify diseases or generate proactive predictions.

3.1 Role of Blockchain in Architecture

In architecture, the Blockchain technology is used for many reasons:

- Secure the data and preserve the data privacy;
- Handle access control for devices - each device owner in the Blockchain registers its presence; thus, all devices are already accounted by the Blockchain - the unknown devices will not be able to send data unless it also has an *a priori* registration;
- Handle access control for linked healthcare institutions;
- Store a link to data stored in the IPFS to protect data integrity and non-repudiation;
- Ensure data traceability; and
- Provide real-time analysis by hosting ML models in the Blockchain.

The Blockchain allows the creation of smart contracts to ensure all of these functionalities. Smart contracts are programs that can be executed and triggered automatically when some predefined conditions have been attained. In this paper, smart contracts are used to: define access policies and verify the authentication, register or delete devices, grant or revoke access to data, create logs for traceability by creating a history of all events and operations made on the data. These contracts can also be used to send alerts to healthcare providers in emergencies. The collected measurements are analyzed by comparing them with the threshold values or via ML models to yield diagnosis, predict diseases and propose treatments.

4. USE CASE: DIABETES MANAGEMENT

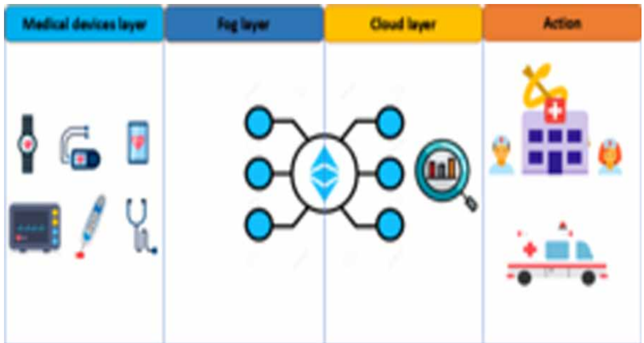
Given the discussed architecture is general, it may be applied to various healthcare applications. To validate the approach, the architecture is illustrated for diabetes management.

Diabetes is a chronic illness that requires one to checkup regularly; also, serious self-care is often needed for one to monitor one's disease progression in order to remain healthy. People with diabetes should therefore adopt a healthy lifestyle with regular self-management to prevent future exacerbations.

To project the architecture for the diabetes application, we express here the composition of the three layers as depicted in **Figure 2**:

- **Medical devices layer:** Nowadays, a growing variety of smart and wearable devices are available for people with diabetes to monitor their glucose levels, blood pressure and to track their daily

Figure 2. The proposed architecture applied to a diabetes management system



activities. Such devices come in many forms, including smart watches, contact lenses, socks or even artificial pancreas, and more. Not surprisingly, these same devices are not only being used to collect the necessary health data, but for automated diabetes management. The data gathered are then forwarded to a smart phone to be encrypted and sent to the IPFS.

- **Fog layer**: Here, a permissioned Ethereum Blockchain can be used to ensure the connection between fog nodes while linking them to the cloud nodes (Healthcare institutions). As noted earlier, Dapp, which provides interfaces that allow a patient to act variously by interacting with different smart contracts, can be deployed here to interact with the Blockchain, serving as the application back end. Thus, instead of using a central server, the application is linked to Blockchain nodes that run smart contracts. After the application installation and registration, each patient will have access to different functionalities informed by transactions. These transactions may be performed for different purposes like to register or remove a device, grant or remove access to the data, store hash data, access to data and provide real-time analysis.
- **Cloud layer:** Here, a distributed cloud is created and nodes are connected to the previous layer via the Blockchain. Concerning using AI for diabetes apps, there are diverse methods as noted by Contreras & Vehi (2018), depending on the purpose: learning how to use information (ANN or artificial neural networks, SVM or support vector machines, NB or Naive Bayes, regression algorithms, etc.), discovering and exploring (k-means, k-nearest neighbor, and so on) or reasoning from information (rule-based reasoning, fuzzy logic, and more).

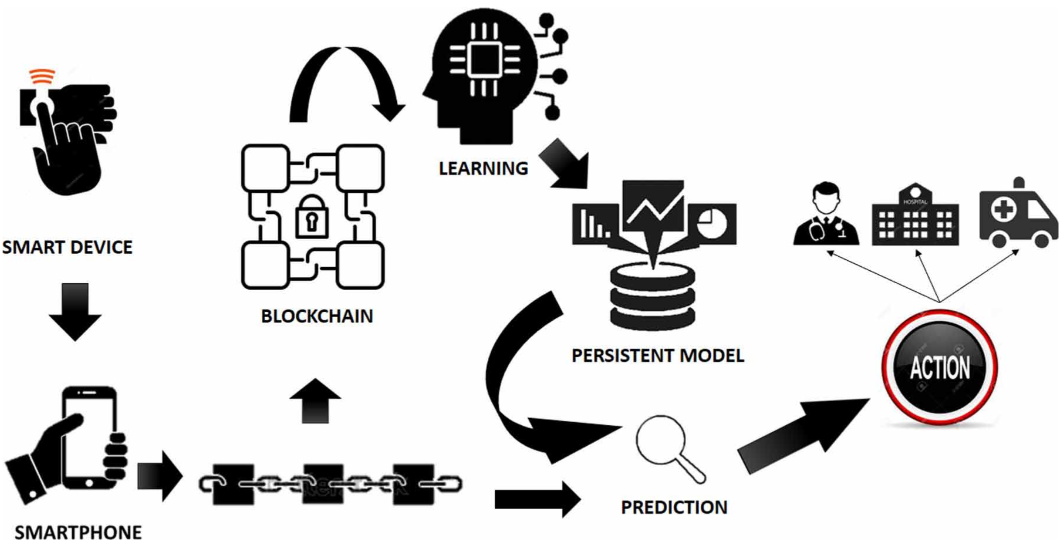
4.1 Demonstration Scenario

In demonstrating the efficiency of the proposed architecture, a full scenario of a diabetes management system will now be presented.

A diabetic patient, after installing the Dapp in his smart phone, can be registered in the Blockchain network with a unique identification (Ethereum address). Once registered, the patient is able to further register his devices in the Blockchain via his smart phone and the Dapp interface. Each device will be identified by a unique set of values; that is, its mac address and the address of its owner (Azbeg et al., 2018). Hence, no one can add a device except the owner himself or herself and just data from the registered devices can or will be accepted. In this sense, the patient can have total control over his/her devices and can be protected against malicious devices.

After registration, each device can then forward the collected data to the IPFS via the smart phone. In the fog layer, a smart contract will analyze the data via a ML model. Then, it will either provide advice to the patient and/or send an alert to the medical team. In emergencies, the system can alert the physician to instruct an ambulance on assisting the patient. For example, one of the most common emergencies with a diabetes patient is hypoglycemia. This can happen when the level of blood sugar is too low. Loss of consciousness is one of the warning signs and it is considered an emergency calling for medical attention. The system can also check the hospital medications stock to verify if the necessary medications are available in stock or not. If a specific drug is unavailable, the system can automate an order to the associated pharmacy. The forwarded data are stored in the IPFS and will be the object of further analysis via ML algorithms to predict diabetes complications, for example. Using the system, a database of medical data of all diabetic patients may be created. This database will then be used to train the ML algorithms so that they can predict possible complications or future danger. Hence, the medical team can take appropriate actions and provide a suitable treatment, **Figure 3**.

Figure 3. Conceptual architecture of the approach. The system is based on two main steps: the learning mode: the system based on the history of multitudes of cases (complete life cycle), then a persisted model is created. The test mode: when the device provides new information related to a patient, the system predicts the state from the persisted model, then a system will react according to the gravity of the situation (send an alert in serious situations)



4.2 ML for Diabetes Prediction

ML is a form of AI that allows computers to learn without having been explicitly programmed for that purpose. In the medical field, the data are generally labeled. Therefore, supervised learning and more specifically classification algorithms will be utilized. They use different parameters (height, weight, frequency of sport, etc.) to determine whether an individual is likely to be diabetic or not. This paper looked at the following four algorithms: Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), and Support Vector Machine (SVM).

The paper split the dataset into two parts (70% - 30%), one to create the model (training) and another to test the model. A simple and effective way to evaluate the model is to look at the confusion matrix shown in **Table 1**:

The Receiver Operating Characteristic (ROC) curves a graphical plot that illustrates the diagnostic ability of a binary classifier system as its discrimination threshold is varied. It takes into account the sensitivity and specificity, making it possible to evaluate a model with binary output. The computation process entails: first, the ROC curve of the algorithm, and second, the area under the curve (values between 1 and 0.5). The closer the area is to 1, the more relevant the model would be.

Table 2 summarizes results of the algorithms realized with the programming language R.

Table 1. Confusion matrix

	Predicted	
	Positive	Negative
Actual true	True positive	False negative
Actual false	False positive	True negative

Precision = (TP+TN)/(TP+FN+TN)

Table 2. Comparison of the four algorithms

Algorithm	Execution Time	Precision	ROC Curve
Logistic regression	7 minutes	91,69%	0,91
Decision Tree	3 secondes	90,59%	0,5
Random Forest	37 minutes	94,31%	0,92
Support vector machine	5 heures	90,58%	0,5

Sensibility = TP/(TP+FN)
Specificity = TN/(TN+FP)

For the current project, it may be inferred that the RF is the most suited algorithm. This work uses the Frankfurt hospital diabetes dataset (Germany)[2], which contains data of 2,000 patients. Each instance has 9 attributes. **Table 3** shows the extraction of the first 20 samples from the dataset, predicting the 'Outcome' characteristic with 0 meaning no diabetes, and 1, diabetes. Of these 2,000 data points, 1,316 are labeled as 0 and 684 as 1 as depicted in **Figure 4**.

Figure 5 shows the distribution of different attributes in the dataset. On examining the graph, we realized that the Insulin and skin-thickness graphs had outliers. For example, it is scarce to have a zero value for the insulin attribute. Thus, the next step is to clean the data via one of these techniques: removing these outliers, avoiding the use of this feature (as it has many outliers) or using just the average values.

4.3 Comparative Study of Algorithms

The RF gives an accuracy of 96.4% (**Table 4**), which is better than the LR model or a single DT, without any adjustment. However, the max_features parameter can be adjusted to see if the result may be improved.

Here, max_depth = 3, limiting the depth of the tree decreases over-adaptation. This leads to less accuracy on the training set (0,800), but an improvement over the test set (0,760). Thus, the RF is the algorithm most adapted to this project as show in **Figure 6**.

Figure 7 shows the importance of each feature in the RF drill. The importance of functionality evaluates the importance of each feature for the decision made by a tree. It is a number between 0 and 1 for each characteristic, where 0 means "not used at all" and 1 means "perfectly predict the target". Features always boil down to 1: "Glucose" is by far the most important feature.

In the same way as the single DT, the RF also places a lot of importance on the "Glucose" function, but it also chooses "BMI" as the second most informative feature. The random nature of the construction of the RF forces the algorithm to take into account many possible explanations. As a result, the RF captures a much larger image of the data than a single tree.

Table 3. Diabetes dataset of Frankfurt hospital (Germany)

	Pregnancies	Glucose	Blood Pressure	SkinThickness	Insulin	BMI	Diabetes Pedigree Function	Age	Outcome
1	2	138	62	35	0	33.6	0.127	47	1
2	0	84	82	31	125	38.2	0.233	23	0
3	0	145	0	0	0	44.2	0.63	31	1
4	0	135	68	42	250	42.3	0.365	24	1
5	1	139	62	41	480	40.7	0.536	21	0
6	0	173	78	32	265	46.5	1,159	58	0
7	4	99	72	17	0	25.6	0.294	28	0
8	8	194	80	0	0	26.1	0.551	67	0
9	2	83	65	28	66	36.8	0.629	24	0
10	2	89	90	30	0	33.5	0.292	42	0
11	4	99	68	38	0	32.8	0.145	33	0
12	4	125	70	18	122	28.9	1,144	45	1
13	3	80	0	0	0	0	0.174	22	0
14	6	166	74	0	0	26.6	0.304	66	0
15	5	110	68	0	0	26	0.292	30	0
16	2	81	72	15	76	30.1	0.547	25	0
17	7	195	70	33	145	25.1	0.163	55	1
18	6	154	74	32	193	29.3	0.839	39	0
19	2	117	90	19	71	25.2	0.313	21	0
20	3	84	72	32	0	37.2	0.267	28	0

Figure 4. Outcome: the number of diabetic and non diabetic patients

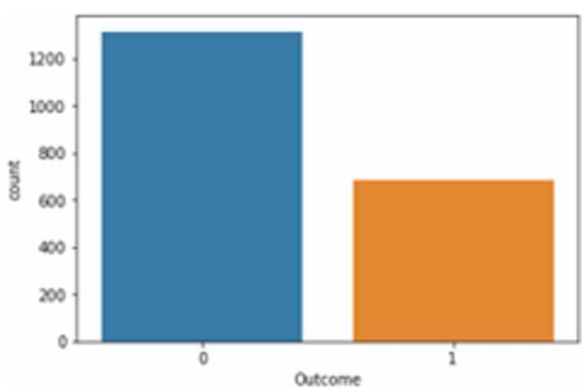


Figure 5. The distribution of different attributes in the dataset

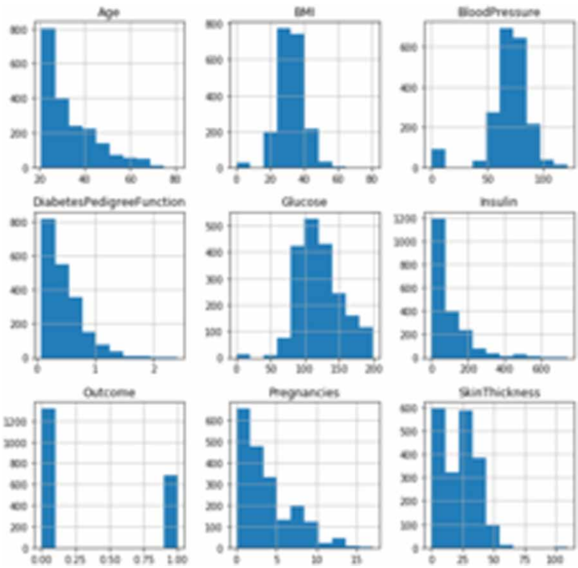


Table 4. Comparative of accuracy on training set and test set

Algorithm	Accuracy on training set	Accuracy on test set
Decision tree	*1*	0,964
Logistic regression	*0,777*	0,776
Random Forest	*1*	0,964
Support vector machine	*0,777*	0,778

Figure 6. Receiver operating characteristic

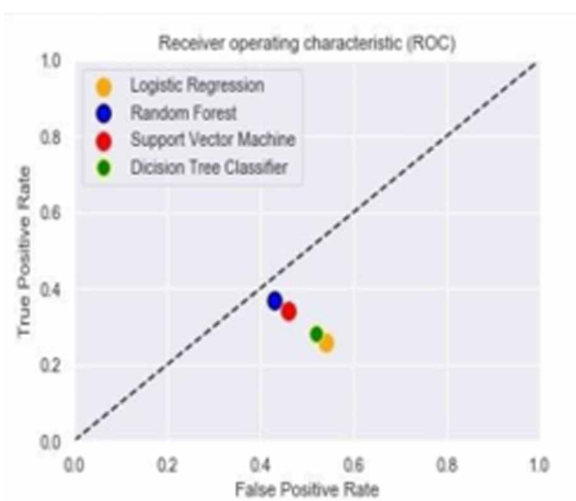
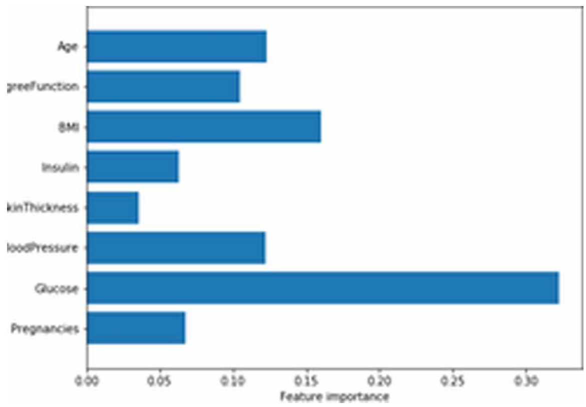
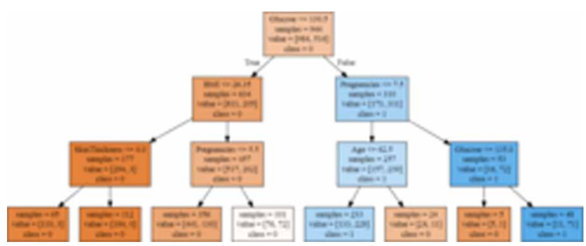


Figure 7. Importance of each feature in the decision tree



In **Figure 8**, a DT is a ML algorithm based on the representation of choices in the graphical form of a tree with different classification decisions (outcomes) placed in the leaf node. The nature of its representation gives an easy understanding and interpretation.

Figure 8. Decision tree model



- The root node split in this tree started with the Glucose attribute;
- Samples: This is the number of samples whose glucose value is less than 130,5;
- Value: Returns the total number of samples for result "0" and "1", for example, in the root node, the value 811 (represents the class "0") is greater than 203 (represents the class "1"), so that this node is classified in the class "0";
- Class: Diabetic - "1" or non-diabetic - "0".

4.4 Features of Architecture

By combining a set of powerful technologies such as IoT, Blockchain, Dapp, FC, CC, and AI, this architecture offers many advantages regarding security, data analysis, predictions, speed of data treatment and reliability as shown in **Figure 9**.

Despite these features, there are still some challenges that could face the implementation of this model. On the one hand, as the architecture is based on IoT devices for data collection, in terms of scalability (Atlam, et al., 2018), it will generate a large amount of data. Thus, a large amount of resources for data processing and storage will also be needed. On the other hand, for privacy reasons, we used a permissioned Blockchain; however, it will limit the access of data for AI (Salah et al., 2019). Therefore, AI processed data will be limited to those data provided by patients using

Figure 9. The advantages of the architecture

the current system. The challenge to draw from additional data sources may be overcome by using oracles, which are external data sources.

5. CONCLUSION AND DISCUSSION

We presented here a novel architecture based on the use of several emerging technologies, namely, Blockchain, IoT, FC and AI for the healthcare systems. Different works were proposed in the literature to secure IoT via Blockchain (Dorri et al., 2017) or to combine IoT-FC with ML for the healthcare sector (Ara & Ara, 2017; Kumari et al., 2018). Here, an architecture that combines all these technologies to benefit from an integration of their features has been advanced. To validate the proposed approach, a diabetes use case was illustrated. Four (4) ML algorithms were used in order to predict diabetes: LR, DT, RF, and SVM. These algorithms were applied to the Frankfurt hospital diabetes dataset with the RF yielding the best accuracy of 96.4%. While this accuracy is high, the application of these algorithms to other datasets is something to be considered in the future; that is, as the accuracy of an algorithm depends on the type of data used in terms of dimension, origin and data nature (Kavakiotis et al., 2017). Therefore, the authors plan to test these various algorithms with other datasets in the near future. Among these datasets, the plan would be to use the created database via data collected with patients' IoT devices. In this way, a dataset with a large amount of data will be available. In addition to predicting diabetes, the dataset could be used to predict possible diabetes complications, for example.

However, the operational mechanism of today's health-related systems has some limitations. One of the most limitation is the scalability issue especially in relation to the volume of data involved. It is not optimal to store the high-volume health data on blockchain as this could cause serious performance issues such as performance degradation or increased response times. As a countermeasure to the problem of scalability, we could propose to store only some condensed information about the data and how they can be accessed on the blockchain and the encrypted health data "off-chain ". Another limitation is interoperability challenge. Indeed, there is not yet an existing standard for developing blockchain-based healthcare applications. That said applications developed on different platforms or by different vendors may not be able to interoperate.

Altogether, we advance healthcare system architecture for remote patient monitoring and management, providing a full handling of data from information gathered from IoT medical devices to the storage and data analysis in the cloud. Additionally, we demonstrate how the healthcare sector can benefit from recent technological advancements and show how these technologies may be jointly leveraged to create a secure and smart system. As a use case, we applied the architecture to the diabetes management system to follow-up, monitor diabetic patients remotely, and predict future complications. The system could also react by alerting the physician and hospital during emergencies. It is hoped that future research will expand our model in the Blockchain network to strengthen the proof of concept with data to further validate our approach.

ACKNOWLEDGMENT

This research was supported by the National Center for Scientific and Technological Research (CNRST).

REFERENCES

Ara, A., & Ara, A. (2017). Case study: Integrating IoT, streaming analytics and machine learning to improve intelligent diabetes management system. *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*. doi:10.1109/ICECDS.2017.8390043

Ashton, K. (n.d.). *That "Internet of Things" Thing*. Academic Press.

Atlam, H., Walters, R., & Wills, G. (2018). Fog Computing and the Internet of Things: A Review. *Big Data and Cognitive Computing*, *2*(2), 10. doi:10.3390/bdcc2020010

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*. doi:10.1109/OBD.2016.11

Azbeg, K., Ouchetto, O., Andaloussi, S. J., Fetjah, L., & Sekkaki, A. (2018). Blockchain and IoT for Security and Privacy : A Platform for Diabetes Self-management. *2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)*, 15. doi:10.1109/CloudTech.2018.8713343

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (n.d.). *Fog Computing and Its Role in the Internet of Things*. Academic Press.

Cachin, C. (n.d.). *Architecture of the Hyperledger Blockchain Fabric*. Academic Press.

Catarinucci, L., de Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Tarricone, L. (2015). An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal*, *2*(6), 515526. doi:10.1109/JIOT.2015.2417684

Contreras, I., & Vehi, J. (2018). Artificial Intelligence for Diabetes Management and Decision Support : Literature Review. *Journal of Medical Internet Research*, *20*(5), e10775. doi:10.2196/10775 PMID:29848472

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile : Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283297. doi:10.1016/j.scs.2018.02.014

Dhanvijay, M. M., & Patil, S. C. (2019). Internet of Things : A survey of enabling technologies in healthcare and its applications. *Computer Networks*, *153*, 113131. doi:10.1016/j.comnet.2019.03.006

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an Optimized BlockChain for IoT. *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI '17*. doi:10.1145/3054977.3055003

Haider Shah, S., Iqbal, K., & Riaz, A. (2018). Constrained Optimization-Based Extreme Learning Machines with Bagging for Freezing of Gait Detection. *Big Data and Cognitive Computing*, *2*(4), 31. doi:10.3390/bdcc2040031

Hung, M. (n.d.). *Gartner Insights on How to Lead in a Connected World*. Academic Press.

Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017). Artificial intelligence in healthcare : Past, present and future. *Stroke and Vascular Neurology*, *2*(4), 230243. doi:10.1136/svn-2017-000101 PMID:29507784

Kanyilmaz, A., & Cetin, A. (2019). Fog Based Architecture Design for IoT with Private Nodes : A Smart Home Application. *2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*. doi:10.1109/SGCF.2019.8782400

Kavakiotis, I., Tsave, O., Salifoglou, A., Maglaveras, N., Vlahavas, I., & Chouvarda, I. (2017). Machine Learning and Data Mining Methods in Diabetes Research. *Computational and Structural Biotechnology Journal*, *15*, 104116. doi:10.1016/j.csbj.2016.12.005 PMID:28138367

Kumar, N. (2017). IoT architecture and system design for healthcare systems. *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*. doi:10.1109/SmartTechCon.2017.8358543

Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Fog computing for Healthcare 4.0 environment : Opportunities and challenges. *Computers & Electrical Engineering*, *72*, 113. doi:10.1016/j.compeleceng.2018.08.015

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 15. doi:10.1109/PIMRC.2017.8292361

Liu, Q., Guan, Q., Yang, X., Zhu, H., Green, G., & Yin, S. (2018). Education-Industry Cooperative System Based on Blockchain. *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. doi:10.1109/HOTICN.2018.8606036

Mahdavinejad, M. S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., & Sheth, A. P. (2018). Machine learning for internet of things data analysis : A survey. *Digital Communications and Networks*, *4*(3), 161175. doi:10.1016/j.dcan.2017.10.002

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications : Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 6275. doi:10.1016/j.jnca.2019.02.027

Murali & Sivakumaran. (2018). *Artificial Intelligence in Healthcare-A Review*. Unpublished. 10.13140/rg.2.2.27265.92003

Mutlag, A. A., Abd Ghani, M. K., Arunkumar, N., Mohammed, M. A., & Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, *90*, 6278. doi:10.1016/j.future.2018.07.049

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf

Ni, J., Zhang, K., Lin, X., & Shen, X. S. (2018). Securing Fog Computing for Internet of Things Applications : Challenges and Solutions. *IEEE Communications Surveys and Tutorials*, *20*(1), 601628. doi:10.1109/COMST.2017.2762345

Noizat, P. (2015). Blockchain Electronic Vote. In *Handbook of Digital Currency* (p. 453461). Elsevier. doi:10.1016/B978-0-12-802117-0.00022-9

Rahman, A., Rahman, T., Ghani, N. H., Hossain, S., & Uddin, J. (2019). IoT Based Patient Monitoring System Using ECG Sensor. *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*. doi:10.1109/ICREST.2019.8644065

Rahman, G., & Wen, C. C. (2018). Fog Computing, Applications, Security and Challenges [Review]. *IACSIT International Journal of Engineering and Technology*, *7*(3), 1615. doi:10.14419/ijet.v7i3.12612

Rajabi Shishvan, O., Zois, D.-S., & Soyata, T. (2018). Machine Intelligence in Healthcare and Medical Cyber Physical Systems : A Survey. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 4641946494. doi:10.1109/ACCESS.2018.2866049

Rajan, J. P., Rajan, S. E., Martis, R. J., & Panigrahi, B. K. (2020). Fog Computing Employed Computer Aided Cancer Classification System Using Deep Neural Network in Internet of Things Based Healthcare System. *Journal of Medical Systems*, *44*(2), 34. doi:10.1007/s10916-019-1500-5 PMID:31853735

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017). Towards using blockchain technology for eHealth data access management. *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)*, 14. doi:10.1109/ICABME.2017.8167555

Roriz, R., & Pereira, J. L. (2019). Avoiding Insurance Fraud : A Blockchain-based Solution for the Vehicle Sector. *Procedia Computer Science*, *164*, 211218. doi:10.1016/j.procs.2019.12.174

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI : Review and Open Research Challenges. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 1012710149. doi:10.1109/ACCESS.2018.2890507

Sharma, P. K., Chen, M.-Y., & Park, J. H. (2018). A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 115124. doi:10.1109/ACCESS.2017.2757955

Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., & Ghafir, I. (2019). The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain : A Survey. *Sensors (Basel)*, *19*(8), 1788. doi:10.3390/s19081788 PMID:31013993

Venkatesh, V. G., Kang, K., Wang, B., Zhong, R. Y., & Zhang, A. (2020). System architecture for blockchain based transparency of supply chain social sustainability. *Robotics and Computer-integrated Manufacturing*, *63*, 101896. doi:10.1016/j.rcim.2019.101896

Wang, Z., Wang, T., Hu, H., Gong, J., Ren, X., & Xiao, Q. (2020). Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Automation in Construction*, *111*, 103063. doi:10.1016/j.autcon.2019.103063

ENDNOTES

1 http://www.zionchina.com/web/home/home
2 https://www.kaggle.com/johndasilva/diabetes

Laila Fetjah is a graduate of a Master's degree in Systems and Networks from the University of Quebec in Montreal and a Doctorate in Computer Science at Hassan 2 University in Casablanca. She joined the professional world as head of an IT Department, Technical Director and then a Professor of Computer Science in Mathematics & Computer Science Department, Faculty of Sciences Ain-Chock Casablanca. Her current research interests include security in e-Health cloud based systems.

Kebira Azbeg received a Master degree in Computer Science Engineering and Internet from the University of Hassan II of Casablanca, Morocco, in 2016. Currently, she is a PhD Student in computer science at the faculty of sciences Ain Chock, University of Hassan II. She is a member at the research and innovation in computer science laboratory "LR2I". Her research interest is securing the IoT and healthcare devices by using the Blockchain technology.

Ouail Ouchetto was born in Morocco. He received the master's degree in applied mathematics from Pierre et Marie Curie University, Paris, France, and the master's degree in informatics from Télécom Bretagne School of Engineers, Brest, France. He received the Ph.D. degree in modeling and engineering science from the University Paris Sud, Orsay, France, in 2006. He was a post-doctoral with University Blaise Pascal, Clermont- Ferrond, France, and an Assistant Professor (Ater) with University Paris Sud, Orsay, France. In September 2010, he joined Aïn Chock Hassan II University, Casablanca, Morocco, as a Professor of mathematic and computer science. His research interests include electrical and electronical engineering, applied mathematics, and computer science.

Said Jai Andaloussi was born in Fez (Morocco) on Octobre 21, 1981. In 2010 he received a Phd degree in computer science jointly supervised by the faculty of science - University of Sidi Mohamed Ben-Abedillah (Fez - Morocco) and Telecom Bretagne (Brest - France). He is a professor of computer science in mathematics & computer science departement, faculty of sciences Ain-chok, Casablanca. He is the author of more than 40 papers. His current research interests include medical information processing, information modeling and analysis in medical images.