




Article

# SMS: A Secure Healthcare Model for Smart Cities

Gautami Tripathi <sup>1</sup>, Mohd Abdul Ahad <sup>1</sup> and Sara Paiva <sup>2,\*</sup>

<sup>1</sup> Department of Computer Science and Engineering, Jamia Hamdard, New Delhi 110062, India; gautami1489@gmail.com (G.T.); itsmeahad@gmail.com (M.A.A.)

<sup>2</sup> School of Technology and Management, Instituto Politécnico de Viana do Castelo, 4900-367 Viana do Castelo, Portugal

\* Correspondence: sara.paiva@estg.ipvc.pt

Received: 17 June 2020; Accepted: 8 July 2020; Published: 13 July 2020



**Abstract:** Technological innovations have enabled the realization of a utopian world where all objects of everyday life, as well as humans, are interconnected to form an “Internet of Things (IoT).” These connected technologies and IoT solutions have led to the emergence of smart cities where all components are converted into a connected smart ecosystem. IoT has envisioned several areas of smart cities including the modern healthcare environment like real-time monitoring, patient information management, ambient-assisted living, ambient-intelligence, anomaly detection, and accelerated sensing. IoT has also brought a breakthrough in the medical domain by integrating stake holders, medical components, and hospitals to bring about holistic healthcare management. The healthcare domain is already witnessing promising IoT-based solutions ranging from embedded mobile applications to wearable devices and implantable gadgets. However, with all these exemplary benefits, there is a need to ensure the safety and privacy of the patient’s personal and medical data communicated to and from the connected devices and systems. For a smart city, it is pertinent to have an accessible, effective, and secure healthcare system for its inhabitants. This paper discusses the various elements of technology-enabled healthcare and presents a privacy-preserved and secure “Smart Medical System (SMS)” framework for the smart city ecosystem. For providing real-time analysis and responses, this paper proposes to use the concept of secured Mobile Edge Computing (MEC) for performing critical time-bound computations on the edge itself. In order to protect the medical and personal data of the patients and to make the data tamper-proof, the concept of blockchain has been used. Finally, this paper highlights the ways to capture and store the medical big data generated from IoT devices and sensors.

**Keywords:** healthcare; IoT; SMS; SDN; Twofish; WSN; mobile edge computing; blockchain; OAuth

## 1. Introduction

The amalgamation of computer science, electronics, and other related technologies has created a synergistic relationship leading to the birth of one of the most prominent technologies branded as the “Internet of Things (IoT)” [1]. The advances in ICT and the emergence of IoT have attracted interests of researchers across the globe and helped in the realization of smart city ecosystems. Since the time IoT was first coined, there have been numerous researches in this field ranging from its application areas to implementation challenges and issues. Today, IoT has been imprinted in almost every area of computing, leading to the concept of “Smart-Environment”, where all the participating objects are interconnected and are capable of sensing, storing, communicating, and sharing information [1]. The advancement in ICT and networked technologies like Bluetooth, Wi-Fi, 3G/4G/5G, NFC/RFID, LiFi, and Smart dust has further expanded this concept [2]. It has also enabled humans to be an active part of the network as one of the primary entities.

These modern-day technologies have their impact on all aspects of human lives including the way they live and their surrounding environment. The emerging concept of smart cities is an example of how modern-day technologies can revolutionize the traditional processes.

A typical smart city is primarily dependent on IoT and other related network technologies for performing its functionalities. The ability to automate the events on the basis of preconditions and dynamically improvising with respect to the changing environment constitutes the major advantages of smart cities. A city is called “smart” if all or most of its services (education, healthcare, transportation, agriculture, businesses, etc.), infrastructure (building, homes, warehouses, etc.), and processing are smart and automated, and can be managed with optimum human interventions [2–4].

As IoT-based environments allow human interaction with the physical world objects and entities, it has found its applications in almost all spheres of a smart city ecosystem. One such application area that has grown in recent years is healthcare. The growth of ICT and related technologies has led to the emergence of a smart healthcare ecosystem where patients, doctors, medical equipment, and hospitals are interconnected to create a smart medical information system. However, to utilize the true capabilities of IoT technology in the healthcare domain, there is a need to develop a secure and privacy-preserved framework that patients and medical fraternity could trust in terms of security, privacy, reliability, and performance [5–7]. This paper proposes a conceptual framework for an “IoT-based healthcare system” for a smart city ecosystem to provide privacy-preserved data capturing, storing, and processing. The proposal also contemplates the use of the Mobile Edge Computing (MEC) paradigm [8,9] for processing the data on the edges of the network in close vicinity to the origin of the data and therefore increase the performance and scalability of the entire system.

### 1.1. Paper Organization

The paper is organized into five sections. The second section highlights the need for transition from the cloud to the edge paradigm, which is a necessity for this type of system. It defines the concept of MEC along with the security vulnerabilities associated with it. The third section gives an overview of the past researches in the area. Several existing “state-of-the-art” approaches for smart healthcare systems are reviewed in this section. This section also identifies the research gaps in the existing literature and the motivation for the current paper. The fourth section provides details about the proposed approach along with the various components of the system, their significance, and usage. The section also introduces the mechanism to secure edge and IoT devices from possible vulnerabilities attacks. The final section provides the conclusion and discusses the future scope of the smart healthcare systems.

### 1.2. Main Contributions

The manuscript proposes an MEC-based healthcare system for smart cities. The main contributions of the paper include:

- Identifying the limitations of classical healthcare systems and their inapplicability in smart cities ecosystems.
- Identifying the need for transitioning from the cloud to edge and the role of mobile edge computing in providing real-time healthcare services.
- Identifying security vulnerabilities in MEC and the possible solutions.
- Proposing a smart healthcare model for smart cities based on MEC, IoT, and blockchain consensus mechanisms for the reliable, faster, secured, and transparent interconnection of participating entities of the healthcare system.

## 2. Need for Transition from Cloud to Edge in a Smart City Ecosystem

The penetration of IoT in everyday lives for providing smarter solutions has resulted in the generation of large volumes of data. With such large volumes of data at our disposal, cloud computing (CC) has emerged as one of the preferred choices for IoT solutions. Cloud computing became jargon in the year

2006, when it was introduced to the world. The term cloud computing further gained popularity in the following years after it was widely used by the tech giants like Amazon, Microsoft, IBM, etc.

The two technological breakthroughs of the modern world, i.e., IoT and cloud computing, have always complemented each other for efficient results. However, the centralized structure of cloud computing has proven to be a limitation for providing solutions in cases where components are geographically dispersed. Edge Computing (EC) was born to meet this challenge by allowing some of the processing to be done at the network nodes that can be either “centralized” or “distributed” or at the “end of the network,” creating the “edge nodes” and contributing to distributed processing. Since its inception in 2005, cloud computing has emerged as a breakthrough technology that brought transformational changes in the way business were run. CC has provided an efficient and cost-effective way to store and process the data in a centralized cloud repository. However, the centralized storage structure is not able to keep up with the increasing demand for the real-time processing of data [9–11]. To address this increasing demand for minimizing the latency, edge computing can provide potential solutions by providing processing capabilities at the “edge of the network”, thus minimizing the overhead caused by the speed of the data transformation and latencies [12–14].

### 2.1. Mobile Edge Computing (MEC)

“Mobile Edge Computing (MEC)” is a computing paradigm wherein the data are processed in close proximity to its original source of generation. MEC involves a distributed intermediate server having some compute, storage, and networking facilities to handle the real-time processing of data for producing fast and instant results. The data that require real-time processing can be easily handled by such intermediate servers to provide instant results. What is important to mention is that, as of 2019, 45% of the data created under IoT solutions is expected to be stored and processed at network edges [15]. One of the main features of EC is the ease of adoption to multi-component and peripheral scenarios, which is commonly found in IoT solutions [11]. In the EC architecture, we assist a part of the processing and storage resources to be at the edges, near sensors or mobile devices, allowing for “agile-connectivity,” “real-time services,” “data optimization,” “security,” and “privacy.” Real-time response, low latency, reduction of network traffic, storage, energy consumption, and bandwidth cost are some of the advantages that can be pointed out to the EC paradigm [10]. The need to adopt a different paradigm from cloud computing to current and future IoT solutions is mainly due to three reasons:

- The large amount of data generated at the edges of the network (sensors, devices, etc.) requires, in a cloud architecture, the transmission of a large amount of data across the network, which is the origin of the bottleneck that is currently seen in the cloud paradigm. If we use the example of a Boeing 787, which is estimated to generate 5 gigabytes of data per second, it is easy to conclude that a system using the cloud paradigm will not scale to support such or similar situations [16].
- Data producers in an IoT solution (such as sensors, mobile devices, traffic lights, lights, appliances, etc.) will grow exponentially and reach billions in the coming years. In a cloud computing architecture, data consumers obtain the information they want after requesting it to the cloud, which will no longer be possible considering the amount and increasing number of data producers.
- In today’s scenarios with the proliferation of mobile devices and even other wearables, data consumers will also act as producers of data (uploading and sharing multimedia contents) and hence the cloud paradigm will not be enough. In addition, the data being produced on the edges tend to be more personal (photos, videos, etc.), raising privacy issues that will be more easily addressed by maintaining edge processing.

Although, MEC seems to be an appropriate solution for handling real-time requests, which the typical cloud computing paradigm fails to acknowledge. There are several vulnerabilities associated with this technology.

## 2.2. Security Vulnerabilities in Mobile Edge Computing

Use of edge computing helps to realize the full potential of IoT in the best possible way. With edge computing, data processing and analysis tasks are brought much closer to the data source. Some major security vulnerabilities and challenge areas with edge computing are [10,11,17–20]:

**Insecure IoT Devices:** The efficiency and reliability of edge computing are highly dependent on the “security” and “privacy” features of the smart devices. The IoT devices and the data generated by them are always at a high risk. Any compromised device might lead to a bad decision. Most of the IoT device manufacturers are mainly concerned about the working of the device and its functionality. There are hardly any inherent security features included within the IoT devices as it is of the least concern [10,11,17–20].

**Identification of Usable Data:** Although processing data at the device level helps to improve the latency and response time, it might lead to incomplete data at the main information repository. Due to the limited processing and storage capabilities at the edge, there are chances that an important portion of the data may be of greater usage if left out [10,11,17–21].

**Lack of Unified Security Standards:** The different IoT devices are mostly of different make and follow their specific syntax, semantics, and operating standards. Up until now, there is no unified security standard available that is universally applicable across all categories of IoT devices. Furthermore, the weakly coupled edge devices on the network are vulnerable to physical and cyber-attacks, making privacy preservation a difficult task [10,11,17–21].

**Distributed Denial of Service (DDoS) Attacks:** DDoS attacks constitute the most widely reported security threats to mobile edge computing. The attackers flood the devices with data packets through compromised devices, which then deny the services to the legitimate users. In addition, a compromised edge device may restrict the normal services by targeting the edge server with a DOS attack [10,11,17–21].

**Side Channel Attacks:** The user’s general data and information patterns can be accessed and collected overtime. This information may not be sensitive and private but, over time, it can be used to profile the user and get ahold of the user’s private data by linking it through side channels [10,11,17–21].

**Malware Attacks:** The entire IoT system can be corrupted with malware through a compromised edge device. Further, a compromised edge device can be used to bypass the whole authentication and authorization process to obtain access of the edge server [10,11,17–21].

## 3. Related Works

The popularity and widespread scope of the IoT technology has attracted several researches in this area in the past decade. The authors in [22] discussed the critical security provisions in “Sensor Network (BSN)”-based state-of-art healthcare ecosystems and presented a secured healthcare model. The researchers in [23] proposed a secured healthcare model using the “certificate-based DTLS” protocol. In [24], the authors presented a review of applications of IoT in healthcare. An efficient health monitoring system for controlling health parameters like “blood pressure (BP),” “hemoglobin (HB),” “blood sugar,” and “abnormal cellular growth” for the underprivileged is presented in [25]. The survey in [26] discusses the RFID technology and its applications for gathering information about the “living environment” of the users. The paper also discusses the various possible new research trends and the challenges for the same. A cloud computing platform for managing the sensors and wearable is presented in [27], which depict the application of the IoT paradigm for providing pervasive healthcare. The authors in [28] proposed a “single sign-on”-based authentication scheme for securing medical IoT data. The authors in [29] propose an interoperable “Smart Hospital System (SHS)” based on technologies like “RFID,” “WSN,” and “smart mobile” using the “Constrained Application Protocol (CoAP)/IPv6” over the “low-power wireless personal area network (6LoWPAN)” and “representational state transfer (REST) network infrastructure.” The presented SHS aimed to collect the “environmental conditions” and patient’s “physiological parameters” using a “hybrid-sensing network.” A control center collects the data, which is made available to the local and remote users by an advanced monitoring application (MA) via a REST web

service. An “ontology-based automating design methodology (ADM)” for “smart rehabilitation systems” using IoT was presented in [30]. The paper also empirically evaluates the proposal on parameters like “feasibility,” “rapidity,” and “effectiveness.” The authors in [31] highlighted the role and applications of IoT in healthcare. The research in [32] proposed a “semantic data model” for data storage and interpretation. Furthermore, a new method for efficient data access “UDA-IoT” was proposed. Finally, the authors presented an “IoT-based system” for “emergency medical services.” The authors in [33] presented a new conceptual framework for a “Home Health Hub Internet of Things (H3IoT)” for monitoring the physiological parameters of elderly people. The authors in [34] presented an overview of various “IoT-based technologies” and further discussed the technical and managerial challenges in its implementation. It also focuses on the three categories of IoT used to enhance customer value for enterprise applications. The authors in [35] investigated the challenges in collection of private data and presented a practical framework named “privacy protector” using the “Slepian-Wolf-coding-based secret sharing (SW-SSS),” to help attain secured sharing of the patient’s personal data. They used a distributed database comprising multiple cloud servers to ensure data privacy and protection. The authors in [36] proposed a “privacy-preserved smart IoT-based healthcare system” for effectively storing big data and “self-adaptive access control.” The proposed model also provides support for “deduplication to optimize space” in a big data storage system. The researchers in [37] analyzed the major concerns in the IoT technology related to the “smart sensors for healthcare applications” including the “wearable and body sensors” and “advanced pervasive healthcare systems.” The researchers talked about the integration of IoT features into the medical devices and healthcare as a whole, thus improving the quality of service and performance parameters like efficiency, privacy, cost, etc. The researchers in [38] proposed an IoT-driven system that collects information related to the patient’s vital parameters like pulse, temperature, etc. They used an Intel Edison to provide multi-tasking capabilities and low power consumption. The authors in [11] presented the basics of edge computing including its definition and need. The authors further discussed the various cases where edge computing can bring significant outcomes. The concept of collaborative edge is also introduced. Lastly, the authors highlighted the different challenges and opportunities in the area of edge computing, paving the way for future research. A “smart healthcare system” based on “edge computing” is proposed in [17]. The proposed healthcare system uses a cognitive computing approach to monitor and manage the patient’s health. The results show that the proposed approach improves the patient’s survival rates in emergency situations. The authors in [18] proposed an algorithm to improve the medical QoS in EC-based healthcare systems. The authors further compared the performance of the proposed “window-based rate control algorithm (w-RCA)” with the traditional algorithm and showed that w-RCA gives improved results. The authors in [19] proposed a resource management system for a SHS based on EC. In the proposed work, the authors introduced a “resource preservation net (RPN)” for emergency departments. The RPN framework is integrated with edge and cloud computing and shows some significant improvements in the patient’s waiting time and length of stay. In [17] and [20], the authors discussed the emergence and need of edge computing and its role in enhancing the services of CC and IoT. The researchers in [39] developed a framework for treatment and assessment of voice disorders using cloud and edge computing. Initially, edge computing was used to process the voice samples, which were then forwarded to a cloud for further processing. The authors used the “Saarbrücken voice disorder database” and achieved an accuracy of 98.5 percent. In [40], the authors presented a mechanism to show how the query results can be authenticated in edge computing. The proposed mechanism creates verification objects to authenticate the queries. The authors in [41] proposed a blockchain-based healthcare system that involves secured and the privacy-preserved interaction of all the participating entities of a healthcare ecosystem. Smart cities are a privileged environment for the adoption of ICT technologies to solve several problems. In [42], the authors address the adoption of big data and analytical treatment of data within a smart city, also presenting a prototype from which it was possible to conclude a set of methods used for analyzing smart healthcare data. In [43], the authors discuss how ICT can improve and impact the effectiveness of healthcare and reduce the costs of these services to citizens. In [44], the authors identify the type of technology used in a smart city regarding

healthcare, the most important applications in this field, its degree of maturity, as well as the greatest barriers to its proliferation. Finally, the main benefits of smart health and future trends in this area are presented and discussed in [45].

### *Research Gaps and Motivations*

The work presented in Section 3 shows that in the last few years, several architectures, frameworks, and methods have been proposed and developed to provide secure and smart healthcare for the patients. However, in recent years, very few reliable and trustworthy frameworks have emerged that can effectively provide a holistically secured, privacy-preserved, cost-effective, smart, and energy-efficient approach for the healthcare ecosystems [46–55]. Some existing solutions talk about securing the patient medical data, while others talk about effectively integrating different entities of the healthcare systems. In healthcare systems, especially with critical care units, real-time processing and decision-making is imperative [56,57]. With issues like network latency, traffic bottleneck, central node dependency, etc., the existing solutions using the “cloud-computing paradigm” fail to address the crucial need of “real-time data processing” and “decision-making” [12–14]. The time taken for the data to travel from the source sensor node to the cloud and return the results to the users is significantly high. The existing cloud-based solutions do not provide any reliable and significant solution to address this issue. Considering the above-mentioned insufficiencies of the existing cloud computing paradigm, it cannot provide a feasible solution for the critical real-time healthcare monitoring use-cases [12,13]. As the IoT devices are strictly power-constrained systems, the implementation of exhaustive and complex cryptographic techniques is not practically possible, because of the limited processing capabilities of the sensor devices. In the past, researchers have shown that cloud computing offers a large number of facilities and advantages compared to the legacy systems; however, in cases of real-time processing and data management, they somehow fail to keep up with the increasing demands for efficiency and satisfy the needs of the users [12–14]. With all these limitations of the classical cloud computing paradigm as motivation, this paper proposed a new framework that combines the capabilities of both cloud and edge computing paradigms to provide real-time, cost-effective, and energy-efficient data processing and management. Blockchain technology is integrated in the proposed framework to ensure the security and integrity of the sensitive and personal data like patient health records [58–60]. Edge computing helps in processing and managing critical use-cases at the edge nodes rather than centralized processing at the cloud. This can facilitate a near-real-time decision-making and delivery of the services. In addition, as the data captured by the sensors are handled on the edge only, a very short distance has to be travelled for the data to reach the edge nodes, which makes it faster, energy efficient, and cost-effective with very few chances of data losses [9–11,17–20,39].

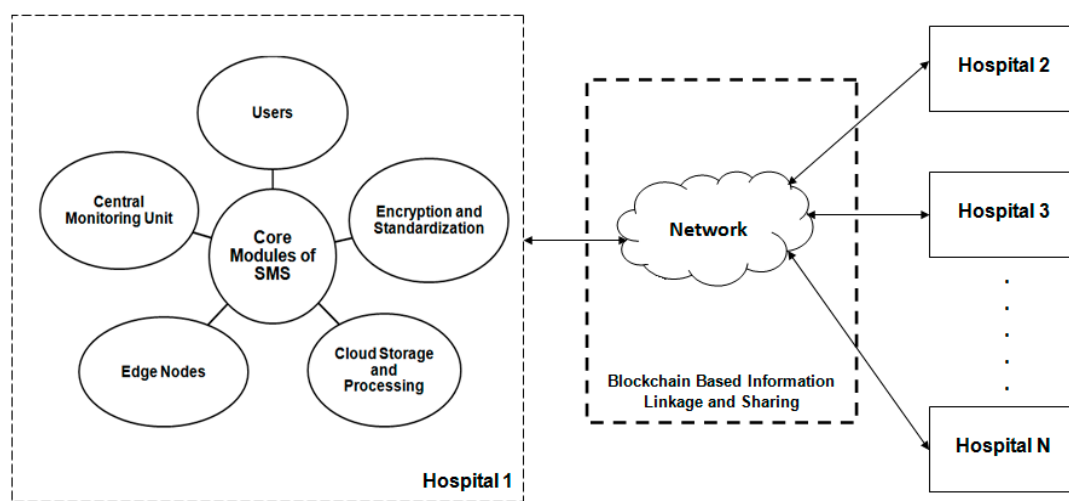
## **4. Proposed SMS Framework**

### *4.1. Overview and Architecture*

The proposed framework for the SMS facilitates the round-the-clock monitoring of patients by the doctors, care providers, and hospitals using smart-wearable devices and sensors. The SMS consists of five modules, namely users, a central monitoring unit, encryption and standardization unit, edge nodes, and cloud storage and processing unit. Figure 1 shows the core components in the SMS framework and their interconnection.

In the proposed framework for the SMS, several hospitals are connected together to facilitate information sharing using blockchain-based information storage. The stakeholders (users, doctors, patients, administrators, care providers) can perform their respective activities by authenticating themselves using the legitimate credentials. Any new user can register in the SMS by providing the respective registration details. Activities like reports downloads, viewing test results, and prescriptions providing diagnosis and suggesting treatments can be done with the help of smart devices using basic internet facilities. As the records of the patients are maintained on blockchains, the possibility of data

tampering is negligible. A smart contract consisting of sets of rules, preferred communication modes, and access rights to be followed by the entities of the SMS enables a secured and privacy-preserved information exchange and transfer. The data/requests that require immediate processing are handled on the edge of the network itself by the edge nodes. In order to overcome the security vulnerabilities of the mobile edge computing framework, the notion of the “OAuth 2.0” [61,62] and “Twofish cryptographic technique” [63,64] has been used in the proposed SMS system. The OAuth 2.0 protocol is used for authentication of the users and provides time-based access to the system. Once the time period is expired, access to the system is revoked. The “Twofish cryptographic technique” is used to encrypt the data captured by the IoT devices. As Twofish uses a Feistel network and symmetric key approach and is a lightweight algorithm, it is very easy to implement on the IoT devices.



**Figure 1.** Core components of smart medical system (SMS) in a network.

#### 4.2. Components of SMS

The Central Monitoring Unit (CMU) is the heart of the SMS framework. All the decisions about data capturing, routing, storage, retrieval, and blocking are taken by it. The Encryption and Standardization Unit (ESU) is responsible for converting the data captured by the sensors into a standard format so that it can be used for analysis. As the SMS employs multiple sensors of varied nature and configuration, the format in which they capture the data is largely different. Therefore, in order to perform a meaningful analysis, it is imperative to convert these intricate and heterogeneous data into a standard format.

The SMS uses the OAuth 2.0 protocol to ensure that only the legitimate personnel get access to the sensitive and protected information like patient’s records. The CMU validates the credentials of the users in real time before allowing access to the patients’ data. These data can also be made available through an SMS app, which can be accessed by the doctors, hospitals, as well as the patients using valid authentication credentials. This can save a major amount of time and effort spent in travelling to the hospitals or doctor’s premises. Furthermore, the Cloud Storage and Processing Unit (CSPU) serves several purposes. First, it acts as a repository for storing the patient’s data generated over the observation period. Secondly, the data from the cloud can be used as reference for similar medical cases. The data stored in the cloud are made available to the CMU for centralized monitoring of the patient’s current health status, which can be used for diagnosis and suggesting treatments. The doctors, as well as the hospitals, can be connected to the CMU to keep track of the patient’s medical history and current state and suggest a treatment or help in diagnosis. In cases of “Critical Care Units (CCU),” “Intensive Care Units (ICU),” “Intensive Critical Care Units (ICCU),” etc., it is imperative to process the data on the edge of the network in order to provide real-time diagnosis and analysis of the data. The unit requires round-the-clock real-time monitoring of the patients. The edge nodes are responsible for performing the processing of the data captured by the sensors, which requires immediate actions and decision-making.

The presented architecture aims to bring together the patients, doctors, and hospitals into a single umbrella for better medical facilities, and better diagnostics and treatments. The movement of data from one source to another in the SMS is governed by Software-Defined Networking (SDN) [65,66]. As SDN provides network flexibility, the data traffic can be dynamically controlled by the CMU in real time. SDN ensures dynamic route management for selecting optimal paths for faster data transfer.

#### 4.3. Three Stages of the Proposed Approach

For better understanding of the process, the proposed approach has been divided into three phases.

##### Phase 1-Data collection

This is the initial step of the proposed SMS framework. In this phase, the “real-time data” of the patients are captured with the help of multiple sensor-based devices including wearable and other medical equipment to collect the physiological parameters of the patients and other health-related data.

##### Phase 2-Data Encryption and Standardization

In the second phase, the information captured by the data collection phase is encrypted and converted into a predefined standard format in order to maintain “consistency,” “confidentiality,” and “privacy” of the data. Data standardization is necessary because of the fact that different devices capture and store the data in their respective format and, in order to maintain the “consistency,” the data must be converted into a predefined standard format. The block diagram given below in Figure 2 presents the working of the data standardization unit.

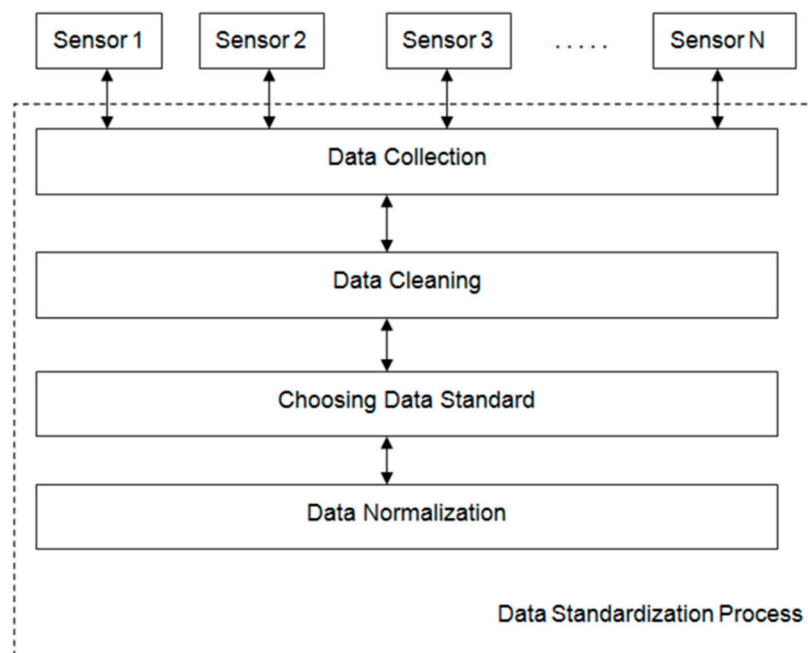


Figure 2. Data standardization process.

Figure 3 presents the architectural framework of the proposed SMS. The data captured by the different sensors are collected in the data collection phase. While capturing the required information, each sensor adds a sensor\_id, model\_no, data format, and size of the data in the data-header field (metadata). This step ensures the “authenticity” and “legitimacy” of the data at later stages (if required). After this, the essential portions among the data are identified and the outliers and noises are removed from the data. Then, the data are converted into the required standard format. Finally, the data are normalized in order to remove any duplicity or inconsistency. All this is governed by the central monitoring unit. The encryption unit is responsible for converting the data collected from the sensors



into an encrypted format to protect it from eavesdroppers (if any). The SMS uses the “Twofish cryptographic technique” to perform the encryption of the data. It is a “symmetric key cryptographic” technique that uses a “Feistel network,” and it is fast and has an intricate internal structure that is very hard to break but, at the same time, fairly simple to embed in the hardware devices because of the availability of its open-source APIs in several prominent languages. Further details about the Twofish algorithm can be found in [63,64].

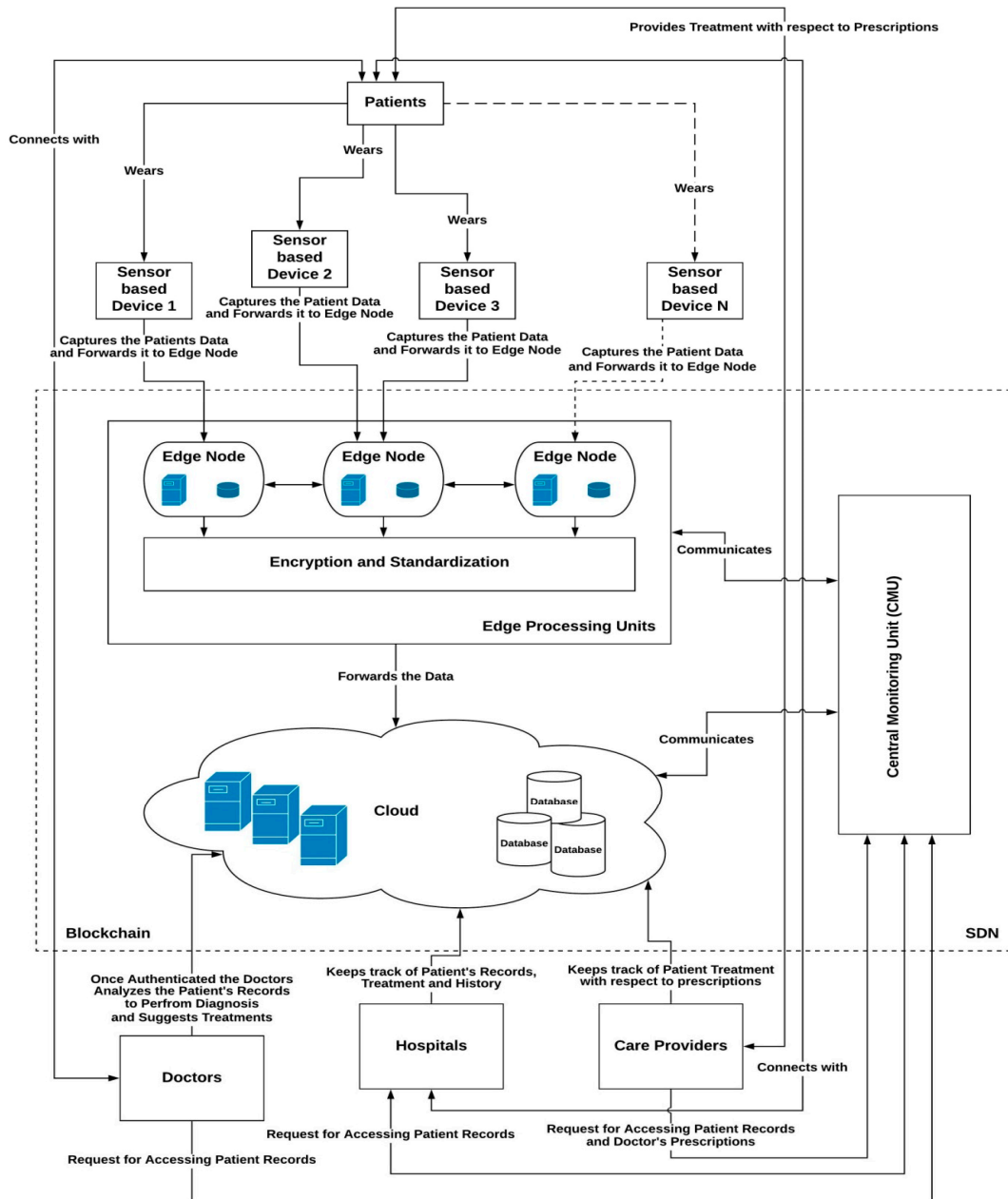


Figure 3. Proposed SMS architecture.

### Phase 3-Data Storage

Once the patient’s data is encrypted and standardized, these data and information are passed to the pre-authenticated account of the patients on the cloud for storage. The proposed SMS uses “OAuth 2.0” for performing the “authentication” and “authorization” process [61,62]. The OAuth protocol is a widely used industry-level authorization and authentication protocol that usually provides predefined threshold

value-based access to the users. This may include time-based access, level-based access, or complete access. Once the threshold value expires, the access is revoked [61,62]. This mechanism is useful for maintaining consistency of the data along with authorization and authentication. The encrypted records from the cloud storage can be made available for any medical assistance and case-studies by doctors, students, and researchers on mutual agreements with the hospitals and patients. In the final phase, the doctors and the hospitals access this data in real time by logging into the central monitoring system and requesting access to the “data and information” of the patients. The proposed SMS framework is a generic concept that can be modelled into any specific medical domain and use-case. The presence of OAuth 2.0, Twofish, and SDN makes it a secured, dynamic, privacy-preserved, intelligent, and dependable framework for the healthcare data management.

The data collected from various sources (wearable devices, fixed equipment, test data, etc.) is initially stored in the local storage units and later transferred to permanent storage hubs. While the data resides in local storage, it is preprocessed and refined to extract useful data for further processing. Once the process of extraction is completed, the extracted data is fed into the data analytics models for obtaining insights about the conditions of the patients and perform predictive and preventive analysis. Some of these analyses (which are urgently required) are done at the edge nodes while detailed analysis is done at the central control units. This serves two purposes, the immediate requirements and firsthand analysis are available in near-real time so that informed decisions can be taken in cases of emergency, while for regular cases, a detailed analysis is performed at the central hubs. This improves the overall performance of the system by minimizing latency, network bandwidth consumptions, and increasing the throughput.

#### 4.4. Role of IoT in SMS

IoT-enabled devices are primarily responsible for sensing and collecting data about the patient and their surroundings. This data sensing, collection, and transfer to hubs are governed by typical IoT protocols. Some of these protocols include [67–70]:

**MQTT:** This is a very lightweight protocol responsible for sharing information between two devices. It supports “machine-to-machine (M2M)” communication and works on the principle of the “publish-subscribe” communication pattern usually using TCP/IP [67].

**OMA-DM:** This is a device management protocol responsible for managing the devices connected in an IoT network. It works in the client server model. OMA-DM works in sessions. A typical session comprises two phases. The first phase is known as the “setup,” while the second phase is known as the “management” phase. The setup phase contains authentication and device information, while in the management phase, the commands issued by DM server are executed by DM clients [67].

**6LoWPAN:** This provides a low-power wireless connection over IPv6. It is used to provide end-to-end connectivity for the transfer of data in a WSN. It has an inbuilt encryption and compression mechanism that takes care of the security and speed of the data transferred [67].

**CoAP:** CoAP is primarily used for low-resourced devices like sensors nodes. They can provide multicast support, minimal overhead, and ease of usage [67].

**XMPP:** This stands for “Extensible Messaging and Presence Protocol”. It is mainly used in “real-time communication” like “instant messaging,” “voice and video calls,” chatting, etc.

**ZigBee:** This is a protocol that uses the IEEE 82.15.4 standard and is used for low-powered sensor devices. They are highly cost-effective and perform very well in several varieties of applications like home automation, personal health monitoring, etc. [67].

The SMS proposes to use an integration of these protocols to effectively capture, store, and transfer the data sensed by the sensors.

#### 4.5. Data Analytics in SMS

The data collected during the process can be used for performing various types of analytics to assist the healthcare community and the stakeholders. Table 1 shows how the integration of data analytics into the traditional healthcare systems impacts the stakeholders.

**Table 1.** Data analytics assisting the stakeholders.

Stakeholders	Impact of Data Analytics
Healthcare practitioners	<ul style="list-style-type: none"> <li>• Designing a personalizing treatment</li> <li>• Monitoring patient's health</li> <li>• Remotely consult the patient</li> <li>• Decision-making using the predictive health analytics</li> </ul>
Government	<ul style="list-style-type: none"> <li>• Manage, maintain, and monitor a unified data record of citizens</li> <li>• Easy identification of disease patterns</li> <li>• Analysis of regional, national, or disease-specific trends in a population</li> <li>• Design and develop health policies, preventive programs, and interventions based on the data from a particular demographic area and population</li> <li>• Efficient response in healthcare emergencies</li> </ul>
Healthcare providers	<ul style="list-style-type: none"> <li>• Analysis of patients' medical history</li> <li>• Better healthcare outcomes based on data</li> </ul>
Pharmaceutical companies	<ul style="list-style-type: none"> <li>• Drug discoveries based on medical data</li> <li>• Market assessment using predictive data analytics</li> <li>• Business intelligence using predictive data analytics</li> <li>• Better customer outreach and engagement</li> </ul>
Patients	<ul style="list-style-type: none"> <li>• Patients have equal participation and control during the overall care process</li> </ul>

#### 5. Role of MEC in the Proposed SMS

In a typical edge computing paradigm, the data are processed in close proximity to the source from where the data is generated as close as possible. This is made possible by deploying dynamic intermediary servers optimally placed in a distributed manner. These servers are capable of performing basic data processing and analysis that can be used to service requests in real time or near-real time. Although there are several security vulnerabilities associated with the classical mobile edge computing paradigm that can affect the edge devices and gain access to the data and information, this paper proposes to implement the OAuth 2.0 protocol, twofish cryptographic approach, and blockchain technology to safeguard the system against such attacks. In the SMS, all the participating devices and entities need to register in the system beforehand. Each device in the SMS can be uniquely identified with a unique key formed by combining the `device_hardware_id` and the `device_registration_id` provided at the time of registration. This unique code along with the hardware id of the device together forms the uniquely identifying key for the device. Figure 4 shows the creation of a unique key for the IoT and edge devices.

The users are authenticated using the "OAuth 2.0" protocol. The protocol provides "role-based access" to the legitimate user for a "specific period of time." Once the time period expires, access to the system is revoked.

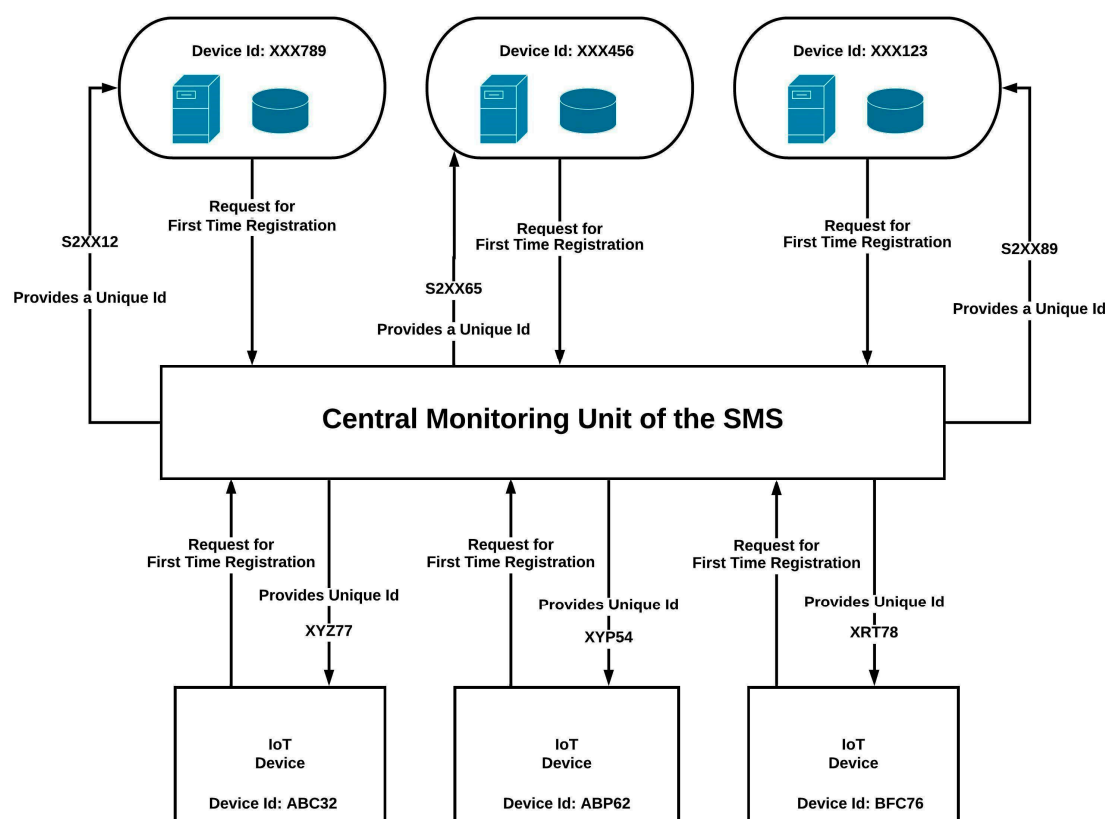


Figure 4. Creation of unique key in SMS.

### Blockchain in SMS

The information exchange between the users, IoT devices, edge devices, and servers are governed by the blockchain mechanism. All the participating entities form a smart contract among each other on mutually agreed conditions (consensus). Blockchain is a digital distributed ledger that consists of a series of timestamped records that are immutable, secured, and linked using cryptographic techniques [41,59,60,71]. Consensus algorithms are used to establish agreement between the nodes on a single state of the ledger across the distributed decentralized system. Proof of work is the most commonly used consensus algorithm that works on the idea that the miner nodes in the underlying network must provide proof of their effort. It is achieved by solving a cryptographic puzzle by the miner nodes. Other popular consensus algorithms include proof of stake, delegated proof of stake, byzantine fault tolerance, etc.

The smart contract is an agreement in the form of a computer code that can be stored on a public database and cannot be manipulated. The entire system works on the if-then premise where the transactions are executed only when the conditions specified in the agreement are met, thus eliminating the need of an intermediary third party [71–73].

In the blockchain-based healthcare systems like the SMS, smart contracts are used to empower the patients to control their own data. Smart contracts can record and safely transfer data. The use of zero-knowledge proofs in healthcare data can allow for anonymous querying and aggregation of patient's medical data and, hence, ensure patients anonymity. Further, using the smart contract, the patient can control the access and usage of their data by establishing an agreement to revoke the access and remove the data once the purpose is fulfilled. Smart contracts can also be used to record the health insurance of patients, which eliminates the need to file lengthy insurance claims in the case of need. Moreover, the health records of patients can easily be accessed while moving from one hospital to another. It also allows efficiency in telemedicine. Broadly, the smart contracts apply to the following aspects of the healthcare system [69–73]:

- Medical data safety
- Interoperability
- Loans and payments
- Health insurance
- Research and development
- Social Service/Philanthropic activities

These smart contracts identify the role, access mechanism, data ownerships, and data exchange policies. As blockchain is a distributed ledger technology that is immutable, there are no chances of data compromises or other tampering issues, as all the entities of the SMS system will be able to uniquely identify the legitimacy of each other. Figure 5 shows the formation of smart contracts between the participating entities of the SMS.

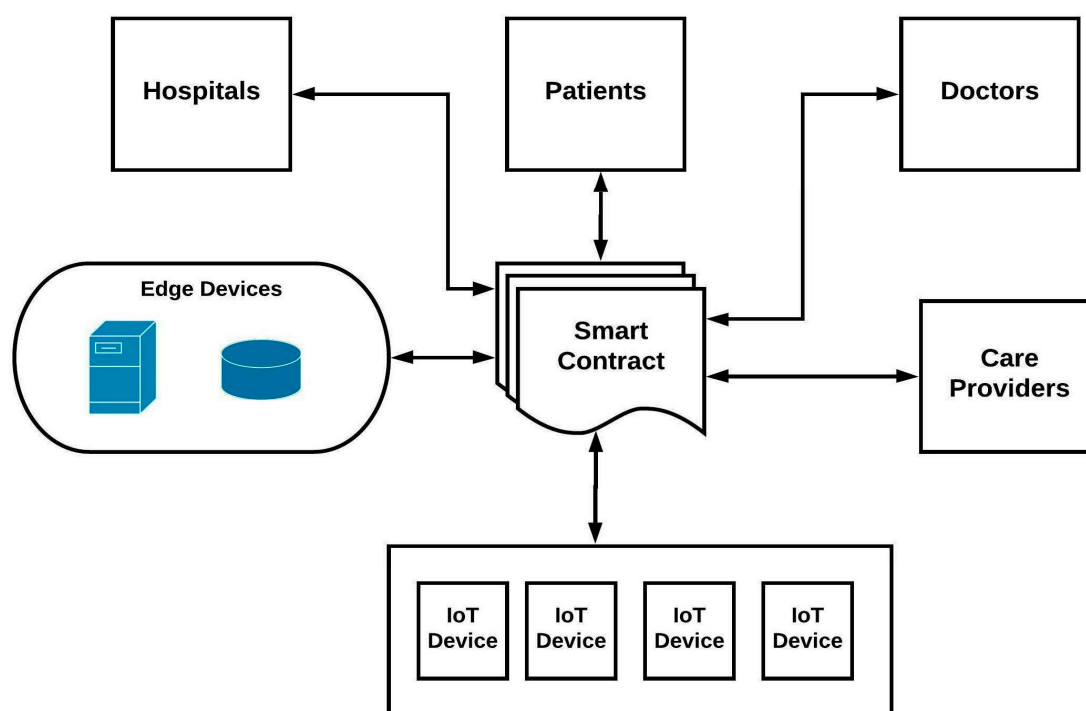


Figure 5. Smart contract in SMS.

There are several types of consensus algorithms that are widely used in blockchain technology. These include “Proof of Work (PoW),” “Proof of Stake (PoS),” “Delegated Proof of Stake (DPoS),” “Proof of Burns (PoB),” “Proof of Capacity (PoC),” “Proof of Elapsed Time,” “Practical Byzantine Fault tolerance,” etc. [71–73]. All these consensus algorithms can be used in different scenarios and for different purposes within a healthcare system. The different participating entities of the SMS can use the combination of these consensus algorithms to provide granular access control, transparency, and security.

In the proposed SMS, critical cases that require real-time 24/7 monitoring of the patient’s physiological parameters can leverage the potentials of edge computing to provide instant diagnosis and alert the care providers of the current situation of the patients. Furthermore, on the basis of extensive real-time data analysis and historical data available in the cloud, models can be developed that can provide predictive healthcare facilities. Consider a situation where a patient is about to get a heart attack, and, based on the constant real-time monitoring and historical data analysis, the doctors are able to predict it well before time. Thus, this predictive healthcare can provide revolutionary measures to know the nature and severity of the event even before it occurs and, thus, can save many valuable human lives. All this is made possible only because of the possibility of processing the data close to its source of origin with the help of edge

computing paradigms. In MEC, the “device relationship management (DRM)” software is responsible for monitoring and managing edge devices. The DRM is capable of providing the facilities like caching, filtering, optimizing, and buffering of the datasets. Algorithm 1 provides the mechanism for handling requests in the SMS.

---

**Algorithm 1** Request Handling in SMS
 

---

```

1: Request → Ri
2: Request Type (RT) → {Urgent, Normal};
3: For ∀ Ri ∈ RT
4:   If (Ri = Urgent)
5:     Forward the Data/Request to Edge Nodes
6:     Process the Data/Request
7:     Return the results to the User
8:   Else
9:     Forward the data/Request to the Cloud
10:    Process the Data
11:    Return the data to the user
  
```

---

## 6. Conclusions and Future Scope

This paper proposes a unique framework for the continuous health monitoring of patients. The proposed framework combines the three modern-day technologies IoT, cloud computing, and edge computing to facilitate efficient medical services. This is particularly helpful in critical cases that require 24 × 7 monitoring of the patients that is otherwise difficult with manual monitoring (nurses or ward boys). The system has the provision to capture any change in the condition of the patients in real time and send alerts to the doctors and care providers. In addition, this information can be used to construct prediction and analytics models using deep-learning techniques that can predict the incoming situation of the patient on the basis of the fluctuations in the vitals of the patients. Furthermore, the patients can be monitored regarding dietary and self-care instructions after they are discharged from the hospital with the help of the wearable devices worn by the patients. The amalgamation of big data and IoT in the proposed model also facilitates the storing of genomic data in a cost-effective and reliable manner and can open new horizons for genomic data analytics for treatments of various chronic and hereditary diseases. In addition, the data collected from the patients can serve as a repository for future medical references, prescriptions, and case studies. As a future scope, we can design a deep-learning-based analytical model for predicting the conditions of the patients in the near future and come up with state-of-the-art methodologies for diagnosis and treatments. As an extension of this work, the proposed model shall be converted into a prototype and will be evaluated with the help of simulation and real datasets.

**Author Contributions:** Conceptualization, M.A.A. and G.T.; methodology, M.A.A. and S.P.; formal analysis, M.A.A., S.P. and G.T.; investigation, M.A.A. and S.P.; resources, G.T. and S.P.; data curation, M.A.A., G.T., S.P. writing-original draft preparation, G.T. and M.A.A.; writing-review and editing, M.A.A. and S.P.; visualization, G.T. and S.P.; supervision, G.T. and S.P. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Ashton, K. That ‘internet of things’ thing. *RFID J.* **2009**, *22*, 97–114.
2. Ahad, M.A.; Paiva, S.; Tripathi, G.; Feroz, N. Enabling Technologies and Sustainable Smart Cities. *Sustain. Cities Soc.* **2020**, *61*, 102301. [[CrossRef](#)]
3. Ahad, M.A.; Tripathi, G.; Agarwal, P. Learning analytics for IoE based educational model using deep learning techniques: Architecture, challenges and applications. *Smart Learn. Environ.* **2018**, *5*, 1–16. [[CrossRef](#)]

4. Ahad, M.A.; Biswas, R. Dynamic merging based small file storage (DM-SFS) architecture for efficiently storing small size files in hadoop. *Procedia Comput. Sci.* **2018**, *132*, 1626–1635. [CrossRef]
5. Ahad, M.A.; Biswas, R. Request-based, secured and energy-efficient (RBSEE) architecture for handling IoT big data. *J. Inf. Sci.* **2019**, *45*, 227–238. [CrossRef]
6. Madaan, N.; Ahad, M.A.; Sastry, S.M. Data integration in IoT ecosystem: Information linkage as a privacy threat. *Comput. Law Secur. Rev.* **2018**, *34*, 125–133. [CrossRef]
7. Tripathi, G.; Ahad, M.A. IoT in Education: An Integration of Educator Community to Promote Holistic Teaching and Learning. In *Soft Computing in Data Analytics*; Springer: Singapore, 2019.
8. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A survey on the edge computing for the Internet of Things. *IEEE Access* **2017**, *6*, 6900–6919. [CrossRef]
9. Satyanarayanan, M. The emergence of edge computing. *Computer* **2017**, *50*, 30–39. [CrossRef]
10. Sittón-Candanedo, I.; Corchado Rodríguez, J. An Edge Computing Tutorial. *Orient. J. Comput. Sci. Technol.* **2019**, *12*, 34–38. [CrossRef]
11. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
12. Sajid, A.; Abbas, H. Data privacy in cloud-assisted healthcare systems: State of the art and future challenges. *J. Med. Syst.* **2016**, *40*, 155. [CrossRef] [PubMed]
13. Khattak HA, K.; Abbass, H.; Naeem, A.; Saleem, K.; Iqbal, W. Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure. In Proceedings of the 2015 17th International Conference on E-health Networking, Boston, MA, USA, 14–17 October 2015.
14. Mahmud, R.; Koch, F.L.; Buyya, R. Cloud-fog Interoperability in IoT-enabled Healthcare Solutions. In Proceedings of the 19th International Conference on Distributed Computing and Networking. Available online: <https://dl.acm.org/doi/10.1145/3154273.3154347> (accessed on 8 June 2020).
15. Evans, D. The Internet of Things: How the next evolution of the Internet is changing everything. *Cisco White Pap.* **2011**, *1*, 1–11.
16. Mark, v.R. Boeing 787s to Create Half a Terabyte of Data Per Flight. Available online: <https://datafloq.com/read/self-driving-cars-create-2-petabytes-data-annually/172> (accessed on 7 December 2016).
17. Chen, M.; Li, W.; Hao, Y.; Qian, Y.; Humar, I. Edge cognitive computing based smart healthcare system. *Future Gener. Comput. Syst.* **2018**, *86*, 403–411. [CrossRef]
18. Sodhro, A.H.; Luo, Z.; Sangaiah, A.K.; Baik, S.W. Mobile edge computing based QoS optimization in medical healthcare applications. *Int. J. Inf. Manag.* **2019**, *45*, 308–318. [CrossRef]
19. Oueida, S.; Kotb, Y.; Aloqaily, M.; Jararweh, Y.; Baker, T. An edge computing based smart healthcare framework for resource management. *Sensors* **2018**, *18*, 4307. [CrossRef] [PubMed]
20. Shi, W.; Dustdar, S. The promise of edge computing. *Computer* **2016**, *49*, 78–81. [CrossRef]
21. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge Computing Security: State of the Art and Challenges. *Proc. IEEE* **2019**, *107*, 1608–1631. [CrossRef]
22. Gope, P.; Hwang, T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2016**, *16*, 1368–1376. [CrossRef]
23. Moosavi, S.R.; Gia, T.N.; Rahmani, A.M.; Nigussie, E.; Virtanen, S.; Isoaho, J.; Tenhunen, H. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* **2015**, *52*, 452–459. [CrossRef]
24. Kulkarni, A.; Sathe, S. Healthcare applications of the Internet of Things: A Review. *Int. J. Comput. Sci. Inf. Technol.* **2014**, *5*, 6229–6232.
25. Rohokale, V.M.; Prasad, N.R.; Prasad, R. A cooperative Internet of Things (IoT) for rural healthcare monitoring and control. In Proceedings of the Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), Chennai, India,, 28 February–3 March 2011; pp. 1–6.
26. Amendola, S.; Lodato, R.; Manzari, S.; Occhiuzzi, C.; Marrocco, G. RFID technology for IoT- based personal healthcare in smart spaces. *IEEE Internet Things J.* **2014**, *1*, 144–152. [CrossRef]
27. Doukas, C.; Maglogiannis, I. Bringing IoT and cloud computing towards pervasive healthcare. In Proceedings of the Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Palermo, Italy, 4–6 July 2012; pp. 922–926.

28. Hou, J.L.; Yeh, K.H. Novel authentication schemes for IoT based healthcare systems. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 183659. [CrossRef]
29. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things J.* **2015**, *2*, 515–526. [CrossRef]
30. Fan, Y.J.; Yin, Y.H.; Da Xu, L.; Zeng, Y.; Wu, F. IoT-based smart rehabilitation system. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1568–1577.
31. Talpur, M.S.H. The appliance pervasive of internet of things in healthcare systems. *arXiv* **2013**, arXiv:1306.3953.
32. Xu, B.; Da Xu, L.; Cai, H.; Xie, C.; Hu, J.; Bu, F. Ubiquitous data accessing method in IoT-based information system for emergency medical services. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1578–1586.
33. Ray, P.P. Home Health Hub Internet of Things (H3 IoT): An architectural framework for monitoring health of elderly people. In Proceedings of the Science Engineering and Management Research (ICSEMR), Chennai, India, 27–29 November 2014; pp. 1–3.
34. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Bus. Horiz.* **2015**, *58*, 431–440. [CrossRef]
35. Luo, E.; Bhuiyan MZ, A.; Wang, G.; Rahman, M.A.; Wu, J.; Atiquzzaman, M. Privacy Protector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems. *IEEE Commun. Mag.* **2018**, *56*, 163–168. [CrossRef]
36. Yang, Y.; Zheng, X.; Guo, W.; Liu, X.; Chang, V. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Inf. Sci.* **2018**, *479*, 567–592. [CrossRef]
37. Firouzi, F.; Rahmani, A.M.; Mankodiya, K.; Badaroglu, M.; Merrett, G.V.; Wong, P.; Farahani, B. Internet-of-Things and big data for smarter healthcare: From device to architecture, applications and analytics. *Future Gener. Comput. Syst.* **2018**, *78*, 583–586.
38. Salunke, P.; Nerkar, R. IoT Driven Healthcare System for Remote Monitoring of Patients. *J. Mod. Trends Sci. Technol.* **2017**, *3*, 100–103.
39. Muhammad, G.; Alhamid, M.F.; Alsulaiman, M.; Gupta, B. Edge computing with cloud for voice disorder assessment and treatment. *IEEE Commun. Mag.* **2018**, *56*, 60–65. [CrossRef]
40. Pang, H.; Tan, K.L. Authenticating query results in edge computing. In Proceedings of the 20th International Conference on Data Engineering, Boston, MA, USA, 2 April 2004; pp. 560–571.
41. Tripathi, G.; Ahad, M.A.; Paiva, S. S2HS-A Blockchain based Approach for Smart Healthcare System. Available online: <https://doi.org/10.1016/j.hjdsi.2019.100391> (accessed on 10 July 2020).
42. Swapnaja; Hiray, R.; Bhraramamba, R. Health Care in Smart Cities: A Survey based on IoT Data Analytics. Available online: [https://xueshu.baidu.com/usercenter/paper/show?paperid=1a6906j0m95f0gn09d6m0cx0f7025367&site=xueshu\\_se](https://xueshu.baidu.com/usercenter/paper/show?paperid=1a6906j0m95f0gn09d6m0cx0f7025367&site=xueshu_se) (accessed on 10 July 2020).
43. Cook, Diane & Duncan, Glen & Sprint, Gina & Fritz, Roschelle. Using Smart City Technology to Make Healthcare Smarter. *Proc. IEEE* **2018**, *106*, 708–722. [CrossRef]
44. Pacheco Rocha, N.; Dias, A.; Santinha, G.; Rodrigues, M.; Queirós, A.; Rodrigues, C. Smart Cities and Healthcare: A Systematic Review. *Technologies* **2019**, *7*, 58. [CrossRef]
45. Al-Azzam, M.; Alazam, M. Smart City and Smart-Health Framework, Challenges and Opportunities. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 171–176. [CrossRef]
46. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
47. Elhoseny, M.; Ramírez-González, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure Medical Data Transmission Model for IoT-based Healthcare Systems. *IEEE Access* **2018**, *6*, 20596–20608. [CrossRef]
48. Gong, T.; Huang, H.; Li, P.; Zhang, K.; Jiang, H. A medical healthcare system for privacy protection based on IoT. In Proceedings of the 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nanjing, China, 12–14 December 2015; pp. 217–222.
49. He, D.; Ye, R.; Chan, S.; Guizani, M.; Xu, Y. Privacy in the Internet of Things for smart healthcare. *IEEE Commun. Mag.* **2018**, *56*, 38–44. [CrossRef]
50. Manogaran, G.; Varatharajan, R.; Lopez, D.; Kumar, P.M.; Sundarasekar, R.; Thota, C. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Gener. Comput. Syst.* **2018**, *82*, 375–387. [CrossRef]



51. Ng, H.S.; Sim, M.L.; Tan, C.M. Security issues of wireless sensor networks in healthcare applications. *BT Technol. J.* **2006**, *24*, 138–144. [CrossRef]
52. Pramanik, M.I.; Lau, R.Y.; Demirkan, H.; Azad MA, K. Smart health: Big data enabled health paradigm within smart cities. *Expert Syst. Appl.* **2017**, *87*, 370–383. [CrossRef]
53. Tarouco LM, R.; Bertholdo, L.M.; Granville, L.Z.; Arbiza LM, R.; Carbone, F.; Marotta, M.; De Santanna, J.J.C. Internet of Things in healthcare: Interoperability and security issues. In Proceedings of the 2012 IEEE international conference on communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; pp. 6121–6125.
54. Uddin, M.Z. A wearable sensor-based activity prediction system to facilitate edge computing in smart healthcare system. *J. Parallel Distrib. Comput.* **2019**, *123*, 46–53. [CrossRef]
55. Zhang, Y.; Gravina, R.; Lu, H.; Villari, M.; Fortino, G. PEA: Parallel electrocardiogram-based authentication for smart healthcare systems. *J. Netw. Comput. Appl.* **2018**, *117*, 10–16. [CrossRef]
56. Kakria, P.; Tripathi, N.K.; Kitipawang, P. A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors. *Int. J. Telemed. Appl.* **2015**, *2015*, 373474. [CrossRef] [PubMed]
57. Zhao, X.H.; Ma, S.N.; Long, H.; Yuan, H.; Tang, C.Y.; Cheng, P.K.; Tsang, Y.H. Multifunctional sensor based on porous carbon derived from metal–organic frameworks for real time health monitoring. *ACS Appl. Mater. Interfaces* **2018**, *10*, 3986–3993. [CrossRef]
58. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
59. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. Blochie: A blockchain-based platform for healthcare information exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (Smartcomp), Taormina, Italy, 18–20 June 2018; pp. 49–56.
60. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 130. [CrossRef]
61. Jones, M.; Hardt, D. The OAuth 2.0 Authorization Framework: Bearer Token Usage. *No. RFC 6750*. Internet Engineering Task Force (IETF). Available online: <https://tools.ietf.org/pdf/rfc6750.pdf> (accessed on 2 June 2020).
62. Boyd, R. *Getting Started with OAuth 2.0*; O'Reilly Media publication, Inc.: Sebastopol, CA, USA, 2012.
63. Schneier, B.; Kelsey, J.; Whiting, D.; Wagner, D.; Hall, C.; Ferguson, N. The Twofish Encryption Algorithm: A 128-Bit Block Cipher. Available online: [https://xueshu.baidu.com/usercenter/paper/show?paperid=af1baf2b83ca69305a23bddb548eab0a&site=xueshu\\_se](https://xueshu.baidu.com/usercenter/paper/show?paperid=af1baf2b83ca69305a23bddb548eab0a&site=xueshu_se) (accessed on 2 June 2020).
64. Bhanot, R.; Hans, R. A review and comparative analysis of various encryption algorithms. *Int. J. Secur. Appl.* **2015**, *9*, 289–306. [CrossRef]
65. McKeown, N. Software-defined networking. *INFO- COM Keynote Talk* **2009**, *17*, 30–32.
66. Kirkpatrick, K. Software-defined networking. *Commun. ACM* **2013**, *56*, 16–19. [CrossRef]
67. Trevor, H. IoT Standards and Protocols. Available online: <https://www.postscapes.com/internet-of-things-protocols/> (accessed on 30 June 2020).
68. Bhushan, B.; Sahoo, G. Routing Protocols in Wireless Sensor Networks. In *Computational Intelligence in Sensor Networks Studies in Computational Intelligence*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 215–248. [CrossRef]
69. Sharma, M.; Tandon, A.; Narayan, S.; Bhushan, B. Classification and analysis of security attacks in WSNs and IEEE 802.15.4 standards: A survey. In Proceedings of the 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA), Dehradun, India, 15–16 September 2017; pp. 1–5. [CrossRef]
70. Sinha, P.; Jha, V.K.; Rai, A.K.; Bhushan, B. Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In Proceedings of the 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 28–29 July 2017; pp. 288–293. [CrossRef]
71. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemeč Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]

72. Zubaydi, H.D.; Chong, Y.W.; Ko, K.; Hanshi, S.M.; Karuppayah, S. A review on the role of blockchain technology in the healthcare domain. *Electronics* **2019**, *8*, 679. [[CrossRef](#)]
73. Kombe, C.; Ally, M.; Sam, A. A review on healthcare information systems and consensus protocols in blockchain technology. *Int. J. Adv. Technol. Eng. Explor.* **2018**, *5*, 2394–7454. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).