This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities

Mohammad Nuruzzaman Bhuiyan[1], *Assistant Professor, Institute of Information Technology (IIT), Noakhali Science and Technology University, Bangladesh,* Dr. Md. Mahbubur Rahman[1], *Professor, Department of Information and Communication Technology, Islamic University, Bangladesh,* Md Masum Billah[2], *Lecturer, Computer Science, American International University-Bangladesh (AIUB), Bangladesh,* Dipanita Saha[2], *Assistant Professor, Institute of Information Technology (IIT), Noakhali Science and Technology University, Bangladesh.*

***Abstract*—The Internet of Things (IoT) is a methodology or a system that encompasses the real world things to interact and communicate with each other with the assistance of networking technologies. This paper describes surveys on advances in IoT-based healthcare methods and reviews the state-of-art technologies in detail. Moreover, this review classifies an existing IoT-based healthcare network and represent a summary of all perspective networks. IoT healthcare protocols are analyzed in this context, and provide a broad discussion on it. It also initiates a comprehensive survey on IoT healthcare applications and services. An extensive insights into IoT healthcare security, its requirements, challenges, and privacy issues are visualized in IoT surrounding healthcare. In this review, we analyze security and privacy features consisting of data protection, network architecture, quality of services, apps development and continuous monitoring of healthcare that are facing difficulties in many IoT-based healthcare architecture. To mitigate the security problems, an IoT-based security architectural model has been proposed in this review. Furthermore, this review discloses the market opportunity that will enhance the IoT healthcare market development.To conduct the survey, we searched through established journal and conference databases using specific keywords to find scholarly works. We applied filtering mechanism to collect only papers that were relevant to our research works. The selected papers were then examined carefully to understand their contributions/research focus. Eventually, the paper reviews were analyzed to identify any existing research gaps and untouched areas of research and to discover possible features for sustainable IoT healthcare development.**

***Index Terms*—IoT, Healthcare, Networks, Architectures, Security**

I. INTRODUCTION

All aspects of our lives witnessed a steady increase in internet technology has become ubiquitous that is infiltrating. Kevin Ashton named the term Internet of Things (IoT) that represents internet-based information with the emerging global services architecture [3]. IoT healthcare applications have the capacity to accurately track people, equipment, specimens, supplies, and can take care of various types of stakeholders including hospitals, diagnoses, nursing homes, and community to analyze the capturing data. Using biometrics information or measuring the important parameters from sensors to get better quality, and efficiently using the resources. To detect the misuse activation as an extreme cardio practice or accelerated exercising as analyzed to training at a methodical movement, the aforementioned data provide relevant information in the analysis and control of the diseases.

In the past decade, the Internet of things (IoT) has become a mega- trend in 4th generation revolution technologies that can offer excellent interconnection to each uniquely identifiable smart object and devices [4] in internet infrastructure. The structure of the advanced connectivity of these devices and services that proceed with the Machine-to-Machine(M2M) [6], [5] scenarios. IoT is a highly powerful distributed network that formed a very large number of objects. The prospect of IoT will be dominated that will serve as global policies to interconnect physical objects, substances, humans, and enabling new ways of working, communicating, interacting, entertaining, and living [8]. The IoT enables to transform physical objects to perform to receive information and to co-ordinate their decisions by utilizing its underlying technologies such as ubiquitous and pervasive computing, embedded devices, intelligence technologies, sensor networks, internet protocols, and domain-specific applications.

The IoT is a new fashioned paradigm in which every physical object which you wear, what/where you drive, what you read/see, and anything including the people you meet, the places you go, will be connected, addressed and controlled remotely [7]. A number of such physical things are getting connected to the internet and share the data with cyberspace [107]. Every year, millions of new IoT devices will be deployed to different application domains [108] throughout the researcher anticipating. In IoT technologies, numerous distributed survey papers related to different aspects of applications already published. As a standard, the study by Atzori et al. [9] includes the foremost intelligence empowering technologies are different components of Wireless Sensor Networks (WSNs), wearable, and wireless. There are lots of appropriate solutions for a broad spectrum of applications in IoT and embedded with smart cities, traffic congestion, waste management, structural health, security, emergency services, logistics, retails, automated control, and health care [6], [10].

An IoT-based system understands the Artificial Intelligent (AI) data with sensing capability and semantic knowledge [11] included various IoT-based application scenarios. Nowadays, the various number of interesting application fields for IoT in healthcare [12] system that allows the offering on timely,

Mohammad Nuruzzaman Bhuiyan[1], Assistant Professor, Institute of Information Technology (IIT), Noakhali Science and Technology University

Dr. Md. Mahbubur Rahman[1], Professor, Department of Information and Communication Technology, Islamic University

Md Masum Billah[2],Lecturer, Computer Science, American International University-Bangladesh (AIUB)

Dipanita Saha[2], Assistant Professor, Institute of Information Technology (IIT), Noakhali Science and Technology University

Manuscript received July 03 2020; revised December 22, 2020.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

excellent telemedicine and healthcare services to patients through remote assistance. Many medical applications such as health monitoring systems, fitness programs, several chronic diseases, and remotely monitoring health treatment and medication at home are provided by employing multiple possible applications. Consequently, IoT-based healthcare are the core objectives of the medical devices, services, actuators, sensors, diagnostic [13] to enrich the end user's experience. Also, the IoT devices can precisely recognize optimum times for regular and consecutive operations. Moreover, the IoT provides dynamic scheduling for more numerous patients using restricted sources by securing the best application and services.

In [161], a data access system which is lightweight and uses a couple of access keys instead of one. In the healthcare sector, the secrecy of patient medical information is of paramount importance. As a result, the medical records of a person is usually available only to himself and a few authorized parties, for example, the local hospital. However, there can be a situation where another legitimate healthcare provider may need the information of the patient who has suddenly fallen ill and brought to them. The proposed model allows a set of Emergency Contact Persons (ECP) to access the medical information of a person in case of an emergency with an alternate key, which is used as a Break-Glass Key. The proposed model is lightweight and the authors ran several simulations to test their system.

In [162], developed a non-invasive breathing monitoring system for diabetic patients to automatically monitor the signs of Ketoacidosis. The work showed excellent outcome in the test results. Their system uses C-band sensing, which is one of the features of upcoming 5G internet recommended in many countries. Although 5G is not very widespread though out the world as of this moment, it will surely be around more in the near future. As a result, the outcome of this novel study shows the path of more studies of similar type.

In another paper [163], developed an S-band frequency-based monitoring system for dementia patients. They used S-band frequency to automatically monitor three wandering patterns of dementia patients, namely, random, pacing and lapping. The extracted features from the wandering patterns of patients in a controlled indoor environment are trained to a machine learning model and then tested with more data to achieve a 90% accuracy output. Their system may be used as a good baseline for similar works of IoTh systems.

We reviewed the security based existing in healthcare application on IoT that described the label of protections. IoT applications default security must be required to protect itself. Any healthcare domain specification systems must be addressed in security, privacy, and trust [7].

This paper analyze a variety of healthcare researches and enlist different healthcare technologies, applications, services, protocols, networks, Security and its requirements, security challenges, different proposed and implemented security models, market opportunity, and open issues to be faced for the IoT. In this regards, this review contributes:

- A survey on state-of-art technologies used in IoT-based healthcare.
- Classifying the existing IoT-based healthcare networks and presenting a summary of each.
- Modeling an analysis of standard IoT healthcare protocols and a detailed discussion on it.
- Providing a broad survey of IoT-based healthcare applications and their services.
- Modeling an extensive insights into IoT healthcare security, its requirements, challenges, and privacy issues in IoT healthcare.
- Designing a proposed model for IoT healthcare security.
- Finally, addresses the market opportunities for IoT-based healthcare technologies.

The rest of the papers are structured as follows: section II related works, section III presenting an IoT healthcare method, section IV explains the IoT healthcare networks, section V IoT healthcare common standard protocols, section VI IoT healthcare Security, its requirements, security challenges, Section VII blockchain based proposed security model, section VIII IoTbased healthcare applications and services, section IX discuss some IoT healthcare challenges and open issues, section X IoT healthcare market opportunities, and finally section XI concludes the overall survey. This work ends with some future research directions.

II. RELATED WORKS

In [118] He et al. introduced anonymous authentication for WBAN with provable security.

In [56] Lo'ai A. Tawalbeh et.al discusses the role of mobile cloud computing and big data analysis in networked healthcare and its capabilities. Healthcare methods, tools, and applications of big data analytics are reviewed in this paper.

In [66] Ho-Gun Ha et.al represents a summary of augmented reality. Its reviews current applications of medication. After explaining the initial concept, brief features of the three elements (Hardware, Software, and application) are presented, which include augmented reality. Authors review various applications applied in the laboratory.

In [100] Sreekanth K U et.al reviews an applications, concepts, and several existing technologies for the healthcare system. They noted the differences between those techniques and a brief explanation in personalized IoT healthcare. They mainly focus on ubiquitous wearable devices that collect various data from the patient body.

In [47] Khan et.al proposed and designed an effective healthcare monitoring system using IoT and RFID tags. The experimental results of this paper shows the output against numerous medical emergencies. In the proposed system, a combination of microcontrollers with sensors is presented to obtain the results of unadulterated assessments, monitor and weigh the patient's health status, and increase the power of the IoT.

In [54] Stephanie B et.al presents sophisticated research related by evaluating strengths, weaknesses, and overall suitability for the wearable body sensor network in IoT healthcare system. The paper highlights the challenges of security, privacy, cleanliness, and low power application, offers suggestions for future research directions.

In [122] Daniel Minoli et.al provides a protocol architecture using OSiRM model, and examines the security tools and strategies that can be gained as part of the IoT deployment. These measures are especially important for e-health and supportive living.

In [42] J M Blythe et.al focus on the CSI methodology for the development. A team of IoT security experts, identifies the security features which preferences discussing the information value, appeal, and potential engagement of a security label.

In [49] Soraia Oueida et.al proposed a resource preservation net (RPN) framework using Pedi Net, integrating with edge and cloud computing suitable for the systems of Emergency Departments (ED). The RPN applies to real-life scenarios where key performance signs, such as patient length of stay, patient health rate, patient waiting times, are shaped and optimized.

In [75] Srinivas et.al proposed an intelligent medicine box model. The wireless sensors alert patients to the medication at the right time and updates about the medicine through notices in an android application.

In [73] Mrs. Pallavi Kulkarni et.al proposed IoT based healthcare monitoring system for soldiers. The proposed system can track the solders and current location using the GPS tracker. It also help securing the cloud data using cryptographic algorithms.

In [120] Hubert Kenfack Ngankam et.al presents the design of an AAL system of smart cities. The proposed architecture, based on microservices system has been experimented and evaluated in the laboratory.

In [112] Dwivedi et.al propose a novel framework of modified blockchain models suitable for IoT devices. The framework try to solve the healthcare problems of using blockchain. Applying the technology, data transmission is more secure over a blockchain-based network.

In [113] Divya Sharma et.al proposed a smart collaborative security model to reduce security risks. They have analyzed IoT security and privacy and other features of security requirements, threat models, and taxonomies from a medical care perspective.

In [114] Kadhim Takleef Kadhim et.al a review of a general outline of the opportunities and challenges of the Internet-based Healthcare Monitoring System (HCMS). They address the application and limitations in the field of IoT healthcare to establish limits in various health sectors and enhance the quality of healthcare.

In [115] Lemlouma et.al proposed a framework for smart and automatic evaluation of elderly dependencies for the e-health solutions. Such frameworks' usability is in the intelligent healthcare solutions deployed in a smart home or smart city environment where special assistance can be made readily available whenever someone is at risk. mHealth services and applications addressed the foremost issues on how to exert benefits of context and description modeling. mHealth is a more challenging field in the critical situations of smart health monitoring for older people.

In [116] Boulemtafes et.al proposed a framework for designing and evaluating context aware mobility supported health monitoring systems. They validated the framework from a theoretical aspect, but suggest further validation with simulations.

In [117] Lemlouma, Tayeb et.al proposed a model to extend the functionalities of IP Multimedia Subsystem (IMS) with e-Health service integration such that the service becomes aware of a patient's situation. This configurable model is not a new architecture, rather an improvement to the existing IMS to make it more scalable and easier to integrate with current e-Health services.

IoT based healthcare applications and devices overcoming the incompetence of the extant healthcare system to collect specific data, real-time approach ability, integrate the data through cloud service, etc. [1]. along with reducing complexity and difficulties. The proficient of m-health and e-health applications utilize to improve and maintain a healthy spirit of life [111]. Table I shows the summary of healthcare technologies comparison between 2016-2020.

We have analyzed different IoT healthcare related scholarly journals for this review and presented a comparison of its methodologies used in the related works. Next, in section III, we will examine the IoT healthcare methods.

III. IoT Healthcare Method

A. Radio Frequency Identification

In healthcare, Radio Frequency Identification (RFID) technology allows the moving of medical equipment with passive RFID tags. Real-Time Location System (RTLS) enables real-time tracking of tagged objects and helps to create a system of connected devices that dynamically track and report any status change about their location, conditions, and amount.

In [46], a survey on the RFID application to body-centric systems is presented which gathers information about (temperature, humidity, and gases) the user's living environment. A complete monitoring existence cycle and effective healthcare monitoring system is described and proposed in [47] that is designed using the IoT and RFID tags. This system evaluates veracious results, supervising, and weighing the health status of the patient and increases the ability of IoT with the combination of a micro-controller with sensors. In [48], an intelligent home based platform using the iHome Health-IoT is proposed and implemented which permits an open platform based iMedBox (intelligent Medicine Box) for the integration of devices and services in the platform with superior connectivity and interchangeability. Passive RFID and arduino ethernet shield enables the communication of intelligent Medicine Packaging (iMedPack).

B. Edge Computing

Edge computing is a network architecture that enables the placement of computational and storage resources within the radio access network (RAN) which helps to improve network efficiency and the delivery of content to end-users. Integrating with custom cloud and edge computing a Resource Preservation Net (RPN) framework is proposed using Petri net which is suitable for the Emergency Departments (ED) systems [49] The framework applies RPN to a real life scenario where key performance indicators such as patient length of stay (LoS), resource utilization rate, and average patient waiting time are modeled and optimized. With the support of mobile cloud computing and edge computing, wireless body area networks can be enhanced for the deployment of healthcare applications and also proposed for secure, safe smart healthcare [50]. Edge computing is most useful for devices like intensive care unit sensors that require instantaneous analysis of data and execution of commands, such as closed-loop systems that maintain physiologic homeostasis [103] Closed-loop control devices as insulin levels, respiration, neurological activity, cardiac rhythms, and GI functions don't require time to be uploaded to the cloud as the sensors are sophisticated. Another, five more edge computing use cases are discussed in [104] for smart Healthcare which includes rural medicine, patient-generated health data, improved patient experience, supply chain, and cost savings.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

Table I: Comparison of methodologies used in the related works (2016-2020)

Year/References	Technologies /Methodologies	Merits	Limitations
2016 [56], [66], [100]	• Mobile-based cloud computing, Big Data • Augmented Reality • Wearable Devices	• Data can be store and use properly • Enhances the perception and entertains patients • Wrist-worn device monitoring, and alert system for patients.	• Requires a lot of memory • Costly to develop AR enabled devices • Not all wearable's are standalone
2017 [47], [54], [122]	• Monitoring system using RFID • Body sensor networks • Open Systems IoT Reference Security Model (OSiRM)	• Monitoring patients health history in hospitals • WSNs Enable Long-Distance Data Collection and Transmission • Precisely separates services, interfaces, and protocols	• Expensive because due to use of batteries • Vulnerable to malicious security attacks • Provides duplication of services in various layers
2018 [42], [49], [75]	• Consumer security Index (CSI) • Resource Preservation Net (RPN) framework using Pedi Net • Intelligent medicine box	• Improve consumer decision and security provision • Average patient waiting time are optimized. • Alerts patients to the medicine at the right time	• Takes more time to implementation • Requires a lot of storage • Drug dispensing machines may be programmed incorrectly
2019 [73], [120], [112]	• Healthcare monitoring system for soldiers • Ambient Assisted Living • Security model of blockchain, PoW	• Tracking solders location and secure their cloud data • Get help with daily Activities • Data are highly resistant to technical failures and malicious attacks	• The battery might drain out • Costly • Lack of data modification private keys
2020 [113], [114]	• WSN security model • Internet-based Healthcare Monitoring System (HCMS)	• Secures the collected data • Monitoring health history of patients in the hospitals	• Data is stolen while securing data • Hospital management maintenance is very expensive

C. Semantics

In [51], an IoT-based Semantic Interoperability Model (IoT-SIM) to provide semantic interoperability among heterogeneous IoT devices in healthcare domain is proposed to provide annotations for data. Resource Description Framework (RDF) is a semantic web framework that is used to annotate patients' data to make it semantically interoperable. To extract records from RDF graph SPARQL query is used. To provide interoperability among smart devices a semantic web enabled architecture is proposed [52]. The Semantic Gateway as Service (SGS) integrated with semantic web technologies enables the communication between protocol such as XMPP, CoAP, and MQTT which are used for semantic reasoning to provide semantic interoperability among communicating messages. SEG 3.0 methodology provides benefits to integrate heterogeneous data collected from different smart devices and provide Semantic interoperability in IoT domain [53]. For a satisfying level of performance among low-power heterogeneous networks, there is a need for interoperability protocols and standards.

D. Cloud Computing

The integration of cloud computing with IoT and the smart hospital information system will enable real-time sensor technologies to collect e-storage of all patient's records including images, documents, and videos from different sensor devices. Three primary services are discussed which are provided by cloud technologies in healthcare environments like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) in [54]. The state of cloud-centric healthcare for health record storage is proposed in [55], which overviews cloud technologies as a complete field. A focus on how a large database could be used for data analysis and trend determination is further considered in [56] and [57] The cloud management structure for e-health which creates an efficient, secure, seamless model in provisioning, processing, protecting, enforcing policies, and prediction of cloud management are described for IoT enabled e-health [58]. This platform increases operational efficiencies to a great extent and reduces the cost of health services.

E. Big Data

The adoption of modern technology is not only about the delivery of better-quality care for patients, but also the sustainability of overall healthcare systems. Big data is characterized by 5 V's such as volume, velocity, variety, veracity, and value. In [59], a data storage model for emergency healthcare is proposed that uses the volume and variety of healthcare data. IaaS and SaaS are used to organize heterogeneous physiological data during an emergency which makes it accessible to relevant healthcare providers. In Table II lists the state-of-arts IoTh technologies features and shortcoming. A WBAN system is proposed in [60] which integrates SaaS, PaaS, and IaaS services to create the cloud model. This system primarily sets up a patient's profile, configure who has access to their data, and decide whether

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

Table II: Summary of state-of-arts healthcare technologies.

Technologies/Methodologies	Contributions	Limitations
Radio Frequency Identification (RFID) [46], [47], [48]	• Gather information about user's living environment. • Supervise the health status and increases the power of IoT. • Enables pharmaceutical packaging (iMedPack).	• High cost, Interference problem, some create signal problem
Edge Computing [49], [50], [103], [104]	• Model patient length of stay (LoS), resource utilization rate, and average patient waiting time. • Use wireless body area networks. and increases the power of IoT. • closed-loop systems maintain physiologic homeostasis. • Provide rural medicine, improved patient experience, cost savings	• Less scalable, no cloud aware, can't perform resource pooling
Semantic [51], [52], [53]	• Provide annotations for data. • Enable communication between XMPP, CoAP, and MQTT protocol. less scalable,level of security, • Provide Semantic Interoperability in IoT domain.	• Reduce scalability and flexibility, high level processing, lack data confidentiality technical problem and privacy
Cloud Computing [54], [55], [56], [57], [58]	• E-storage of patient's records. • Maintain a large database. waiting time. • Enforce policies, and predict cloud data mobility, no cloud aware, management for IoT enabled e-health.	• Relay on internet connection, less scalable,level of security, technical problem
Big Data [59], [60], [61], [69]	• Organize heterogeneous physiological data during an emergency. • Patient's data is truly secured. and private. • Extract important information and remove redundant data.	• Data quality, cyber security risk, compliance, cost
Grid Computing [62], [63], [64]	• Drug discovery. • Extends decision making in healthcare, and private. • Provide infrastructure for medical and bioinformatical research.	• Lack of grid software and standards
Augmented Reality [65], [66], [67], [68]	• Train medical practitioners hand-eye coordination. • Increases the sense of presence among participants. technology,low performance level • Provide infrastructure for medical and bioinformatical research.	• Expensive to implement and develop AR lack of security

they want their monitoring to be continuously or periodically on their demand but the system lacks security mechanisms which need to be incorporated to ensure that the patient's data is truly secured and private. A sensor-based system is designed to describe the relationship between the patient's emotional responses and physiological changes [61]. The system enables data mining techniques for the extraction of important information and removal of redundant data from the database where algorithms are applied which focuses on the accumulation of big data set where machine learning could be applied. Another big data management research in the cloud using machine learning is considered [69].

F. Grid Computing

Grid computing is emerging as a promising solution to some of the most technical challenges facing e-Health such as drug discovery. With the massive demands on computer-processing power, and the intensity of real-time data throughput grid computing easily outclasses traditional IT systems. A mobile grid management framework as a key enabling technology for IoT based next generation ubiquitous healthcare solutions is proposed [62]. In another research represents an overview of grid computing, explains the potential uses for grid computing, and proposes a decision framework that extends the Enterprise Desktop Grid architecture to extends decision making in healthcare systems [63].

In [64], MediGRID established a grid infrastructure for medical and bioinformatics research. It enhances the location independent collaboration of researchers by providing grid services in a controlled e-Science platform and gives access to a broad spectrum of applications for bioinformatics, medical image processing, and clinical research.

G. Augmented Reality (AR)

Augmented reality allows us to bring the most useful information from the digital realm into our perception of the environment around us where Virtual Reality (VR) creates an entirely new world. Education is an obvious application of augmented reality in healthcare where workers need to learn a huge amount of information about anatomy and the way the body functions. In [65], presents a distributed medical training prototype designed to train medical practitioners' hand-eye coordination when performing endotracheal incubation's with the help of AR paradigm. A novel Adaptive Synchronization Algorithm (ASA) ensures the shared state maintenance of the collaborative AR environment that increases the sense of presence among participants. An overview of augmented reality and reviews of recent applications in medicine is presented in [66]. AR not only helps the healthcare worker to visualize and interact with three dimensional representations of bodies but also helps patients as a tool for education. Other applications of AR in the medical domain are in ultrasound imaging [67] and optical diagnostics [68].

In the above section, we have analyzed the IoT healthcare methods and reviewed the state-of-arts healthcare technologies. Based on these technologies we will review the IoT healthcare networks in section IV.

IV. IoT Healthcare Networks

A. The IoThNet Topology

The IoThNet topology applies to the composition of distinct components and shows typical outlines of healthcare circumstances that specify whereby a composite computing network handles large numbers of important symptoms and sensor data [13], [138] through remote monitoring. It can respond based on the aforementioned method where that caregivers will be capable to observe the patient conditions from every place [15].

The IoThNet topology applies to the composition of distinct components. It shows typical outlines of healthcare circumstances that specify whereby a composite computing network handles large numbers of essential symptoms and sensor data [13], [138] through remote monitoring. After that, it analyzed and stored the independent data in an appropriate database [62]. It can respond based on the method, as mentioned earlier, where caregivers will be capable of observing the patient conditions from every place [15].

IoThNet topology gateways and access service also needed the Internet protocol (IP), Global System Mobile (GSM) for maintaining the streaming of medical data. For healthcare applications, there are related conceptual structures located in [139], [140], [141], [112]. intelligent Medicine Packaging (iMedPack) and medicine box (iMedBox) recognized in various wireless models as a collection of multiple sensors and interfaces [13].
The IoT healthcare infrastructure of topology that integrates the clinical devices with numerous IoT devices are connected through the healthcare gateways to the health-IoT cloud to investigate and store the collected data [142].

B. The IoThNet Architecture

The principle of the IoThNet architecture specified the IoThNet's physical elements techniques and their functional organization [97]. The architecture of IoThNet has some issues that remained recognized the ability of computer systems of the IoT gateway, caregivers, Wireless Local Area Network (WLAN), multimedia streaming, and secure communications [135].

We have explained in multiple studies [141], [142], [143], [144], [135] that the concept of IoThNet, the sensor, and wearable data transmission over the 802.15.4 protocol have been used in IPv6 and 6LoWPAN network [13]. Data returned by sensor nodes, including the representatives of the User Datagram Protocol (UDP) [13]. There are four alternative methods for addressing mobility [150] including routers. To connect different directed acyclic graph (DAG) and Information Object (DIO) waiting for another possible root nodes. DAG sends the information messages between those routers, soliciting routers, and sending DIS messages to describe the quickest methods of the mobile node itself and initiates both.

In IoThNet architecture has three complex e-Health delivery services as composition, signalization, and data transmission [145]. Methods in the IoThNet while the support of heterogeneous service configuration, signalization protocols accept the Quality of Service (QoS) procedure and resource allocation.

The state of cloud computing synthesis in [59], the data sharing architecture, the structure of the IoThNet platform and IoThNet architecture involves together, which is explaining in the following subsection.

C. The IoThNet Platforms

In the IoT system, the IoT healthcare network platform model is the services platform that is focused on the resident health information as represented in figure 1

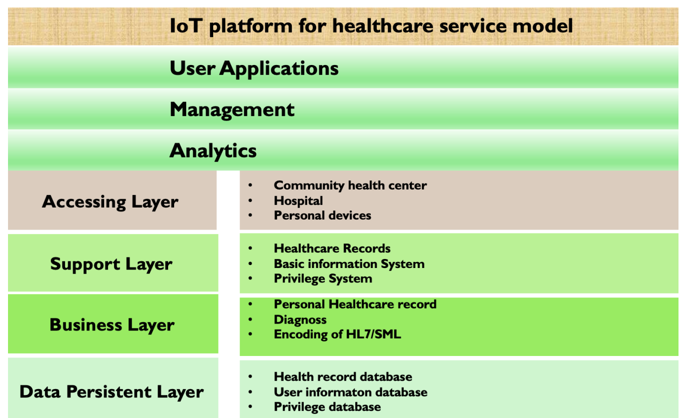

Figure 1: IoT functional framework of platform model for health information service model [14].

It helps to classified the different healthcare models how caregivers can access the different databases according to the healthcare support layer [151]. A related idea of data platforms as the middleware of smart objects and the business layer that describes in [83]. Here model secures the associated interoperability and the automated design methodology platform organized for the IoT network [83]. During the collection of health data, it provides many users with various sensors, enabling the IoT gateway to share the support control devices.

The appliance and software interfaces established using the interface standardization, health data compositions (Electronic Health Records: EHR), and security systems as shows in figure 2 that securely associated interoperability [13] with the proposed structure involves the multidisciplinary optimization, and applying to control the management. The IoThNet, Automating Design Methodology (ADM) platform, is used for recovery objectives, is shows in figure 3 [97]. Especially for particular recovery objectives. In [59] describes IoThNet, and health data are composed utilizing a support control mechanism utilizing a three-layer cloud architecture platform for obtaining omnipresent client data. Several number of studies [146], [147], [148] have explore their concern of IoThNet platform issues. The semantic platform architecture is introduced in [149]. In table III provide the features and availability of topology of IoT healthcare.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

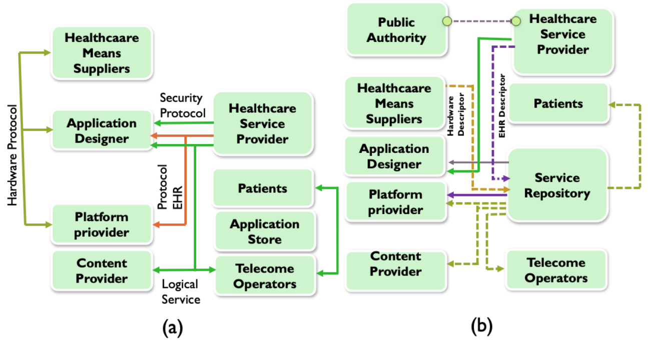

Figure 2: IoThNet Platform Interfaces (a) without standardization (b) with standardization [13]

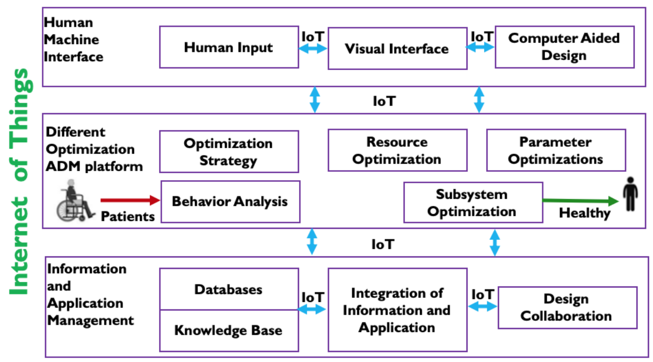

Figure 3: Design methodology of IoThNet framework [97]

Table III: Features and availability of IoT Healthcare Topology

IoT healthcare topology	Features & Availability
IoThNet Topology	• Cloud Computing • Heterogeneous Network(HetNet) • Stored and Analysed independent data • Observe the patient condition • Streaming of ultrasounds healthcare data
IoThNet Architecture	• IPv6 based 6LoWPAN data transmission • Standard gateway protocol stack • Router Addressing protocol
IoThNet Platform	• Human-machine interface • Data and Semantic Interoperability • Secure and scalable transmission • Cloud architecture platform

In this section, we have reviewed different IoT healthcare framework functionalities and IoTh network platform. In section V we will present a survey on IoT healthcare common standards and protocols.

V. IoT Common Standards Protocols

In IoT common standards, several standards aimed to help and analyze the significance and services that we can use for IoT solutions to connect different devices to the internet. Many organizations formed the protocols to efforts the IoT which is driven by the Institute of Electrical and Electronics Engineers (IEEE), EPC-global, Internet Engineering Task Force (IETF), EPCglobal, European Telecommunications Standards Institute (ETSI), and the World Wide Web Consortium (W3C) [4].

In this review, we analyze the three different IoT protocols such as Application Protocols, Service Discovery Protocols, and Infrastructure Protocols. Besides, in IoT applications, few standards protocols may not be supported [4]. In the following, we represent the survey and describe the core functionality of the common standard protocols. Infrastructure protocols used to connect to the devices for exchanging data with protecting and ensure optimum security through the Internet Protocol (IP) network. IP networks are comparatively complex and require more memory, and power, whereas non-IP systems allow less power and memory.

A. Application Protocols

1) Constrained Application Protocol (CoAP): CoAP is an HTTP functional, lightweight Internet Application Protocol and defined in standard RFC 7252 developed by IETF Constrained RESTful Environments (CoRE) [17]. It is used in automation, social networks, and micro-controllers by GET, PUT, POST, and DELETE methods. REST relies on the stateless, client-server architecture that exposes and applies to web services clients and servers like the Simple Object Access Protocol (SOAP) [4].

CoAP can provide separate types of file formats including XML and JSON and bounded in UDP, during the IoT applications, that makes it a proper CoAP. Moreover, some HTTP functionalities to satisfy CoAP reconstruction IoT requirements fundamentals. Based on the standard communication protocol, the REST-CoAP protocol sends a request to the application endpoints and sends back the reply of services and resources in the application. figure 4 shows the overall functionality of the CoAP protocol.

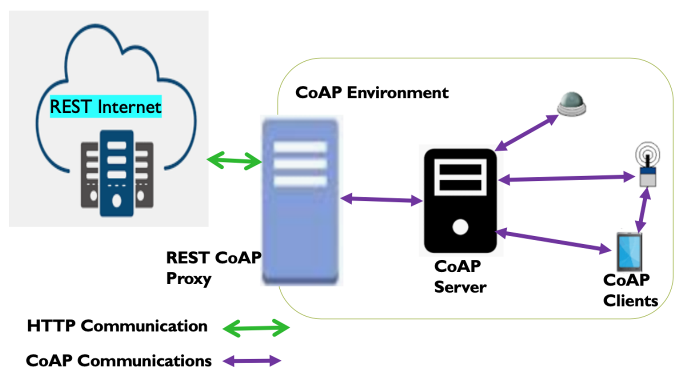

Figure 4: CoAP Protocol [17]

CoAP has two sub-layers such as messaging and request/response that detects the duplication and provides secure transmission across the UDP transport layer. On the other hand, REST communication handles the request/response sublayers. CoAP utilizing the four types of message, namely confirm able, non-conformable, reset, and acknowledgement demonstrated as responses.

The separate acknowledgement method implies the particular server for a particular time before responding to a distinctive client. The method of non-conformable acknowledgment CoAP sends data to the client without waiting for an ACK message, while user IDs have used to identify the duplicates. During the dropping message, the REST message responds with the server or transmission issues occur [4]. CoAP uses GET, PUT, POST, and DELETE methods through the HTTP to perform the Create, Retrieve Update, and Delete (CRUD) methods [4]. CoAP uses the first four bytes of the header format of the encoding message which length is between zero to eight bytes acts as requests and responses of CoAP using the token value. A standard CoAP message can be among

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

10 to 20 bytes. The protocol is designed for Machine-to-Machine (M2M) applications such as tracking monitoring and alert automation. Some of the main features provided by CoAP follows as [17], [18]:

- M2M requirements are constrained using by Web protocol environments.
- UDP [RFC0768] binding with unrestricted security maintaining with unicast and multicast requests.
- Resource observation supports to monitor the application using the publish/subscribe mechanism.
- Block-wise resource transport exchanged the data between the client and the server.
- The web connection range of Constrained RESTful Environments (CoRE) to provide the resources based on the clients' Resource discovery URI path.
- Compliance of interacting with certain things that acts the common REST architecture allows the CoAP with HTTP by a proxy server.
- The protocol of CoAP that developed the Datagram Transport Layer Security (DTLS) layer is integrated with exchanged the confidential message.

2) Message Queue Telemetry Transport (MQTT): Substantive to the Internet is the so-called Internet of Things (IoT) is creating an extensive Machine-to-Machine (M2M) network. So all of the devices and sensors and systems and actuators can connect to and communicate on the Internet, and with that, they need a communications protocol. IoT understands each other, and one of those protocols is the message queue telemetry transport MQTT is a TCP based subscribe and publish messaging protocol designed for lightweight M2M communications. We have interacted with those devices into IoT devices and sensors. Machines themselves are communicating with each other on the back end, and most IoT data centre traffic is the M2M traffic. It was initially developed by IBM in 1999 and was standardized in 2013 at OASIS [19]. It is based on the hub-and-spoke model, let's figure out how MQTT works. Figure 5 shows the architecture of MQTT [4].

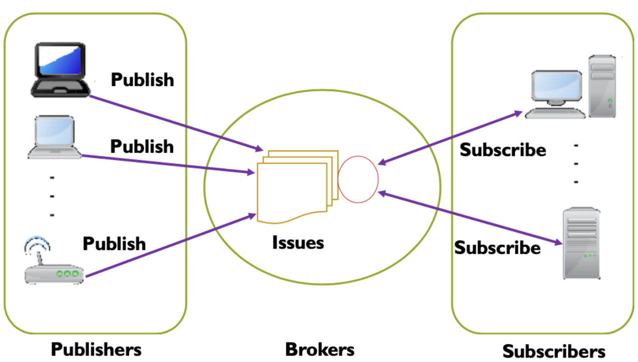

Figure 5: The architecture of MQTT [19]

Embedded devices are connecting with MQTT networks with applications and middleware services [4]. MQTT has been used in many applications like healthcare applications, low-cost consumption, and Facebook notifications.It allows for the clients to send concise one-hop messages to the broker and also receive messages if they've subscribed to a specific topic.

Clients update the topic of speed or publish the speed information, for instance, it publishes speed as 15 MPH. Clients who subscribed to the topic of speed will get the information as new pieces of information related to the topic published or updated. These clients can publish or receive messages based on a particular topic from a security state. So those clients can undoubtedly log on password authentication has become an oasis standard.

Researchers have been struggling with over the last couple of years, particularly with IoT standards in communications and connect Wi-Fi TCP/IP. As far as IP is concerned, Message Queue Telemetry Transport (MQTT) that is work in Machine-to-Machine (M2M) and Internet of Things (IoT) environment with various data like accelerometer, light intensity, etcetera, via Bluetooth LE to a Raspberry Pi and a local visualizing display. The data sent from the sensor to its *Raspberry Pi* is also published to the cloud via MQTT.

3) Extensible Messaging and Presence Protocol (XMPP): Extensible Messaging and Presence Protocol (XMPP) is a communication standard used in IoT originally developed for Instant Messaging (IM) formalized by the IETF model utilizing for different video calling, telepresence, multi-party chatting, and voice [20] and is actively extended by the XMPP Foundation. XMPP provides instant messaging applications to manage authentication, access control, privacy analysis, hop-by-hop, and end-to-end encryption, and adaptability with other protocols [21]. Figure 6 shows the ultimate performance of the XMPP protocol, in which gateways can connect among different messaging systems [21].

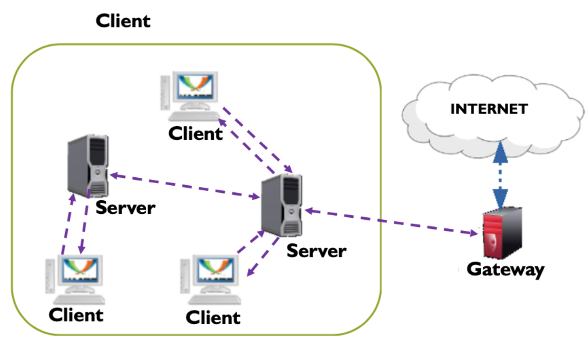

Figure 6: Communications in XMPP [21]

XMPP message content is based on Extensible Markup Language (XML), a text-based means of transferring structured data, and understandable to a human reader as well as machines. XML is related to HTML, a protocol used to construct web pages, and both of these are known as markup languages. The keyword extensible is an indication that XMPP can be adapted to use in many cases. This extensibility leads to full freedom to create compatible versions which can intercommunicate utilizing standard internet protocol.

TCP as a transport medium makes XMPP universally transmittable; it may also be transported over HTTP by which means it may penetrate firewalls. XMPP has been around for some implementations aimed at many purposes already exist further scope for flexibility. There are numerous extensions developed by the XMPP foundation, and XMPP uses gateways to make other protocol services available on an XMPP network. It also has a means of discovering services and presence on a network and is designed to support instant pushing of messages over an established TCP link. Instant Message (IM) a client connects to a server to establish a TCP session then opened between the two participants.

XMPP allows standard internet encryption-based TLS authentication. The security layer implements a specified form of authentication as the XML stream is opened to the local server from the sending client. Note that this is an open stream tag for the XML closing stream. Thus the exchange as a whole is encapsulated in an XML stream that shows how the stream is set up. The stream is not fully established until the service conditions are met; the server sends conditions called features required. Only encryption TLS is asked for features that may be mandatory or negotiable and may include other stipulations such as the compression method over a single TCP connection. XMPP allows for instantaneous transmission which is useful for monitoring devices as same the privacy measures that are used for instant messages can be applied to the data transfer.

XMPP uses universal protocols and can travel across textual firewalls depending on the configuration, minimizing overhead on the XMPP payload. The benefits of leveraging and existing developing technology come with certain information that is maintained and extended under the XMPP standards. Using XML requires XMPP that is a text-based transmission over the high network.

4) Advanced Message Queuing Protocol (AMQP): Advanced Messaging Queuing Protocol is an extensive common standard in IoT application protocol for focusing on message-oriented environments [22]. AMQP allows the IP systems messages to be passed between applications one to one, one to many, and exactly-once delivery method. AMQP is a new standard designed that enables interoperation and communication and sharing of resources between new and legacy applications. It requires secure transport protocol infrastructure and middleware acts as a conduit between applications and shared resources ties organizations and technologies across time and space.

AMQP transport mechanism is the communication that supports various broker architectures which may be used to receive cue route and deliver messages. It's interoperable reliable open standardized complete and safe to supports various broker architectures that may be used to receive cue route and deliver messages or be used Peer-to-Peer (P2P) the new features provided by AMQP.

AMQP is an efficient protocol that separates the wire from broker architectures and management. The multiple broker architectures are supported, including P2P message security global addressing extensible layering. For supporting multiple messaging standards consortium that is created by AMQP. The frame size is four bytes. Inside the frame, the position of the body is given by Data Offset (DOFF). The field Type shows the format and design of the frame.

5) Data Distribution Service (DDS): Open standard protocol, DDS is the publish-subscribe protocol or data distribution service for real-time M2M communications that has been deployed by Object Management Group (OMG) [23], particularly user interaction priority. It's collecting the edge outliers that send an SMS notification then push it through to a predictive model. Publishers and subscribers produce and consume the Distributed Relational Information Model (DRIM) that a centralized server to store the specific information of the application. DDS has a very powerful QoS model which is based on a set of two policies for that quality of service control end-to-end property. DDS relies on Quality of Service (QoS) like MQTT or AMQP publish-subscribe application protocols which uses multi-casting and provide a broker-less architecture to make unique and high reliability to its applications [4].

B. Service Discovery Protocols

The IoT requires the large scalability of resource management mechanisms that can obtain self-configured register and discover resources and services in an effective, and active way. In IoT, the area of DNS Service Discovery (DNS-SD) and multicast DNS (mDNS) is one of the efficient and powerful protocols [4]. Our analysis studies confirm light versions of IoT. mDNS and DNS-SD protocols have been designed primarily as resource-rich devices, environments [24], [25].

1) Multicast DNS (mDNS): Multicast Domain Name System (mDNS) is to solve the host names to IP addresses and purpose for base systems in some IoT applications that can make the task of a unicast DNS server [26]. It seems to unicast the Domain Name System that is utilizing for the same programming interfaces, zero-configuration services, to check the packet formats, and operating semantics. While it can work with unicast DNS servers with stand-alone capability.

Apple Bonjour and Linux nss-mDNS services published the mDNS protocol as RFC 6762, and implemented by multicast User Data-gram Protocols (mUDP). mDNS client requires solving a hostname, and IP multicast query message communicates with clients that require the host to recognize the hostname. IP address and the target machine includes the multicasts a message. A subnet can message to update mDNS caches to all devices. By default, top-level domain mDNS mainly resolves hostnames. The structure of the Packet mDNS ethernet frame is a multicast UDP packet to the MAC address. DNS, UDP port format based on the IPv4 address or IPv6 address that has two parts the header and the data.

QTYPE and QCLASS indicate the two 2-byte flags that the Flags will usually for a query and a response and data begins with a domain name. A list of segment strings defined by The FQDN is starting with the hostname and closing with the top-level domain. Each string consists of a UTF-8 length byte that is terminated with the FQD, and a null string follows NLD. IPv4 address record consists of a 2-byte type field, 2-byte class field, a 32-bit signed integer. The part of the class value is not to be interpreted with a cache-flush bit. A practical illustration that uses mDNS service data can be observed in [4].

2) DNS service discovery (DNS-SD): DNS-based service discovery (DNS-SD) is the pairing functional services for clients based on the message DNS (mDNS) [4]. Using the DNS-SD protocol, for the client's services in a particular standard network like mDNS [4], without external administration in zero configuration aids to connect machines or configuration [27]. It uses UDP, to send the packets from mDNS to DNS using specific multicast addresses. DNS-SD support to service discovery mechanism that has to implement for the RESTful web interface. It also has weighted load balancing which is quite rare and priority-based features.

C. Infrastructure Protocols

1) Routing Protocol for Low Power and Lossy Networks (RPL): According to [4], The link-independent routing protocol based on IPv6 is a working organization normalized for resource-constrained nodes called RPL [28], which provides routing across low-power and lossy links (ROLL) [29]. Several IoT routing protocols like simple and complex, multipoint-to-point, point-to-multipoint, and point-to-point [4] support RPL. Routing Protocol for Low Power and Lossy

Networks (RPL) is a distance vector routing protocol based on Destination Oriented Acyclic Graphs or DODAGs that show the nodes diagrams.

To control the routing topology and to maintain the routing information RPL uses four types of control messages is given bellow:

I. *DODAG Information Object(DIO)*: It multicasts downwards. A given node In a DODAG may multicast this message, which lets other nodes know about it, Things like whether the node is grounded or not, whether it has two modes of operation (MOP) storing or non-storing, and it announces other nodes "if they are interested to join" and it is based on destination IPv6 addresses [30].

II. *DODAG Information solicitation(DIS)*: When no announcement is heard, and if a node wants to join a DODAG, it sends a control message. For that, it wants to know if any DODAG exists.

III. *DODAG Advertisement Object(DAO)*: It is a request send by a child to parent or root. This message requests to allow the child to join a DODAG.

IV. *DAO Acknowledgment(DAO-ACK)*: It is a response send by a root or parent to the child, this response can either be Yes or No [30].

V. *Consistency check*: Deals with security.

2) 6LowPAN: IoT 6LowPAN communication protocol is an acronym in for IPV6 over low-power wireless personal area networks implementation of the internet. There are common IoT communications standards like limited packet size that link-layer technologies rely on some different versions of technologies, e.g., a maximum of 127 bytes for IEEE 802.15.4, various addresses lengths, and low bandwidth [31], [32].

In 2007, The IETF 6LoWPAN working group developed the standard [4]. The IPv6 over Low Power WPANs required by the 6LoWPAN is mapping services [31]. The IoT common standard addresses header compression, reducing capacity or performance to reach the IPv6 Maximum Transmission Unit (MTU), and link layer to support forward the multi-hop delivery [32].

6LoWPAN is supported by a combination of some headers using Datagrams. There are four types of headers that are recognized through the two bits [31] No 6LoWPAN Header(00), Dispatch Header(01), Mesh Addressing(10), and Fragmentation(11).

According to [32] by NO 6LoWPAN Header, packets that do not confront the 6LoWPAN specification will be discarded. The compression of IPv6 headers or multicasting is performed by specifying the Dispatch Header. Mesh Addressing header identifies those IEEE 802.15.4 packets that have to be forwarded to the link-layer. For datagrams whose lengths PC exceeds a single IEEE 802.15.4 frame, the Fragmentation header should be used. 6LoWPAN removes a lot of IPv6 overheads in such a way that a small IPv6 datagram can be sent over a single IEEE 802.15.4 hop in the best case. It can also compress IPv6 headers to two bytes [32].

3) IEEE 802.15.4: The Medium Access Control (MAC) and physical layer (PHY) is a Low-Rate Wireless Private Area Networks (LR-WPAN) [16] that is developed based on the IEEE 02.15.4 standard protocol. Low Rate Wireless Personal Area Network (LR-WPAN) is the most common low power consumption, low data 2.4 GHz, and 16 5-MHz channels with 250 kbps. The Physical data rate is 50 kbps application. Peak current depends upon the symbol rate like multilevel 4b/symbol, Direct Sequence Spread Spectrum (DSSS), CSMA/CA, Backoff, Beacon, Coordinator.

Types of Full Function Device (FFD) and Reduced Function Device (RFD). FDDs become the coordinator and can also route the message to other nodes. FFDs that start a PAN become the coordinator in a Star topology to communicate to/from the coordinator, and P2P topology directly can communicate. Nodes join by sending an association request to the coordinator to assign a 16-bit short address to the device. Devices can use either the short address or EUI-64 address.

4) Bluetooth Low Energy (BLE): The short-range uses with less power, consumption, or energy efficiency are called Bluetooth Low-Energy (BLE). The range of BLE about 100 meters that are standard Bluetooth while its latency is 15 times less [33]. It promotes the Internet of Things(IoT) that has been used for Low development and module costs to perform by a transmission power between 0.01 mW to 10 mW [4], [34].

The Bluetooth Low Energy (BLE) common standard rapidly developed by smartphone models. The utility of applying the BLE standard has been explained in vehicle-to-vehicle communications with fully wireless sensor systems [33], [35]. In terms of power loss device to the ratio of transmission energy [36] where BLE is also more effective. BLE network stack that sends and accepts bits using the Physical (PHY) Layer. The Link Layer services through medium access, connection establishment, error control, and flow control are providing over the Physical (PHY) layer [4].

Multiplexing data flows, fragmentation, and reassemble the packets provided by the Logical Link Control and Adaptation Protocol (L2CAP). Generic Attribute Protocol (GATT) upper layers that give effective data collecting from the sensors and Generic Access Profile (GAP) [4]. In star topology, BLE allows things to explore as administrators or menials channels [4]. Nowadays, it is more powerful with low power technology in smartphones unlike ZigBee, Z-Wave, LoRa, and others.

5) EPCglobal: The collaborative connection of Electronic Product Code (EPC) that is transforming to commerce around the unlocking benefits for companies and consumers. EPC global being that initial planning activities for the improvement of EPC and standard RFID technology [4]. RFID standard tags participate in product information to the users [37]. Beyond the EPC global, IoT required of its openness, scalability, interoperability, and security [38].

There are several types of EPCs are 96-bit, 64-bit (I), 64-bit (II), and 64-bit (III). EPCs control over 16,000 organizations' unique identities by 64-bit, including 1 to 9 million products. There are 33 million serial numbers of each type [4]. Besides, 268 million companies with unique identities support the 96-bit type with 16 million classes of products and 68 billion consecutive estimates during specific class [4]. Radio signal transponder (tag) and tag reader consists of the RFID system [4]. Figure 7 shows the radio waves that work using RFID.

Thailand traffic congestion is a real barrier to everyday Commerce EPC is helping trading partners remove the roadblocks incoming deliveries are received and processed instantly. Misplaced merchandise is no longer a problem

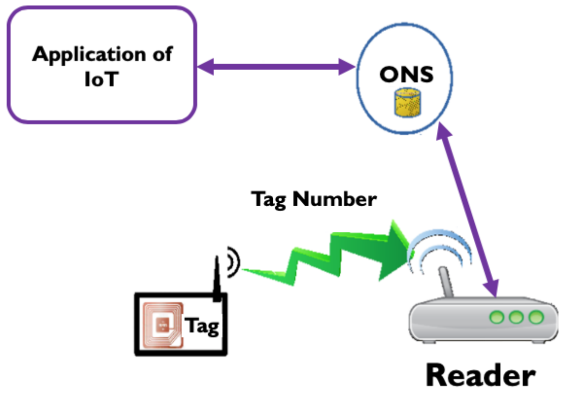

Figure 7: RFID system [4]

as EPC helps locate products in the stock. Hong Kong to Japan trading partners are capturing, sharing and utilizing real-time EPC data to better manage the flow of product and information from the point of manufacture to final distribution, the existence of the standards allow such adoption. Now well European perspective, the recent development of EPC an RFID is actually getting into the implementation level has really moved.

6) LTE-A (Long Term Evolution-Advanced): The future of mobile/cellular communications will be very different from what we are used to today. The new technologies LTE-A encompasses tremendous impact protocols on human possibilities as the world continues to become more connected using 5G and the evolution of 4G for Machine-Type Communications (MTC) [39]. LTE was introduced some six years ago, which is 10 times faster than 3G, then LTE has evolved to LTE-Advanced that is increasing data rates by another factor. LTE-A improves the user experience through increases in bandwidth efficiency and reduced latency. LTE-A uses Orthogonal Frequency Division Multiple Access (OFDMA) [4]. The architecture of the Core Network (CN) in LTE-A that controls mobile devices and IP packet flows [4]. Another part that is the Radio Access Network (RAN) provides wireless transmission and radio access protocols [4].

The first LTE networks were limited to a maximum carrier bandwidth of 20 MHz. LTE-Advanced increase that to 100 MHz by combining or aggregating up to five carriers. LTE-Advanced aggregates up to 32 carriers, a massive 640 MHz bandwidth. LTE-Advanced not only allows the use of more spectrum, but it also does so more efficiently by increasing the number of antenna paths, and it serves a single radio cell with sixteen and later up to 64 antenna paths. LTE-Advanced radio networks reduced latency to 10 milliseconds for mission-critical Public Safety Communication (PSC)s and cost-efficient connectivity to the Internet of Things(IoT).

This protocol has challenges before-mentioned as a significant network bottleneck when a high volume of devices are accessing the network [39]. Another challenge, Quality of Services (QoS) can be negotiated with access to the network. Those difficulties reviewed in [39] along with a resolution based on support learning for eNB selection [40].

7) Z-Wave: Low-power wireless communication protocol believed in Z-Wave. Z-Wave protocol allows multiple wireless devices to communicate with each other affordably and reliably with easy to use smart products. Z-Wave was first developed by a startup company named chancy's, which was founded by two Danish engineers. In 2008, it was acquired by ZenSys (Currently Sigma designs) after seeing the potential of this technology and decided to join their alliance, which is formally known as G Wave Alliance. Z-Wave provides around 30 meters of point-to-point communication that transfers the small data transmission [4]. Secure communication is desirable in this protocol by unrestricted ACK messages [4]. Table IV reports the characteristics of IoT common standard protocols. Wi-Fi, Bluetooth and other radios that can produce

Table IV: Characteristic of IoT Common Standard Protocol

Protocol Name	Characteristic
CoAP	• Web Transfer protocol (RESTfull). • Application protocol. • Support separate file formats. • IPv6 support. • UDP connection
MQTT	• M2M Networks. • TCP based subscribe and publish Message • Application and middle ware services.
XMPP	• Communication standard based on IM • Transferred structure data • TCP service protocol • Internet encryption base authentication.
AMQP	• Message oriented Communication • Sharing resources and enable interoperation's • P2P communication
DDS	• Real-tiem M2M communication • Store the specific application information • End-to-end property (Quality-of-Service) • Sharing the distributed data between different things
mDNS	• Monitor the hostname to IP. • Control the unicast DNS. • UDP port format. • IPv4 or IPv6 supported.
DNS-SD	• Pairing functional services. • Client based services • UDP supported
RPL	• Proactive RESTfull application. • IPv6 supported. • Routing access protocol. • To control and maintain the routing topology. • Deals with security
6loWPAN	• Mapping the communication standard services. • UDP connection. • IPv6 supported. • Recognized multiple header compression.
IEEE 802.15.4	• P2P communication technology. • Star topology communication.
BLE	• Perform short range transmission. • Vehicle-to-vehicle communication. • Wireless sensor communication.
EPCglobal	• Using the RFID technology. • Using Radio signal transponder (tag).
LTE-A	• Mobile and cellular communication. • Control the mobile devices. • Using Radio Access Network (RAN). • Serves single radio cell.
Z-Wave	• Using game-changer method in IoT. • Low power wireless communication protocol. • Unrestricted ACK messaging. • Control the network topology.

interference whereas used its band 8.42 MHz and Z-Wave uses a low power consumption for the operation. The Z-Wave protocol controller keeps network topology that is performed by the source routing method and allows the tracking inside a packet [4].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

The above section surveys and analyzed the IoT common standard protocols and provide different IoT healthcare topologies, and its features. In the next section VI will reviews the IoT healthcare security system.

VI. IoT Healthcare Security

A. Security Requirements

Wearables healthcare applications distribute personal and private data [41]. Security threats like Denial-of-Service (DoS) are targeted by hackers connected to the Internet and attackers interfere with medical data, and unauthorized access can be pursued to control health data and conflict with medical analysis. Therefore, modernized security applications are required concerning IoT health devices is a challenging task.

1) Scalability: In general, healthcare applications are connected to the Internet for IoT. The amount of IoT applications continuously developed, and also devices are getting connected to the global information network [41]. For instance, a body temperature sensor or a heart monitor may be connected to the internet and reveals the concerned caregiver of the user's health conditions [41]. IoT applications collect a large number of data. Before-mentioned users are connected at home staying at home network, where as they are connected to the office network during the office work [41]. For these circumstances, healthcare application needs a security algorithm that is a serious challenge for different networks configurations.

2) Communications Media: In common, IoT healthcare devices are connected to networks through an extensive range of wireless common standards protocols such as Zigbee, Z-Wave, Bluetooth, Bluetooth Low Energy (BLE), WiFi, GSM, WiMax, and 3G/4G [13].

3) Multiplicity of Devices: IoT healthcare networks devices covering the proficient computer to low-end RFID tags. According to the range, the ability of devices depends on their computation, energy, memory, and embedded software [13] Accordingly, the challenges multiplicity that can also provide the mildest of security devices.

4) A multi-protocol Network: Based on IoT healthcare devices may transmit data to other devices through a particular network protocol to the IP network. A health device may connect an IoT health network anyplace, anytime [13]. Also, IoT healthcare devices can transmit within a network either appropriately (with proper exit notification) or disgracefully (abruptly) [13] with powerful network topology. Accordingly, during the aforementioned dynamic network topology is a hard challenge for devising a security model.

5) Attacks based on Information Disruptions: An attacker to provide incorrect information and transfer the integrity of the information during the manipulated or analyzed health data [13] Such attacks include the following [86].

Interruption: Data transmission links to be dropped or unavailable during the Denial-of-Service (DoS) attacks. Healthcare service availability, system functionality, and design ability is the kind of network attack threatens network [13].

Interception: The fact of preventing the medical information provided in messages to threaten data privacy and confidentiality [13].

Modification: Several modifications are being carried out through the IoT health networks that obtain illegal entrance and tamper to generate chaos and mislead innocent entities into the health data.

Fabrication: Threaten message authenticity and confuse innocent participants is an adversary forge messages by injecting false information.

Replay: An adversary replays existing messages to threaten message freshness. Also, this increases confusion and misleads innocent entities.

6) Attacks Based on Host Properties: According to [45], host properties of attacks are the three kinds of attacks that describes below:

User Compromise: The user's health devices and networks by cheating or stealing by adversary comprise. User compromise attacks that delicate data, like user data, cryptographic, and passwords.

Hardware Compromise: Hardware may extract on-device program codes, keys, and data with physical devices. A malicious code compromised an attacker may re-program with devices.

Software Compromise: Some software limitations, such as system software, applications, operating systems, and the attackers take those advantages. buffer overflow and resource exhaustion, are the malfunction or dysfunction states.

7) Confidentiality: Confidentiality guarantees the idea of the inaccessibility of unauthorized users for individual medical information. Besides, confidential messages continue sharing their content with listeners. Data confidentiality can be improved by using Public Key Encryption (PKI). PKI creates an effective approach to data encryption as it can provide a high level of confidence for exchanging information in an insecure environment. Atzori et al. [9] presents a conceptual design and a prototype implementation of a system based on IoT gateways that aggregate health sensor data and resolve privacy issues through digital certificates and PKI data encryption.

8) Integrity: Integrity ensures that consistency in actions and values that received medical data do not alter by an opponent and aren't intercepted. Also, the integrity of collected data and content should not be agreed upon.

9) Authentication: The identity of the peer, which is authenticated communication make sure only authorized users to allow an IoT health device to secure.

10) Availability: The survivability of IoT healthcare services intends to increase local or cloud services to authorized agents while required, supporting denial-of-service (DoS) assaults. The availability relates to the capacity of the IoT applications to concurrently render services for everyone in several areas.

11) Data Freshness: All IoT healthcare system provides amazing time-varying frequencies; there is a must to assure that every information is safe. Data freshness combines data freshness and key freshness [13] because data freshness signifies that all data set is current and ensures that no adversary replace the old information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

12) Non-Repudiation: Non-repudiation expertise controls the broadcast message which is sent by the authenticator node.

13) Authorization: The particular allowed nodes are convenient for network security or applications that defining access rights/privileges to devices, which is relevant to message security by the authorization.

14) Resiliency: The security system should be protecting the system/ device/data from any attack. Resiliency ensures that the ability to improve from the difficulties.

15) Fault Tolerance: The application of security services should be processed to particular systems such as software malfunction, understanding the device [13].

16) Self-Healing: IoT healthcare devices may break or run out of power. During these circumstances, all collaborating devices should facilitate a minimum level of security [13].

B. SECURITY CHALLENGES

1) Restriction on Computation: Now, IoT health applications and services are embedded within terms of low-speed processors, and low energy consumption. Also, IoT healthcare applications are not well-designed to make computationally high. Processing frequency only seems a actuator or sensor. Consequently, preparing a condensed preservation clarification that reduces source using and maximizes the challenging task [13]. Processing speed is the computational speed of a system in the uncertainty restrictions. Thus, researchers should focus on standard cryptographic systems that expect complicated computations are infeasible reducing devices [43].

2) Memory Limitations: The significance of data progresses at a surprisingly large data storage becomes a significant challenge in healthcare. Most IoT healthcare applications have low latency memory and have very low memory [13] devices are activated utilizing an embedded operating system(OS), several software systems. Data storage also concerns data security. To assure that data distributed within IoT application in the healthcare system is securely transferred using sufficient data storage. As we move ahead, this is a significant challenge for data storage that addresses security. It is required to have massive storage for this large amount of health data. So, IoT healthcare applications and databases need to be a very scalable infrastructure of memory [13].

3) Uncertainty: Nowadays, tremendously increasing the use of IoT-based healthcare devices. These applications collect a massive number of health-related data and based on the collected data. The healthcare system defines the perception of prospective healthcare systems [41]. In this context, Knowles et al. [44] propose the point of risk/uncertainty, which all describes as “a lack of understanding about the reliability of a particular input, output, or function of a system that could affect its trustworthiness”.

C. A THREAT MODEL

IoT threatens one of the initial activities in the security engineering process. Threat modeling and its role in the risk management process through a threat modeling approach that includes identifying the system architecture. IoT systems threat model based on a relatively simple IoT system all organizations that have limited resources to deploy on security measures, and there are so many security tools, technologies, and techniques. Security value integrating threat modeling into the risk management process and their impacts on the system, where to extend the defensive technologies.

Healthcare data flows can see the high-value assets in the intelligently identify threats to the system that choose from deriving the systems. There are multiple approaches to threat modeling and reviewed a particular communication system. The thread model collects data and supports trend analysis to be determined based upon data. Additionally, supported real-time data security to maintain the integrity of all data collected, the confidentiality of sensitive data within the system to determine that the data might be sensitive.

IoT health devices and networks are exposed to security comprises the development of the local network, cloud networks, and cloud services with enhanced interaction between IoT devices, networks, cloud services, and applications [13]. Table V addresses the features of IoT healthcare security requirements and challenges.

Table V: IoT healthcare Security requirements and challenges

IoT Healthcare Security	Features issue
Security Requirements	• Denial-of-Service(DoS) • Unauthorised access • confidentiality of data • Making trusted platforms • Authenticity • Data transmission control
Security Challenges	• Maintain the standardization • Interaction with Internet • Connect the scalable networks • Integrate the data management • Control security protocol • Embedded devices with software
Attack Taxonomy	• Integrate with analyzed health data • New technical paradigm
A Thread Model	• Integrate to risk management process with thread model

D. AN ATTACK TAXONOMY

The Internet of Things (IoT) transfers the data over the Internet that involves a complex network. The vital extension of IoT in healthcare applications that may require safety-critical services and sensitive data to be embedded online. We reviewed the network security of healthcare domains that taxonomy of attack between the IoT networks like tangible, predictable threats to support IoT developers for information on the chance of security.

After reviewing the different IoT healthcare security requirements, their challenges, various threat models and attack taxonomy, the authors proposes a Blockchain based architectural model in section VII.

VII. PROPOSED MODEL

In the health care system, medical information are sensitive by nature, and keeping them safe and secure is a challenging task. Regardless of how IoT is used in healthcare, the attack surface and vulnerabilities for the IoT infrastructure remain pretty much the same since the security risks are inherent to any connected system/device. There are several angles to this problem- malicious hackers, naive unaware users and malicious software all can wreak havoc.

In recent years, blockchain is an emerging decentralized architecture and distributed computing paradigm that has been concentrated in bitcoin and cryptocurrencies applications [164]. Multi-tier blockchain protocol processes with different authorities applying by peer-to-peer healthcare communications for securing the patient's data [165]. We have approached raising concerns in the domain of IoT-based healthcare which is gained blockchain technology and compare with the existing model/technologies. The witness of blockchain applications is used in IoT healthcare [166]. To differentiate the distinct act of surveyed protocols are analyzed using several frameworks to implement suitable applications such as fault tolerance, drawbacks of the security, scalability and trad-offs [167].

We have to consider the possibility that a device can be hijacked by an unscrupulous person willing to do harm, making the fidelity of the device doubtful. A device can also be infested with malware.

We also have to consider the data transfer path and devices on that path for possible eavesdropping or manipulation to destroy integrity of the data. The other attack surface is the servers that will store the data, but that is not our concern at the moment since safeguarding data storage is a commonly researched issue with standard processes in place.

Therefore, we propose a security model for IoT based healthcare information system that is focused on the following aspects - keeping a device from being hacked/hijacked and providing security and integrity of the data from IoT enabled sensors and the edge server. The other issue of naive user is not of any concern since it relates mostly to proper user training and user consciousness and better robust firmware and software design.

Furthermore, our model concentrates on IoT infrastructure of large scale health care service centers such as hospitals and clinics where IoT enabled devices will constantly monitor both indoor and outdoor patients' health condition and/or serve other purposes. But smaller scale or personal IoT health monitoring system may also benefit from the model. To sum up our focus-

1. Provide robust security mechanism that will ensure device safety so that someone with ulterior motives may not be able to gain access and take control of a device.

2. When data about health conditions of patients are transmitted from the sensor to the edge server, provide end-to-end security and confidentiality to ensure integrity and validity of data.We propose:

i. Barebone operating system for medical IoT devices/sensors that will only contain minimum viable interface to the outside world by limiting network services/OS level commands.

ii. To ensure data integrity, include blockchain for hardening record related processing such as creation, deletion and updates. Although IoT and blockchain have different working principles and architecture, the integration of these two networks is attainable by using a software platform. Therefore, in this section, an integrated IoT based blockchain network platform for enhancing the security issues of the smart health care system is proposed. To mitigate the security problems, an IoT-based security architectural model has been proposed in this review. Figure 8 illustrates the general architecture of proposed approach and represents the connection between different types of actors. IoT Sensor devices, IoT gateways, and blockchain network, each of the technology has a different role in this architecture. The IoT sensor devices are responsible to perceive the medical data by using sensors such as Pressure sensors, Heart rate sensors, electroencephalogram sensors, airflow sensors, etc. Then, the collected sensing data are forwarded to the IoT gateway device by wireless LAN or similar other technology. Upon reception, the gateway device transmitted the received data to the blockchain network through wired or wireless connections.

Finally, received data are processed in the IoT blockchain end and recorded in its peer node. Generally, blockchain is a peer Figure 8 proposed model of IoTh based Networks including blockchain to-peer network platform where each node contains the same record of data storage. In the healthcare blockchain, when an initiator generates a new health record, it signs the record with its private key and initiates a data storage request.

In the meantime, the initiator broadcasts this request to all other nodes in the network for validation. All other peers participated in the validation process and tried to acquire the nonce. The peers who get the nonce earliest will validate the record. Next, the validates result will be broadcast to all other peers of the network. Once the data is stored in the blockchain, no one can modify or delete the record. It ensures data integrity. However, in the architecture, we have proposed an ordered peer network in the blockchain part. Each pair maintains its own IoT data. This network provides data privacy by apply access control mechanisms and preventing unauthorized access to the network. To obtain any record, firstly, the node needs to register and become a part of this blockchain network. Before any node can join in the blockchain, it must be approved and be declared with an authenticated certificate. A security manager on the platform will continuously monitor the security and protection issues of the network. By the use of valid IDs and access permission, patients can view the medical record documents. Thus the network also facilitates the regulatory conformance. IoT healthcare network configures a secured communication protocol (Zigbee, Z-wave) that consists of the patient's data to prepare the synchronization and retrieve the data. The collected data connected with different services to identify health reviews. The IoT server has the ability for verifying the user for monitoring, interpret, and approve health analysis [16].

IoThNet maintenance access to the determination abilities the communication and response of medical data and allows the use of healthcare information. The entirety of the aspects of the Internet of Things (IoT) is the system of wearable's patterns, secured with software, electronics, sensors, actuators, and connectivity which allow the assessable methods to relate and transfer data [128].

Proof of Work (PoW) that transaction is simply recognized and tested the method to complete computational activity has been used by approving connections based on blockchain security [128]. Its handle by Hash computation [128] including designing a block. Hash is unique and created by the Secure Hash Algorithm (SHA-256) with cryptographic Hash [128]. Blockchain gives the most useful relevant technology concerning the healthcare system.

Blockchain-based security is not free from challenges. In terms of large scale and performance, the challenges of blockchain-based security depend on transaction network speeds and standardization.

To verify blocks, currently using several agreement mechanisms by blockchains, including PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake),

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

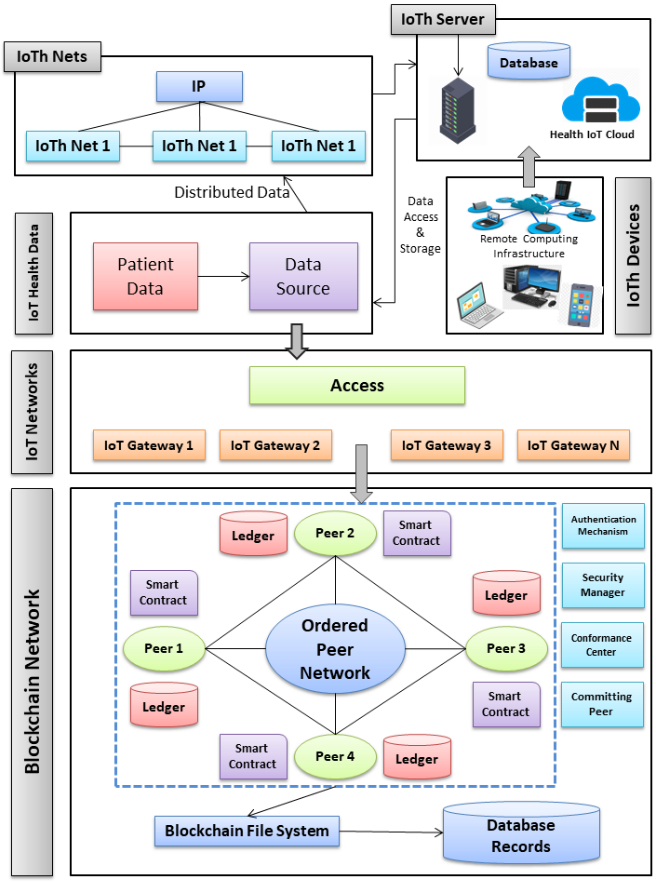

Figure 8: Proposed model of IoTh based Networks including Blockchain

PoA(Proof of Authority) [168].

This security model will help-keeping a device from being hacked and integrate data from IoT enabled sensors and edge servers. In section VIII will represents the IoT healthcare applications and services (A & S).

VIII. IoT Healthcare Applications and Services

A. *IoT Healthcare Applications*

1) Dropping Emergency Room Waiting Time: Reducing waiting time in the emergency department is a top priority for most healthcare systems. New research gives hospitals a big data-based framework so that they can easily maintain the problems. With predictive analytics, the average flow of patients through an ED can be determined by the algorithm using IoT. The algorithm identifies wait times during patients' admission, the average flow of patients through an ED so that hospital authorities can keep their average wait time at a reasonable level [101]. One research shows that a New York hospital makes a partnership with GE to install IoT based special sensors on hospital beds where the sensors will indicate whether a bed is free or occupied by a patient [102]. In [2], a wireless sensor network MEDiSN is developed for monitoring patients' physiological data during disaster events and the emergency period, which comprises Physiological Monitors (PMs) to deliver medically actionable data.

2) Telehealth: Telehealth is essentially allowing remote monitoring of citizens of all ages to monitor vital health data and to take control of their well-being. In [70], IoT based real-time monitoring is proposed for active and real-time engagement of patients, hospitals, caretaker, and doctors. The suggested algorithm predicts the minimum time for separating messages and measures the minimum queue sizes for the health care personals nods to manage the traffic and avoid the dropping of messages. The blending of IoT and telemedicine in [105] reveals CyberMed and which helps people to use medical devices made for the patients. The collected data gets transmitted to the cloud for nearly instantaneous evaluation by the physician and ensure wearability and data quality. A telemetric system based on IoT provides telemedicine facilities to track bed-ridden patients and monitor patients' health is proposed in [110].

3) Tracking of Information: The integration of available medical technologies with the IoT as well as with patients and their environment has given a new scope for data collection and making better decisions. Focuses on the IoT devices can be used to improve the health of people, along with ensuring that there are no mistakes in the process of medication and medicine delivery is proposed in [71]. RFID and IoT two core technologies for effective smart patient tracking systems where IoT is used for data storing and analysis while RFID enables the tracking of relevant patient information. The analysis may be performed in real-time, getting information from tags location and transfer it to the IoT cloud [106]. A ZigBee, and GSM wireless technology-based approach for collecting the current updates of patients. A wireless body area sensor networks (WBASNs) technology using ZigBee is reported in [72] to continuously monitor human health and its location. Another research in [73] proposes a system comprise of tiny wearable physiological equipment, sensors, transmission modules using a cryptographic algorithm to track a soldier's health status and current location using GPS.

4) Drug Management: In the healthcare sector, drug compliance and adverse drug reactions (ADR) are two of the most important issues regarding patient safety. 15 % of the patients suffer clinically significant interactions due to patient non-compliance to drug dosage and schedule of intake in addition to suffering from polypharmacy. An innovative system named movital is proposed in [74], which is based on the IoT technologies for drug identification and the monitoring of medication. In [109] medication management for their patients through IoT-enabled smart pillboxes is proposed by Wisepill Technologies and Aeris. They are collaborating to help pharmaceutical businesses and healthcare organizations around the world. An intelligent home-based medicine box with wireless connectivity along with an android application is proposed in [75] which helps patients by giving alerts for their medication at the right time and doctors to be in more close communication. In [76] an IoT based model is illustrated to monitor the real-time effect of the drug through wearable devices or mobile, which will detect the side effects of medicines if any occurs and improve the quality of drugs by pharmaceutical organizations.

5) Food Management: Automated monitoring of the nutritional content of food is important not only for infants but also for adults' health development. In [77], a new IoT based fully automated nutrition monitoring system named Smart-Log is introduced. This system compromises a novel 5-layer perceptron neural network, a Bayesian Network-based accurate meal prediction algorithm, Wi-Fi enabled sensors for food nutrition quantification, and a smartphone. In [78], we introduce a real-time food intake monitoring system which gets acceleration data from the sensor placed on the wrist of the user during a meal. The system detects peaks and gives real-time feedback regarding eating trends such as a total number of bites, bites-taken rate, and eating speed is provided to the user. Using a weighing sensor and radio-frequency-identification (RFID), a smart dining table is constructed to measure the weight of food intake.

6) Determination of Glucose Level: Over a prolonged period, diabetes is considering as a group of metabolic disorders characterized by a high blood sugar level. A steady level in blood glucose leads to glucose toxicity, which contributes to cell dysfunction and the pathology grouped as complications of diabetes. Keeping track of blood glucose uncover individual patterns of blood glucose changes and helps in perceiving the planning of foods, medications, and activities, which will affect to follow up on one's diabetes. A somatic data blood glucose collection transmission device for an internet of things (IoT) was revealed by the utility model in [80], which involves a blood glucose collector, a mobile phone or a computer, and a background processor. An IoT-based multi-parameter medical acquisition detector proposed in [81] ensures the stability and accuracy of long-distance data transmission and the contemporary existence of ZigBee wireless network, Wi-Fi wireless network, Bluetooth radio network, 3G, 4G wireless network, cable network which transmit the useful data quickly and accurately in different environments. Besides, an m-IoT based non-invasive glucose level sensors from the patients are linked via IPv6 connectivity to the relevant healthcare provider, and the 6LoWPAN protocol enables wireless sensor devices based on the IEEE 802.15.4 standard is proposed in [79].

7) Monitoring of Electrocardiogram: Monitoring of ECG introduces a new method based on Cypress Wireless Internet Connectivity for Embedded Devices (WICED), Internet of Things (IoT) platform. Open-source protocols like CoAP/HTTP, MQTT, TLS/TCP, DTLS/UDP, and OMALWM2M for data communication and device management are used for the utilization of IoT. In this method, data are gathered using a wearable monitoring node and are transmitted directly to the IoT cloud using Wi-Fi [82]. Many studies [83], [85], [87] have explicitly discussed IoT-based ECG monitoring. A realization of a comprehensive detection algorithm of an ECG signal at the application layer of ECG, belonging to the technical field of the IoT.

This includes a series of detection methods, standards, and threshold parameters based on the wavelet transform technique, and the improved envelope transforms to the ECG signal and detects and identifies the specific shape and position of the P and T wave (QRS wave group). The detection algorithm has a false detection rate of 0.89% through the MATLAB simulation and the MIT-BIH database mark comparison [84]. An IoT-based ECG monitoring system [88] composed of a portable wireless receiving processor and a wireless acquisition transmitter. Cardiac function can be identified on a real-time basis by integrating a search automation method for the detection of abnormal data.

8) Monitoring of Blood Pressure (BP): The carry-on blood pressure (BP)/pulse rate/blood oxygen monitoring intelligent location terminal in [89] is revealed by the utility model, which is based on an IoT. The monitoring device achieves real-time measurement for physical signs, which involve a BP collecting and processing device and an all-in-one blood oxygen/ pulse rate probe. A subscriber identity module (SIM), a general packet radio service (GPRS) module, and an antenna compromises as a data communication device. Table VI presents the IoTh care applications, its accessing technologies, advantages and limitations.

In [90] a motivating scenario of communications structure between a health post and the health center was represented where continuously BP must be controlled remotely. An Apple mobile computing device that can make communication with BP devices is addressed in [91]. The combination of a Keep In Touch (KIT) BP meter and a Near Field Communication and Radio Frequency Identification (NFC) enabled KIT mobile phone is used for BP monitoring, which is based on the IoT is addressed in [92].

9) Monitoring of Oxygen Saturation: For the noninvasive non-stop monitoring of blood oxygen saturation, pulse oximetry is suitable. For health monitoring using the Wireless Sensor Networks (WSN), a wearable pulse oximeter can be adapted to the IoT network is illustrated in [93]. The combination of pulse oximetry with the IoT is important for technology-driven medical healthcare applications. A technique of using Constrained Application Protocol (CoAP) based WSN ensures the monitoring of medical sensors that discuss the potential of IoT-based pulse oximetry [94]. A bluetooth health device profile and the sensor connects directly to the Money platform which manages the device connectivity. In [95], the continuous remote monitoring of the patient's health is observed by an IoT-optimized low power/low-cost pulse oximeter.

10) Rehabilitation System: Problems associated with aging populations and the lack of health facilities IoT-based smart rehabilitation systems are becoming a greater way to mitigate this problem. For the improvement of rehabilitation training of the hemiplegic patients, IoT-based control system comprises training robots, a coordinator, and monitoring equipment where each of them relates to the wireless network is proposed in [96]. In [97], an ontology-based automating design methodology (ADM) is illustrated where computers understand the symptoms and medical resources and help to take the strategy automatically. Body Sensor Networks (BSN) are amplified to provide an immersive engagement of the rehabilitation exercise and translate into an augmented reality world for stroke patients and consultation by medical consultants [98]. Although much research suggests that the childhood autism language training systems wirelessly communicate with the centralized monitoring platform using an IoT-based centralized training center [99] and an integrated application system for prisons [100].

B. ***IoT Healthcare Services***

1) Ambient Assisted Living (AAl): To allow an independent and safe lifestyle, Ambient Assisted Living (AAL) evolves technical systems to monitor personal communication between older people, their environment, and relevant group of caregivers. Using the combination of keep In Touch (KIT) and Closed Loop Healthcare, a central AAL paradigm can be realized through the IoT is discussed in [92]. In [120], proposed an architecture that is based on microservices and software component which examine the requirements and specifications of AAL systems in smart homes, in efforts to describe and evaluate how they would be transposable in the case of smart cities. In [121] proposed an IoT prototype system for AAL called AAL-IoTSys, which includes a Smart IoT Gateway as a critical component to enable interoperability from several heterogeneous devices. This system uses different communication protocols and technologies (e.g., WiFi, ZigBee, Bluetooth, IEEE 802.15.4, 6LowPAN) to monitor environmental (temperature, humidity, C02), health (heart rate) and location (GPS) parameters in the older people's houses. A novel IoT protocol architecture is proposed in [122] which evaluates security tools and techniques that can be leveraged as part of the deployment of IoT that are important for e-health and AAL.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

Table VI: IoTh Medical application used in the review

Application	Advantages	Limitations	Accessing Technology
Dropping Emergency Room Waiting Time [101], [102], [2]	• Use predictive analytics for flow of patients • Monitor physiological data during emergency	• Need to improve scalability increase energy consumption	• IoT based special sensors, wireless sensor network • MEDiSN
Telehealth [70], [105], [110]	• Minimum time for separating messages • Ensure wear ability and data quality • Track bed-ridden patients	• Requires a high-quality security module, requires technical training, server problems can make virtual communication impossible	• Real-time monitoring, telemetric system. • CyberMed
Tracking of Information [71], [106], [72], [73]	• Track patient information • Continuous monitor human location	• Security of information, continuous Internet connections	• RFID tag • ZigBee, and GSM wireless technology • Wireless body area networks (WBASNs) sensor
Drug Management [74], [109], [75], [76]	• Drug identification and monitoring of medication • IoT-enabled smart pillboxes • Give alerts for medication	• Interruption can cause problem	• Wisepill technologies and Aeris wireless connection
Food Management [77], [78]	• Real-time food intake monitoring system • Construct a smart dining table	• Need cost effective sensor system • A Bayesian Network	• Novel 5-layer perceptron neural network • Weighing sensor • RFID
Glucose Level [79], [80], [81]	• Ensure the stability and accuracy of long-distance data transmission • Keep track of blood glucose	• Need operator technique, exposure, environmental and patient factors • 6LoWPAN protocol	• ZigBee wireless network, • Bluetooth radio network • IEEE 802.15.4
Electrocardiogram [82], [83], [84], [85] [87], [88]	• Detect threshold parameters • Transform of ECG signal • Detect specific shape • Position of the P and T wave (QRS) wave group.	• Data stream mining and context awareness technologies • MATLAB simulation	• CoAP/HTTP, MQTT, • TLS/TCP, DTLS/UDP
Blood Pressure (BP) [89], [90], [91], [92]	• Real-time BP measurement	• Continuous Internet connection • Keep in Touch (KIT) BP meter • RFID	• Near Field Communication
Oxygen Saturation [93], [94], [95]	• Monitor blood oxygen saturation	• Low power/low-cost pulse oximeter • Realtime monitoring	• Wireless Sensor Networks (WSN) wearable pulse oximeter • CoAP protocol
Rehabilitation System [96], [97], [98], [99], [100]	• Provide rehabilitation exercise • Rehabilitation training of hemiplegic patients	• Proper knowledge about training. • IoT sensors.	• Body Sensor • Networks (BSN)

2) m-Health: Mobile computing, medical sensor, and communications technologies are considered as m-health for health care. In [123], a new concept is introduced which interconnects 6LoWPAN with emerging 4G networks and matches the functionalities of m-health and IoT for a new and innovative future (4G health) applications. In [124], describe the acquisition of m-health data via medical gadgets and wearables and application of this data in monitoring various health conditions. Also, discuss confidentiality, privacy, and security issues in the context of a secure m-health system. IoT combined with RFID technology enables a whole new context for smart objects that can combine their physical and virtual existences. A web-based application establishes a use case scenario for the evaluation of the IoT architecture which presents the combination of smart objects, security solutions, and mobile communications, one may remotely take care of patients' well-being, establish a ubiquitous AAL for Mobile Health applications is presented in [125].

3) Adverse Drug Reaction: In the healthcare sector, Adverse drug reactions (ADR) is an important issue regarding patient safety. An innovative system is proposed in [74], which is based on IoT for the drug identification and the monitoring of medication. They introduced an IoT-based personal healthcare device called movital, which supports several IoT identification technologies; barcode, RFID, and NFC. In [127], how IoT technology is applied in a pharmaceutical system to examine drugs to detect ADR, harmful effects of pharmaceutical excipients, allergies, complications, and contraindications related to liver and renal defects, and harmful side effects during pregnancy or lactation is illustrated. This system is based on NFC and barcode identification technologies, which have been integrated with common devices such as smart-phones, PDAs, and PCs. In [128], a Drug Dosage Checker system was developed which is based on the IoT paradigm on a mobile platform that allows dosage checking from anywhere. The user interface was designed using the Eclipse IDE (Integrated Development Environment), Extensible Markup Language (XML), Java,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

Android Emulator ADT (Android Developer Tool), and SQLite to implement a self-contained transactional SQL database engine.

4) Semantic Medical Access: In smart healthcare, the use of semantics and ontologies has led to a service called Semantic Medical Access (SMA) that helps in processing ubiquitous data available in the medical cloud. In [129], an outline of Semantic Medical Monitoring Framework proposed with the help of cloud-based IoT techniques to show how to collect, integrate, and interoperate IoT data flexibly and also to support medical emergency services. All these data will be stored in the cloud, and medical data will be connected to a medical rule engine through a web service called "THINK SPEAK". The use of semantic medical access that can share a large amount of medical data by using different ontologies is presented in [130]. It also discussed the issues of semantic medical access in context with the IoT environment.

5) Children Health Information (CHI): In [131], a smart and secure application for monitoring of total health and mental status of the children is presented where the system uses the C4.5 decision algorithm. This system enables the child to get involved with some android games. The game scores, sensor readings are analyzed by the system and actions are taken accordingly. For the secure transmission and the classification of the child's behavior, Apache Ranger is used. An IoT supported multi-platform system for remote monitoring and early detection of mother-child health condition, which constitutes portable medical devices with multiple sensors, is proposed in [132]. Table VII summarize the IoTh care services and its merit and shortcoming. A mobile application works as a mobile gateway for the devices and as a portal for accessing context-aware personalized information.

6) Embedded Context Prediction (ECP): In [133], an on-chip context predictor based sparse sensing technology with smart transmission architecture is proposed, which manages the amount of data acquired from sensors in the Body Area Networks (BANs). The proposed architecture uses intelligent sparse sensing, which removes the collection of redundant data, thereby reducing the amount of data generated. To derive meaningful physiological parameters and context-aware data and patient-centric decision making a new paradigm for ubiquitous healthcare is proposed in [134]. This paradigm requires real-time processing of wirelessly collected relevant data and algorithms for acquiring context awareness (e.g., location, ambient conditions, current physical activity) to extract knowledge about the health condition of patients.

7) Wearables: Reliable, seamless connectivity is accelerating technological innovation and opening new business opportunities in IoT, portable, and wearable technologies. Health and fitness- oriented wearable devices offer biometric measurements such as heart rate, perspiration levels, and even complex measurements like oxygen levels in the bloodstream are also becoming available. Technology advancements may even allow alcohol levels or other similar measurements to be made available through a wearable device. Tracking body temperature might provide an early indication of whether a cold or the flu is on the way is discussed [136]. In [137], the building blocks of "Wearable IoT (WIoT)" including wearable sensors, internet-connected gateways, and cloud and big data support is presented to transform the health and wellness information of the healthcare sector.

Here authors reviews the most recent healthcare applications and services (A & S) that are present in the healthcare sector. Most of these Application and its related services are not free from challenges. To complete the review process authors found several challenges and open issues which will discuss in section IX. These will help the researchers, academicians, pharmacist, healthcare stock holders, doctors and nurses for future development of IoT healthcare.

IX. IoT HEALTHCARE CHALLENGES AND OPEN ISSUES

Many academicians, researchers, engineers, healthcare providers are working hard on designing and implementing different types of IoT-based healthcare services and on unraveling various architectural and technological problems associated with those services. In this context, there are several other challenges and open issues that need to be carefully considered. We have considered both explored and unexplored issues surrounding IoT healthcare services below:

A. Standardization

Many vendors are manufacturing different types of IoT healthcare devices and more vendors are trying to join with them. Small vendors don't have enough trained human resources to integrate the embedded IoT devices. This lack of integration of different IoT devices creates a new problem. There is no standard protocol or regulation that can make those devices compatible with each other. Without compatibility across devices, functionality, and adaptability of the IoT Healthcare system come into question. That is the reason Standardization is an open issue of IoT healthcare. So for the standardization of protocols and communication between devices are needed to be addressed.

B. Security

In IoT based healthcare applications data privacy and security are the most notable open issues. Security is the main controlling access to patient's personal information. In the IoT based healthcare data, privacy is very pivotal. Based on the design, development, and application, IoT healthcare devices can collect data. The huge data is stored and transferred regularly and hackers try to use this data against the patients. Hackers replicate the ID to buy drugs to misuse their futures. These replicate ids make questionable in various applications to the IoT based healthcare architecture is not well protected and conk out to provide the privacy and security of data.

C. Cost

Medical patients are increasing day by day around the world that is increasing the use of IoT based devices dramatically in the last couple of years. The demand for IoT devices in upgrading and the cost is also increasing. There is no comparative study regarding the IoT healthcare devices according to the knowledge of the Author. That's why cost analysis is an open issue in the IoT healthcare system. The cost of the healthcare monitoring system is a major issue in developed and developing countries. The cost of acquiring IoT based healthcare facilities is still not feasible for ordinary mankind.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

Table VII: IoTh Medical services used in the review

Services	Merits	Limitations
Ambient Assisted Living (AAl) [119], [120], [121], [122]	• Enable interoperability from several heterogeneous devices • Monitor health and GPS parameters	• Costly • Don't provide higher level of care • Require daily monitoring or treatment
m-Health [123], [124], [125]	• Monitor 24*7 health conditions • Smart objects that can combine physical and virtual existences	• Security of data • Limited access to medical records. • Lack of accuracy
Adverse Drug Reaction [126], [127], [128]	• Drug identification • Detect harmful effects of pharmaceutical excipients	• Knowledge of smart technologies availability of technologies
Semantic Medical Access [129], [130]	• Help in processing ubiquitous data • Use different ontologies	• IoT of security issues • No correct information about SMA framework
Children health Information (CHI) [131], [132]	• Classify the child's behavior • Detect mother and child health condition	• Availability of knowledge • Data security
Embedded Context Prediction (ECP) [133], [134]	• Eradicate the collection of redundant data • Acquire context awareness to extract knowledge	• Availability of modern technology and sensors
Wearables [136], [137]	• Biometric measurement of heart rate, oxygen level • Transform the health and wellness information.	• Offer plenty of distractions. • Costly • Lack of privacy

D. Quality of services (QoS)

Healthcare is a very sensitive issue and a question of life and death. That's why it requires the highest quality of services available 24/7. These systems will be available, reliable, and must maintain mandatory quality of services (QoS) in the IoT based Healthcare system. IoT healthcare system is mainly used in real-time applications. The system needs data from the sensors to be collected, transferred, processed, analyzed, and used on time. But sometimes IoT devices fail to provide the information on time. That's why QoS is considered a challenge to the IoT healthcare system. It is also becoming a big challenge to produce a meaningful diagnosis within acceptable time frames (considering QoS), where wearable systems deal with the real-time life-critical application. It is very important to overcome these challenges by ensuring QoS.

E. Network Architecture

Authorization and authentication are very important in the IoT healthcare network architecture for the users of IoT healthcare systems. Researchers have proposed various types of network architecture. The previously developed three layers of network architecture cannot fulfill the requirements of healthcare applications. The latest five-layer architecture has low storage capacity and energy. Healthcare devices are lightweight and can only save a few bytes. IoT healthcare network architecture is failing to fulfill the requirements of security, privacy, and storage. That's why network architecture of IoT in healthcare is an open issue.

F. Technology Transition

In every second different IoT healthcare devices are inventing and new technology is taking over its position. Upgrading from the current medical system and existing network configuration to the latest IoT based system and network is a major challenge. The transition from the old system to a new system has to be seamless. Otherwise, the whole system could fall into a hazardous situation. For this reason, technology is considered as an open challenge of IoT healthcare. Flexibility and compatibility of devices are needs to ensure the elderly and chronic patients

G. Power Consumption

The different manufacturing companies installing various IOT-based medical devices around the globe. Power is very limited around the world. So power Consumption is an open issue for the vendors. When the vendors are creating IoT devices they don't think about the power. That's why they face the power problem. The IoT medical devices have to be operating non-stop and connected to the internet all the time to produce real-time data for the patients. Some of them may consume a huge amount of power. Without a continuous energy supply, the IoT-based Healthcare infrastructure will collapse.

H. Data protection

Data security in the healthcare application is a growing issue with an increasing number of breaches of the Data Protection. The act being reported to the Information Commissioner's Office (ICO) can serve a monetary penalty for a serious breach of the data protection act provided the incident has the potential to cause substantial damage or substantial distress to affected individuals with potential consequences. So, Data protection is being considered as an open issue of IoT healthcare. Hackers try to hack data to use it against patients and doctors. Both patients and doctors susceptible to the threat of a data breach when working with sensitive information on the move there are a growing number of health care authorities private practices hospitals and clinics recognizing these threats and upgrading their visual security to protect their confidential on-screen data and adhere to the Data Protection.

These above challenges and open issues will help to improve the future IoT healthcare sector. In next section X will describe and reviews the IoT healthcare market opportunities and recent development of IoT healthcare.

X. IoT HEALTHCARE MARKET OPPORTUNITIES

The IoT contributes to a huge market possibility with smart objects for machinery companies, Internet service providers,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3062630, IEEE Internet of Things Journal

and application developers. Machine-to-Machine (M2M) transit issues do require to develop up to 45% of the entire internet platform [152], [153].

The increase of IoT is getting life-improving progress on the Internet of Medical Things (IoMT). The impact of the IoT healthcare application that is bulged to grow the most prominent commercial industries such as Mobile Health (mHealth) and telecare that allows preventive wellness of diagnosis, treatment, and monitoring services.

According to a new report by Grand View Research, The IoT healthcare market capacity is projected to reach USD 534.3 billion by 2025 growing at a CAGR 19.9% over the estimate years. IoT healthcare sector growth in grants for the solutions that making the connected devices.

IoT network in healthcare systems growing for real-time data monitoring amidst healthcare to control chronic diseases such as congestive heart failure, diabetes, autism, heart disease, insomnia, asthma, and blood pressure. The growing significant amount of the IoThNet platform has provided market advancement with a more reliable and initial analysis of disease tracking as mentioned earlier. Grand View Research has also segmented the global IoT in the healthcare market based on element, IoThNet technology, end-user, utilization, and county.

According to [154], the IoT in healthcare market includes essential explication providers, such as Agamatrix (US), Armis (US), Capsule Technologies (US), Comarch SA (Poland), Cisco Systems (US), GE Healthcare (US), IBM Corporation (US), Intel (US), KORE Wireless (US), Medtronic (Ireland), Microsoft Corporation (US), OSP Labs (US), Resideo Technologies (US), Royal Philips (Netherlands), SAP SE (Germany), Sciencesoft (US), Softweb Solutions (US), STANLEY Healthcare (US), Telit (UK), and Welch Allyn (US).

By Region, the IoT in the healthcare market is divided into the following segments, North America(US, Canada), Europe (UK, Germany, France, Rest of Europe), Asia Pacific ((APAC), China, Japan, India, Rest of (APAC), Middle East and Africa (MEA), Latin America (Brazil, Mexico, Rest of Latin America).

Recent Developments in IoT healthcare:

- In January 2019, IBM Watson [160] launches a new feature IQcast Medtronic partnered with existing product sugar. It would contribute patients a hypoglycemic effect to monitor their low glucose level by predicting the occurrence.
- In April 2019, based on the telehealth [70] platform Royal Philips and Spencer Health Solutions developed to chronically sick patients in selected European Union (EU) countries to offer in-home medication adherence [152].
- In 2016, worldwide IoT healthcare recorded revenues amounted to 24 billion and this number is predicted to increase to over 135 billion by 2025 [155].
- In the next several decades, the IoT healthcare services transformed into evidence-based policies, and technologies that can be observed to enhance any instances of effective implementations like e-Health policies and strategies [159]. It has been an essential goal during many management drives across the world.
- The Indian government has budgeted Rs.70.6 billion to develop 100 smart cities in the country services [156] and intends to construct a 15 billion IoT industry in India by 2020 to improve the number of connected devices from throughout 200 million to over 2.7 billion [157]. In the India's healthcare sector, those applications simply to support the application of IoT. The Japanese government has been going forward to some policies for e-Health friendly references [158] such as cost-saving and enhanced clinical consequences over health IT.
- In both developing and developed countries, mobile phones are used for a wide range of public health initiatives [4].

Figure 9 shows the Internet of Things in Healthcare Market Size, Share and Trends Analysis Report Component of (Service, System Software) which is gradually increased.

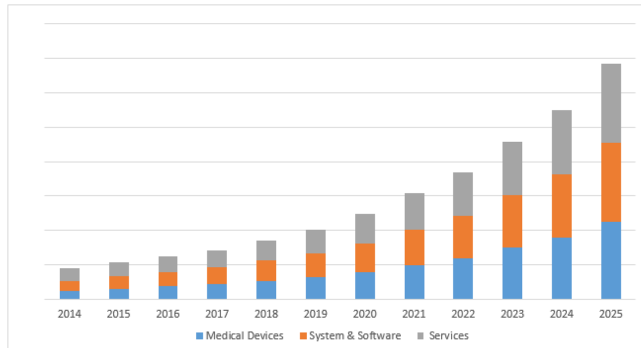

Figure 9: IoT healthcare market size and trend analysis of services, systems & software [155]

XI. CONCLUSIONS AND FUTURE DIRECTIONS

The improvement of healthcare systems with the integration of IoT technologies is reshaping the future of this sector. In this review we started our discussion with the technologies currently being adopted in the IoTh systems, for example, RFID, Edge Computing, Semantic Analysis, Augmented Reality, etc. We analyzed and presented their benefits and challenges. After that, we discussed the current network topologies, architectures and platforms being used for IoT in healthcare. Following that, we elaborately discussed all the major application protocols, service delivery protocols and infrastructure protocols currently being researched and deployed in IoT common standards. Another major part of our work is the comprehensive review of the security aspect of the IoT healthcare systems. In this part, we have discussed the security requirements of an IoTh system in general and the usual challenges to fulfill those requirements. We also proposed a top level architecture of an IoTh system using Blockchain that can meet the contemporary security challenges. After that, we discussed the applications and services where IoT is contributing significantly in the healthcare sector. As a part and parcel to our review we included the challenges and open issues that IoTh is yet to overcome as well as the opportunities that are still there in the healthcare market.

authors of this paper are found out that most of the review papers are application-based, where our review covers not only application but also state-of-arts technologies, standard protocols, security and privacy, and market opportunities, which are the specialty of this paper.

Throughout the globe, researchers are thriving to improve the healthcare system by introducing their novel ideas, innovative devices, and sophisticated software. The main focus of this review was various contemporary IoT networks and its protocols, architectures, and platforms. This paper provides information on IoT healthcare research activities concerning chronic disease supervision, monitoring of elderly individuals, and private health. The key concerns with the IoT healthcare systems, like security, privacy, authentication, energy consumption, computation power, resource management, quality of services, etc. are discussed here in detail. We tried to provide the future researchers of the area with a comprehensive review of current IoT healthcare technologies, their applications, challenges, and the remaining open issues. The widespread adoption of IoT-based healthcare will increase day by day in the upcoming years. IoTh is expected to be a fundamental part of any healthcare solution in the coming fourth industrial revolution. In this regard, this study will hopefully work as a fundamental guide to the future visionaries of the field and provide them with a simple reference point.

References

[1] Shinde, S and Phalle, V "A Survey paper on internet of things based healthcare system" In *International Advanced Research Journal in Science, Engineering and Technology*, volume 4, 2017

[2] Ko, JeongGil and Lim, Jong Hyun and Chen, Yin and Musvaloiu-E, Rvăzvan and Terzis, Andreas and Masson, Gerald M and Gao, Tia and Destler, Walt and Selavo, Leo and Dutton, Richard P "MEDiSN: Medical emergency detection in sensor networks" In *ACM Transactions on Embedded Computing Systems (TECS)*, volume 10, pages 1–29, 2010

[3] Hwang, Tzonelih and Gope, Prosanta "provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets" In *Wireless personal communications*, volume 77, pages 197–224, 2014

[4] Al-Fuqaha, Ala and Guizani, Mohsen and Mohammadi, Mehdi and Aledhari, Mohammed and Ayyash, Moussa "Internet of things: A survey on enabling technologies, protocols, and applications" In *IEEE communications surveys & tutorials*, volume 17, pages 2347–2376, 2015

[5] Aijaz, Adnan and Aghvami, A Hamid "Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective" In *IEEE Internet of Things Journal*, volume 2, pages 103–112, 2015

[6] Hller, J and Tsiatsis, V and Mulligan, C and Karnouskos, S and Avesand, S and Boyle, D "From machine to the internet of things: introduction to a new age of intelligence", In *Elesvier*, 2014

[7] Laplante, Phillip A and Laplante, Nancy "The internet of things in healthcare: Potential applications and challenges" In *IT Professional*,volume 18, pages 2–4, 2016

[8] Vermesan, Ovidiu and Friess, Peter and others "Internet of things-from research and innovation to market deployment" In *River publishers Aalborg*,volume 29, pages 2–4, 2014

[9] Atzori, Luigi and Iera, Antonio and Morabito, Giacomo "The internet of things: A survey computer networs " In *River publishers Aalborg*,volume 29, pages 2787–2805, 2010

[10] Tan, L and Wang, N "Future internet: The internet of things" In *River publishers Aalborg*, 2010

[11] Islam, SM Riazul and Uddin, M Nazim and Kwak, Kyung Sup "The IoT: Exciting possibilities for bettering lives: Special application scenarios" In *IEEE Consumer Electronics Magazine*, volume 5, pages 49–57, 2010

[12] Pang, Zhibo "Technologies and architectures of the Internet-of-Things (IoT) for Health and Well-being" In *IKTH Royal Institute of Technology*, 2013

[13] Islam, SM Riazul and Kwak, Daehan and Kabir, MD Humaun and Hossain, Mahmud and Kwak, Kyung-Sup "The internet of things for health care: a comprehensive survey" In *River publishers Aalborg*,volume 3, pages 678–708, 2015

[14] Dhanvijay, Mrinai M and Patil, Shailaja C "Internet of Things: A survey of enabling technologies in healthcare and its applicationse", In *Computer Networks*, pages 113–131, 2019

[15] Ko, JeongGil and Lu, Chenyang and Srivastava, Mani B and Stankovic, John A and Terzis, Andreas and Welsh, Matt "Wireless sensor networks for healthcare", In *Proceedings of the IEEE*, pages 1947–1960, 2010

[16] IEEE Standards Association and others "IEEE Std 802.15. 4-2011, IEEE standard for local and metropolitan area networks—part 15.4: Low-rate wireless personal area networks (LR-WPANs)", In *IEEE*, 2011

[17] Shelby, Zach and Hartke, Klaus and Bormann, Carsten and Frank, B "Coap: An application protocol for billions of tiny internet nodes", In *IEEE Internet Computing*, pages 62–67, 2012

[18] Lerche, Christian and Hartke, Klaus and Kovatsch, Matthias "Industry adoption of the Internet of Things: A constrained application protocol survey", In *Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012)*, pages 1–6, 2012

[19] Locke, Dave "Mq telemetry transport (mqtt) v3. 1 protocol specification", In *IBM developerWorks Technical Library*, volume 15, 2010

[20] Saint-Andre, P "Extensible Messaging and Presence Protocol (XMPP): Core. internet engineering task force", In *October 2004. RFC 3920 (Proposed Standard)*, 2011

[21] Jones, M Tim "Meet the extensible messaging and presence protocol (xmpp)", In *IBM developerWorks, Markham, ON, Canada*, 2009

[22] Waher, Peter and Doi, Y "OASIS advanced message queuing protocol (AMQP) version 1.0", In *International Journal of Aerospace Engineering Hindawi www.hindawi.com*, 2018

[23] Ungurean, Ioan and Gaitan, Nicoleta-Cristina " Data distribution service for real-time systems-A solution for the internet of things enviroments.", In *Annals of the University Dunarea de Jos of Galati: Fascicle II, Mathematics, Physics, Theoretical Mechanics*, 2015

[24] Jara, Antonio J and Martinez-Julia, Pedro and Skarmeta, Antonio "Lightweight multicast DNS and DNS-SD (lmDNS-SD): IPv6-based resource and service discovery for the Web of Things", In *2012 Sixth international conference on innovative mobile and internet services in ubiquitous computing*, pages 731–738

[25] Klauck, Ronny and Kirsche, Michael, "Chatty things-Making the Internet of Things readily usable for the masses with XMPP", In *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, pages 60–69, year 2012

[26] Cheshire, S and Krochmal, M "Multicast DNS, server", In *Request for Comments. Internet Engineering Task Force (IETF)*, year 2013

[27] Cheshire, Stuart and Krochmal, Marc "DNS-based service discovery", In *RFC 6763, February*, year 2013

[28] Vasseur, J and Agarwal, Navneet and Hui, Jonathan and Shelby, Zach and Bertrand, Paul and Chauvenet, Cedric "RPL: The IP routing protocol designed for low power and lossy networks", In *Internet Protocol for Smart Objects (IPSO) Alliance*, volume 36, year 2011

[29] Winter, Tim and Thubert, Pascal and Brandt, Anders and Hui, Jonathan W and Kelsey, Richard and Levis, Philip and Pister, Kris and Struik, Rene and Vasseur, Jean-Philippe and Alexander, Roger K "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.", In *rfc*, volume 6550, pages 1–157, year 2012

[30] Clausen, Thomas and Herberg, Ulrich and Philipp, Matthias "A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL)", In *2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 365–372, year 2011

[31] Palattella, Maria Rita and Accettura, Nicola and Vilajosana, Xavier and Watteyne, Thomas and Grieco, Luigi Alfredo and Boggia, Gennaro and Dohler, Mischa "Standardized protocol stack for the internet of things", In *2011 IEEE communications surveys & tutorials*, pages 1389–1406, year 2012

[32] J. W. Hui and D. E. Culler "Extending IP to low-Power, wireless personal area networks", In *Internet Computing, IEEE*, volume 12, pages 37-45, year 2008

[33] Frank, Raphael and Bronzi, Walter and Castignani, German and Engel, Thomas "Bluetooth low energy: An alternative technology for VANET applications", In *2014 11th annual conference on wireless on-demand network systems and services (WONS)*, pages 104–107, year 2014

[34] DeCuir, Joseph "Introducing bluetooth smart: Part 1: A look at both classic and new technologies.", In *IEEE Consumer Electronics Magazine*, pages 12–18, year 2013

[35] Mackensen, Elke and Lai, Matthias and Wendt, Thomas M "Bluetooth low energy (BLE) based wireless sensors", In *SENSORS, 2012 IEEE*, pages=1–4, pages 1–4, year 2012

[36] Siekkinen, Matti and Hiienkari, Markus and Nurminen, Jukka K and Nieminen, Johanna "How low energy is bluetooth low energy? comparative measurements with zigbee/802.15. 4", In *2012 IEEE wireless communications and networking conference workshops (WCNCW)*,pages 232–237, year 2012

[37] Jones, Erick C and Chung, Christopher A "RFID and Auto-ID in planning and Logistics" In A Practical Guide for Military UID Applications", In *CRC Press*, 2016

[38] Minoli, Daniel "Building the internet of things with IPv6 and MIPv6: the evolving world of M2m communications", In *John Wiley & Sons*, 2013

[39] Hasan, Monowar and Hossain, Ekram and Niyato, Dusit "Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches", In *IEEE communications Magazine*, 2013

[40] Niyato, Dusit and Wang, Ping and Kim, Dong In "Performance modeling and analysis of heterogeneous machine type communications", In *IEEE Transactions on Wireless Communications*, pages 2836–2849, 2013

[41] Pattnaik, Prasant Kumar and Mohanty, Suneeta and Mohanty, Satarupa "Smart healthcare analytics in IoT enabled Environment", In *Springer*

[42] Blythe, JM and Johnson, SD "The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices", In *IET*, 2018

[43] Hodgson, Roderick "Solving the security challenges of IoT with public key cryptography", In *Network Security*, volume 2019, number 1, pages 17–19, 2019

[44] Knowles, Bran and Smith-Renner, Alison and Poursabzi-Sangdeh, Forough and Lu, Di and Alabi, Halimat "Uncertainty in current and future health wearables", In *Communications of the ACM*, volume 61, number 12, pages 62–67, 2018

[45] Law, Yee Wei "Key management and link-layer security of wireless sensor networks: Energy-efficient attack and defense", 2005

[46] Amendola, Sara and Lodato, Rossella and Manzari, Sabina and Occhiuzzi, Cecilia and Marrocco, Gaetano "RFID technology for IoT-based personal healthcare in smart spaces", In *IEEE Internet of things journal*, volume 1, number 2, pages 144–152, 2014

[47] Khan, Sarfraz Fayaz "Health care monitoring system in Internet of Things (IoT) by using RFID", In *2017 6th International Conference on Industrial Technology and Management (ICITM)*, pages 198–204, 2017

[48] G. Abinaya, K. P. Sampoornam "An Efficient Healthcare System in IoT Platform Using RFID System", In *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)*,volume 5,2, 2017

[49] Oueida, Soraia and Kotb, Yehia and Aloqaily, Moayad and Jararweh, Yaser and Baker, Thar "An edge computing based smart healthcare framework for resource management", In *Sensors, Multidisciplinary Digital Publishing Institute*,volume 18,number 12, pages 4307, 2018

[50] Otoum, Safa and Ahmed, Muayad and Mouftah, Hussein T "Sensor Medium Access Control (SMAC)-based epilepsy patients monitoring system", In *2015 IEEE 28th Canadian conference on electrical and computer engineering (CCECE)*, pages 1109–1114, 2015

[51] Jabbar, Sohail and Ullah, Farhan and Khalid, Shehzad and Khan, Murad and Han, Kijun "Semantic interoperability in heterogeneous IoT infrastructure for healthcare", In *Wireless Communications and Mobile Computing*, volume 2017, year 2017

[52] Desai, Pratikkumar and Sheth, Amit and Anantharam, Pramod "Semantic gateway as a service architecture for iot interoperability", In *2015 IEEE International Conference on Mobile Services*, pages 313–319, 2015

[53] Yrard, Amelie and Serrano, Martin "Connected smart cities: Interoperability with seg 3.0 for the internet of things", In *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 796–802, 2016

[54] Baker, Stephanie B and Xiang, Wei and Atkinson, Ian "Internet of things for smart healthcare: Technologies, challenges, and opportunities", In *IEEE Access*, volume 5, pages 26521–26544, 2017

[55] Sultan, Nabil "Making use of cloud computing for healthcare provision: Opportunities and challenges", In *IEEE Access*, volume 34, pages 177–184, 2014

[56] Lo'ai, A Tawalbeh and Mehmood, Rashid and Benkhlifa, Elhadj and Song, Houbing "Mobile cloud computing model and big data analysis for healthcare applications", In *IEEE Access*, volume 4, pages 6171–6180, 2016

[57] Dimitrov, Dimiter V "Medical internet of things and big data in healthcare", In *Healthcare informatics research*, volume 22, number 3, pages 156–163, 2016

[58] Vargheese, Rajesh and Viniotis, Yannis "Influencing data availability in IoT enabled cloud based e-health in a 30 day readmission context", In *10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pages 475–480, 2014

[59] Xu, Boyi and Da Xu, Li and Cai, Hongming and Xie, Cheng and Hu, Jingyuan and Bu, Fenglin "Ubiquitous data accessing method in IoT-based information system for emergency medical services", In *IEEE Transactions on Industrial informatics*, volume 10, number 2, pages 1578–1586, 2014

[60] Ghanavati, Sara and Abawajy, Jemal and Izadi, Davood "An alternative sensor cloud architecture for vital signs monitoring", In *2016 international joint conference on neural networks (IJCNN)*, pages 2827–2833, 2016

[61] Lin, Kai and Xia, Fuzhen and Wang, Wenjian and Tian, Daxin and Song, Jeungeun "System design for big data application in emotion-aware healthcare", In *IEEE Access*, volume 4, pages 6901–6909, 2016

[62] Viswanathan, Hariharasudhan and Lee, Eun Kyung and Pompili, Dario "Mobile grid computing for data-and patient-centric ubiquitous healthcare", In *2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT)*, 36–41, 2012

[63] Brust, Charles "Grid computing in a healthcare environment: A Framework for enterprise design and implementation", In *MWAIS 2009 Proceedings*, 2009

[64] Weisbecker, Anette and Falkner, Jürgen and Rienhoff, Otto "MediGRID–Grid Computing For Medicine and Life Sciences", In *Grid Computing*, pages 57–65, 2009

[65] Hamza-Lup, Felix G and Rolland, Jannick P and Hughes, Charles "A distributed augmented reality system for medical training and simulation", In *arXiv preprint arXiv:1811.12815*, 2018

[66] Ha, Ho-Gun and Hong, Jaesung "Augmented reality in medicine", In *Hanyang Medical Reviews*, volume 36, number 4, pages 242-247, 2016

[67] State, Andrei and Chen, David T and Tector, Chris and Brandt, Andrew and Chen, Hong and Ohbuchi, Ryutarou and Bajura, Michael and Fuchs, Henry "Observing a volume rendered fetus within a pregnant patient", In *Proceedings Visualization'94*, pages 364–368, 1994

[68] Argotti, Yann and Davis, Larry and Outters, Valerie and Rolland, Jannick P "Dynamic superimposition of synthetic objects on rigid and simple-deformable real objects", In *Computers & Graphics*, volume 26, number 6, pages 919–930, 2002

[69] ahoo, Prasan Kumar and Mohapatra, Suvendu Kumar and Wu, Shih-Lin "Analyzing healthcare big data with prediction for future health condition", In *IEEE Access*, volume 4, pages 9786–9799, 2016

[70] Al-Majeed, Salah S and Al-Mejibli, Intisar S and Karam, Jalal "Home telehealth by internet of things (IoT)", In *2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 609–613, 2015

[71] Mishra, Subhra Shriti and Rasool, Akhtar "IoT Health care monitoring and tracking: A survey", In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, pages 1052–1057, 2019

[72] Govindaraj, A and Banu, Dr S Sindhuja "GPS based soldier tracking and health indication system with environmental analysis", In *International Journal of Enhanced Research in Science Technology & Engineering*, volume 2, number 12, pages 46–52, 2013

[73] K. Pallavi, K. Tripti "Secure fealth monitoring of soldiers with tracking system using IoT: A survey", In *International Journal of Trend in Scientific Research and Development (IJTSRD)*, Vol. 3, no. 4, May-Jun 2019

[74] Jara, Antonio J and Zamora, Miguel A and Skarmeta, Antonio F "Drug identification and interaction checker based on IoT to minimize adverse drug reactions and improve drug compliance", In *Personal and ubiquitous computing*, volume 18, number 1, pages 5–17, 2014

[75] Srinivas, M and Durgaprasadarao, P and Raj, V Naga Prudhvi "Intelligent medicine box for medication management using IoT", In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pages 32–34, 2018

[76] Prajapati, Bharat and Parikh, Satyen M and Patel, Jignesh "An IoT base model to monitor real time effect of drug", In *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, pages 26–27, 2018

[77] Sundaravadivel, Prabha and Kesavan, Kavya and Kesavan, Lokeshwar and Mohanty, Saraju P and Kougianos, Elias "Smart-Log: A deep-learning based automated nutrition monitoring system in the IoT", In *IEEE Transactions on Consumer Electronics*, volume 64, number 3, pages 390–398, 2018

[78] Mendi, Engin and Ozyavuz, Ocal and Pekesen, Emrah and Bayrak, Coskun "Food intake monitoring system for mobile devices", In *5th IEEE International Workshop on Advances in Sensors and Interfaces IWASI*, volume 64, number 3, pages 31–33, 2013

[79] Istepanian, Robert SH and Hu, Sijung and Philip, Nada Y and Sungoor, Ala "The potential of internet of m-health things "m-IoT" for non-invasive glucose level sensing", In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 5264–5266, 2016.

[80] Guan, Zhang Jing "Somatic data blood glucose collection transmission device for internet of things", In *Chinese Patent*,volume 202, number 838, pages 653, 2013

[81] Lijun, Z "Multi-parameter medical acquisition detector based on internet of things", In *Chinese Patent*,volume 202, number 960, pages 774, 2013

[82] Deshpande, Uttam U and Kulkarni, Milan A "Iot based real time ecg monitoring system using cypress wiced" In *International Journal*

of Advanced Research in Electrical, Electronics and Instrumentation Engineering, volume 6, 2014

[83] Yang, Lin and Ge, Yanhong and Li, Wenfeng and Rao, Wenbi and Shen, Weiming "A home mobile healthcare system for wheelchair users" In *Proceedings of the 2014 IEEE 18th international conference on computer supported cooperative work in design (CSCWD)*, pages 609–614, 2014

[84] Xiaogang, Y and Hongjiang, L and Jiaqing, W and Wentao, T "Realization of comprehensive detection algorithm of electrocardiogram signal at application layer electrocardiogram monitoring Internet of Thing" In *Chinese Patent*, pages 112, 2011

[85] Castillejo, Pedro and Martinez, Jose-Fernan and Rodriguez-Molina, Jesus and Cuerva "Integration of wearable devices in a wireless sensor network for an e-health application" In *IEEE Wireless Communications*,volume, pages 38–49, 2013

[86] Zia, Tanveer A and Zomaya, Albert Y "Quality of security through triple key scheme in wireless sensor networks" In *Wireless Communications and Mobile Computing*, pages 722-732, 2010

[87] Agu, Emmanuel and Pedersen, Peder and Strong, Diane and Tulu, Bengisu and He, Qian and Wang, Lei and Li, Yejin "The smartphone as a medical device: Assessing enablers, benefits and challenges" In *2013 IEEE International Workshop of Internet-of-Things Networking and Control (IoT-NC)*, pages 48–52, 2013

[88] Liu, Ming-Liang and Tao, Liu and Yan, Zhou "Internet of things-based electrocardiogram monitoring system" In *2Chinese Patent*, volume 102, pages 118, 2012

[89] Xin, TJ and Min, B and Jie, J "Carry-on blood pressure/pulse rate/blood oxygen monitoring location intelligent terminal based on Internet of Things" In *Chinese Patent*,volume 202, pages 315, 2013

[90] Puustjärvi, Juha and Puustjärvi, Leena "Automating remote monitoring and information therapy: An opportunity to practice telemedicine in developing countries" In *2011 IST-Africa Conference Proceedings*, pages 1–9, 2011

[91] Tarouco, Liane Margarida Rockenbach and Bertholdo, Leandro Márcio and Granville, Lisandro Zambenedetti and Arbiza, Lucas Mendes Ribeiro and Carbone, Felipe and Marotta, Marcelo and De Santanna, Jose Jair Cardoso "Internet of things in healthcare: Interoperatibility and security issues" In *2012 IEEE international conference on communications (ICC)*, pages 6121–6125, 2012

[92] Dohr, Angelika and Modre-Opsrian, Robert and Drobics, Mario and Hayn, Dieter and Schreier, Günter "The internet of things for ambient assisted living" In *2010 seventh international conference on information technology: new generations*, pages 804–809, 2010

[93] Larson, Eric C and Lee, TienJui and Liu, Sean and Rosenfeld, Margaret and Patel, Shwetak N "Accurate and privacy preserving cough sensing using a low-cost microphone" In *Proceedings of the 13th international conference on Ubiquitous computing*, pages 375–384, 2011

[94] Khattak, Hasan Ali and Ruta, Michele and Di Sciascio, Eugenio Eugenio "CoAP-based healthcare sensor networks: A survey" In *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014*, pages 499-503, 2014

[95] Larson, Eric C and Goel, Mayank and Boriello, Gaetano and Heltshe, Sonya and Rosenfeld, Margaret and Patel, Shwetak N "Spirosmart: Using a microphone to measure lung function on a mobile phone" In *Proceedings of the 2012 ACM Conference on ubiquitous computing*, pages 280–289, 2012

[96] Guangnan, Zhang and Penghui, Liu "IoT (Internet of Things) control system facing rehabilitation training of hematologic patients" In *Chinese Patent*, pages 045, 2012

[97] Fan, Yuan Jie and Yin, Yue Hong and Da Xu, Li and Zeng, Yan and Wu, Fan "IoT-based smart rehabilitation system" In *IEEE transactions on industrial informatics*, pages 1568–1577, 2014

[98] Tan, Benedict and Tian, Oliver "Short paper: Using bsn for tele-health application in upper limb rehabilitation" In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pages 169–170, 2014

[99] Liang, S and Zilong, Y and Hai, S and Trinidad, M "Childhood autism language training system and internet-of-things-based centralized training center" In *Chinese Patent*, pages 661, 2011

[100] Sreekanth, KU and Nitha, KP "A study on health care in internet of things" In *International Journal on Recent and Innovation Trends in Computing and Communication*, volume 4, pages 44–47, 2016

[101] [online]http://www.healthcarebusinesstech.com/ed-wait-times-analytics/

[102] [online]http://www.healthcarebusinesstech.com/iot-hospital-future

[103] [online]https://healthtechmagazine.net/article/2019/08/will-edge-computing-transform-healthcare

[104] [online]https://www.vxchnge.com/blog/edge-computing-use-cases-healthcare?

[105] [online]https://www.iotforall.com/how-iot-enables-tomorrows-telemedicine/

[106] [online]https://www.scnsoft.com/blog/rfid-and-iot-in-a-smart-hospital-benefits-and-challenges-of-smart-patient-tracking

[107] [online]www.gartner.com,the internet of things will transform the data center

[108] Finding success in the new iot ecosystem: Market to reach $3.04 trillion and 30 billion connected things in 2020, In http://www.idc.com/getdoc.jsp?, year 2014.

[109] [online]https://iiot-world.com/smart-healthcare/medication-management-for-patients-through-iot-enabled-smart-pillboxes/

[110] S.Ojas , S. Akshay , S. Rohitkumar, A.Trupti "IoT based telemedicine system" In *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*

[111] Saminathan, Sasippriya and Geetha, K "Real-time health care monitoring system using iot" In *International Journal of Engineering & Technology*, volume 7, pages 484–488, 2018

[112] Dwivedi, Ashutosh Dhar and Srivastava, Gautam and Dhar, Shalini and Singh, Rajani "A decentralized privacy-preserving healthcare blockchain for iot" In *Multidisciplinary Digital Publishing Institute*, volume 19, number 2, pages 326, 2019

[113] Sharma, Divya and Tripathi, RC "Performance of internet of things (IOT) based healthcare secure services and its importance: Issue and challenges" In Available at SSRN 3565782, 2020

[114] Kadhim, Kadhim Takleef and Alsahlany, Ali M and Wadi, Salim Muhsin and Kadhum, Hussein T "An overview of patient's health status monitoring system based on internet of things (IoT)" In Wireless Personal Communications, pages 1–2, 2020

[115] Lemlouma, Tayeb and Laborie, Sébastien and Roose, Philippe and Rachedi, Abderrezak and Abdelaziz, Kenza "A study of mobility support in wearable health monitoring systems: Design framework" In CRC Press/Taylor & Francis, 2014

[116] Boulemtafes, Amine and Rachedi, Abderrezak and Badache, Nadjib "A study of mobility support in wearable health monitoring systems: Design framework" In 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), pages 1–8, 2015

[117] Lemlouma, Tayeb and Rachedi, Abderrezak and Chalouf, Mohamed Aymen and Chellouche, Soraya Ait "A new model for NGN pervasive e-Health services" In 2013 First International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech) pages 1–5, 2013

[118] D. He , S. Zeadally , N. Kumar , J.H. Lee "Anonymous authentication for wireless body area networks with provable security" In *IEEE*, volume 11, number4, pages 2590–2601, 2016

[119] Dohr, Angelika and Modre-Opsrian, Robert and Drobics, Mario and Hayn, Dieter and Schreier, Günter "The internet of things for ambient assisted living" In *2010 seventh international conference on information technology: new generations*, pages 804–809, 2010

[120] Ngankam, Hubert Kenfack and Pigot, Hélène and Parenteau, Maxime and Lussier, Maxime and Aboujaoudé, Aline and Laliberté, Catherine and Couture, Mélanie and Bier, Nathalie and Giroux, Sylvain "An iot architecture of microservices for ambient assisted living environments to promote aging in smart cities" In *International Conference on Smart Homes and Health Telematics*, volume 11, pages 154–167, 2019

[121] Yacchirema, Diana C and Palau, Carlos E and Esteve, Manuel "Enable iot interoperability in ambient assisted living: Active and healthy aging scenarios" In *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pages 53–58, 2017

[122] Minoli, Daniel and Sohraby, Kazem and Occhiogrosso, Benedict "IoT security mechanisms for e-health and ambient assisted living applications" In *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pages 13–18, 2017

[123] Istepanian, Robert SH and Sungoor, Ala and Faisal, Ali and Philip, Nada "Internet of m-health things'm-IOT" In *IET*, 2011

[124] Almotiri, Sultan H and Khan, Murtaza A and Alghamdi, Mohammed A "Mobile health (m-health) system in the context of IoT" In *2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW)*, pages 39-42, 2016

[125] Santos, Alexandre and Macedo, Joaquim and Costa, António and Nicolau, M João "Internet of things and smart objects for M-health monitoring and control" In *Procedia Technology*, volume 16, pages 1351–1360, 2014

[126] Jara, Antonio J and Zamora, Miguel A and Skarmeta, Antonio F "Drug identification and interaction checker based on IoT to minimize adverse

drug reactions and improve drug compliance", In Personal and ubiquitous computing, pages 5–17, 2014

[127] Jara, Antonio J and Alcolea, Alberto F and Zamora, MA and Skarmeta, AF Gómez and Alsaedy, Mona "Drugs interaction checker based on IoT" In *2010 Internet of Things (IOT)*, pages 1–8, 2010

[128] G.O. Babalol, I.O. Olaniyan "A mobile based drug dosage checker on internet of things platform" In *2010 Internet of Things (IOT)*, volume, pages 226-236

[129] B.V. Lahari, S. Erukala, A. Sasank "A novel semantic medical access monitoring system for e-health applications using internet of medical things" In *International Journal of Engineering Technology*, volume 9, pages 265-272, 2018

[130] Bommasani, Lahari Vyshnavi and Babu, Erukala Suresh and Aluri, Sasank "A novel semantic medical access monitoring system for e-health applications using internet of medical things" In *International Journal of Engineering Technology*, volume 7, pages pp. 265-272, 2018

[131] Binu, PK and Akhil, V and Mohan, Vinay "Smart and secure iot based child behaviour and health monitoring system using hadoop" In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, volume 7, pages 418–423, 2017

[132] Kadarina, Trie Maya and Priambodo, Rinto "Preliminary design of internet of things (IoT) application for supporting mother and child health program in Indonesia" In *2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP)*, volume 7, pages 1–6, 2017

[133] Kiran, MPR Sai and Rajalakshmi, Pachamuthu and Acharyya, Amit "Context based sparse sensing technique and smart transmission architecture for iot enabled remote health monitoring applications" In *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 4151–4154, 2014

[134] Viswanathan, Hariharasudhan and Chen, Baozhi and Pompili, Dario "Research challenges in computation, communication, and context awareness for ubiquitous healthcare" In *IEEE Communications Magazine*, volume 50,number 5, pages 92–99, 2012

[135] Rasid, Mohd Fadlee A and Musa, Wan Mardiana Wan and Kadir, Nurul Ashikin Abdul and Noor, Anas M and Touati, Farid and Mehmood, Waiser and Khriji, Lazhar and Al-Busaidi, Asma and Mnaouer, A Ben "Embedded gateway services for internet of things applications in ubiquitous healthcare" In *2014 2nd International Conference on Information and Communication Technology (ICoICT)*, pages 145–148, 2014

[136] [online]https://www.mouser.com/applications/article-iot-wearable-devices/

[137] Hiremath, Shivayogi and Yang, Geng and Mankodiya, Kunal "Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare" In *2014 4th International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, pages 304–307, 2014

[138] Yuce, Mehmet R "Implementation of wireless body area networks for healthcare systems" In *Sensors and Actuators A: Physical*, volume 162, number 1, pages 116-129, 2010

[139] Zhao, Wei and Wang, Chaowei and Nakahira, Yorie "Medical application on internet of things" In *Sensors and Actuators A: Physical*, 2011

[140] Yang, Ning and Zhao, Xingli and Zhang, Hong "A non-contact health monitoring model based on the internet of things" In *2012 8th International Conference on Natural Computation*, pages 506–510, 2012

[141] Jara, Antonio J and Zamora, Miguel A and Skarmeta, Antonio F "Knowledge acquisition and management architecture for mobile and personal health environments based on the internet of things" In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1811–1818, 2012

[142] Imadali, Sofiane and Karanasiou, Athanasia and Petrescu, Alexandru and Sifniadis, Ioannis and Vèque, Véronique and Angelidis, Pantelis "eHealth service support in IPv6 vehicular networks" In *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 579–585, 2012

[143] Doukas, Charalampos and Maglogiannis, Ilias "Bringing iot and cloud computing towards pervasive healthcare" In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 922–926, 2012

[144] Shahamabadi, Mohammadreza Sahebi and Ali, Borhanuddin Bin Mohd and Varahram, Pooria and Jara, Antonio J "A network mobility solution based on 6LoWPAN hospital wireless sensor network (NEMO-HWSN)" In *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 433–438, 2013

[145] tek, Pawe, and Rucinski, Andrzej "IoT as a service system for e-health" In *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, pages 81–84, 2013

[146] Zhang, Xiao Ming and Zhang, Ning "An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and tele-medicine" In *2011 international conference on computer and management (CAMAN)*, pages 1–4, 2011

[147] Vazquez-Briseno, Mabel and Navarro-Cota, Christian and Nieto-Hipolito, Juan I and Jimenez-Garcia, Elitania and Sanchez-Lopez, JD "A proposal for using the internet of things concept to increase children's health awareness" In *CONIELECOMP 2012, 22nd International Conference on Electrical Communications and Computers*, pages 168–172, 2012

[148] Jia, Xueqin and Chen, Hao and Qi, Fei "Technical models and key technologies of e-health monitoring" In *2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 23–26, 2012

[149] Miori, Vittorio and Russo, Dario "Anticipating health hazards through an ontology-based, IoT domotic environment" In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 745–750, 2012

[150] Bui, Nicola and Bressan, Nicola and Zorzi, Michele "Interconnection of body area networks to a communications infrastructure: An architectural study" In *European Wireless 2012; 18th European Wireless Conference 2012*, pages 1–8, 2012

[151] Wang, Weihua and Li, Jiangong and Wang, Ling and Zhao, Wendong "The internet of things for resident health information service platform research" In *IET, 2011*

[152] Evans, Dave "The internet of things: How the next evolution of the internet is changing everything", volume 1, number 2011, pages 1–11, 2011

[153] Taylor, Stuart "The next generation of the internet revolutionizing the way we work, live, play, and learn" In *CISCO, San Francisco, CA, USA, CISCO Point of View*, volume 12, pages 6, 2013

[154] [online]https://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html

[155] [online]https://medium.com/datadriveninvestor/7-staggering-stats-on-healthcare-iot-innovation-fe6b92774a5c

[156] Bonomi, Flavio and Milito, Rodolfo and Zhu, Jiang and Addepalli, Sateesh "Fog computing and its role in the internet of things" In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pages 13–16, 2012

[157] Rochwerger, Benny and Breitgand, David and Levy, Eliezer and Galis, Alex and Nagin, Kenneth and Llorente, Ignacio Martín and Montero, Rubén and Wolfsthal, Yaron and Elmroth, Erik and Caceres, Juan and others "The reservoir model and architecture for open federated cloud computing" In *IBM Journal of Research and Development*, volume 53, number 4, pages 13–16, 2009

[158] Chang, Hyunseok and Hari, Adiseshu and Mukherjee, Sarit and Lakshman, TV "Bringing the cloud to the edge" In *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, volume 53, number 4, pages 346–351, 2014

[159] Manyika, James and Chui, Michael and Bughin, Jacques and Dobbs, Richard and Bisson, Peter and Marrs, Alex "Disruptive technologies: Advances that will transform life, business, and the global economy" In *IDC iView: IDC Analyze the future*,volume 180 volume 180, number 2012 pages 1–16, 2013

[160] Nay, C "The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east" In *BM Res., Armonk, NY, USA*,volume 180 volume 180, number 2012 pages 1.56, 2013

[161] Yang YANG, Ximeng LIU, Robert H. DENG "Lightweight break-glass access control system for healthcare internet-of-things", In *IEEE Transactions on Industrial Informatics*, Volume: 14, Issue: 8, 2018

[162] Xiaodong Yang, Dou Fan, Aifeng Ren, Nan Zhao, Muhammad Alam "5G based user-centric sensing at c band," In *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 5, pp. 3040-3047, May, 2019.

[163] Xiaodong Yang, Syed Aziz Shah, Aifeng Ren, Nan Zhao, Dou Fan, Fangming Hu, Masood Ur Rehman, Karen M. von Deneen, Jie Tian "Wandering pattern sensing at s-band," In *IEEE Journal of Biomedical and Health Informatics,* Vol. 22, Iss. 6, pp. 1863-1870. November, 2018.

[164] Yuan, Yong and Wang, Fei-Yue "Blockchain and cryptocurrencies: Model, techniques, and applications," In *IEEE Transactions on Systems, Man, and Cybernetics: Systems* Volume 48, pages 1421-1428, 2018.

[165] Badr, Shaimaa and Gomaa, Ibrahim and Abd-Elrahman, Emad "Multi-tier blockchain framework for IoT-EHRs systems," In *Procedia Computer Science* Volume 141, pages 159–166, 2018.

[166] Siyal, Asad Ali and Junejo, Aisha Zahid and Zawish, Muhammad and Ahmed, Kainat and Khalil, Aiman and Soursou, Georgia "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," In *Cryptography* Volume 3, pages 3, 2019.

[167] Xiao, Yang and Zhang, Ning and Lou, Wenjing and Hou, Y Thomas "A survey of distributed consensus protocols for blockchain networks," In *IEEE Communications Surveys & Tutorials* Volume 22, pages 1432-1465, year 2020.

[168] Sahoo, Swagatika and Fajge, Akshay M and Halder, Raju and Cortesi, Agostino "A Hierarchical and Abstraction-Based Blockchain Model," In *Applied Sciences* Volume 9, pages 2343, year 2019.