Internet of Things in healthcare: A Survey on Protocol Standards, Enabling Technologies, WBAN Architectures and Open Issues.

Vidyadhar, Jinnappa Aski, Vijaypal Singh Dhaka, Anubha Parashar, and Sunil Kumar

***Abstract*— This paper provides a state-of-art review on healthcare-IoT infrastructure, prominently focusing on protocol standards, enabling technologies, wireless body area network (WBAN) architectures and implementation issues. Internet of Things enchains the seamless healthcare devices from an actuate-sense-communicate (ASC) network in a proliferative channel in order to develop an operationally connected healthcare environment (OCHE). Sensors and actuators are the essential components of any IoT system that generates enormous data, and this data is communicated across the network concerning elementary statuses and stored in a distributed cloud platform. This paper begins by providing a brief horizontal overview of the IoT system. The enhanced technical details pertaining to healthcare scenarios such as WBAN architecture, layered healthcare IoT architecture, and enabling technologies are described in the forthcoming fragments of the paper. Authors have then provided a brief summary of the most anticipated protocol stacks and design issues that allows researchers and healthcare professionals to understand swiftly how the numerous protocols put together to attain desired functionalities without having to get through standards and RFCs. Authors have also explored recent state-of-art to identify some of the key challenges of the healthcare IoT domain and a short summary of each related research is presented. Moreover, the relation between Healthcare IoT and other disruptive technologies such as Blockchain and Big Data is being described. Finally, the authors explicated the detailed use-case scenarios to demonstrate how the numerous protocols and architectures presented in the paper could put together to attain desired healthcare services.**

***Index Terms*— Actuate-Sense-Communicate (ASC) Network, Healthcare Internet of Things (HIoT), Miniaturization, RFID, Sensors, Security, Ubiquitous Computing, and WBAN.**

I. Introduction

Many parts of the globe witnessed a consistent rise in elderly people due to the sudden increase in the reduced life expectancy ratio from the recent past. Based on a recent United Nation report, it is expected to have more than 2 billion old-age people by the year 2050 [1]. Chronic illnesses and imbalanced lifestyles are the major concerns towards the formation of an ageing society. Unfortunately, modern healthcare infrastructure is greatly impacted by the excessive load on the system to treat such disorders, causing an increased demand for hospital resources such as beds and nurses [2]. Apparently, there's a necessity to reform a stable solution for dealing with such excessive pressure on healthcare institutions while continuing to provide quality services to the outpatient departments (OPDs) [3].

Internet of Things is being most popular technology to offer an impactful solution to deal with treating chronic patients effectively. These solutions include remote sensing and predictive maintenance. The driving forces of already existent variants for connected scenarios such as smart grids [4], mobile cellular services [5], connected cars [6] etc., have now become the elementary ingredients for building advanced communication systems. Internet of things plays a pivotal role in driving such systems by offering real-time services. Creating and deploying such advancements in already established commercial entities such as healthcare and medicine industries remains a crucial point of discussion for many researchers. The major cause of concern is how to provide secured, miniaturized, and cost-effective remote services in the healthcare domain. Although many researchers trying to standardize the solutions to the major issues such as security, energy optimization and miniaturization in the healthcare-IoT realm, however, the results are yet away from the real-world application requirements [7, 8, 9, 10, 11]. In addition to the healthcare sphere, an application spectrum of IoT cuts across several areas covering home automation, smart energy management, industrial automation, education, retail marketing etc. Fig. 1 illustrates the recent trends in IoT application segments along

This paragraph of the first footnote will contain the date on which you submitted your paper for review, which is populated by IEEE. It is IEEE style to display support information, including sponsor and financial support acknowledgment, here and not in an acknowledgment section at the end of the article. For example, "This work was supported in part by the U.S. Department of Commerce under Grant BS123456." The name of the corresponding author appears after the financial information, e.g. *(Corresponding author: M. Smith).* Here you may also indicate if authors contributed equally or if there are co-first authors.

The next few paragraphs should contain the authors' current affiliations, including current address and e-mail. For example, First A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@ boulder.nist.gov).

Second B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

Third C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba 305-0047, Japan (e-mail: author@nrim.go.jp).

Mentions of supplemental materials and animal/human rights statements can be included here.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org

with subsidiary applications within each segment and their interactions through secure wireless protocols. Each domain offers its services to other domain-independent applications through sensors and actuators. Compliance through the homecare and in-house prescription management by the healthcare facilitator is another potential feature of healthcare IoT. Besides, various medical diagnostic devices, sensor nodes and imaging apparatuses are viewed as the fundamental blocks of the IoT. Healthcare services devised by IoT paradigm are expected to be cost-efficient and improve the quality of life by enriching the user experience. Therefore, amongst all its application subset, healthcare attracts attention for not just the noble cause but also due to the highly influential nature on the socio-economic factors.

In order to match the user requirements in contrast with the market mobility, the technology enhancements of emerging IoT healthcare services need to grow proportionally with innovations. Besides, healthcare devices need to be designed such that the customer needs should be fulfilled in terms of service availability (anytime to anywhere) [12]. Similarly, protocol up-gradations required to be kept compatible with the increase in heterogeneous health parameters. Moreover, the modern IoT challenges need not be concerned about toning the existing Internet architecture as traditional Internet architecture is viable to adopt modifications. For example, underlying protocols must be aware of the tremendous number of healthcare devices willing to connect to the Internet and it should house seamless connections. Internet-connected devices in 2010 had already overshot the globe's human population [13]. Thus, exploiting an outsized addressing space (IPV6) turns out to be extremely important to meet consumer demands for connected healthcare devices. Data security and user privacy are the outermost essential requirements in healthcare designs due to the inherent openness nature of the Internet to vulnerabilities [14]. In addition, cost-efficient delivery of IoT-enabled healthcare services should be ensured along with strategic management and monitoring of these deployed devices.

Recently, several healthcare researchers published their studies in domain-specific journals, which covers the different aspects of healthcare IoT such as patient monitoring systems, WBAN architectures, and communication protocols. As a result, there can be seen a wide range of prototype and service implementations in the field. Moreover, several of these survey studies overviews the IoT applicability in healthcare sector, where the discussion only covers the characteristics of fundamentals of HIoT, while combined parametric discussion is still missing in the literature review. However, in this proposed study, authors have holistically surveyed HIoT covering wide range of parameters such as WBAN architectures, enabling technologies, protocol standards and future scope. The research dimensions are increasing timely in terms of issue identification of existing infrastructures, network architecture enhancements, platforms, interoperability, and testbed designs etc. In addition, the deployment of IoT services in the medical field requires to be abided by certain legal policies and guidelines designed by governing entities and organizational bodies across the globe. However, IoT yet needs the high-level attention of the research community, as there is a rapid rise in the needs of the healthcare domain. At this point in time, IoT realization in the healthcare context is estimated to be useful for several stakeholders of the purview. In this regard, this paper overall the latest trends in IoT-enabled healthcare research and reveals numerous challenges that must be addressed to elevate healthcare technologies through innovations. Therefore, an overview of the paper contribution allied with the recent state-of-art in the field can be summarized as:

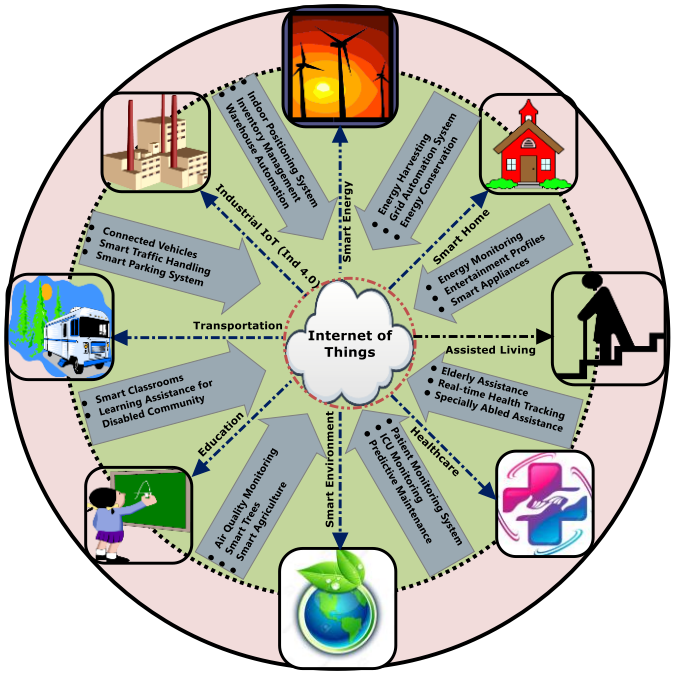

Fig. 1. Overall IoT application spectrum with domain independent services of each segment.

- In comparison to other survey articles in the healthcare IoT domain, this study astutely provides deeper insights about the most appropriate IEEE, IETF, IANA and IAB protocol standards to enable community members to swiftly understand without digging through standard specifications and RFCs.
- Authors provide extensive summaries of the recent research articles from the categories such as WBAN architectures, healthcare services and applications, security frameworks, and protocol standardization. The shortcomings of each summary have been identified. Furthermore, the authors explored the integral relationship between Healthcare-IoT and other disruptive technologies including Blockchain and Big Data.
- Authors provide the detailed descriptions of common WBAN architectures, service discovery protocols of Internet-enabled healthcare applications.
- Authors, then describe the exhaustive versions of

healthcare use-cases to demonstrate how the numerous protocols and architectures presented in the paper could put together to attain desired healthcare service outcomes.

The remaining part of the paper is structured as follows: Section II describes a summary of application history and commercial opportunities for IoT enabled healthcare products. Section II also describes the employed research methodology in this review. Section III and IV discourses the inclusive architectures of healthcare IoT and enabling technologies respectively. The enabling technologies include sensors, actuators communication protocols, gateway protocols, data processing units and service-oriented architectures (SOA). The standardized WBAN architectures are discussed in section V. The coexistent disruptive technologies such as blockchain and big data techniques that can redefine the healthcare infrastructure are discussed in section VI. Section VII discusses IoT use cases in chronic disorder management system. At last section VIII presents the concluding remarks

II. IoT Origin in Healthcare and Commercial Opportunities

A. The origin of IoT in healthcare and commercial opportunities

The IoT concept was introduced by Kevin Ashton in the year of 1999 during a conference with a presentation title "Internet of Things" [15]. Later in the year 2001 and onwards, the technology started outreaching many research institutions and commercial establishments due to the advancements in wireless communication technologies (WCT) and their operational capabilities. A scientific report was published in 2002 by the National Science Foundation (NSF), which emphasized the ways of interfacing information technologies with nanotechnologies [16]. This report was aiming to observe how these innovations dramatically influence improving the quality of life and productivity of a nation. Thus, IoT has been a topic of global interest for more than a decade now. However, the interoperation of IoT with the healthcare industry has begun recently with the potential understandings of how healthcare IoT (HIoT) is beneficial in reducing the cost of medical care through real-time service offerings. Thus, Internet of Things has re-standardized healthcare horizontal with its endless set of applications.

The increasing need for wireless wearable devices has recently emerged as the new powerful tools for developing healthcare applications using flexible electronics, application-specific integrated circuits (ASIC), energy harvesting and low power electronics [17]. Smart sensors, WCT, microcontroller units (MCUs) and cloud services assist in building advanced household health measurement devices which help in building data acquisition units for real-time monitoring [18] and analytical purpose. Object identification in IoT healthcare technologies need to be combined with wireless techniques such as RFID, low Bluetooth energy (BLE), Wi-Fi etc., in order to connect things to the network, so as to monitor, tag and control objects over the network infrastructure [19,20]. The possible instances of IoT aware healthcare architecture include automatic patient identification, tracking health records, biomedical devices from remote places, prescription management system, real-time monitoring of patient's biomedical information [21]. Furthermore, RFID, ultrahigh-frequency (UHF) radio operated devices, wireless sensor network (WSN) are the pioneering technological components of implementing any healthcare devices. RFID is one of the oldest inventions of radio communication technologies (RCT) that act as a primary ingredient of the latest HIoT innovations.

The global market space for IoT was estimated to be USD 606 billion in 2014 [22]. Technological advancements and increasing stakeholders are likely to drive the global market over the next few decades. Radical advances in WCTs, ICTs and increasing penetrations of internet and broadband services have created phenomenal impacts in HIoT realm. The global market is expected to be hit by more than 212 billion connected devices by the end of 2020 [23]. By 2022 traffic generated from M2M, Machine to Human (M2H), Machine to Things (M2T) is predicted to create up to more than 45% of the whole network traffic [22]. Fig. 2. Depicts the incredible market share of HIoT and other IoT areas till the year 2025. However, these predictions take an abundant part in building the nation's economy as the manufacturing industry growth will be massive during this era. As shown in Fig. 2. The Healthcare industry and transportation sectors are projected to constitute the largest impact on the global market by 2025. Besides, as per the report of McKinsey Global Institute, the growth rate of the number of connected devices in recent years has been increased by 300% [24].

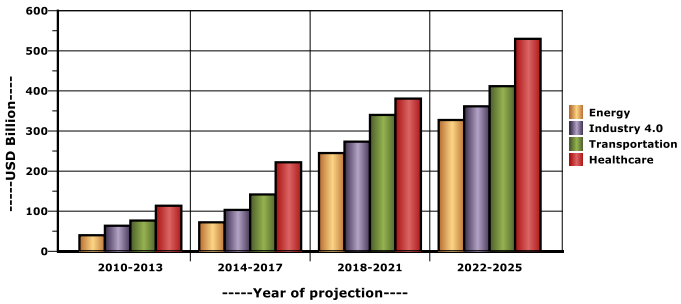

Fig. 2. Competitive market sharing projection of HIoT for 2025.

Wikibon's prediction intuits that the value created from the HIoT to be about $1110 billion by 2020 with the Investment Return (IR) growing to more than 110% compared to 12 % in 2013 [25]. On the other hand, Navigant has produced an eco-scientific report recently, according to which it was predicted that Building Automation Systems (BAS) market would rise from $58 billion in 2013 to reach $100 billion by 2021 [25]. On the other hand, technology giants have started increasing their R&D investments in the HIoT domain so as to retain the benefits of early market players. These industries are highly competitive, and they can deploy the latest technological innovations in product implementation. Major involvements in the product line industry can be observed by Philips, Siemens, ABB, Cisco Systems Inc, and Huawei Technologies. In general,

all of the aforementioned statistics potentially signifies the growth of automation in healthcare and manufacture industries will be rapid in the near future. Therefore, this evolution provides a novel opportunity to traditional healthcare device manufacturers for transmuting their devices into smart HIoT devices.

B. Review Methodologies

The authors have incorporated three phases in performing the analytical studies of state-of-art healthcare infrastructures in accordance with the guidelines given in [26, 27]. As per these study guidelines, the review implementation is carried out in three phases: review planning, review conducting and review documentation. In addition to these guidelines, authors have further enhanced the study by including review classifications and result analysis phases explicitly (see fig. 3).

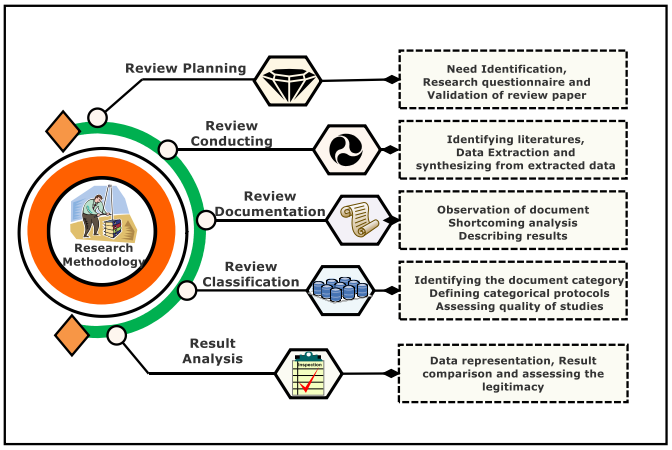

Fig. 3. Adopted research methodology for this study

The review planning phase of HIoT infrastructures is carried out by a gradual procedure which involved the following steps: (1) identification of need and fundamental prerequisites for the systematic state-of-art review on Healthcare IoT infrastructures and constituting technological components, (2) Outline the research questionnaire along with the motivational objectives (see fig. 4.), investigate the research gap, and expose the shortcomings of the current studies and (3) validate/authenticate the assessment of the selected review papers of the subject HIoT infrastructures and associated enabling technologies. In order to optimize the research objectivity of this study, authors implement the following steps additionally. The steps are, review classification: this step is performed to classify the review articles based on different parameters such as wireless protocol related articles, WBAN architecture-related articles, enabling technology-related articles and case-study based articles. Each of the classified articles has been further evaluated qualitatively and results are verified from each class. The final step is result analysis: each of the categorical articles is studied and the results from those studies are quantified in a tabular form, similar results are identified and compared with each other. Therefore, it is observed from each of those articles at last whether the mentioned research goal is attained. A short summary of each such article is described in the below section. The objective of the research questionnaire (fig. 4.) is to provide a better understanding of how conventional healthcare systems are being replaced by HIoT using advanced data processing units. In addition, it involves the selection criteria of an MCUs for designing such HIoT systems.

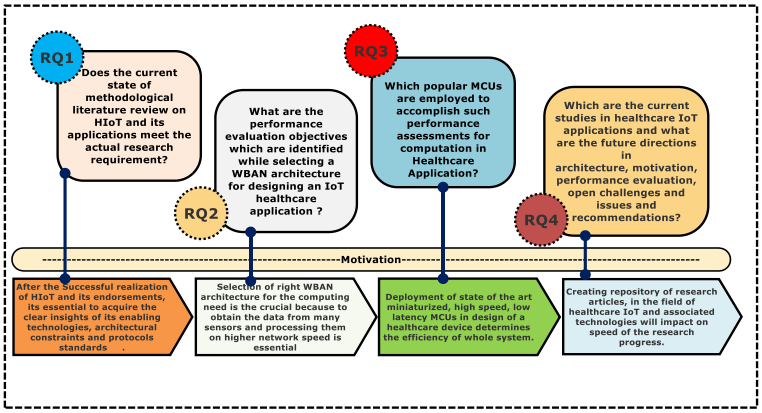

Fig. 4. Questionnaire-motivation based methodological approach for designing HIoT review

III. SERVICE ORIENTED ARCHITECTURE (SOA) FOR HIOT INFRASTRUCTURE

The primary objective of the IoT is to connect a heterogeneous set of objects through the generic Internet infrastructure and make them talk to each other concerning their status. Therefore, the flexible layered architecture for designing such heterogeneous IoT systems is critically important. Although, there are several SOAs are proposed by many researchers so far, there is no such reference model available in the literature [32]. Further, efforts are made to create a common IoT-aware, intelligent architecture [21] for patient tracking and monitoring of health parameters used within the hospitals or medical institutes. Standardization of SOA architecture is yet another open issue in the field of IoT system universalization. However, there are several architectures with varying layers [33], [34], [35] in recent state-of-art mainly including physical/object, network and application layers in their abstract form. Fig. 5 explains the detailed, five-layered SOA for healthcare applications. This is being abstracted by combining many multi-layered SOAs from [33-37]. Functionalities of each layer are featured in the subsection below.

a. Object/context Layer: The primary layer of the generic IoT architecture is the Object layer. The object layer can be interchangeably called by perception layer or things layer or context layer. This layer certainly adds context for the applications. The main function of the Object layer is to acquire the various forms of data from physical entities by sensor devices and process them locally for remote transmission. The constituent elements of the Object layer are sensors, actuators, MCUs, RFID tags/readers and physical entities from which the data need to be extracted. In the healthcare context, the entity is the patient body. The Object layer is responsible for the standardization of heterogeneous object configuration in a plug-and-play manner irrespective of underlying infrastructures [34] such as type of MCU, developing environments, type of sensor etc. The object layer initiates the data creation phase for big data analysis. The data generated at this layer gets transferred to the cluster head/gateways for further

transmission to the upper layers.

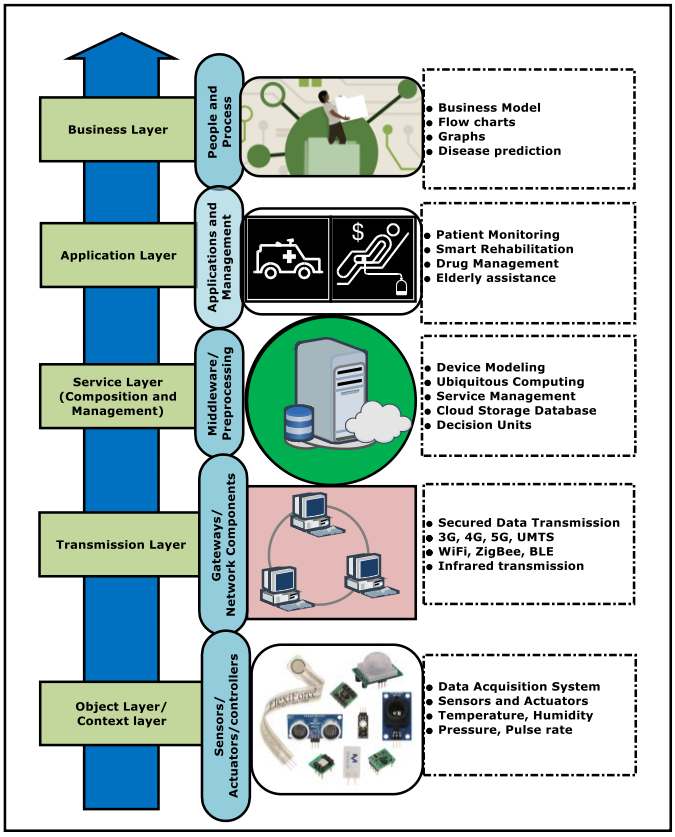

Fig. 5. Layered SOA for Healthcare infrastructure

b. Transmission Layer: The transmission layer transfers the data generated by the object layer to the service composition layer through various gateway devices such as GSM, RFID transmitters, BLE, UMTS, NFC, ZigBee, LAN, WAN, PAN etc. Besides, healthcare devices are mostly personalized with access control mechanisms to ensure the proper access rights at the transmission layer. Additionally, this layer initiates the pre-processing of data for cloud computing purpose using various transformations as per the cloud infrastructural needs [35].

c. Service Layer (Composition and Management)/ Middleware layer: Every healthcare device should have individual credentials while accessing the middleware layer components [38]. The service management layer acts as a bridge that connects the device and the requested service in the cloud computing environment based on the DNS and port address of the requested resources. This layer allows application developers and programmers to directly interface heterogeneous physical entities without considering any specifications of hardware platforms. This layer also composes the different middleware services such as service abstraction and protocol standardization [37]. These services are offered to the network-wide protocols.

d. Application Layer

The application layer offers the services to its large set of end-users via mobile and desktop applications as per the requirements of the users. For example, the application layer would provide the healthcare data such as body temperature, blood pressure, ECG patterns, pulse rate etc. to the users on a request basis. In other words, this layer focuses on analyzing diverse health data collected over a period from the data acquisition/Object layer [39]. The application layer includes a wide range of healthcare application verticals such as elderly assistance, real-time monitoring of patients, ICU monitoring, assisted living and patient prescription management systems [39-43].

e. Business Layer: The business (administration) layer sits on top of all the layers managing the operations of the application layer and other subsequent layers implicitly. The functionalities of this layer include building statistical graphs, reports and flowcharts to support business decisions. This layer deals with creating bigdata application for predictive analysis in chronic disorders by taking a large number of datasets from the input layer. The essential components of this layer are people and processes. In other words, this layer comparatively analyses the output of preceding layers with the predicted results in order to enhance business modelling while maintaining user privacy [44].

Observations: The layered architecture of IoT invoke most of the concepts from computer networks protocol stacks (TCPIP) and hence this may not confront the normalization of real IoT environments as the network layer technologies do not hold all the capabilities to transform the data to the IoT platforms. Besides, these structures are designed specifically to address WSNs and WBANs of the healthcare universe. Moreover, the service composition in SOA based architectures are chosen to run on some resource constraint environments while minimizing the time and energy complexities of IoT devices in communicating with other devices. Like in TCPIP, layers in SOA based architectures also have the feasibility to offer the services to consequent layers. The diverse data from the object layer has to be managed intelligently so that smart monitoring of the patient is possible from a centralized or distributed cloud environments. Hosting business layer applications on a powerful computing machine is necessary due to the need of computing unstructured and complex data. Considering the aforementioned points and simplicity of SOA, it is preferable to use five-layered architectures for designing HIoT applications.

IV. EXISTING WORK

This section explores both survey and implementation work carried considering HIoT research area. The first part of this section explores the latest implementation approaches and the second part deals with the review/survey articles published in recent years.

A. Review of latest implementation approaches in Healthcare-IoT (HIoT)

Some of the articles from the field of healthcare IoT implementations have been summarized in the below section. The parameters considered for selecting the articles for this sections are, HIoT system design constraints, security of HIoT devices, the energy efficiency of a healthcare device, data accessing methods and WBAN architectures. The summary of each paper is presented with the identified shortcomings.

Ramson et al. [18] presented a modular approach for designing an automated healthcare device for household utility. The authors have mainly focused on designing a physical

device that is accessible by RFID number issued to the subscribed user. The device comes up with a non-invasive bio-patch, once this patch is attached to the user body, different biological parameters such as ECG, body temperature and EEG information start flowing towards the doctor site where the doctor can visualize those parameters in real-time. Based on the user authentication, the system guides the user to follow up on the prescriptions suggested by doctors. Therefore, this system empowers a resolution for the noncompliance problem of medicine by periodically encouraging patient and providing accurate medicine on regular intervals as per the uploaded prescription by the medical practitioner. Shortcomings: Although, the proposed technique provides a real-time solution for monitoring body parameters, the issue relies upon the type of material used for making the patch. Due to the random folding and repeated usages, the silicon layer from the patch may peel off. Related to security, there must have been an access control mechanism to avoid unauthorized accesses and digital intrusions. The authors did not focus on emergency and delay related parameters. An improved GUI system implementation would have been an added advantage for the system users in terms of user-friendliness.

Zhang et al. [45] introduced a security algorithm called cypher-text policy attribute-based encryption (CP-ABE) pattern that ensures adequately tuned access control and information security HIoT scenario. Authors have subsequently described the design policies of their algorithm through various secrete key parameters issued to users such as user-key and subscriber ID which relate to a set of inevitable attributes of the system. Authors have basically emphasized their central interest on designing an attack free model which obtains the health records from central cloud infrastructure. These data points can be viewed by the list of users with their secrete key. The key is matched with the underlying access policies, once there a match found the user will be given access to view his/her health records. Authors have also compared their work with co-existing algorithms and claim better results. Shortcomings: The proposed scheme is well implemented to restore the receiver's attribute while protecting attribute information from ciphertext attacks. However, since the complexity of the algorithm that protects the attribute information from attacks is directly associated with operational levels at the description process. Hence the requirement of high computational power is essential. Therefore, how to reduce high computational power requirement is an urgent issue to be resolved. The proposed scheme is vulnerable to various kinds of leakage attacks such as side-channel attacks, and cold-boot attacks. User experience seems to be poor in the proposed scheme as it creates additional load on the server with an increase in attribute size.

Pirbhulal et al. [46] produced an access control algorithm for highly personalized healthcare devices comprised of a wireless body sensor network (WBSN) which generates random binary sequence (RBS) based on heartbeat patterns. In the proposed system the privacy enforcement in accessing the healthcare device is keyed by heartbeat-based RBS which ensures confidentiality. The technique behind the proposed mechanism is to detect the inter-pulse-interval (IPI) and incorporate it as an attribute to the cyclic block encoding procedure from which each IPI extracts many entropic bits. The conversion of an IPI to an RBS is carried out by a simple cyclic block encoding technique in the proposed scheme. The authors tested their algorithm on a hardware platform designed to monitor the ECG signals from the human body that detects more than 95% accurately. Authors also claim that their algorithm produced an extensive better result with the four-time faster running time than the existing RBS based schemes. Shortcomings: Although the randomness quality of the proposed IPI-based approach is found to be efficient in comparison with many existing approaches, the bottleneck throughput issue is still a concern. It is remarked that only 8 bits of random binary sequences are generated for every 60 PPMs (pulse per minute) of relative throughput. This is a quite low throughput in comparison with the other existing algorithms that produce 1024 random bits for the same relative throughput.

Wu et al. [47] implemented an autonomous solar-energy powered WBAN for low radio power-driven (BLE) wearable healthcare devices used in connected healthcare applications. Various bio-parameters like body temperature distribution, heart rate and ECG patterns can be measured using the proposed system. These bio patches are powered by solar energy harvesting units that act on output-driven maximum power point tracking technique (MPPT). The authors designed a cloud-centric mobile application for monitoring and tracking healthcare records and produce alarm notifications whenever data point reaches beyond the threshold values. Different kinds of commercial plug-in sensors (pulse, temperature and ECG) are interfaced with Atmega328P MCU to create the data acquisition system. Shortcomings: The wearability needed to be enhanced in terms of user comfort using flexible electronic PCBs. Data security is an essential element in any personalized IoT healthcare devices. Access control mechanisms and efficient security algorithm for data transmission in remote storage units, would have contributed in constituting a secured healthcare device. Although the data acquisition system of the proposed architecture remains efficient in acquiring data from sensor nodes, the transmission and processing latency is the major bottleneck for real-time handling of data in the cloud

Arunkumar et al. [48] introduced a mechanism that represents the collection, integration and interoperation of data from several heterogeneous HIoT platforms and used in emergency medical services. The proposed mechanism intent to structure the various forms of physiological data collected from IoT platforms and prepare it to be readily available to an appropriate healthcare provider during emergency circumstances. The cloud architecture can house the ubiquitously collected data from several IoT nodes of different types through metadata modal. NoSQL database models are used to store the data. Authors have conducted experimentations to demonstrate the physical entities in an information model through the hardware implementations. The IoT device aims to interface the numerous healthcare sensors such as temperature, pulse and ECG and RF tags. Authors compared their work with various existing methodologies in terms of Model-Driven nature, knowledge-centric nature, activity-centered and user-centric nature and observed extensively better results. Shortcomings: One area of improvement in the proposed work is access control, which is considered only on an elementary level. Further security

enhancements would bring more power to the system. The proposed work requires human intervention at a higher level to extract data from the patient body, an autonomous technique to collect the data from the human body would have been made user experience rich. The proposed model has a portability issue as they have used a proprietary data model that cannot be easily transformed when there is a change in platform.

Abawajy et al. [49] presented a methodological work on pervasive patient health monitoring (PPHM) infrastructure used in healthcare applications. An energy optimized cloud-powered ECG Telemonitoring service towards patient care was detailed in the proposed article. In this work, the authors have designed an implantable, invasive sensor pad that can be attached externally to the patient body to gather the physiological parameters. The monitoring system detects the normal and abnormal levels of various blood and body parameters such as blood sugar, glucose level, Pulse-Oximetry and ECG continuously or on-demand. All these data points are stored on a medical server for further analysis. In order to optimize the bandwidth and energy efficiency of the system, a fuzzy-based data fusion technique that distinguishes between true and false values and hence only process true value data set. Authors have further ensured the improved resource utilization by an explicit scheduling algorithm that schedules both real-time and offline services. The authors have also described the feature extraction through an analytical engine for providing good patient care. It was observed from the system implementation that there will be an alarm signal which raises as and when it reads the abrupt variations in health conditions and threshold crossing. The authors evaluated the proposed framework using an emulator-based approach on real ECG signals from the Congestive Heart Failure Database (CHFD) and observed high accuracy. Shortcomings: The infrastructure design methodologies needed to put much focus on information security and privacy protection. How to ensure the security of such highly confidential health data would have been emphasized in greater detail. Although authors claim that they have developed a wearable sensor device, the main issue is related to the installation complexity.

Moosavi et al. [50] proposed a secure energy-efficient scheme for mobile healthcare applications that provides the datagram security at the transport layer. The proposed scheme is lightweight and requires less computational and communicational power. Authors pertain their architecture to multi-layered architecture. An access control mechanism is employed for providing protected resource accesses. The proposed article demonstrates the real-time patient monitoring system which was implemented by various biosensors and a data processing unit (MSP430 micro-controller). Authors ensured high-level security at device and cloud levels by employing various cryptographic primitives such as SHA-256, AES, and elliptic curve cypher suit. Shortcomings: The proposed security model has some fatal flaws such as the model can be an easy victim of various insider attack due to the nature of wireless communication thus disturbing routing strategies. The proposed model does not suit IP-based WSNs because they originally not designed for the 6LoWPAN protocol. So designing a base platform for 6LoWPAN is an interest of many network researchers in the recent past. The proposed system also exhibits localization issue as locator need to change on a regular basis to enable continuity on the receiving packets.

Zhang et al. [51] proposed a dynamic authentication protocol that protects user privacy through bio-hash based function and a multi-factor authentication key in medical application. The proposed scheme employs the biometric verification method on the server without revealing the user's biometric pattern to the server and thus generates a verification key by preserving the user's anonymity at the initial level. A generic biometric template is diffused with a random string in order to prevent the server to know the user details. The algorithm uses EX-OR operation for creating two strings and they are matched at the server-side with the non-real values rather than matching with the real values of a biometric template. The proposed algorithm is lightweight in nature as they use only bio-hash functions throughout. The authors compared their scheme with other related works and observed reduced computational cost and communication cost as the model adopts lightweight hash and bio-hash operations. Therefore, the proposed scheme can meet the energy consumption demands and security needs of e-health systems successfully. Shortcomings: The proposed doesn't implement the access control mechanism. The ownership transfer mechanism and user traceability features would have been empowered the system more effectively. The model is vulnerable to DDOS attacks, de-synchronization attacks, and insider attacks. The proposed scheme doesn't verify the password and smart card at the server-side, rather only verifies the user biometric credentials hence this scheme is not truly a three-factor authentication scheme.

Yang et al. [52] modelled an access control protocol for emergency healthcare situations called lightweight break-glass access control mechanism. This protocol works in two modes: normal mode access control technique for normal monitoring of healthcare parameters, emergency mode access control technique for emergency healthcare conditions. A break-glass access control technology enables the medical doctor to access the health records of a patient by skipping the access transfer policies in order to frame the immediate treatment strategies during critical healthcare situations. This mechanism is implemented through the access token generation phase which is executed on cloud platforms. The algorithm is attributed by a healthcare infrastructure provider (HIP), the patient (PA), the data users and the emergency contact person. The key generation unit generates the public-secrete key pair for the entire system and the patient and data users are attributed by these keys. A break-glass key is generated by a patient during emergency medical conditions through his/her assigned password. Once the break-glass key is generated the verification of correctness of the details is performed at the decryption side algorithm. Shortcomings: Although the proposed algorithm has slightly better efficiency in terms of communicational cost than existing, it cannot accomplish the trusted revoking of the data from a compromised node deployed at a large-scale application such as smart city and giant healthcare networks. The proposed algorithm doesn't explain the resistance methodologies towards cold-boot attacks under the random oracle model. Because the public key size is variable in nature, the break glass access control mechanism

may experience computational complexities at the time of emergency condition.

Shao et al. [53] introduced a reconfigurable UHF RF-based sensing solution that operates as a standard sensing platform for advanced IoT applications specifically used in various horizontals such as healthcare and smart city applications. The design implications are supported by the low power electronics thus eliminating high power needs. The authors demonstrated the implementation of the proposed design in analog frontend and the digital core block phases. Authors have designed an RFID transmitter-receiver pair with a multithreaded programming approach which operates in an isolated environment within a single electronic chip. The Amplitude Shift Keying (ASK) demodulator is designed using low power Schottky diode in order to achieve low power requirement. The experimental IoT system allowed authors to perform on two different test modes such as Continuous data transmitting test mode, and Data logging test mode. This allowed authors to learn about the stability factor of multimode configuration in a digital design. Shortcomings: The proposed approach involved the usage of a small external battery that could be recharged by the power transmission sources. However, a detailed circuit design for efficient battery management is not available in the article. The application of semi-passive techniques to RFID directly is a complicated process, which leads to high power consumption or larger IC space problem. This shall be overcome by employing additional design techniques such as common mode feed-forward loops or ripple reduction loops. The major issue relies upon scalability as it is difficult to reduce the path-loss probability in the dense multipath and multi-user environment.

B. State-of-the-art HIoT survey

The recent review studies in the Healthcare IoT domain explores most of its facets. However, there are continuous breakthroughs happening in IoT technologies day by day, especially in the Healthcare domain. Therefore, it's essential to bring out such updating for the benefits of the community. Several recent surveys address the specific aspects of healthcare IoT such as sensing, communication and data analytics/interference [82]. The survey that addresses IoT integrated applications for kids is being detailed in [83]. The application aspects of HIoT in a variety of fields including elderly health parameter monitoring, ambient assisted living (AAL), rehabilitation, wearable devices for household applications have been reviewed with the greater details in [84] [85] [86] and [87] respectively. The HIoT application emphasizing the building of rural infrastructure in developing countries have been detailed in [88]. The various other reviews focusing on device and data security, and communication protocols of HIoT applications have been comprehensively described in [89-90,115]. The review focusing on the analysis of HIoT in the cloud computing view is detailed in [91]. The application/business layer components of SoA of HIoT such as machine learning/deep learning applications are explored in [92]. The IoT applications in building smart home designs used in monitoring health parameters via centralized architectures have been discussed in [93]. In addition, there are several studies whose central discussion flows around high-risk environments in industries [94], HIoT enabling technologies [131], HIoT security [132], Interoperability standards [133], mental health monitoring applications [95] and smart homes [96]. Most of these articles describe only individual aspects of HIoT. Distinct from the abovementioned studies, this survey aims to design a holistic survey covering core parts of HIoT application area. The areas covered in our study are protocol stacks, communication protocols, architecture standards, security aspects, WBAN architectures and the relationship of IoT blockchain and big data have been explicitly detailed. Table 1 summarizes the comparison of comparison of related works and our contribution.

Table 1: Existing surveys on HIoT topics and our new contribution

Survey	Key Topic	Coverage-Matrix of parameters				Taxonomy	Observations
		Protocol standards	Enabling technologies	WBAN architectures	Open Issues		
[25]	Protocols and Enabling technologies	Partial	Yes	No	No	No	Comparison of standards is missing
[82]	Healthcare IoT with clinical prospects	Partial	No	No	No	Yes	The survey scope is only limited to the clinical analysis
[83]	General IoT applications in Healthcare	No	No	No	No	Yes	The survey is abstracted only for general terminologies
[84]	HIoT with device prospects	Yes	Yes	No	No	No	The discussion is only limited to the device design strategies
[88]	HIoT Application and security challenges	No	Yes	Yes	Yes	No	The survey has a limited scope of HIoT spectrum
[115]	Future of HIoT	No	Yes	No	Yes	Yes	The study investigates more generalized HIoT applications and its Hypothesis
[131]	Enabling technologies in HIoT	No	Yes	No	No	No	The study only aims to discuss enabling technologies
[132]	HIoT data security	No	No	No	No	No	The study only aims to discuss HIoT data security technologies
[133]	HIoT interoperability	No	No	No	No	No	The study only aims to discuss HIoT interoperability security technologies
Our survey	Complete coverage of HIoT spectrum	Yes	Yes	Yes	Yes	Yes	A holistic discussion of HIoT is provided

V. HIoT ENABLING TECHNOLOGIES

The realization of IoT in real-world problem sectors such as healthcare is made possible through various enabling technologies. In this section, the authors provide a brief introduction about the most relevant enabling technologies used in actualization IoT in the healthcare industry. A major part of these enabling technologies covered by hardware components namely sensors, actuators, gateway modules, wireless modules and data processing units as shown in fig. 6. Protocol stacks (wireless/wired) and cloud infrastructures are the network and storage related technological components respectively. Data processing units are sometimes referred to as local processing units (LPU) or microcontroller units (MCU). The objective of this section is not to provide a comprehensive overview of each of these technological components, rather the aim is to picture a high-level understanding of their roles in developing HIoT applications. However, the deep learners will find the descriptive information for each individual technologies elsewhere [27-29]. The proposed taxonomy (see fig. 6) is

inquisitively based on the various architectural components of HIoT presented over the upcoming sections.

A. Sensors and actuators

The ever-growing advancements and expansions in sensing technologies of physical and biomedical parameters reveal a new era of application development in the field of healthcare IoT. The visionary categorization of IoT in the aspects of things, the internet and semantic technologies indicates the elementary understandings of "Anytime, anywhere, anything and any media" connection. In this context, IoT wireless technological components have played a vital role in achieving one to many relationships with the human to devices, thus exceedingly more than one connected device per person [30]. The body sensor network (BSN) is one of the major technological intents of any healthcare IoT designs where a person's biological parameters can be monitored continuously using tiny-sized, battery-operated self-configurable wireless sensor nodes (WSN) for acute or chronic disease analysis. The practical implementation of IoT systems at the object layer may include many sensors and actuators which constitutes the data acquisition system. There exist numerous types of sensors nodes in the healthcare context. These nodes either comes in a package or individual sensor units that depend on the application requirements. Such package of e-health sensor node comprising sensor units for monitoring various biological parameters such as pulse rate, ECG, blood pressure, foot pressure, body temperature, gait angle, indoor air quality etc.

E-health sensor nodes can be further classified into several types depending on the application area in the health monitoring context. In [31], authors have classified e-health sensor node in three classes for their application of fog assisted diabetic patient monitoring in cardiovascular disease analysis. The types are as flows: low data rate sensor nodes that deals with lower data transmission rate from sensor nodes to cloud, high data rate sensor nodes deal with higher data transfer rate from object layer to storage layer and hybrid data rate sensor nodes that deals with the transmission of sensor data in a moderated manner.

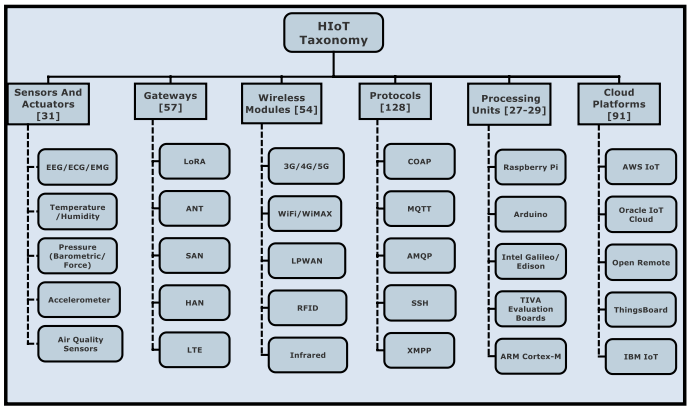

Fig. 6. HIoT taxonomical representation of enabling technologies

B. Communication gateways and technologies in HIoT

In general, IoT technology can made of things (sensors, communication devices, MCUs etc.) cloud infrastructure and mobile application considering its usages in various fields. It's needless to say that IoT is an embedded discipline that fabricates both hardware and software components. Different hardware components exhibit different computational, communicational, connectivity, storage and data processing capabilities. For example, desktop computers have got powerful storage, processing and network capabilities. Whereas, BSN has got limited capabilities in terms of computation, communicational and storage-related tasks in comparison with desktop computers. However, IoT enables both BSN and desktop computer to interact with each other with a specified set of communicational protocols such as gateways and wireless modules. Gateways are the wireless devices that channelize the sensor data packets to the destined routers through a wide range of protocols in any healthcare applications [54].

IoT can have several indigenous wireless networks such as WBAN, BSN, WSN and wireless mesh networks. These components play a key role in exchanging data across the networks. Gateways are featured by the capability of getting their knowledge leveraged by optimally executing the network algorithms at the local level. Hence, it's worth noting that the gateway devices are the network components that handle complex communicational events [55]. LoRaWAN is a low power long-range and lower bitrate wireless gateway protocol that can be housed as an infrastructural solution for many HIoT applications. It incorporates LoRA modulation for enabling several HIoT consumer devices using medium access control (MAC) mechanism [56].

Further, the gateway technologies are advanced enough to offer storage as a service (SAAS). In this category, SAN network gateways stand forefront. The process of deploying SAN topologies in large scale healthcare applications is a step-by-step procedure. First, the SAN must be designed keeping in mind the futuristic scalability and current needs of the application. Next, the related services in terms of hardware and software requirements in conjunction with the SAN networks should be identified. Finally, the management of SAN through software and hardware should be handled by the SAN providing vendor. Similarly, home area network (HAN) gateways are used effectively as load balancers [57] for sensor-based applications where many WSNs are deployed at a location. The advanced HAN design techniques enabled gateways to incorporate low power routing [58]. Likewise, adaptive network topology (ANT) is another gateway technology that is like BLE concept and primarily used in sports and fitness sensory applications. In telecommunication, another potential gateway technology is the long-term evolution (LTE) gateway. This gateway employs standard techniques for wireless broadband communication in mobile sensor applications. Further, this gateway tends to improve the speed and capacity using multiple radio interfaces [59] [60].

C. Wireless communication technologies (WCT) and supported protocols

Wireless communication technologies supporting protocol stacks act as a backbone for IoT healthcare subsystem, which brings the key objectivity in transmitting data to the remote areas. Predominantly there are three types of WCTs Viz. (i) short distance wireless communication technologies

(SDWCTs) (ii) Moderated long-range wireless communication technologies (MLWCTs), (iii) long-range wireless communication technologies (LWCTs). However, long-range wireless communication technologies involved in transmitting data packets through high power transceivers such as 3G/4G/5G antennas and mainly used in mobile and internet data transfer. This part covers only the SDWCTs and MLWCTs in detail.

a. Short Distance Wireless Communication Technologies (SDWCTs):

Implementation of HIoT application mostly involves any of these SDWCTs such as BLE, ZigBee, infrared and RFID at data acquisition (DAQ) level design. The varied operational radio frequencies and standards of these technologies cause respective variations in data transfer rates, security standards, number of nodes allowed (single hope/multi hope), energy consumption and deployment costs. Short-range radio-based transmission systems are significantly used in designing such WSNs.

Zigbee is a standardized IEEE 802.15.4 based wireless protocol, it was initially designed by an association of Zigbee special interest group and now the protocol up-gradation and maintenance is carried by Zigbee alliance. This protocol was designed to realize the operational capabilities of a low power wireless area network (LPWAN) incorporation with multiple access control (MAC) at the physical layer [61]. Zigbee devices are typically embedded on radio enabled MCU. Zigbee native network ideally supports both star and tree topologies. Infrared communication technology is another breakthrough in the area of embedded communication which is generally used in distance finding and object detection applications.

b. Moderated long range wireless communication technologies (MLWCTs)

Wi-Fi is another 802.11 based family member of radio communication technologies that are typically used in creating a local area network of devices for internet access. Wi-Fi is recognized as a trademark of the Wi-Fi alliance. Currently, Wi-Fi-based LANs are available in many of the hospitals, due to the low-cost implementations. Therefore, Wi-Fi enabled short distance services in hospitals for monitoring and real-time service offering purpose are popular these days. WiMAX is an extensional service to Wi-Fi which operates on the 802.16 sets of standards and provides multiple physical and MAC layer opportunities. WiMAX can be used to provide internet access to the consumers either at the home, city or across the countries. It is an utmost important task of selecting a WCT for HIoT applications to satisfy the need for wireless computing. Hence, numerous parameters are considered in selecting a WCT among which a patient body reaction to radiation level is crucial. Security and latency are the other major parameters in selecting a WCT.

D. Standardized IoT protocols and processing units

a. HIoT protocol stacks

The representation of diverse data acquired from various medical and environment sensors is accomplished by numerous data aggregation techniques and resilient encryption standards over the Internet. Selection of an appropriate wireless protocol stack and MCU for implementation of HIoT application plays an important role in handling medical emergencies by the remote systems. Therefore, an efficient transmission layer protocol that allows service discovery and self-configuration must be developed in order to transform the physical layer data into the encoded medical data. The protocols are capable to facilitate flexible device addressing, efficient routing strategies, interoperability of heterogeneous devices and most importantly the inter-connectivity to the wide internet via wired and wireless media. The aforesaid functionalities are implemented in the context of IEEE 11073 [62] set of standards and are executed at HIoT devices. The aim of IEEE 11073 set of standards is to facilitate interoperability among different entities (healthcare service providers, doctors, medical devices, caretakers and service management units) while ensuing standardized interconnection interface for personal health devices (PHDs) [63]. The device specializations are further supported by the extensive subset of IEEE 104XX series of sub-standards which are realized for a different set of healthcare sensors. At present, there are several researchers working on ambient assisted living (AAL) topic that enhances the quality of life of an elderly community by offering connected health services [63]. In his context authors describe the network infrastructure that employs the specially designed protocol for constrained environments called CoAP (constrained application layer protocol) stacks. The next part of this session includes a brief overview of each such protocols used in implementing connected health applications.

Fig. 7 illustrates the interconnection of various healthcare entities such as user devices, healthcare service provider, and cloud computing units independently while ensuring the quality of service. In the prospect of IEEE 11073 standard, data aggregators are the sensors/ actuators attached to user PHDs. As per the same context, the communicating endpoints are nomenclatures by agent and manager (see fig. 7). Generally, each PHDs are equipped with only one gateway at a time, creating a one-to-one relationship between PHD (agent) and external Internet (manager). However, multiple associations can be created by one manager with its agents, creating a one-to-many relationship. IoT provides a platform for several types of resource constraint environments to be operated under its capabilities. Keeping this in mind, a tremendous amount of research is being carried by the industry as well as academia to develop a protocol stack in order to run applications efficiently and effectively independent of the underlying architecture. IETF's IPV6 protocol stack which operates Low Power Wireless Personal Area Network (6LoWPAN) is a typical example for showcasing such efforts [64]. The major objective of 6LoWPAN is to provide IP (internet protocol) support for minor low power HIoT devices which are limited by the high computational requirements. 6LoWPAN enables IPV6 data delivery over the IEEE 802.15.5 network and it runs on a confined environment that supports standard data encryption schemes.

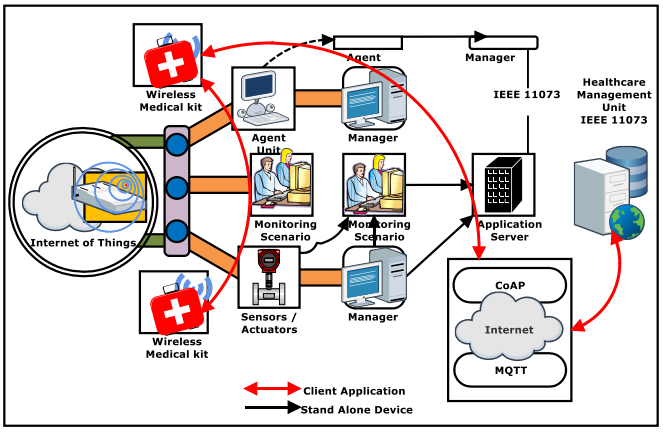

Fig. 7. Abstract implementation of CoAP and MQTT in the context of IEEE 11073 based IoT wireless applications

Although 6LoWPAN was trying to offer the resolution for network layer datagram (TCP) architecture related issues, Constrained Application Protocol (CoAP) was proposed at a higher level in order to enhance the internet governance for medical applications [65]. CoAP works on a representational state transfer (REST) model in order to get used to constrained nodes and networks in IoT infrastructure. This protocol support M2M applications such as smart health, industrial automation and smart city applications. CoAP interacts with the underlying MCU which has most commonly 8bit RAM and ROM through serial or parallel communication interfaces.

MQTT is another such standard protocol that shares most of the features from CoAP. Once the MQTT used to be called by the name Telemetry Transport protocol. MQTT is mainly used in publishing message services which indirectly invokes TCP implementation in its abstract form. This technology was initially designed and developed by IBM global. They used MQTT for connecting remote devices with a simple code snippet. MQTT employs a publish-subscribe communication model that enables the connected nodes to exchange messages asynchronously via a message broker. The message broker signifies a middleman who exchanges the messages between a specific client that published its requirements and a specific node. Nevertheless, MQTT is an advanced lightweight version of extensible messaging and presence protocol (XMPP) and advanced message queuing protocol (AMQP). Fig. 8 shows the descriptive comparison of various protocol technologies with respect to different criteria.

Technology	Criteria					
	Closed Firewall	Low Bandwidth and Low latency	Interoperable data format	Overload handling	Failure Notification Propagation	Quality of Service
AMQP [56]	√	√	X	X	I	I
MQTT [67]	√	√	X	X	I	I
CoAP [87]	√	√	√	X	X	X
REST [76]	√	X	X	X	X	√
6LoWPAN [89]	√	~	√	X	X	√
XMPP [68]	√	XL~B	~	~	~	√

√→Yes, X→No, I→Fragile, XL~B→No Low Latency and Partially Bandwidth , √ (Mesh)→Yes for Mesh topology, ~→Partial

Fig. 8. HIoT protocol comparison matrix

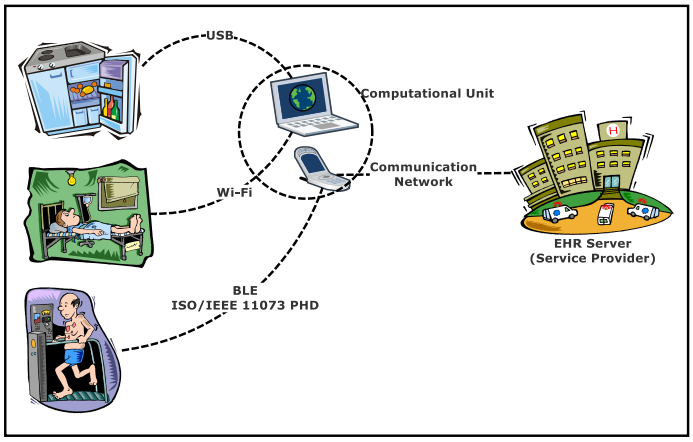

Fig. 9. Monitoring applications with heterogeneous wireless protocol standards

Recent advancements in networking infrastructures have made it possible for creating miniaturized, low power health monitoring devices. These devices are creating an adverse network in connected health scenarios. Many healthcare providers offer their own devices with specific protocol standards thus building proprietary medical solutions for their diverse consumers. This initiates the essence of having a standardized end-to-end communication protocol framework for resolving interoperability related issues. Keeping interoperability in mind, there's a need for developing a universal plug-n-play sensor device for healthcare monitoring applications in order to transform and integrate biomedical data. Eventually, focusing on healthcare device communication in the prospect of patient care (ISO/ IEEE 11073 PoC) [62], the technical advancements in uHealth [66] design strategies has eased the implementations of lightweight PHDs. In this view, fig. 9 shows the standard interoperability use cases in a medical scenario.

b. Microcontrollers for HIoT device design and selection criteria

The realization of HIoT application at the design phase involves not just adding sensors for collecting biomedical data, but also a selection of suitable microcontroller unit (MCU) that facilitates a platform of interface for these sensors is another important aspect. The term "Smart-Object" is derived from the fact that an MCU is being utilized for creating these embedded devices. In the field of embedded computing, MCU can be thought of as a tiny computer that has a bus interface unit (BIU) and execution unit (EU) in its architectural form and allows external entities to talk to each other via serial or parallel communication buses through GPIOs. Microcontrollers are used in pre-processing the physical data by means of conditioner circuits and transmit wirelessly to the local or remote storage space for analysis. Once the data is made available in cloud space, the analytical tools further take care of data for high-level analysis and provide reports to the user through a rich GUI. More often, the word microcontroller is used interchangeably with a microprocessor in literature, but there's a much difference in the application and architectural point of view. Therefore, the authors use these words more sensibly wherever required. Although several researchers have

reported the use cases of heterogeneous cores in general-purpose monitoring applications and embedded systems so far, the corresponding applications in IoT microcontrollers have yet to be realized [67,68]. The major challenges associated with integrating heterogeneity to the microcontroller/microprocessor are the total number of kernel cores and channelizing the schedule of appropriate cores to the applications. The designers must spend much time determining the best cores for a corresponding application in order to potentially optimize the MCU core configurations. In the healthcare sector, given the monitoring application requirements and execution parameters, it is the major responsibility of an application designer to determine the execution core either dynamically or statically [69]. The static core scheduling approach suffices the need of mapping core and application when the application is known beforehand. Whereas dynamic scheduling allocates the core by evaluating the application characteristics at runtime.

In the context of healthcare, the minimum features of any computational units (MCU) are expected to adhere to the following characteristics. Fig. 10. Shows the detailed specifications of numerous MCUs for healthcare application design.

- Physical entity sensing (Object layer)
- The data communication interface (Transmission layer)
- Computer vision (Service composition layer)
- Data compression and extraction (Service layer management)
- Data security (Application layer)
- Fault tolerance (Business layer)

It is noted that the above feature set is not so extensive, however, they denote a wide verity of computational tasks of any HIoT computational units (MCU). In this section, the authors explain the specific functionalities of the aforementioned features using emerging healthcare applications.

Physical entity sensing: As described in section III, the primary layer (object layer) is responsible for handling several kinds of sensor devices for creating a network of devices. Sensors are the constitutional elements of a data acquisition system (DAQ) and DAQs are the building blocks of any embedded systems. During the sensing phase, the activation events entropies, information and biomedical changes are captured and stored in local storage for further processing or decision making. The data from these sensors needed to be fused in order to create robust data qualitatively and quantitatively through a generic process called sensor fusion [70]. Sensor fusion can be achieved through mathematical computations such as addition, multiplication, subtraction, aggregating, mean and mediations. There are several algorithms to create sensor fusion that can involve different levels of complexity in terms of time and space.

In the healthcare domain, there are several body area networks (BAN) [71-73] for monitoring biomedical parameters continuously with the help of attached sensors. The sensors include a wide range of medical applications to measure ECG patterns, pulse rate, body temperature, blood pressure, EMG, and EEG non-invasively. These devices are provided by the healthcare service provider for daily usages at the patient's residences. In addition, there are multiple invasive biomedical devices that are used to measure blood molecules such as glucose, WBC count etc. The regularizations of these devices are made routinely by service providers in order to improve upon the quality of service.

Data communication interface: Section IV (B), discusses the possible communication gateways and protocols in brief. In this section, the authors illustrate the special type of communication function called software-defined radio (SDR) [74]. This function implements the hardware systems of the object layer such as filter, modulator etc. into a virtually visualized software module. SDR provides cutting edge solution for IoT enabled communication services by allowing software implementations and emulations for communication technologies and gateways without needing hardware updates. Further, SDR supports the packaged implementations of trans-receiving antennas, analog-digital converters (ADC), digital-analog converters (DAC), DSPs and FFTs. SDRs can be generally implemented on SoC, FPGAs, DSPs, customized microprocessors and/or general-purpose microprocessors [75].

Computer vision: Healthcare IoT has tremendously benefitted from image processing applications. Image processing denotes the application spectrum where any form of signal analysis requires an image or stream of images (video) as input and from which image features and characteristics are extracted for decision making. In this context there exist several image-driven applications, which help medical diagnosis very efficiently. For instance, Gulshan et al. [75] present a work in detecting diabetic retinopathy using fundus images. Fundus images are the retinal images captured by an eye surgeon by a fundus camera in order to analyses the image for detection and predicting extremities. There are several microprocessors that can be employed in image processing-based applications. They offer the interface for additional cameras. Since the image processing applications are generally data-rich, memory-intensive and computationally optimized, there is a necessity to have the computationally extensive microprocessor to fulfil all such needs.

Data compression and extraction: It is essential to have lesser bandwidth systems in order to ensure the quick trans-retrieval of heavy data and further to avoid the bandwidth limitation issues due to increased radio applications in the current scenario. Bandwidth requirements can be further balanced in few scenarios such as continuous video surveillance by adopting capture optimization techniques. Where the camera is enhanced in such a way that the system captures only the images that have some object/human motion into it [77]. This enables the wireless data transmission system to have lesser bandwidth to transfer. In another way, many IoT devices are resource-constrained, and the data compression initiates the essence of accommodating a larger amount of unstructured data, thus reducing transmission latency [78].

Compression is referred to as the representation of a piece of information using fewer bits than the original. This representation process is called encoding. If the data is encoded at the source, this encoding process is called source encoding. The represented data bits should not be altering the meaning of

the actual message; such encoding is said to be lossless. Lossless encoding is sometimes referred to as data extraction. In lossless encoding, the redundant bits are removed in order to concisely denote the actual information. These data compression techniques embedded in a microcontroller for enabling on-chip data compression.

Data security: It's noted that the nature of IoT application tends to be open or potentially unsafe for deploying in the internet because the traditional internet is susceptible to vulnerabilities. This open nature enriches the data decrypt or crypt analyzer to guess the bandwidth and hence to operate the privacy of closed-loop systems. Several researchers have already proved that wearable medical devices such as IoT enabled pacemakers and portable defibrillators are susceptible to internet attacks including replay attacks and closed-loop insider attacks [79,80]. Since its inception, HIoT device security has significantly overcome the security breaches in any closed loop IoT devices through executing generic security algorithms at the microcontroller level without changing the device core functionalities.

Fault tolerance: Fault tolerance is the ability of a system to reconfigure its operational capabilities with adjustable alternatives during service outages without changing the output quality. This feature is most important in HIoT scenarios, as the IoT devices are likely deployed in an unstructured environment such as monitoring complex biomedical parameters invasively. Maintaining QoS in such complex situations is no less than a challenge. Hence reconfigurable microprocessors in adverse situations are needed to implement flawlessly to contribute to quality improvements. Imposing fault tolerance capability should not increase in overheads of the existing workload. Fault tolerance is achieved generally through hardware-based techniques such as the redundant array of independent disks (RAID) [81]. In RAID, redundant disks/drivers are employed to deliver the fault tolerance during the occurrence of system failure. Moreover, the fault tolerance can be included in IoT devices at the cost of space and energy overheads.

Microcontroller Selection criteria: Microprocessors functioning styles are different than that of microcontroller, as MCUs are designed especially for embedded computations, whereas microprocessors are found in all desktop computers with the generic processing unit embedded into them. While MCUs are limited by computational capabilities when compared with a conventional computer processor, the low price makes them an ideal solution for small embedded applications wherein mathematical commutations only are not the sole purpose of those applications. The Healthcare industry is enriched by these embedded computers and their data transformational capabilities. In order to deterministically identify the suitability of an MCU while designing a device prototype, one should consider certain facts and key features of MCUs to strengthen the design strategies. The followings are some of the key considerations for selecting an MCU for their design of HIoT embedded applications.

- *Architectural reliance:* The architecture of an MCU represents the internal structures and their dependence on the external interfaces. There are majorly two architectural types available. 1. Von Neumann Architecture (VN architecture): This uses the single bus for fetching the instruction address as well as the data from external peripherals. Therefore, data transferring, and address fetching cannot be achieved simultaneously rather than scheduling approach. 2. Harvard architecture: Unlike the VN architecture, the data and instructions are fetched from a separate bus.
- *Bit length:* An MCU can be of multiple bit lengths like 8-bit, 16 bit, 32 bit and 64 bit, which means the maximum data handled by execution unit (EU) at one clock cycle. This depends upon the size of the word used in instruction. Higher the bit processing capacity higher the performance of computation. Higher bit length would also add extra overhead to increased space complexity.
- *Communication interfaces*: The communication interface between MCU and sensors/actuators are essential in order to achieve analog/digital communications. These interfaces are sometimes referred to as ADCs that converts analog to digital signals, DACs that convert digital to analog signals and PWMs that generates the continuous pulses for generating voltages to motors. In addition, UART, SPI (serial peripheral interface), and I2C (inter-integrated IC) are the communication interfaces for serial and parallel data transfer.
- *Operating voltage range:* This is an important criterion to be considered in selecting the right MCU for the right applications as it directly denotes the voltage level at which a particular device conduct. Individual sensor devices have got their own different voltage ranges, so in order to match this range, the MCU should be capable enough to offer a wider range of voltage outputs. Measurements from sensor/ actuators need to be represented via voltage variations. Generally, most of the MCUs support voltage ranges of 3.3 and 5V DC. Depending upon the step size, the sensed values are represented with certain calibrated accuracy. Using an MCU that produces 3V output for the sensor devices which operates for 5V is not a wise decision since there would be an additional step-up device required to fill these voltage gaps.
- *GPIOs and Space constraints*: GPIO is an abbreviation for general-purpose input-output. Using GPIO, the interfacing of sensors and peripherals are done. Higher the number of GPIO, the higher the number of sensor devices that can be connected to MCU. Depending upon the size of the MCU, the number of GPIOs varies. These further influences defining the package type. Commonly, there are MCUs with the DIP package. This type of MCU package allows mounting the device on a breadboard.

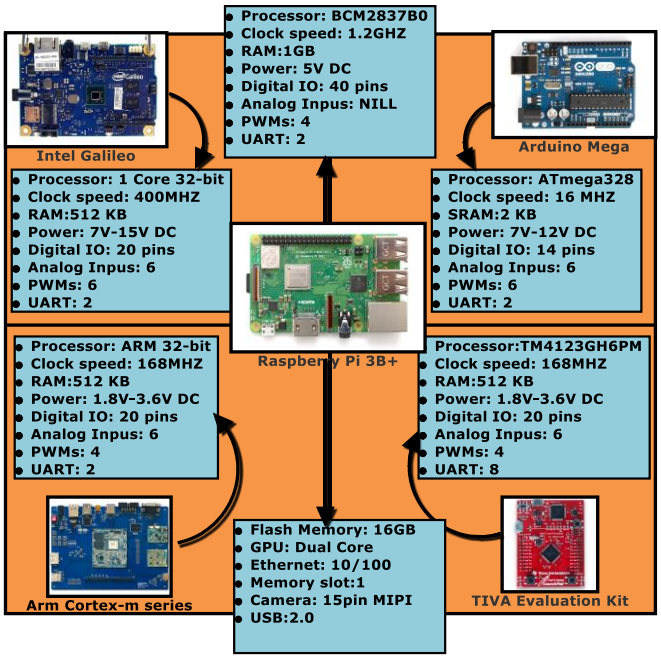

Fig. 10. Specifications of state-of-the-art MCUs for HIoT applications

E. Cloud and Fog computing in Healthcare IoT

HIoT can be visualized from three viewpoints- Internet vision, Thing's vision and semantic vision [20]. In Internet vision-based architectures, the internet services are the main components of that system, whereas data is being generated by the 'Things'. In Things vision, the smart things are the center of attraction. Finally, in Semantic vision, HIoT can be visualized by semantic services such as cloud computing, fog computing and context-aware technologies. In this paper, the authors focused on the cloud-centric realization of HIoT. A conceptual framework that combines the smart sensors and HIoT application is shown in Fig. 11. The proposed framework realizes not only the full potential of cloud computing but also the systematic integration of the object layer with the application layer. The cloud computing unit acts as a bridge between data acquisition platforms and data analytics platforms.

- *Interoperability amongst cloud and fog computing:* Recent explorations of IoT consider cloud computing as the backbone of IoT enabled solutions. Nevertheless, the limitation of such cloud-centric infrastructures entails the multi-hop distance from the data acquisition systems, thus creates geographically centralized architectures. This would create an additional economic burden. Therefore, it's essential to the outlook for an efficient solution that brings computing resources close to data generating sources. Fog computing is one such approach that is extensively used in the latest architectures. This approach is further strengthened by the increasing demands of low-cost edge computing devices across commercial manufacturing entities. Further, achieving interoperability between cloud and fog computing enchains with the complex coordination of IoT applications, services and growing demands of intelligent healthcare solutions. This further ascertains the stability, security and quality of service by making the best use of distributed resources. Nonetheless, there are certain challenges in extending such interoperability over traditional cloud-based architectures. In this regard, several researchers have tried to explore the healthcare use-case via integrated cloud-fog cross platforms extended upon conventional cloud infrastructure [98].

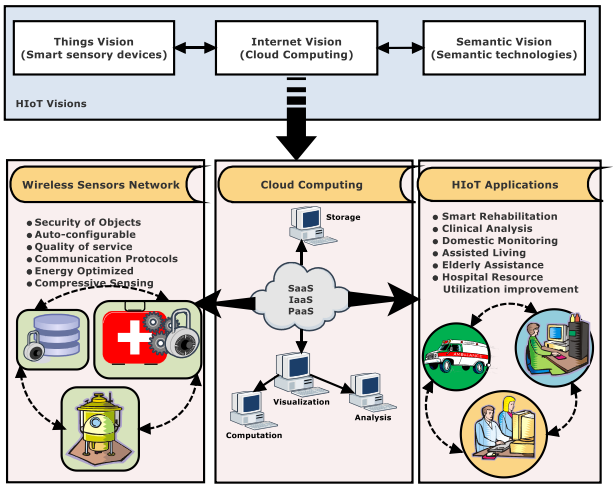

Fig. 11 A conceptual framework that integrates data generators and data users via cloud infrastructure

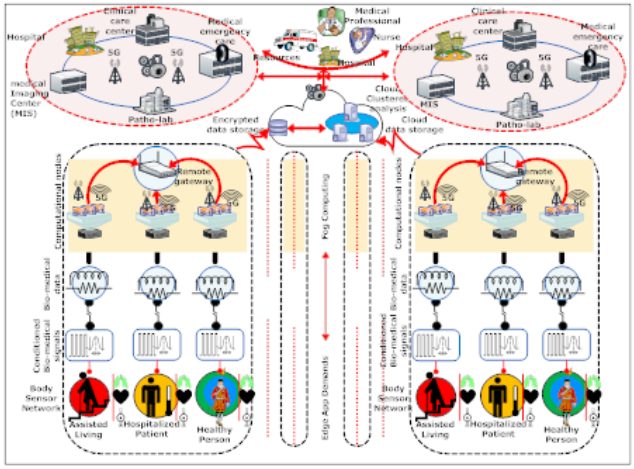

Fig. 12 An interoperable reference framework for clod-fog integration in HIoT

Sensing and monitoring are considered as important aspects of the healthcare IoT domain. Cloud-based solutions act as an interface between sensing and monitoring profiles. Cloud-based solutions provide widely accepted healthcare solutions across geographical areas. Several researchers have produced a significant amount of work in the cloud computing domain of the healthcare sector [99-102]. However, centralizing the cloud

centers according to the geographical areas made the data transmission pass through the multi-hop distances for storage and processing. Such multi-hop distance transmission would adversely leave an impact on latency while transmitting sensitive healthcare information. In addition, managing cloud resources while accepting data from heterogeneous resources from healthcare solutions would require more sophisticated task management algorithms. These algorithms should be capable enough to deal with high traffic of incoming data in an uneven and unsorted pattern.

Therefore, fog computing is providing the best solution for such problems raised by cloud centric HIoT applications. Fog computing offers a wide variety of lightweight and personalized computational resources that can be deployed towards HIoT data sources. In fog computing solutions, several low power computational devices such as routers, gateways along with the services and management tools implement the local tiny applications at the edge side [103].

components mainly depends upon the load connected. The other responsibilities of a cluster head include monitoring resource (MCs) activities, secured access controlling of devices, inter and intracluster communication establishment and preservation of associated metadata. Dynamic assignment of cluster head responsibilities has been adopted in case of hardware breakdowns of the current cluster head. This policy is constructed while ensuring no degradation in system performance and QoS. The cluster centric fog computing framework shown in fig. 12 can be visualized as a cloud enabled IoT healthcare solution, where each fog nodes acts as a separate server that constantly in connection with the centralized database. Several researchers have worked on cloud-based or fog-based healthcare solutions in the recent past. Few state-of-the-art cloud/fog infrastructure models have been summarized in table 2.

Table 2: Summary of state-of-the-art cloud/fog computing models

S.No	State-of-the-art	Year of Publication	Healthcare IoT	Cloud/Fog Computing	Interoperability	Major Contribution	Addressed problem
1	[104]	2017	✓	✓	✗	Edge/Mesh computing paradigm design	Gateway devices could be applied in creating interoperability
2	[105]	2017	✓	✓	✓	Multi model design for fog and identification of shortest path between clustered fogs	Response time needed to be improved for emergency situation
3	[106]	2017	✓	✓	✗	Fog assisted Patient monitoring system was designed	Real-time processing of data from neurological events such as brain stroke etc.
4	[107]	2015	✗	✓	✗	A method that alleviates IoT resource management issues through cloud computing	Interoperability and scalability needs to be introduced
5	[108]	2017	✓	✓	✗	common authentication mechanism that rely on certificate based DTLS	Prevention of DDoS attacks in healthcare application domains
6	[109]	2015	✓	✓	✗	Creation of micro data centers for healthcare application needs	Cloud of Things to solve emergency healthcare problems
7	[110]	2017	✓	✓	✗	Design of a fog infrastructure for patient health monitoring in HIoT application	Data Security algorithm for sensitive health data

✓ =Present, ✗=Absent

These applications perform some local processing of data close to data sources thus by distributing the load of resources amongst various such fog units. Moreover, it reduces the problem of multi-hop distances to a greater extent and promotes flexibility. Fog computing infrastructure is made of special-purpose network devices named fog nodes or computational nodes and is responsible for performing pre-processing of data acquired from heterogynous resources (see fig. 12). Multiple such nodes will create a cluster. And there are multiple clusters that interact with the centralized cloud infrastructure. Each fog nodes are equipped with a micro-core (MC) for processing, storage elements and internet bandwidth. The bottom-most fog nodes are located at a very close distance with the HIoT devices. These lower layer fog nodes can be called by the name of gateway nodes. The lower level fog nodes are further used to condition the signal so that processing is easier.

In a cluster, few nodes perform the communication-related tasks while other components are responsible for database related task execution. Each healthcare solution maintains the individual cluster and there can be multiple clusters taking care of one healthcare application. The load distribution in a cluster is largely performed by a cluster head depending upon the resource availability in a dynamic way. The number of cluster

VI. WIRELESS BODY AREA NETWORK (WBAN) ARCHITECTURE IN HIOT APPLICATIONS

In any HIoT application, Wireless Body Area Network (WBAN) plays a vital role in collecting patient biomedical data. WBAN is made of miniaturized, low power and autonomous wireless sensor nodes. These sensor nodes allow a medical practitioner to remotely monitor, visualize and provide feedback to the patients in real-time. This is the simplest and reliable way to take care of one's health, especially for those who are suffering from chronic disorders. These wireless sensor nodes can form various topologies amongst themselves such as bus, star, mesh and tree. Nodes are individually capable to transfer the collected data to the network. However, considering energy optimization as a major concern, it's always preferred to assign the communication capabilities to one of the nodes. In this section, the authors reviewed various architectures and proposed a standard WBAN architecture and their implementation strategies for HIoT application.

Efficiency of a healthcare monitoring system for chronic disorder patients is immensely depending upon power requirements and the size of wearable devices etc. In such cases system requires a low power sensor nodes and power optimization algorithms running in Medium Access Control

(MAC) layer. However, conventional computer network MAC layer protocols mainly focus on flow control, error control, effective utilization of bandwidth, improving latencies and reduction of noises. Consequently, energy optimization of WSN is one of the major requirements while considering system design. It's essential to incorporate these protocols in conjunction with already existing protocols of MAC layer. It's observed that the major reason for energy optimization is idle listening of link layer, excessive over heads, inappropriate utilization of bandwidth, improper execution of periodic listening and control overhead packets.

In this section, the authors propose a conceptual framework of WBAN architecture as shown in fig. 13. The proposed architecture plays a vital role in energy optimization as its traffic adaptive. The proposed architecture categorizes

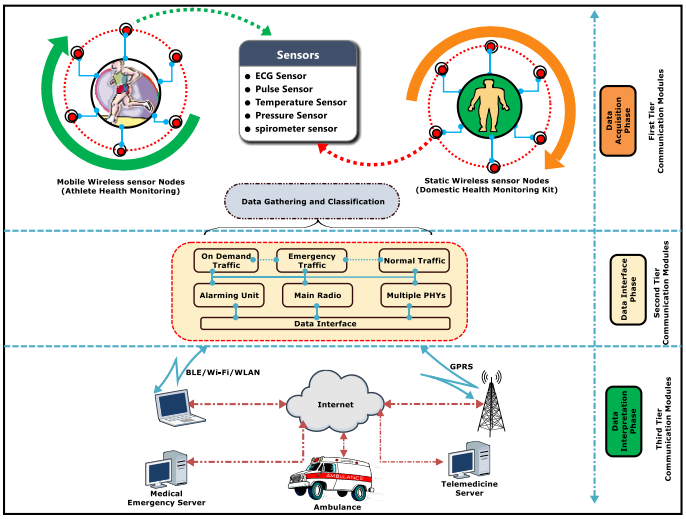

Fig. 13 Generic WBAN architecture for healthcare

healthcare traffic into 3 classes such as normal traffic, on-demand traffic and emergency traffic. Channelizing the traffic with such classes is believed to improve the efficiency as compared to single traffic WBANs. Here, normal traffic is executed on a periodic basis by any of the nodes who are acting as a cluster head for that scenario During emergency situations, the node identifying emergency is responsible for initiating the emergency traffic. Many times, such emergency situations are highly unpredictable. On-demand traffic is initiated through application interfaces either from the hospital side or from the patient side. Here, one of the nodes acts as a coordinator and take care of transmission during on-demand request periods. These protocols can be implemented in MAC layer and are responsible for increasing the network lifetime by reducing the power consumption levels. The normal traffic is ignited by traffic-based wake-up calls periodically, whereas on-demand and emergency traffic use the node initiated the radio-wake up call.

A. Communication modes inWBAN

The WBAN architecture has been visualized through tier based communication modes. Each tier is equipped with its own communication protocols and privacy rules along with access controlling. The security requirements, data rate and operational range of each communication tier varies with respect to the topology and their physical structure. This session, we briefed various communication related activities considering each tier.

applications

First Tier Communication modules: In this tier, all communication entities are bound by transmitter and receiver. Generally, these are on-body sensors and actuators which resides on the human body and collect bio parameters. The human body hosts both transmitter and receiver that transfer human body parameters to the nearest communication node. Several biosensors such as EEG sensor, ECG sensor, pulse sensor, temperature sensors, spirometer and pressure sensor are acting as a transmitter. The data rate and efficiency of the sensor network depend upon the properties of SoC devices, operating frequencies of the sensor nodes, and QoS factors [111]. The sensors are used to capture the biomedical responses of the body under both static and dynamic cases.

Second Tier Communication modules or Intermediate communication modules: Communication at tier-2 is represented by the direction of data flow from on-body to off-body devices. The traffic generated from tier-1 is channelized to the ongoing communication medium depending upon the traffic type and need. The regular biomedical data traffic is flowing through the normal traffic channel, where the patient can choose the period to upload the data. In emergency cases, the data captured during such situations will automatically route to the emergency channel. Whereas the on-demand data channel is chosen by the doctor depending upon needs. Several studies have shown the utilization of the human body as a communication medium between WBAN and connected off-body gateway, as the human body conducts for electrons. The gateways can either be deployed in connection with the body or they can be at a remote place [112,113].

Third Tier Communication modules or End-Device communication modules: The communication protocols defined in this tier are well defined from the object/physical layer to the application layer. WLAN, BLEs, and GPRS protocols are popular communication modules in this tier. The gateways are directly connected to medical servers through the underlying channel. There must be a proper authentication mechanism to access such protected resources.

B. Security requirements and Implementation challenges in WBAN

WBAN certainly requires numerous security and privacy measures for ensuring secured data and device accesses in HIoT applications. The security goals such as privacy, confidentiality and data integrity are the vital facets of any secured communication. The underlying security infrastructure must take care of implementing these features [114]. The efficiency of a WBAN is majorly dependent on the security and privacy of user data devices in any healthcare application. Security is defined in terms of the ability of WBAN systems to protect data and associated devices from unauthorized accesses; so as to provide security to the patient data and devices there must be a proper access control mechanism implemented centrally. This

access controlling can be achieved in various ways, role-based access controlling, capability-based access controlling and attribute-based access controlling [115]. However, privacy is defined by the ability of a system to control, collect and usage of patient's information. For example, privacy suggests patient to choose not to disclose his/her data to any third-party insurance companies from the hospital admiration so as to refrain from misusing his/her healthcare data. In addition, privacy is a major fact that one can choose themselves to be protected from illegal usage of personal data. As there might be a tendency that if patient data is illegally distributed to any other agencies that they can use such personal information to influence on patient's job or creating an unstable mental situation or for the public humiliation. Therefore, it's important for a patient to know who is using his data. Fig. 14 illustrates the various modes of data collection from different patients and securely transferring them to a database. Fig. 14 also depicts various aspects of access controlling suitable for centralized infrastructure. In this section, we discuss the most anticipated security goals that ensure the safety of a WBAN system in healthcare applications.

Data Confidentiality: Data confidentiality deals with the protection of patient's confidential data from unauthorized accesses which are very often in WBAN systems due to its nature of exposure to open access vulnerabilities. The reliability of WBAN is purely depending on the level of data exposure to vulnerabilities. As it's known that the wireless transmission medium is the backbone of any WBAN, and the risk of intruders is high in such exposed mediums. Therefore, it's extremely important to provide high security to such attacks so as to prevent from hazardous impacts of data thefts [117-119].

Data and device Integrity: Data integrity mainly refers to the various measures taken by the WBAN system to protect the ingredient of a message transferred between first-tier modules to cloud infrastructure. The integrity of a data and device should further ensure that the data and device must not be manipulated by any unauthorized parties. In addition, the data origin must be verifiable.

Data and device availability: The availability of data and device mainly ensures accessibility from an authorized entity. The data and device must be made available all the time for various usages.

Freshness of the data: The data freshness feature of an IoMT WBAN should ensure that the data integrity and confidentiality of the data is protected from unauthorized recordings and replaying the data in an irregular pattern so that the WBAN system gets confused about the origin. The responsibility of the WBAN coordinator is to ensure that the old data is not recycled again and again. There are two techniques to ensure that data freshness such as strong freshness which promises extra delay in addition to frame ordering and week freshness that is limited only to the ordering of frames but not guarantee any delays [118,121].

Network Availability: The network availability feature of secured WBAN ensures that the medical practitioners are timely viewing the patient's data so as to keep a regular check on the health status of critical patients. Since the sensitive information is carried out all the time, it's the responsibility of the network administrator to make it available all the time as and when it is required.

Authentication of healthcare data and device: All the data and device concerned with the medical application must be authenticated in a secured way. Authentication does not only provide security to data and device but also verifies the legitimacy of the user and origin of data. There are numerous kinds of data and device access controlling techniques used nowadays. Majorly, attribute-based, capability-based and role-based access controlling techniques are prominent.

Secured Key management: Delivering the key distribution to WBAN involves complex encryption and decryption operations in order to securely transmit the control of data and device to the participating entities. The coordinator responsibility is to add or remove the nodes involved in data transmission depending upon their needs [118].

Security rules: The essence of security and privacy in healthcare field is a universal concern. The prominent way of providing security and privacy is by generating and regulating the rules and policies. These policies are concerned to the person who wish to access the healthcare data and device. According to the rule defied in the hierarchy of a healthcare system, he/she shall be given rights to access the protected resources. For instance, a user by definition may be a doctor and can access only the patients enrolled under him. In the same way, patient user can only be able to view his biomedical data rather than just giving him access to view other's data. The American Health Insurance Portability and Accountability Act (HIPAA) provides numerous sets of instructions/guidelines for healthcare workers, and administration to ensure privacy of patient data. These guidelines are followed by worldwide doctors and healthcare service providers. The fine of $250,000 and or jail of 10 years is imposed on the people who breaks basic guidelines [122]. The table 3 shows the prominent security threats, security goals and requirement and the available security solutions while dealing with WBANs.

Table 3: HIoT data and device security threats and available security solutions

S.no	State-of-the-art	Privacy/security threat	Security goals	Available solution
1	[123]	Illegal Access	Setting up the trust through key establishment	cryptographically Securing public key and distributing random key
2	[124]	Message decoding	Privacy and confidentiality	Access controlling in network and data link layer
3	[125]	Message manipulation	User authenticity and Integrity	Digital signature and hashing of public and private keys
4	[126]	Denial of services (DoS)	Resource availability	Removal of redundancy and detection of intruder
5	[127]	Sensor node compromising	Resilience to node compromising	Detection of inconsistency and revocation of compromise d node through proofing
6	[128]	Attacks in routers	Security in routing	Routing protocols for secured transmission
7	[129]	Malicious activities	Group management and data aggregation securely	Establishing secured group communication
8	[130]	User Device compromising	Device management	Intrusion detection

VII. FUTURE DIRECTION

Discussion in the field of WBAN's security issues certainly determines the clear needs for further enhanced research in this

area. Although there have been constant efforts of studies in the field of WBAN security, we cannot ignore the untouched security areas such as access controlling and authentication. Moreover, security, quality of service (QoS), and privacy are given equal importance in designing any HIoT application. Most of the surveys have focused on security alone, whereas ignoring QoS and privacy concerns brings its own cost to the system. In the case of domestic HIoT applications, sensory devices transfer data to the centralized facility which is outside their communicable radio range. Routing and message forwarding are therefore critical in terms of security and privacy. There are numerous routing algorithms proposed, however, none of them is completely resilient to potential security attacks.

Routing mainly suffers from the two major security attacks such as Denial of Service (Dos) and Distributed Denial of Service (DDoS). Infectious information using these attacks can be injected into the router such that the routing information is all malicious in nature. In addition, the current research proposals are addressing only the security concerns of static wireless sensor networks within an HIoT application, while there's a minimal study is observed in litterateur about the security concerns of mobile WSNs or ad-hoc networks [146].
Trust management is another area of focus as far as WBAN security is concerned. Trust may be defined as the capacity of a node to be considered worthy in reliably and securely transmitting information from one node to another node. These internode interactions are used in knowing the status of an individual node. For establishing trust amongst the nodes, there must be a mutual association between any pair of trusted entities. Data aggregators or sensor nodes qualify to be the entities here. There must be an established association between each pair of trusted entities for securely interchanging the information. Therefore, trust management is an important aspect in managing WBANs effectively and efficiently.

The patient's medical information is accessible from all the involved entities such as doctors, nurses, administration etc., There must be proper policies defined at the core of HIoT security algorithms so that only authorized person can have access to entitled data. In light of this, highly sophisticated access control policies must be designed and incorporated in HIoT application.

VIII. CONCLUSION

Internet of Things in healthcare (HIoT) has changed the way of thinking about healthcare services through its remote provisioning and data accessibility from anywhere. The collected data is investigated by medical professionals about if there are any inconsistencies and hence an alarm signal is generated if finds any such. This form of medicine is being called by the latest name medicine 4.0, the new generation environment for monitoring the patients through remote care and prescriptions powered by cloud and IoT infrastructure. Our survey reviews the latest technologies in HIoT and allied application areas. Several HIoT architectures implemented through various computing paradigms are detailed in this study. These architectures are driven by WBAN, communication modules, cloud infrastructures, machine learning and blockchains. The capabilities of big data and machine learnings have been exploited through various HIoT applications while achieving service performance and improved resource utilization. The role of edge computing in overcoming latency related issues is significant in the healthcare domain. This eliminates the constant need for multi-hop data transmissions over an unsecured network architecture, henceforth contributing towards data security to a greater extent. We discussed various aspects of fog computing, edge computing and their implementation strategies. The significance of big data is realized in our review by comparing the benefits of IoT and blockchains. The abstract implementation of multi-tier based WBAN architecture implementation is discussed in greater detail. The enhanced technical details pertaining to healthcare scenarios such as WBAN architecture, layered healthcare IoT architecture, and enabling technologies are described in the forthcoming fragments of the paper. Authors have then provided a brief summary of the most anticipated protocol stacks and design issues that allows researchers and healthcare professionals to understand swiftly how the numerous protocols put together to attain desired functionalities without having to get through standards and RFCs. Authors have also explored recent state-of-art to identify some of the key challenges of the healthcare IoT domain and a short summary of each related research is presented. Finally, the authors explicated the detailed use-case scenarios to demonstrate how the numerous protocols and architectures presented in the paper could put together to attain desired healthcare services.

REFERENCES

[1] World Population Ageing 2013, United Nations, New York, NY, USA, 2013, pp. 8–10.

[2] E. Perrier, Positive Disruption: Healthcare, Ageing and Participation in the Age of Technology. Sydney, NSW, Australia: The McKell Institute, 2015.

[3] Baker, Stephanie B., Wei Xiang, and Ian Atkinson. "Internet of things for smart healthcare: Technologies, challenges, and opportunities." IEEE Access 5 (2017): 26521-26544.

[4] Deng, Ruilong, Zaiyue Yang, Mo-Yuen Chow, and Jiming Chen. "A survey on demand response in smart grids: Mathematical models and approaches." IEEE Transactions on Industrial Informatics 11, no. 3 (2015): 570-582.

[5] Liang, Chengchao, and F. Richard Yu. "Wireless virtualization for next generation mobile cellular networks." IEEE wireless communications 22, no. 1 (2015): 61-69.

[6] Malekian, Reza, Kevin Curran, Christian Fischer Pedersen, Bin Cao, and Xuewei Qi. "Guest Editorial Special Issue on Sensor Technologies for Connected Cars: Devices, Systems and Modeling." IEEE Sensors Journal 18, no. 12 (2018): 4775-4776.

[7] Sitaraman, Srikrishna, Tony Contreras, Ray Kahidi, Ganesh Bhatt, Terry Bowen, and Mohammad Ahmed. "Mixed-signal glass module for IoT applications." In 2017 Pan Pacific Microelectronics Symposium (Pan Pacific), pp. 1-6. IEEE, 2017.

[8] Liu, Xilong, and Nirwan Ansari. "Toward Green IoT: Energy Solutions and Key Challenges." IEEE Communications Magazine 57, no. 3 (2019): 104-110.

[9] Chung, Ming-An. "A miniaturized triple band monopole antenna with a coupled branch strip for bandwidth enhancement for IoT applications." Microwave and Optical Technology Letters 60, no. 9 (2018): 2336-2342.

[10] Lizzi, Leonardo, Fabien Ferrero, Philippe Monin, Christophe Danchesi, and Stéphane Boudaud. "Design of miniature antennas for IoT applications." In 2016 IEEE Sixth International Conference on Communications and Electronics (ICCE), pp. 234-237. IEEE, 2016.

[11] Torun, Hakki Mert, Colin Pardue, Mohamed LF Belleradj, Anto K. Davis, and Madhavan Swaminathan. "Machine learning driven advanced packaging and miniaturization of IoT for wireless power transfer solutions." In 2018 IEEE 68th Electronic Components and Technology Conference (ECTC), pp. 2374-2381. IEEE, 2018.

[12] Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17, no. 4 (2015): 2347-2376.

[13] Qadri, Yazdan Ahmad, Ali Nauman, Yousaf Bin Zikria, Athanasios V. Vasilakos, and Sung Won Kim. "The future of healthcare internet of things: a survey of emerging technologies." IEEE Communications Surveys & Tutorials 22, no. 2 (2020): 1121-1167.

[14] Vidyadhar J. Aski, Shashank Gupta, and Bharat Sarkar. "An Authentication-Centric Multi-Layered Security Model for Data Security in IoT-Enabled Biomedical Applications." In IEEE 8th Global Conference on Consumer Electronics (GCCE 2019), IEEE Consumer Electronics Society, Osaka, Japan, Oct. 15-18th, 2019. (Accepted, in Press)

[15] Singh, Pradeep, and Ajay Kumar. "5G Networks and Internet of Things (IoT)." AIJR Abstracts (2022): 43.

[16] Sarma, Hemen, Sanket J. Joshi, Ram Prasad, and Josef Jampilek, eds. Biobased Nanotechnology for Green Applications. Springer International Publishing, 2021.

[17] Moses, Oyawale Adetunji, Libo Gao, Haitao Zhao, Zhuo Wang, Mukhtar Lawan Adam, Zhehao Sun, Kaili Liu et al. "2D materials inks toward smart flexible electronics." Materials Today 50 (2021): 116-148.

[18] Ramson, SR Jino, Walter D. Leon-Salas, Zachary Brecheisen, Erika J. Foster, Cliff T. Johnston, Darrell G. Schulze, Timothy Filley et al. "A self-powered, real-time, LoRaWAN IoT-based soil health monitoring system." IEEE Internet of Things Journal 8, no. 11 (2021): 9278-9293.

[19] Zaman, Shakila, Muhammad RA Khandaker, Risala T. Khan, Faisal Tariq, and Kai-Kit Wong. "Thinking out of the blocks: Holochain for distributed security in iot healthcare." IEEE Access 10 (2022): 37064-37081.

[20] Xia, Kaishu, Clint Saidy, Max Kirkpatrick, Noble Anumbe, Amit Sheth, and Ramy Harik. "Towards Semantic Integration of Machine Vision Systems to Aid Manufacturing Event Understanding." Sensors 21, no. 13 (2021): 4276.

[21] Catarinucci, Luca, Danilo De Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone. "An IoT-aware architecture for smart healthcare systems." IEEE Internet of Things Journal 2, no. 6 (2015): 515-526.

[22] Internet of Things Market Size, IoT Industry Report, Apr. 2016. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/iot-market

[23] Brauner, Philipp, Manuela Dalibor, Matthias Jarke, Ike Kunze, István Koren, Gerhard Lakemeyer, Martin Liebenberg et al. "A computer science perspective on digital transformation in production." ACM Transactions on Internet of Things 3, no. 2 (2022): 1-32.

[24] Choi, Tsan-Ming, Subodha Kumar, Xiaohang Yue, and Hau-Ling Chan. "Disruptive technologies and operations management in the Industry 4.0 era and beyond." Production and Operations Management (2021).

[25] Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17, no. 4 (2015): 2347-2376.

[26] Yeh, Kuo-Hui. "A secure IoT-based healthcare system with body sensor networks." IEEE Access 4 (2016): 10288-10299.

[27] Wen, Weimin, Cuijuan Shang, Zaixiu Dong, Huan-Chao Keh, and Diptendu Sinha Roy. "An intrusion detection model using improved convolutional deep belief networks for wireless sensor networks." International Journal of Ad Hoc and Ubiquitous Computing 36, no. 1 (2021): 20-31.

[28] Chegini, Hossein, Ranesh Kumar Naha, Aniket Mahanti, and Parimala Thulasiraman. "Process automation in an IoT–fog–cloud ecosystem: A survey and taxonomy." IoT 2, no. 1 (2021): 92-118.

[29] Behura, Aradhana, and Sushree Bibhuprada B. Priyadarshini. "Assessment of load in cloud computing environment using C-means clustering algorithm." In Intelligent and cloud computing, pp. 207-215. Springer, Singapore, 2021.

[30] VNI complete forecast highlights, 2018. [Online]. Available: https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast highlights/pdf/United_States_Device_Growth_Traffic_Profiles.pdf.

[31] Gia, Tuan Nguyen, Imed Ben Dhaou, Mai Ali, Amir M. Rahmani, Tomi Westerlund, Pasi Liljeberg, and Hannu Tenhunen. "Energy efficient fog-assisted IoT system for monitoring diabetic patients with cardiovascular disease." Future Generation Computer Systems 93 (2019): 198-211.

[32] Zhan, Kai. "Sports and health big data system based on 5G network and Internet of Things system." Microprocessors and Microsystems 80 (2021): 103363.

[33] Gomathi, P., S. Baskar, and P. Mohamed Shakeel. "Concurrent service access and management framework for user-centric future internet of things in smart cities." Complex & Intelligent Systems 7, no. 4 (2021): 1723-1732.

[34] Yang, Dongmei, Yunhui Zhou, Wentao Huang, and Xianwei Zhou. "5G mobile communication convergence protocol architecture and key technologies in satellite internet of things system." Alexandria Engineering Journal 60, no. 1 (2021): 465-476.

[35] Srivastava, Abhishek, and Dushmanta Kumar Das. "A comprehensive review on the application of Internet of Thing (IoT) in smart agriculture." Wireless Personal Communications (2021): 1-31.

[36] Kumar, Adarsh, Carlo Ottaviani, Sukhpal Singh Gill, and Rajkumar Buyya. "Securing the future internet of things with post-quantum cryptography." Security and Privacy 5, no. 2 (2022): e200.

[37] Philip, Nada Y., Joel JPC Rodrigues, Honggang Wang, Simon James Fong, and Jia Chen. "Internet of Things for in-home health monitoring systems: current advances, challenges and future directions." IEEE Journal on Selected Areas in Communications 39, no. 2 (2021): 300-310.

[38] Da Cruz, Mauro AA, Joel JPC Rodrigues, Arun Kumar Sangaiah, Jalal Al-Muhtadi, and Valery Korotaev. "Performance evaluation of IoT middleware." Journal of Network and Computer Applications 109 (2018): 53-65.

[39] Vilela, Pedro H., Joel JPC Rodrigues, Petar Solic, Kashif Saleem, and Vasco Furtado. "Performance evaluation of a Fog-assisted IoT solution for e-Health applications." Future Generation Computer Systems 97 (2019): 379-386.

[40] Malasinghe, Lakmini P., Naeem Ramzan, and Keshav Dahal. "Remote patient monitoring: a comprehensive study." Journal of Ambient Intelligence and Humanized Computing 10, no. 1 (2019): 57-76.

[41] Selem, Enas, Mohammed Fatehy, Sherine M. Abd El-Kader, and Hamed Nassar. "THE (Temperature Heterogeneity Energy) Aware Routing Protocol for IoT Health Application." IEEE Access 7 (2019): 108957-108968.

[42] Hamidi, Hodjat. "An approach to develop the smart health using Internet of Things and authentication based on biometric technology." Future generation computer systems 91 (2019): 434-449.

[43] Hossain, Mahmud, SM Riazul Islam, Farman Ali, Kyung-Sup Kwak, and Ragib Hasan. "An Internet of Things-based health prescription assistant and its security system design." Future generation computer systems 82 (2018): 422-439.

[44] Ali, Omer, Mohamad Khairi Ishak, Muhammad Kamran Liaquat Bhatti, Imran Khan, and Ki-Il Kim. "A Comprehensive Review of Internet of Things: Technology Stack, Middlewares, and Fog/Edge Computing Interface." Sensors 22, no. 3 (2022): 995.

[45] Zhang, Yinghui, Dong Zheng, and Robert H. Deng. "Security and privacy in smart health: Efficient policy-hiding attribute-based access control." IEEE Internet of Things Journal 5, no. 3 (2018): 2130-2145.

[46] Pirbhulal, Sandeep, Heye Zhang, Wanqing Wu, Subhas Chandra Mukhopadhyay, and Yuan-Ting Zhang. "Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks." IEEE Transactions on Biomedical Engineering 65, no. 12 (2018): 2751-2759.

[47] Wu, Taiyang, Fan Wu, Jean-Michel Redouté, and Mehmet Rasit Yuce. "An autonomous wireless body area network implementation towards IoT

connected healthcare applications." Ieee Access 5 (2017): 11413-11422.

[48] Arunkumar, N., V. Pandimurugan, M. S. Hema, H. Azath, S. Hariharasitaraman, M. Thilagaraj, and Petchinathan Govindan. "A Versatile and Ubiquitous IoT-Based Smart Metabolic and Immune Monitoring System." Computational Intelligence and Neuroscience 2022 (2022).

[49] Abawajy, Jemal H., and Mohammad Mehedi Hassan. "Federated internet of things and cloud computing pervasive patient health monitoring system." IEEE Communications Magazine 55, no. 1 (2017): 48-53.

[50] Moosavi, Sanaz Rahimi, Tuan Nguyen Gia, Ethiopia Nigussie, Amir M. Rahmani, Seppo Virtanen, Hannu Tenhunen, and Jouni Isoaho. "End-to-end security scheme for mobility enabled healthcare Internet of Things." Future Generation Computer Systems 64 (2016): 108-124.

[51] Zhang, Liping, Yixin Zhang, Shanyu Tang, and He Luo. "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement." IEEE Transactions on Industrial Electronics 65, no. 3 (2017): 2795-2805.

[52] Yang, Yang, Ximeng Liu, and Robert H. Deng. "Lightweight break-glass access control system for healthcare Internet-of-Things." IEEE Transactions on Industrial Informatics 14, no. 8 (2017): 3610-3617.

[53] Shao, Zhuang, Yumei Wen, Ping Li, Guoda Wang, Yao Wang, Tao Han, and Xiaojun Ji. "Passive Distributed Sensor Array Using Multiple RF Sensing Tags." IEEE Internet of Things Journal (2022).

[54] Pinto, Sandro, Jorge Cabral, and T. Gomes. "We-care: An IoT-based health care system for elderly people." In 2017 IEEE International Conference on Industrial Technology (ICIT), pp. 1378-1383. IEEE, 2017.

[55] Diyan, Muhammad, Bhagya Nathali Silva, Jihun Han, ZhenBo Cao, and Kijun Han. "Intelligent Internet of Things gateway supporting heterogeneous energy data management and processing." Transactions on Emerging Telecommunications Technologies 33, no. 2 (2022): e3919.

[56] Augustin, Aloÿs, Jiazi Yi, Thomas Clausen, and William Townsley. "A study of LoRa: Long range & low power networks for the internet of things." Sensors 16, no. 9 (2016): 1466.

[57] Bazydło, Grzegorz, and Szymon Wermiński. "Demand side management through home area network systems." International Journal of Electrical Power & Energy Systems 97 (2018): 174-185.

[58] Manimuthu, Arunmozhi, and Ramadoss Ramesh. "Privacy and data security for grid-connected home area network using Internet of Things." IET Networks 7, no. 6 (2018): 445-452.

[59] Sardar, Santu, Amit K. Mishra, and Mohammed Zafar Ali Khan. "LTE commsense for object detection in indoor environments." IEEE Aerospace and Electronic Systems Magazine 33, no. 7 (2018): 46-59.

[60] Wong, Ian C., Karl F. Nieman, and Nikhil U. Kundargi. "Signaling and frame structure for Massive MIMO cellular telecommunication systems." U.S. Patent 9,985,701, issued May 29, 2018.

[61] Moridi, Mohammad Ali, Youhei Kawamura, Mostafa Sharifzadeh, Emmanuel Knox Chanda, Markus Wagner, and Hirokazu Okawa. "Performance analysis of ZigBee network topologies for underground space monitoring and communication systems." Tunnelling and Underground Space Technology 71 (2018): 201-209.

[62] ISO International Organization for Standardization, ISO/IEEE11073, available at http://standards.ieee.org/findstds/standard/11073-20601-2014.html (accessed Nov. 4, 2019).

[63] Qiu, Sen, Zhengdong Hao, Zhelong Wang, Long Liu, Jiayi Liu, Hongyu Zhao, and Giancarlo Fortino. "Sensor combination selection strategy for kayak cycle phase segmentation based on body sensor networks." IEEE Internet of Things Journal (2021).

[64] Zhang, Quan, Tao Jin, Jianguo Cai, Liang Xu, Tianyiyi He, Tianhong Wang, Yingzhong Tian, Long Li, Yan Peng, and Chengkuo Lee. "Wearable Triboelectric Sensors Enabled Gait Analysis and Waist Motion Capture for IoT-Based Smart Healthcare Applications." Advanced Science 9, no. 4 (2022): 2103694.

[65] Al Enany, Marwa O., Hany M. Harb, and Gamal Attiya. "A Comparative analysis of MQTT and IoT application protocols." In 2021 International Conference on Electronic Engineering (ICEEM), pp. 1-6. IEEE, 2021.

[66] Donzia, Symphorien Karl Yoki, and Haeng-Kon Kim. "Development of Smart U-Health Care Systems." In Software Engineering in IoT, Big Data, Cloud and Mobile Computing, pp. 33-47. Springer, Cham, 2021.

[67] Rohith, M., and Ajeet Sunil. "Comparative Analysis of Edge Computing and Edge Devices: Key Technology in IoT and Computer Vision Applications." In 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), pp. 722-727. IEEE, 2021.

[68] Ali, Javid, Tahir Maqsood, Naima Khalid, and Sajjad A. Madani. "Communication and aging aware application mapping for multicore based edge computing servers." Cluster Computing (2022): 1-13.

[69] Yao, Yu, Yukun Song, Hu Ge, Ying Huang, and Duoli Zhang. "A communication-aware and predictive list scheduling algorithm for network-on-chip based heterogeneous muti-processor system-on-chip." Microelectronics Journal (2022): 105367.

[70] Xu, Danfei, Dragomir Anguelov, and Ashesh Jain. "Pointfusion: Deep sensor fusion for 3d bounding box estimation." In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 244-253. 2018.

[71] Ortiz, Guadalupe, Meftah Zouai, Okba Kazar, Alfonso Garcia-de-Prado, and Juan Boubeta-Puig. "Atmosphere: Context and situational-aware collaborative IoT architecture for edge-fog-cloud computing." Computer Standards & Interfaces 79 (2022): 103550.

[72] Rathore, M. Mazhar, Awais Ahmad, Anand Paul, Jiafu Wan, and Daqiang Zhang. "Real-time medical emergency response system: exploiting IoT and big data for public health." Journal of medical systems 40, no. 12 (2016): 283.

[73] Awotunde, Joseph Bamidele, Sanjay Misra, Oluwafisayo Babatope Ayoade, Roseline Oluwaseun Ogundokun, and Moses Kazeem Abiodun. "Blockchain-Based Framework for Secure Medical Information in Internet of Things System." In Blockchain Applications in the Smart Era, pp. 147-169. Springer, Cham, 2022.

[74] Yue, Xuejun, Yongxin Liu, Jian Wang, Houbing Song, and Huiru Cao. "Software defined radio and wireless acoustic networking for amateur drone surveillance." IEEE Communications Magazine 56, no. 4 (2018): 90-97.

[75] Zhang, Jiaqi, Ruijuan Zheng, Xuhui Zhao, Junlong Zhu, Junwei Xu, and Qingtao Wu. "A computational resources scheduling algorithm in edge cloud computing: from the energy efficiency of users' perspective." The Journal of Supercomputing (2022): 1-22.

[76] Gulshan, Varun, Lily Peng, Marc Coram, Martin C. Stumpe, Derek Wu, Arunachalam Narayanaswamy, Subhashini Venugopalan et al. "Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs." Jama 316, no. 22 (2016): 2402-2410.

[77] Huang, Shih-Chia, Huibin Liu, Bo-Hao Chen, Zhijun Fang, Tan-Hsu Tan, and Sy-Yen Kuo. "A Gray Relational Analysis-Based Motion Detection Algorithm for Real-World Surveillance Sensor Deployment." IEEE Sensors Journal 19, no. 3 (2018): 1019-1027.

[78] Xue, Dongmei, Haichuan Ma, Li Li, Dong Liu, and Zhiwei Xiong. "aiWave: Volumetric Image Compression with 3-D Trained Affine Wavelet-like Transform." arXiv preprint arXiv:2203.05822 (2022).

[79] Shahid, Jahanzeb, Rizwan Ahmad, Adnan K. Kiani, Tahir Ahmad, Saqib Saeed, and Abdullah M. Almuhaideb. "Data protection and privacy of the internet of healthcare things (IoHTs)." Applied Sciences 12, no. 4 (2022): 1927.

[80] Karimian, Nima, Paul A. Wortman, and Fatemeh Tehranipoor. "Evolving authentication design considerations for the internet of biometric things (IoBT)." In Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, p. 10. ACM, 2016.

[81] Asnaashari, M., Avalanche Tech Inc, 2015. Method of managing throughput of redundant array of independent disks (raid) groups in a solid state disk array. U.S. Patent Application 14/168,642.

[82] Habibzadeh, Hadi, Karthik Dinesh, Omid Rajabi Shishvan, Andrew Boggio-Dandry, Gaurav Sharma, and Tolga Soyata. "A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective." IEEE Internet of Things Journal 7, no. 1 (2019): 53-71.

[83] Yeole, Anjali S., and Dhananjay R. Kalbande. "Use of Internet of Things (IoT) in healthcare: A survey." In Proceedings of the ACM Symposium on Women in Research 2016, pp. 71-76. 2016.

[84] Thakar, Anandi T., and Sharmil Pandya. "Survey of IoT enables healthcare devices." In 2017 International Conference on Computing Methodologies and Communication (ICCMC), pp. 1087-1090. IEEE, 2017.

[85] Rodrigues, Joel JPC, Dante Borges De Rezende Segundo, Heres Arantes Junqueira, Murilo Henrique Sabino, Rafael Maciel Prince, Jalal Al-Muhtadi, and Victor Hugo C. De Albuquerque. "Enabling technologies for the internet of health things." Ieee Access 6 (2018): 13129-13141.

[86] Bisio, Igor, Alessandro Delfino, Fabio Lavagetto, and Andrea Sciarrone. "Enabling IoT for in-home rehabilitation: Accelerometer signals classification methods for activity and movement recognition." IEEE Internet of Things Journal 4, no. 1 (2016): 135-146.

[87] Hussain, Saddam, Syed Sajid Ullah, Mueen Uddin, Jawaid Iqbal, and Chin-Ling Chen. "A Comprehensive Survey on Signcryption Security Mechanisms in Wireless Body Area Networks." Sensors 22, no. 3 (2022): 1072.

[88] Pawar, Ankush B., and Shashikant Ghumbre. "A survey on IoT applications, security challenges and counter measures." In 2016 International Conference on Computing, Analytics and Security Trends (CAST), pp. 294-299. IEEE, 2016.

[89] Hathaliya, Jigna J., and Sudeep Tanwar. "An exhaustive survey on security and privacy issues in Healthcare 4.0." Computer Communications 153 (2020): 311-335.

[90] Akpakwu, Godfrey Anuga, Bruno J. Silva, Gerhard P. Hancke, and Adnan M. Abu-Mahfouz. "A survey on 5G networks for the Internet of Things: Communication technologies and challenges." IEEE access 6 (2017): 3619-3647.

[91] Dang, L. Minh, Md Piran, Dongil Han, Kyungbok Min, and Hyeonjoon Moon. "A survey on internet of things and cloud computing for healthcare." Electronics 8, no. 7 (2019): 768.

[92] Durga, S., Rishabh Nag, and Esther Daniel. "Survey on machine learning and deep learning algorithms used in internet of things (IoT) healthcare." In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 1018-1022. IEEE, 2019.

[93] Talal, Mohammed, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. A. Alsalem et al. "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review." Journal of medical systems 43, no. 3 (2019): 42.

[94] Thibaud, Montbel, Huihui Chi, Wei Zhou, and Selwyn Piramuthu. "Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review." Decision Support Systems 108 (2018): 79-95.

[95] de la Torre Díez, Isabel, Susel Góngora Alonso, Sofiane Hamrioui, Eduardo Motta Cruz, Lola Morón Nozaleda, and Manuel A. Franco. "IoT-based services and applications for mental health in the literature." Journal of medical systems 43, no. 1 (2019): 11.

[96] Jiang, Hongbo, Chao Cai, Xiaoqiang Ma, Yang Yang, and Jiangchuan Liu. "Smart home based on WiFi sensing: A survey." IEEE Access 6 (2018): 13317-13325.

[97] Mahmud, Redowan, Fernando Luiz Koch, and Rajkumar Buyya. "Cloud-fog interoperability in IoT-enabled healthcare solutions." In Proceedings of the 19th international conference on distributed computing and networking, pp. 1-10. 2018.

[98] Hanumanthappa, J., Abdullah Y. Muaad, J. V. Bibal Benifa, Channabasava Chola, Vijayalaxmi Hiremath, and M. Pramodha. "IoT-Based Smart Diagnosis System for HealthCare." In Sustainable Communication Networks and Application, pp. 461-469. Springer, Singapore, 2022.

[99] Chen, Min, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, and Long Hu. "Privacy protection and intrusion avoidance for cloudlet-based medical data sharing." IEEE transactions on Cloud computing (2016).

[100] Mahmud, Shahid, Rahat Iqbal, and Faiyaz Doctor. "Cloud enabled data analytics and visualization framework for health-shocks prediction." Future Generation Computer Systems 65 (2016): 169-181.

[101] Tsiachri Renta, Pelagia, Stelios Sotiriadis, and Euripides GM Petrakis. "Healthcare sensor data management on the cloud." In Proceedings of the 2017 Workshop on Adaptive Resource Management and Scheduling for Cloud Computing, pp. 25-30. 2017.

[102] Zhang, Yin, Meikang Qiu, Chun-Wei Tsai, Mohammad Mehedi Hassan, and Atif Alamri. "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data." IEEE Systems Journal 11, no. 1 (2015): 88-95.

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

[104] Sahni, Yuvraj, Jiannong Cao, Shigeng Zhang, and Lei Yang. "Edge mesh: A new paradigm to enable distributed intelligence in internet of things." IEEE access 5 (2017): 16441-16458.

[105] Zohora, Fatema Tuz, Md Rezwanur Rahman Khan, Md Fazla Rabbi Bhuiyan, and Amit Kumar Das. "Enhancing the capabilities of IoT based fog and cloud infrastructures for time sensitive events." In 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), pp. 224-230. IEEE, 2017.

[106] Vora, Jayneel, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, and Joel JPC Rodrigues. "FAAL: Fog computing-based patient monitoring system for ambient assisted living." In 2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom), pp. 1-6. IEEE, 2017.

[107] Kliem, Andreas, and Odej Kao. "The Internet of Things resource management challenge." In 2015 IEEE International Conference on Data Science and Data Intensive Systems, pp. 483-490. IEEE, 2015.

[108] Rajagopalan, Aditya, Manisha Jagga, Anju Kumari, and Syed Taqi Ali. "A DDoS prevention scheme for session resumption SEA architecture in healthcare IoT." In 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), pp. 1-5. IEEE, 2017.

[109] Aazam, Mohammad, and Eui-Nam Huh. "Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT." In 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, pp. 687-694. IEEE, 2015.

[110] Elmisery, Ahmed M., Seungmin Rho, and Mohamed Aborizka. "A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services." Cluster Computing 22, no. 1 (2019): 1611-1638.

[111] Hogg, Tad. "Acoustic power management by swarms of microscopic robots." Journal of Micro-Bio Robotics (2022): 1-10.

[112] Fairhurst, Merle T., Francis McGlone, and Ilona Croy. "Affective touch: a communication channel for social exchange." Current Opinion in Behavioral Sciences 43 (2022): 54-61.

[113] Cornet, Brian, Hua Fang, Hieu Ngo, Edward W. Boyer, and Honggang Wang. "An Overview of Wireless Body Area Networks for Mobile Health Applications." IEEE Network 36, no. 1 (2022): 76-82.

[114] Mehmood, Gulzar, Muhammad Zahid Khan, Muhammad Fayaz, Mohammad Faisal, Haseeb Ur Rahman, and Jeonghwan Gwak. "An energy-efficient mobile agent-based data aggregation scheme for wireless body area networks." Computers, Materials & Continua 70, no. 3 (2022): 5929-5948.

[115] Qadri, Y. A., Nauman, A., Zikria, Y. Bin, Vasilakos, A. V., & Kim, S. W. (2020). The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. IEEE Communications Surveys and Tutorials, 22(2), 1121–1167. https://doi.org/10.1109/COMST.2020.2973314.

[116] Iqbal, Jawaid, Muhammad Adnan, Younas Khan, Hussain AlSalman, Saddam Hussain, Syed Sajid Ullah, and Abdu Gumaei. "Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis." Journal of Healthcare Engineering 2022 (2022).

[117] Cunha, Vanice Canuto, Damien Magoni, Pedro RM Inácio, and Mario M. Freire. "Impact of Self C Parameter on SVM-based Classification of Encrypted Multimedia Peer-to-Peer Traffic." In International Conference on Advanced Information Networking and Applications, pp. 180-193. Springer, Cham, 2022.

[118] Cheng, Qingfeng, Yuting Li, Wenbo Shi, and Xinghua Li. "A Certificateless Authentication and Key Agreement Scheme for Secure Cloud-assisted Wireless Body Area Network." Mobile Networks and Applications 27, no. 1 (2022): 346-356.

[119] Tewari, Anurag, and Prabhat Verma. "Security and privacy in e-

healthcare monitoring with WBAN: A critical review." International Journal of Computer Applications 136, no. 11 (2016).

[120] Rajasoundaran, S., A. V. Prabu, Sidheswar Routray, Prince Priya Malla, G. Sateesh Kumar, Amrit Mukherjee, and Yinan Qi. "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks." Computer Communications 187 (2022): 71-82.

[121] Sreedevi, A. G., T. Nitya Harshitha, Vijayan Sugumaran, and P. Shankar. "Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review." Information Processing & Management 59, no. 2 (2022): 102888.

[122] Chowdhury, Fahim Shahriar, Asif Istiaque, Adil Mahmud, and Mohammad Miskat. "An implementation of a lightweight end-to-end secured communication system for patient monitoring system." In 2018 Emerging Trends in Electronic Devices and Computational Techniques (EDCT), pp. 1-5. IEEE, 2018.

[123] Khalaf, Osamah Ibrahim, Carlos Andrés Tavera Romero, Shahzad Hassan, and Muhammad Taimoor Iqbal. "Mitigating hotspot issues in heterogeneous wireless sensor networks." Journal of Sensors 2022 (2022).

[124] Bhasin, Vandana, Sushil Kumar, P. C. Saxena, and C. P. Katti. "Security architectures in wireless sensor network." International Journal of Information Technology 12, no. 1 (2020): 261-272.

[125] Merah, Lahcene, Pascal Lorenz, Chaib Noureddine, and Ali-Pacha Adda. "Securing information using a proposed reliable chaos-based stream cipher-with real-time FPGA-based wireless connection implementation." (2022).

[126] Haller, Piroska, and Béla Genge. "Using sensitivity analysis and cross-association for the design of intrusion detection systems in industrial cyber-physical systems." IEEE Access 5 (2017): 9336-9347.

[127] Iqbal, Jawaid, Muhammad Adnan, Younas Khan, Hussain AlSalman, Saddam Hussain, Syed Sajid Ullah, and Abdu Gumaei. "Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis." Journal of Healthcare Engineering 2022 (2022).

[128] Mutalemwa, Lilian C., and Seokjoo Shin. "Secure routing protocols for source node privacy protection in multi-hop communication wireless networks." Energies 13, no. 2 (2020): 292.

[129] Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. "Survey of intrusion detection systems: techniques, datasets and challenges." Cybersecurity 2, no. 1 (2019): 20.

[130] Begli, MohammadReza, Farnaz Derakhshan, and Hadis Karimipour. "A layered intrusion detection system for critical infrastructure using machine learning." In 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), pp. 120-124. IEEE, 2019.

[131] Dhanvijay, Mrinai M., and Shailaja C. Patil. "Internet of Things: A survey of enabling technologies in healthcare and its applications." Computer Networks 153 (2019): 113-131.

[132] Jabeen, T., Ashraf, H., & Ullah, A. (2021). A survey on healthcare data security in wireless body area networks. Journal of ambient intelligence and humanized computing, 12(10), 9841-9854.

[133] Lee, Euijong, Young-Duk Seo, Se-Ra Oh, and Young-Gab Kim. "A Survey on Standards for Interoperability and Security in the Internet of Things." IEEE Communications Surveys & Tutorials 23, no. 2 (2021): 1020-1047.

Vidyadhar Jinnappa Aski received his B.E in Electronics and Communication Engineering from Vishweshwariah Technological University, Belagavi, Karnataka in 2013. He holds two master's degrees in the field of embedded systems and instrumentation from MAHE Manipal and control and embedded instrumentation from ESIGELEC, Rouen, France. He is currently working as Head of Emerging Technology CoE at Mahindra and Mahindra's Group Technology Office, Mumbai. He is responsible for architecting, implementing, and deploying R&D use cases in IIoT, Ind 4.0 and mfg 4.0 areas powered by machine vision, deep learning and data modelling techniques. Before joining Mahindra and Mahindra, he was working as an assistant professor in dept. of Computer and Communication Engineering of Manipal University Jaipur. He had also worked as a research associate in ABB corporate research center, Ladenburg, Germany for two years. His research interests include but not limited to Data science, IoT in healthcare, IIoT, Computer network, and Wireless sensor networks etc. He has published several research articles in indexed journals and conferences of international repute.

Vijaypal Singh Dhaka, is a Professor and Head Dept. of Computer and Communication Engineering, Manipal University Jaipur, India. His area of research includes Machine Learning, ANN, Pattern Recognition, Medical Imaging Effective Database Communication Strategies and Technology for Social Change. He is an enthusiastic and motivating technocrat with 15 years of research and academic experience. He has hundreds of research papers published in high impact factor journals of SCI indexed, and other reputed journals. His research expertise includes Artificial Intelligence, Pattern recognition and Medical Imaging. He has received 10 IPRs He authored 6 books and guided 11 research scholars to earn Ph.D. He has organized several international conferences supported by ACM, Springer and Elsevier.

Anubha Parashar is a Ph.D. candidate at Manipal University Jaipur, India. She received her M.Tech degree in Computer Science and Engineering from VCE Rohtak, India, in 2016 and B.Tech degree in Computer Science and Engineering from PDMCE Bahadurgarh, India, in 2013. Her research interests include Gait Recognition, Biometrics, Deep Learning, Computer Vision, Pattern Recognition, and IoT.

Sunil Kumar is currently working as Associate Professor at Manipal University Jaipur. He completed his PhD in 2015 and M.Tech. (CSE) in 2001. He has teaching experience of more than 16 years. He is a reviewer of many reputed international journals and TPC member of many conferences. He is a senior member of IEEE**.**