ISBN: 978-81-956262-8-1 | https://rchub.in/call-for-book-chapter/it-industry-4-0/

The Internet of Things (IoT) in Healthcare: A Review of Enabling Technologies, Standards Protocols, Security, and Market Opportunities

Dr. Govinda Rajulu.G
Professor and HOD CSD
St. Martin's Engineering College
Dhullpally Near Kompally,
Secunderabad - 500100

Dr.Venkatesan .D
Assistant Professor
Department of CSE
St. Martin's Engineering College
Dhullpally Near Kompally,
Secunderabad - 500100

Dr. S. Rabindranath
Associate Professor
Department of CSE
Amc Engineering College,
Banglore-56008

Abstract

The Internet of Things (IoT) is a method or system that allows real-world objects to connect and communicate with one another via networking technology. The state-of-the-art technology and describes surveys on improvements in IoT-based healthcare methods. In addition, this assessment categorises an existing IoT-based healthcare network and provides a description of all potential networks. In this context, IoT healthcare procedures are examined and a broad conversation is held. It also kicks off a large-scale survey on IoT healthcare apps and services. In IoT surrounds healthcare, extensive insights on IoT healthcare security, its requirements, problems, and privacy issues are visualised. . This analysis, catch data protection, network design, Quality of Services (QoS), app development, and continuous healthcare monitoring as well as other security and privacy elements that are problematic in many IoT-based healthcare infrastructures. An IoT-based security architecture model has been developed in this review to address the security issues. Furthermore, this study reveals a market potential that will boost the growth of the IoT healthcare market. It screening system to only collect papers that were relevant to our investigation. The papers that were chosen were then thoroughly scrutinised to determine their contributions and research focus.

Introduction

The Internet of Things (IoT) is a new paradigm in which every physical object you wear, drive, read/see, and anything else, including people you meet and locations you visit, will be connected, addressed, and controlled remotely. There are many suitable solutions for a wide range of IoT applications, including traffic congestion, waste management, structural health, security, emergency services, logistics, retail, automated control, and healthcare. Medical equipment, services, actuators, sensors, and diagnostics all aim to improve the end user's experience through IoT-based healthcare. In addition, IoT devices can detect the best times for repeat and sequential actions. examined an existing IoT-based security-based healthcare application that described the label of protections. The default security of an IoT application

must be needed to defend itself. Security, privacy, and trust must be handled in any healthcare-domain specification systems.

This book adds the following in this regard.

1) A survey of cutting-edge technologies for IoT-based healthcare.
2) Classifying and presenting a summary of existing IoT-based healthcare networks.
3) Modeling and analysis of typical IoT healthcare protocols, as well as a full discussion.
4) Conducting a comprehensive survey of IoT-based healthcare applications and services.
5) Modeling in-depth insights into IoT healthcare security, including its requirements, problems, and privacy concerns.
6) Developing a recommended IoT healthcare security model.
7) Finally, market potential for IoT-based healthcare technologies are discussed.

I. IOT HEALTHCARE METHOD

Cloud Computing (A)

Real-time sensor technologies will be able to collect e-storage of all patient records, including photographs, documents, and videos, from various sensor devices, thanks to the integration of cloud computing with IoT and the smart hospital information system. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are three key services provided by cloud technologies in healthcare environments (IaaS) A focus on the utilisation of a huge database for data analysis and trend detection. For IoT-enabled e-health, the cloud management structure is defined, which enables an efficient, safe, and seamless model in provisioning, processing, protecting, enforcing regulations, and cloud management prediction.

Big Data

The adoption of current technology is important not just for providing higher quality care to patients, but also for the long-term viability of healthcare institutions. Volume, velocity, variety, veracity, and value are the five V's that define big data. The amount and variety of healthcare data are used to suggest a data storage paradigm for emergency healthcare. During an emergency, IaaS and SaaS are utilised to organise heterogeneous physiological data and make it accessible to relevant healthcare specialists. proposes a WBAN system that

combines SaaS, PaaS, and IaaS services to build a cloud paradigm. The link between the patient's emotional responses and physiological changes is described using a sensor-based system. The technology provides data mining approaches for extracting key information and removing superfluous data from databases, using algorithms that focus on the collection of large data sets for which machine learning could be used. Another cloud-based large data management study using machine learning is being investigated.

Grid computing

Grid computing is emerging as a possible answer to some of e-most Health's technical problems, such as medication development. It is proposed to use a mobile grid management framework as a key enabler for IoT-based next-generation ubiquitous healthcare solutions. Another study provides an overview of grid computing, explains its potential applications, and proposes a decision framework that builds on the Enterprize Desktop Grid architecture to improve healthcare decision-making. MediGRID is a grid infrastructure dedicated to medical and bioinformatics research. It enhances the location- independent collaboration of researchers by providing grid services in a controlled e-Science platform and gives access to a broad spectrum of applications for bioinformatics, medical image processing, and clinical research.

Virtual Reality

Virtual reality (VR) creates an altogether new world, allowing us to incorporate the most useful information from the digital domain into our view of the environment around us. provides an overview of AR as well as reviews of recent uses in medicine. AR not only aids healthcare workers in visualising and interacting with 3-D body models, but it also aids patients as an educational tool. Ultrasound imaging and optical diagnostics are two further medical applications of AR.

I. IOT HEALTHCARE NETWORKS

1.IoThNet Topology II

The IoThNet topology refers to the grouping of different components. It depicts common healthcare scenarios in which a composite computing network manages huge quantities of vital symptoms and sensor data through remote monitoring . For preserving the streaming of medical data, IoThNet topology gateways and access services

required IP, global system mobile (GSM). To investigate and store the collected data, IoT devices are connected to the health-IoT cloud via healthcare gateways.

2. IoThNet Architecture

The idea of the IoThNet architecture specified the IoThNet's physical elements' procedures and their functional organisation . The capabilities of computer systems of the IoT gateway, caregivers, wireless local-area network (WLAN), multimedia streaming, and secure communications remain recognised in the IoThNet design.The IoThNet architecture includes three complex e-Health delivery services: composition, signalization, and data transmission . The Quality of Services (QoS) procedure and resource allocation are accepted by methods in the IoThNet that enable heterogeneous service configuration and signalization protocols.

3.**IoThNet Platforms (H)**

The IoT healthcare network platform concept is a service platform centred on resident health information in the IoT system. It aids in classifying the various healthcare models and how caregivers can access various databases based on the healthcare support layer.

II.IOT COMMON STANDARDS PROTOCOLS

Several standards targeted at assisting and analysing the significance and services that we may use for IoT solutions to link various objects to the Internet are included in IoT common standards.

1.Application Protocols

CoAP (Constrained Application Protocol) is an HTTP functional, lightweight Internet Application Protocol established in the RFC 7252 standard developed by the Internet Engineering Task Force (IETF) for constrained restful environments (CoRES) . The GET, PUT, POST, and DELETE methods are utilised in automation, social networks, and microcontrollers. REST is based on a stateless client-server architecture that exposes and applies to Web service clients and servers such as SOAP (SOAP).

The following are some of CoAP's primary features:

1) Web protocol infrastructures impose limitations on M2M requirements.

2) With unicast and multicast requests, UDP [RFC0768] binding with unlimited security is maintained.

3) Resource observation aids in the application's monitoring via the publish/subscribe technique.

4) Data was sent between the client and the server using blockwise resource transport.

5) The CoREs' Web connection range for delivering resources based on the clients' resource discovery URI path.

6) The CoAP with HTTP through a proxy server is enabled by the compliance of dealing with specific objects that work as the common REST architecture.

7) The datagram transport-layer security (DTLS) layer is incorporated with the CoAP protocol for transmitting secret messages.

***2*.Message Queue Telemetry Transport**

The Internet of Things, or IoT, is forming a vast M2M network. So all of the devices, sensors, systems, and actuators can connect to the Internet and communicate, and they'll need a communication protocol to do so. Clients can send brief one-hop messages to the broker, as well as receive messages if they've subscribed to a specific topic. Clients can change the topic of speed or post speed facts, such as 15 MPH. Clients who have subscribed to the topic of speed will receive updates as new information on the subject is published or updated. Clients who have subscribed to the topic of speed will receive updates as new information on the subject is published or updated. These clients can send or receive messages from a security state based on a certain topic. Password authentication has become an industry standard, therefore those clients can surely log on.

***3*.Extensible Messaging and Presence Protocol**

The XMPP Foundation actively extends the Extensible Messaging and Presence Protocol (XMPP), a communication standard used in IoT that was originally developed for instant messaging (IM), formalised by the IETF model, and used for different video calling, telepresence, multiparty chat- ting, and voice . XMPP allows IM clients to manage authentication, access control, privacy analysis, hop-by-hop and end-to-end encryption, and compatibility with other protocols . XMPP uses global protocols and, depending on the settings, can pass through textual firewalls, reducing XMPP payload overhead. The

advantages of utilising and developing technology are accompanied by certain data that is kept and enhanced by the XMPP standards.

4.Advanced Message Queuing Protocol

(AMQP) is a widely used IoT application protocol that focuses on message-oriented systems [22]. The Advanced Message Queuing Protocol (AMQP) allows IP systems communications to be delivered one-to-one, one-to-many, or exactly once across applications. AMQP is a new standard that allows for interoperability, communication, and resource sharing between new and existing applications. It necessitates a secure transport protocol architecture as well as middleware that acts as a conduit between applications and shared resources, connecting companies and technology across time and place.

5.Service Discovery Protocols

The Internet of Things necessitates large-scale resource management methods that can receive self-configured registers and actively discover resources and services. DNS service discovery (DNS-SD) and multicast domain name system (mDNS) are efficient and powerful protocols in the IoT . Our research backs up light forms of IoT. The mDNS and DNS-SD protocols were created with resource-intensive devices and situations in mind.

IoTh-based networks including blockchain

Medical information is sensitive by nature in the healthcare system, and keeping it safe and secure is a difficult challenge. Because security threats are inherent to every linked system/device, regardless of how IoT is employed in healthcare, the attack surface and vulnerabilities for IoT infrastructure remain largely the same. Malicious hackers, naive ignorant users, and malicious software are all capable of wreaking devastation.

Blockchain is a new decentralised architecture and distributed computing paradigm that has primarily been used in bitcoin and cryptocurrency applications in recent years . Peer-to-peer healthcare communications use multitier blockchain protocol processes with diverse authorities to secure patient data . We've approached addressing concerns in the sphere of IoT-based healthcare using blockchain technology and comparing it to existing models and technologies. In IoT healthcare, the witness of blockchain apps is used .

To distinguish the unique act of the surveyed protocols, they are studied utilising numerous frameworks to construct appropriate applications, such as fault tolerance, security

limitations, scalability, and tradeoffs.It must examine the possibility that a gadget could be hijacked by an unscrupulous person intent on causing harm, casting doubt on the device's authenticity. Malware can also be installed on a gadget.

It must additionally analyse the data transfer path and devices along it for possible eavesdropping or data modification in order to compromise data integrity. The servers that will store the data are another attack surface, but that is not our worry for now because data storage security is a well-studied topic with well-established procedures. As a result, we propose a security model for an IoT-based healthcare information system that focuses on the following aspects: preventing hacked/hijacked devices and ensuring the confidentiality and integrity of data from IoT-enabled sensors and the edge server. The other issue of the ignorant user is unimportant because it largely concerns good user training and awareness, as well as more robust firmware and software architecture.

This model also focuses on the IoT infrastructure of large-scale healthcare service facilities, such as hospitals and clinics, where IoT-enabled devices will continuously monitor both indoor and outdoor patients' health states and/or serve other functions. However, the methodology could be useful for a smaller scale or personal IoT health monitoring system. The following summarises our focus:

1) Providing a powerful security mechanism that ensures device safety, preventing someone with nefarious intentions from gaining access and taking control of a device.

2) When data regarding patients' health conditions is transmitted from the sensor to the edge server, end-to-end security and confidentiality are provided to assure data integrity and validity. It suggest:

a) Barebone OS for medical IoT devices/sensors that will only have a minimal feasible access to the outside world by limiting network services/OS level instructions;

b) To assure data integrity, using blockchain for protecting record-related processing such as creation, deletion, and updates. Despite the fact that IoT and blockchain have different operating principles and architectures, they can be linked utilising a software platform. As a result, in this section, an integrated IoT-based blockchain network platform for improving the smart healthcare system's security challenges is proposed. This review proposes an IoT-based security architecture model to address the security issues. The proposed approach's overall architecture and depicts the connections between various sorts of actors.

Each technology, such as IoT sensor devices, IoT gateways, and blockchain networks, plays a particular role in this architecture. Sensors such as pressure sensors, heart rate sensors, electroencephalogram sensors, airflow sensors, and others are used by IoT sensor devices to perceive medical data. The acquired sensing data is then transmitted over wireless LAN or another comparable technology to the IoT gateway device. After receiving the data, the gateway device sent it to the blockchain network via wired or wireless connections. Finally, the IoT blockchain end processes the received data and records it in its peer node. In general, blockchain is a peer-to-peer network platform that includes blockchain, where each node has the identical data storage record. When an initiator creates a new health record on the healthcare blockchain, it signs it with its private key and sends a data storage request. Meanwhile, the initiator broadcasts this request for validation to all other nodes in the network. All of the other peers took part in the validation process and attempted to obtain the nonce. The record will be validated by the peers who receive the nonce first. The approved result will then be transmitted to all other network peers.

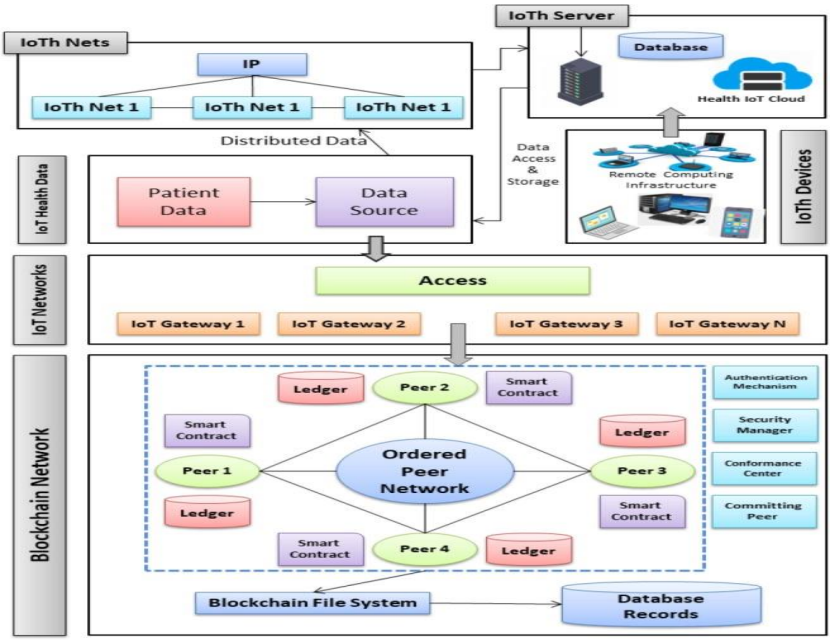

Fig1. IoTh-based networks including blockchain

No one can change or delete a record once it is stored on the blockchain. It maintains data consistency. However, in the blockchain section of the design, we recommended an ordered peer network.Each couple is in charge of their own IoT data. This network protects data by employing access control measures and prohibiting unauthorised network access. To obtain

any record, the node must first register with the blockchain network and become a member. Any node that wants to join the blockchain must be approved and have an authenticated certificate. On the platform, a security manager will continuously monitor the network's security and protection issues.

Patients can examine medical record papers with appropriate IDs and access permission. As a result, the network aids regulatory compliance. To prepare the synchronisation and retrieve the data, the IoT healthcare network configures a protected communication protocol (ZigBee, Z-wave) that contains the patient's data. The information gathered was linked to several services in order to identify health reviews. The IoT server can verify the user for health analysis monitoring, interpretation, and approval [16]. IoThNet provides access to the determination capabilities for medical data exchange and response, as well as the usage of healthcare data. The IoT encompasses all components of wearable patterns, which are safeguarded with software, electronics, sensors, actuators, and connectivity, allowing assessable techniques to relate and transfer data.

By approving connections based on blockchain security, Proof of Work (PoW) has been utilised to simply recognise and evaluate the way to finish computational activity. Hash computation is used to handle it, which includes creating a block. The Secure Hash Algorithm (SHA-256) with cryptographic Hash creates a unique hash. Blockchain is the most important and beneficial technology in the healthcare sector.

Blockchain-based security is not without flaws. The challenges of blockchain-based security in terms of size and performance are dependent on transaction network speeds and standardisation. To validate blocks, blockchains are now employing a variety of consensus mechanisms, including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Proof of Authority (PoA) .

This security architecture will aid in the prevention of device hacking and the integration of data from IoT-enabled sensors and edge servers. The IoT healthcare applications and services will be represented in Section VIII (A & S).IoThNet provides access to the determination capabilities for medical data exchange and response, as well as the usage of healthcare data. The IoT is defined as a system of wearable patterns safeguarded by software, electronics, sensors, actuators, and connectivity that enables assessable techniques to relate and transfer data.

I. Security Requirements

1.Scalability:

2.Communications Media

3.Multiplicity of Devices

4.Multiprotocol Network

5.Attacks Based on Information Disruptions

6.Attacks Based on Host Properties

7.Confidentiality

8.Integrity:

9.Resiliency

10.Authentication:

11.Availability

12.Data Freshness

13.Nonrepudiation:

14.Authorization

15.Fault Tolerance

16.Self-Healing

B. **Security Challenges**

1.Restriction on Computation

2.Memory Limitations

3.Uncertainty:

C. **Threat Model**

D. **Attack Taxonomy**

II.IOT HEALTHCARE APPLICATIONS AND SERVICES

1.IoT Healthcare Applications

2.Dropping Emergency Room Waiting Time

3.Tracking of Information:

4.Drug Management:

5.Food Management

6.Determination of Glucose Level

7.Monitoring of Electrocardiogram

8.Monitoring of Blood Pressure

9.Monitoring of Oxygen Saturation

10.Rehabilitation System

III.IoT Healthcare Services

1.Ambient Assisted Living:

2.m-Health:

3.Adverse Drug Reaction:

4.Semantic Medical Access

5.Children Health Information

6.Embedded Context Prediction

7.Wearables:

IV.IOT HEALTHCARE CHALLENGES AND OPEN ISSUES

1. Standardization

2.Security

3.Cost

4.Quality of Services

5.Network Architecture

6.Technology Transition

7.Power Consumption

8.Data Protect

III.IOT HEALTHCARE MARKET OPPORTUNITIES

For machinery businesses, Internet service providers, and application developers, the Internet of Things contributes to a large market opportunity with smart items. M2M transit concerns necessitate the development of up to 45% of the Internet platform . On the Internet of Medical Things, the rise of IoT is bringing life-improving improvements (IoMT). The influence of IoT healthcare applications is expanding to increase the most important

commercial businesses, such as Mobile Health (mHealth) and telecare, which allow for preventative wellness of diagnosis, treatment, and monitoring services.

According to Grand View Research, the IoT healthcare market capacity is expected to reach USD billion by 2025, with a CAGR of 19.9% over the forecasted years. Grants for the IoT healthcare sector are increasing the solution that making the connected devices.

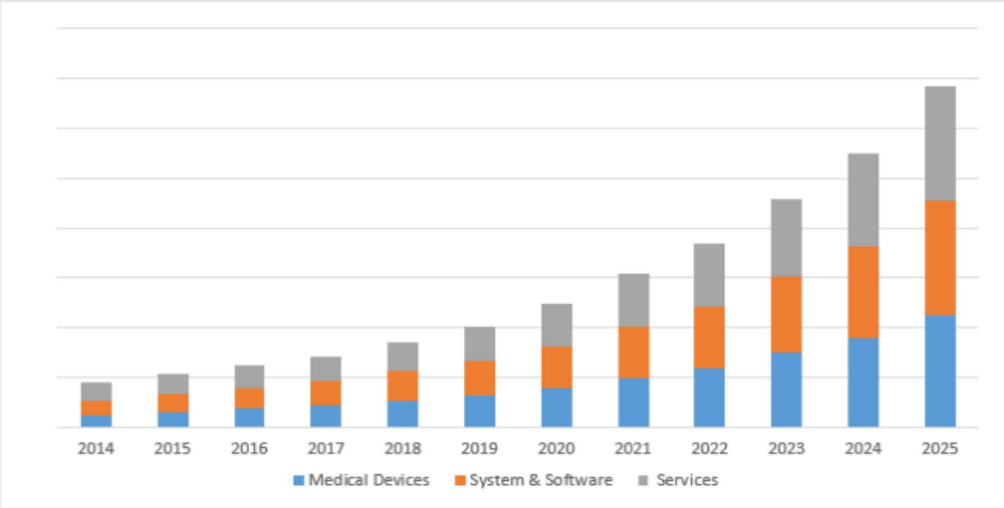

Fig 2. IoT healthcare market size and trend analysis of services, systems, and software

IV.CONCLUSION AND FUTURE DIRECTIONS

The future of healthcare is being reshaped by the integration of IoT technologies into healthcare systems. We began our discussion in this overview with the technologies now being used in IoT systems, such as RFID, edge computing, semantic analysis, and augmented reality. We examined and highlighted their advantages and disadvantages. Following that, we discussed existing IoT network topologies, designs, and platforms in healthcare. Following that, we went over all of the primary application protocols, service delivery protocols, and infrastructure protocols that are currently being investigated and deployed in IoT standards in great detail. Another important feature of our work was a thorough examination of the security aspects of IoT healthcare systems. We've gone through the security requirements of an IoT system in general, as well as the issues that come with meeting those criteria.

It also proposed a top-level architecture for an IoT system that uses Blockchain to address current security issues. Following that, we explored the applications and services that IoT can provide to the health-care sector. It highlighted the hurdles and open issues that IoTh has yet to overcome, as well as the potential that remain in the healthcare market, as part of our analysis. Researchers all across the world are working to enhance healthcare by introducing

unique ideas, innovative gadgets, and sophisticated software. This evaluation focused on several modern IoT networks, as well as their protocols, designs, and platforms. This article discussed IoT healthcare research initiatives in the areas of chronic disease management, geriatric monitoring, and personal health. Security, privacy, authentication, energy consumption, compute power, resource management, QoSs, and other critical challenges with IoT healthcare systems are explored in depth here. We attempted to present a complete evaluation of current IoT healthcare technologies, their applications, problems, and unresolved topics for future researchers in the field. In the coming years, the mainstream use of IoT-based healthcare will accelerate. In the approaching fourth industrial revolution, the Internet of Things is projected to be a critical component of any healthcare solution. In this regard, our research should serve as a foundational guide for future field visionaries and offer them with a straightforward reference point.

REFERENCES

[1] S. Shinde and V. Phalle, "A survey paper on Internet of Things based healthcare system," *Int. Adv. Res. J. Sci. Eng. Technol.*, vol. 4, pp. 131–133, Jan. 2017.

[2] J. Ko *et al.*, "MEDiSN: Medical emergency detection in sensor networks," *ACM Trans. Embedded Comput. Syst.*, vol. 10, pp. 1–29, Aug. 2010

[3] T. Hwang and P. Gope, "Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets," *Wireless Pers. Commun.*, vol. 77, pp. 197–224, Jul. 2014.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015

[5] A. Aijaz and A. H. Aghvami, "Cognitive machine-to-machine commu- nications for Internet-of-Things: A protocol stack perspective," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 103–112, Apr. 2015.

[6] J. Hller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Oxford, U.K.: Elesvier, 2014.

[7] P. A. Laplante and N. Laplante, "The Internet of Things in healthcare: Potential applications and challenges," *IT Prof.*, vol. 18, no. 3, pp. 2–4, May/Jun. 2016

[8] O. Vermesan and P. Friess, *Internet of Things-From Research and Innovation to Market Deployment*, vol. 29. Aalborg, Denmark: River Publ., 2014, pp. 2–4.

[9] L. Atzori, A. Iera, and G. Morabito, *The Internet of Things: A Survey Computer Networks*, vol. 29. Aalborg, Denmark: River Publ., 2010, pp. 2787–2805.

[10] L. Tan and N. Wang, *Future Internet: The Internet of Things*. Aalborg, Denmark: River Publ., 2010

[11] S. M. R. Islam, M. N. Uddin, and K. S. Kwak, "The IoT: Exciting possibilities for bettering lives: Special application scenarios," *IEEE Consum. Electron. Mag.*, vol. 5, no. 2, pp. 49–57, Apr. 2016.
[12] Z. Pang, *Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-Being*, IKTH Roy. Inst. Technol., Stockholm, Sweden, 2013.
[13] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, *The Internet of Things for Health Care: A Comprehensive Survey*, vol. 3. Aalborg, Denmark: River Publ., 2015, pp. 678–708.
[14] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, Apr. 2019.
[15] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, "Wireless sensor networks for healthcare," *Proc. IEEE*, vol. 98, no. 11, pp. 1947–1960, Nov. 2010.
[16] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard 802.15. 4-2011, 2011.
[17] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes," *IEEE Internet Comput.*, vol. 16, no. 2, pp. 62–67, Mar./Apr. 2012.
[18] C. Lerche, K. Hartke, and M. Kovatsch, "Industry adoption of the Internet of Things: A constrained application protocol survey," in *Proc. IEEE 17th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Krakow, Poland, 2012, pp. 1–6.
[19] D. Locke, *MQ Telemetry Transport (MQTT) V3.1 Protocol Specification*, vol. 15, IBM Develop. Works Techn. Lib., Armonk, NY, USA, 2010.
[20] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): Core," Internet Eng. Task Force, RFC 3920, 2011.