Contents available at ITME Online Repository

INNOVATIVE TRENDS IN MULTIDISCIPLINARY ENGINEERING

International Peer-Reviewed Journal of the School of Engineering & Technology

K.R. Mangalam University, Gurugram

Journal Homepage: **https://itme.krmangalam.edu.in/**



Transformation of Internet of Medical Things in Healthcare: Architecture and Security

Javed Azmi[a,*]

[a] *Jamia Hamdard, New Delhi*

DOI: 10.68343/ITME.2026.0102.9

ARTICLE INFO

Article history:
Received 30 March 2026
Revised 2 May 2026
Accepted 20 May 2026
Available online DD Month 2026

Keywords:
IoMT
healthcare
architectures
sensors
technologies
security
challenges

ABSTRACT

The Internet of Medical Things plays an important role in healthcare by improving the dependability, precision, and efficiency of healthcare devices. The IoMT has several healthcare applications, and its revolution is transforming modern medical care with fascinating technological, social, and economic ramifications. While it addresses several sectors, we focus on IoMT's significance in the healthcare system. A range of technologies can reduce overall costs connected with the treatment and control of serious diseases. Wearable and mobile apps currently assist health education, fitness programs, diagnosis monitoring, and integrated illness prevention. This paper focuses on the IoMT framework for healthcare, IoMT architecture, technologies, security advancements, and challenges issues that have been made in the field. Substantial advancements in terms of tools and technology along with protection are being achieved, which have been amplified by the rapid implementation of IoMT for smart healthcare around the world.

1. Introduction

The growth of Internet of Things (IoT) technology has its impact on a day-to-day basis. It marked a solution to reduce the pressure on the healthcare system. IoT is an integration of data connected through the internet. It can provide a connected set of anything, any place, any time, any services for anyone on any network. In addition, it offers real-time health status of the patients to the healthcare system [1]. One of the most acceptable application domains for IoT is healthcare and medical care. The application of medical Internet of Things includes remote health monitoring of chronic disease, elderly care and fitness programs. Another possibility of IoT application is integration with medication and treatment by doctors at home. Essential parts of IoT are sensors, medical and imaging devices required for diagnosis of the individual. The healthcare system can reduce cost, enhance the quality of life and satisfy the individual experience. Smooth and continuous supply for various devices restored at the perfect time is efficiently identified by IoT. The optimum use of limited resources and services for more patients is ideally scheduled by IoT [2].

The main objective of IoT is to provide easy and worthwhile interaction with uniformity and secure connectivity across each patient, hospital and healthcare facility. On the other hand, IoT through advanced and wireless technologies can help early diagnosis, real-time monitoring of chronic diseases and medical crises [3]. The essential role played by the medical server, gateway and health database is in keeping electronic health records (EHR) and providing information at the time of requirement or emergency

* Corresponding author. E-mail: **azmijaved@gmail.com**

© 2026 The Authors. Published by K.R. Mangalam University, Gurugram.
Selection and double-blind peer-review under the responsibility of School of Engineering & Technology.
This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0).

healthcare [4]. In recent years, the broad area of IoT has attracted the attention of many researchers to show its efficiency in the healthcare field by focusing on many practical challenges. IoMT-based healthcare research requires a framework, architecture and platform, interoperability and issues of security [5].

2. Internet of Medical Things

With rapid advances in science, technology and healthcare as well as the rise of smart medical devices, the healthcare system has changed radically [6]. Furthermore, advances in technological development have transformed a variety of physical services into digital systems and applications that can be accessed from a distance. IoT and its integration into healthcare systems have had a huge influence on user life and the medical profession. Patient, doctor, drug (pharmacist) and diagnosis are all part of the conventional health system [7]. In order to provide safer, faster and more affordable services, researchers and businesses are turning to IoMT applications. There are a lot of innovative and achievable suggestions for improving and evolving the conventional medical IoMT system. These improvements apply to all components, including architecture, application, technology, networking, and security [8]. Data transmission in the healthcare system, which can be used for short-range or long-range transmission, is used to connect IoMT devices [9]. Vulnerability, invasion, defense, and reduction are all aspects of the healthcare system's security. It focuses on advancements in IoMT applications, technologies, architectures and security. Security measures, threat models, and attacks are among the security features [10]. An approach for device authentication with risk assessment was introduced in order to promote an encrypted IoMT system. The technique's specified analytical methods are suitable for specific IoMT devices; vulnerabilities, threats and attacks were all part of their analysis for sensor-collected data, data-user identification and management platforms among the data analyzed [11]. In a confidentiality IoMT monitoring device to apply to the blockchain component, the goal is to safely store processed data from sensors with data security [12]. Cloud data and applications such as online, mobile, real-time, and non-real-time, wearable sensor devices and security systems are all part of the IoMT medical system [13].

The sensors or medical devices are embedded with computing devices and transmit or accept data to a cloud platform over a shared network, as it improves the quality of the healthcare system and finally enhances patient satisfaction. A cloud-based smart-device and artificial intelligence automaton interaction was also reported. Body area sensing has been developed to function as part of an IoMT regular health monitoring system that includes both the sensor and the data provider [14]. Through IoMT technology, the patient's health records are collected and transmitted to a cloud platform for doctors to use for decision making and analysis of disease diagnosis and clinical care.

3. IoMT Framework for Healthcare

3.1. IoMT Network

IoMT is a healthcare framework in which clinical application is completely utilized with cloud computing and IoMT. This framework gives conventions to help the correspondence and broadcast of crude clinical signs from different sensors and savvy gadgets to an organization of fog nodes. The essential part of IoT healthcare is the IoMT healthcare network; it supports access to the IoMT backbone to help send and receive healthcare data and facilitates the utilization of healthcare-modified communication [15]. The healthcare system can aggregate information about a person's care condition through heterogeneous sensors; this aggregated information is sent to the remote network for processing and outcomes are displayed. Figure 1 shows that the IoMT network comprises three components: topology, architecture and platform [16]. In the IoMT healthcare framework, every component has a unique purpose; the detail of each component is discussed here:

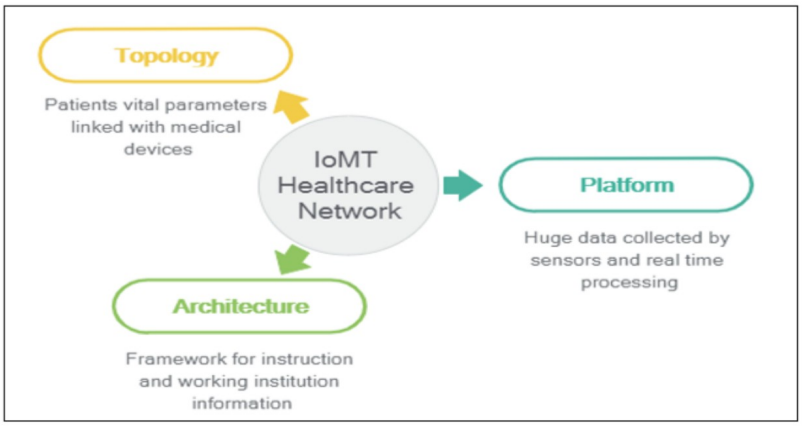


Figure 1. IoMT healthcare Network (IoMTNet) Issues

3.2. IoMT Network Topology

The topology describes the unusual arrangement of different elements in an IoMT healthcare network and depicts optimal network conditions. Figure 2 describes a typical IoMT and cloud computing grid healthcare topology, which consists of three elements: namely data sources, service providers and hardware resources [17]. A data source shows a network of interconnected sensors on wearable devices which are responsible for collecting an individual's vital signs and progressively transmitting raw data such as body temperature, blood glucose (ECG), electromyography (EMG) and oxygen saturation. The service provider analyses the processed data and then stores it on the cloud. Finally, the hardware resource not only monitors patients but also accesses the data from any place, and if required, an immediate decision is also given when the condition of the patient is critical [18].

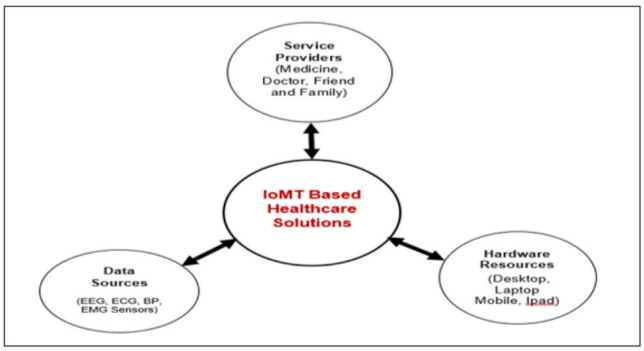


Figure 2. A conceptual diagram of IoMT Network describes the topology

Portable healthcare devices capture a patient's vital parameters and important organ functions, as sensors embedded in individuals are stored [19]. In the same way, the IoMTNet topology can be linked with medical devices connected to the IoT healthcare system. The fundamental elements designing the IoMTNet topology are examining healthcare services related to various activities. It involves the medical services before and after the treatment process, from the aspects of medical care service providers. These activities have been visualized in the prospective view of unexpected incidents in medical services [20].

3.3. IoMT Architecture

The IoMT architecture describes the framework for instructions to the IoMTNet's objective, where working institution information is accumulated by various sensors or taken from stored data and transmitted to a gateway on fog computing to further send to the cloud. Fog sensors play an important part in the hospital information system (HIS) by implementing the instantiation of the system in the clinic or hospital and enhancing the administration and anticipation of electronic records [21]. The data is collected in the cloud, and proceeds for the development of extraction and statistical examination by equipment centered on big data processing, online analysis of data [22]. In recent years, more and more clarifications have been proposed for cloud and computing in time-critical healthcare applications.

3.3.1. Cloud Computing

It is a latest model of computing that provides automatic provisioning of resources that can be available from any place, any time on any network. Cloud computing is one of the important technologies of IoMT. It is installed at the middle layer, also called the processing layer, in the five-layer IoMT architecture as shown in Figure 3. In IoMT the sensor technologies create a large amount of information that can be stored and analyzed with the help of cloud structure [23].

The various data stored in the cloud, aggregated through multiple sensors, is an aid for physicians to monitor patients' health by analyzing the information [24]. Physicians can provide suitable medication or instructions, either manually or automatically via computer. There are benefits to using cloud computing but there is still one challenge with it: latency [25]. The information aggregated by the sensors has to move further via the internet and then reach the cloud for data investigation, and again the processed data must be transmitted via the internet and at least reach the physician's device. This might be a time-consuming process, which is not feasible for critical healthcare services; in such conditions latency should be avoided by utilizing fog computing [26]. Let us have a glance at fog computing.

3.3.2. Fog Computing

It allows information processing to be taken away from the cloud and moved forward to the sensors, this reduces latency and allows physicians to provide initial healthcare [27]. Fog computing assembles sensors and local gateways to store and execute initial data processing. A fog node contributes monitoring, preprocessing, storage and security services [28]. The monitoring service permits the node to observe resources and services being provided. The pre-processing service allows the node to perform preliminary data processing, which might be needed for providing critical healthcare. The storage service allows data to be segregated, and the security element handles data integrity, data confidentiality and privacy of data. Intrinsic advantages of fog computing can be involved at the networking layer and perception layer of the IoMT's layered structure [29]. Fog computing facilitates the processing of computing, storage and internet services between cloud computing, information centers and end devices.

3.4. IoMT Layered Architecture

IoMT is a multilayered architecture. Three layers, such as perception layer, network layer and application layer, are the most inherent architecture layers and could not overcome the requirement of application [30]. The next is a four-layered architecture, which has an essential role in the growth of IoMT. There were also some issues regarding privacy, security and storage in this four-layered architecture, so a five-layer architecture has been introduced to make IoMT more secure and authentic. In this paper, we discuss the five-layer architecture [31]. The newly five-layered architecture is considered to have the ability to manage the needs of IoMT. Multi-layer IoMT architecture is used in IoMT cloud platform technology to support large-scale expansion while supporting failover for storage failure recovery. It can make IoMT applications more secure and easily accessible. The following are the five layers of the architecture, as shown in Figure 3 [32–37]:

3.4.1. Perception Layer

This is also called the acquisition layer, which is the foundation of IoMT. The major function of this layer is to collect data such as blood pressure, temperature, heart rate, etc., using sensors, and then the collected data is transmitted to the next layer, the network layer.

3.4.2. Transmission Layer

It behaves like a link between the perception layer and processing layer. It carries and transfers the collected data of physical parameters using sensors. It comprises wireless and wire-based components and is employed for interconnecting smart objects and internet devices with the internet.

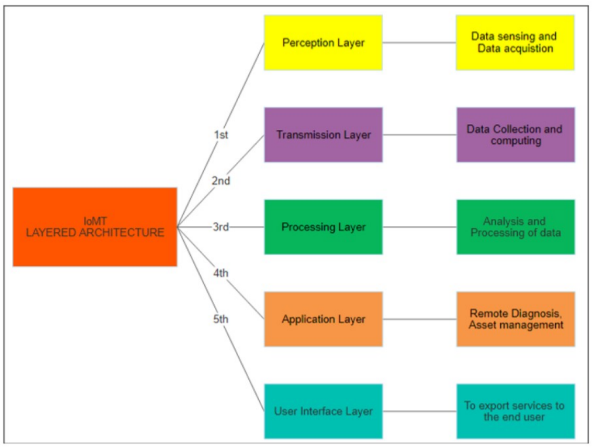


Figure 3. An overview of five layers architecture

3.4.3. Processing Layer

It is a middle layer that aggregates the data received from the transmission layer, which carries out diagnosis on the collected data, removes data that has no meaning, and also extracts data that has more importance. It also eliminates the issues of big data, where a huge amount of data is processed that can influence IoMT performance.

3.4.4. Application Layer

This fourth layer provides all applications used in the IoMT technology in which IoMT has been employed. This layer refers to the interaction through which people communicate with connected IoMT sensors or devices below the middle layer (processing layer) for administration, communication and commanding. As there is a huge amount of information in the healthcare system, there is a tendency to move forward to the cloud platform for integrity, scalability and cost reduction.

3.4.5. User Interface Layer

The fifth and final layer includes monitoring, visualization, mediation and analysis tools for the aid of medical providers and emergency responders. This can work on various platforms such as web, smartphones, etc. This layer defines an extensive act of an application and behaves like a controller of a medical system. The layer manages the business logic for the health profession and also collects data from the IoMT environment.

3.5. IoMTNet Platform

The IoMTNet Platform focuses on the computer system and network platform; it has a large amount of data from heterogeneous sensors formed by wearable devices, and it can execute real-time information processing and act accordingly [38]. The platform utilizes IoMTNet topology to manage IoMT elements and IoMT architecture to select appropriate applications between elements of IoMT. The responsibility of the IoMTNet platform is to verify that sensors work independently so that the person can communicate efficiently. Further, the IoMTNet platform must employ use cases, strong communication techniques, dashboard visualization and IoMT applications [39].

The following are the performance characteristics of five major platform approaches:

3.5.1. Easy Connectivity

An ideal IoMT platform simply connects the device and carries out device functions enclosed in a cloud-central service and applies systematically to gain view and fulfill institutional modification.

3.5.2. Simple Device Management

An application of IoMT devices enhances asset accessibility, output expansion, reduced unexpected interruption and minimizes asset maintenance costs.

3.5.3. Data Ingestion

This smartly modifies and accumulates IoMT data. Application Programming Interfaces (APIs) facilitate the extraction of information that's required, like a link between data and the cloud. From multiple data sources and platforms the data is ingested, and important values are removed using utility processes.

3.5.4. Data Analysis

This provides a better viewpoint from large amounts of IoMT data to give appropriate suggestions and upgrade operations. To obtain real-time diagnosis while observing the current situation of a patient and take appropriate decisions, an automatic dashboard makes this entire process easy to understand.

3.5.5. Reduced Threat

Action is taken on alert notifications and incidents are extracted, developed anywhere in organizational environments, from an automatic dashboard.

4. IoMT Security

The protection and privacy of critical and sensitive healthcare data pose challenging healthcare security issues. There are numerous threats, risks and hazards that can affect distinct layers of the IoMT architecture. The exposure of various malware invasions on IoMT security systems aims at security demands such as information integrity, confidentiality, authenticity and availability. Recent actions or plans lay more stress on key principal management, access control, authentication and intrusion detection [40]. It is important to identify and evaluate various approaches to IoMT privacy and security, including security requirements, threat models, vulnerabilities and these solutions from the healthcare perspective, in order to support the adoption of IoMT in the medical domain [41].

4.1. Security Requirement

The following security requirements need to be focused on for countermeasures of secure systems in IoMT-based healthcare systems [42]:

4.1.1. Integrity

Integrity refers to a way to ensure that healthcare data is sealed and accurate. It means that the context of stored data should not undergo unauthorized deletion, false insertion, or alteration during diagnosis.

4.1.2. Confidentiality

This ensures the protection of medical information from being accessed by unauthorized persons. Along with this, the confidential data is prevented from disclosing its context to intruders.

4.1.3. Authorization

This is another security requirement that is utilized to verify a device or user for a data application. It is generally followed by an authentication method to verify the gadget and users.

4.1.4. Authentication

Various IoMT systems face weak authentication, which leads to deterioration in energy consumption, hardware and other computing resources, giving advantages to eavesdroppers.

4.1.5. Availability

Availability is a property that ensures data is accessible to authorized users. The other type of threat is a Denial-of-Service (DoS) attack, in which a cloud resource providing a service is made unavailable to the intruder. In a DoS attack, the attack prevents patient health data from being uploaded to the cloud service and also makes it unable for medical professionals to extract the data through the IoMT scenario when they try.

4.2. Security Challenges

Conventional security mechanisms cannot fulfill and ensure IoMT security requirements; latest techniques are required to address the current challenges faced by IoMT. These challenges are as follows [43]:

4.2.1. Computational Limitation

IoMT health devices are integrated with slow processor units. The CPU of these devices has less power with respect to speed, and these devices are not made to execute computationally intensive operations. They are said to behave simply as an actuator or sensor. Henceforth, there is a requirement to find security countermeasures that reduce resource utilization while increasing the performance of security, which is a challenging task.

4.2.2. Energy Limitation

IoMT healthcare networks have typical tiny health sensors with restricted battery power. These devices save energy by switching to power-saving mode when not required or not in use, and also work on a low CPU speed.

4.2.3. Memory Limitation

Healthcare devices have less on-device memory, which is activated using an integrated operating system. Their memory may not be enough to perform complex security rules.

4.2.4. Scalability

IoMT devices have exponential growth, and therefore more and more gadgets are getting connected to the global data network. It becomes a challenging task to design an extremely scalable security method according to security requirements.

4.2.5. Mobility

Most of the time devices are not fixed at one place but are mobile in nature, depending on the user. These devices are connected to the network via an IoMT service provider. For example, a wearable is linked to the home internet when the person is at home, whereas it connects to a different network when the user is at the workplace. Different operating configurations and settings exist for different networks. As a result, implementing a mobility-compliant security mechanism is a major undertaking.

4.3. Threat Model

Due to the vast attack surface, IoMT devices and networks are susceptible to security attacks. Firstly, the threat framework extends across local networks, cloud networks and cloud services. Other systems have expanded interconnections among IoMT healthcare devices, cloud networks, cloud services and applications. The last one includes mechanisms venturing on hardware and software. There may be intrinsic as well as extrinsic threats originating, which may harm the network. The threat shows more severity if it arises within a proximal network from an IoMT device [44].

4.4. Attack Taxonomy

The IoMT model is growing rapidly to produce various supplementary IoMT devices and services that are

anticipated. Recent and upcoming IoMT healthcare sensors, devices and networks need to be protected from the venture of attackers, who may frame different kinds of security threats. These attacks may be physical, predictable and many more threats, which are difficult to anticipate [45].

5. Challenges of IoMT

In the healthcare sector, IoMT technology is widely used; therefore several challenges are required to be treated by healthcare researchers and organizations. Various research efforts are being made to treat many issues in the application and technology of IoMT. There are also some severe issues that need to be addressed. In this section, some of the important challenges such as standardization issues, interoperability of data, latency and energy efficiency are discussed below [46]:

5.1. Standardization Issues

In the last few years, there have been many merchants producing a wide range of products and gadgets, with new merchants also joining this race. As a result of increased competition and demand for more devices, they must adhere to all protocols for an interoperable interface and agreement across devices, which causes compatibility problems. There is a need for action to avoid device diversity. For this we require a committee that can standardize device and technology. There was a broad range of subjects like transmission layers, protocol status and also the data perception layer, information collection interface and sensor interface on which standardization should be considered. EHR is a valuable service and one of the major standardization issues.

5.2. Interoperability of Data

IoMT covers a vast range of disciplines as it extends into different areas with incompatible levels, where the problem of interoperability can arise. To get significant and medically applicable results, the data collected from several IoMT devices should be collected and assessed, or else it is of no use. To get maximum utilization of IoMT technology, it is crucial that almost every IoMT device is compatible with the others, permitting the transmission of information to all users utilizing the technology.

5.3. Latency

Network latency is a responsibility at the network layer and transmission layer in efficiently utilizing healthcare applications. The type of healthcare application is also a factor in latency. At the time of emergency services, for example real-time surgeries, latency in transmitting healthcare application data will have a severe effect. To overcome network latency, a fog-based IoMT healthcare structure helps decrease transmission latency by performing proximal data processing near the sensors instead of sending data to the cloud, which incurs further latency.

5.4. Energy Efficiency

Sensors are used to capture patient health parameters at the perception layer, which depends upon battery power. The reduction of battery power directly affects the check of sensor nodes; therefore, at the time of emergency healthcare, the function of the system is crucial. To overcome this drawback, robust WBAN is applied for healthcare, which uses solar energy as an alternative for battery power.

5.5. Infrastructure Costs

IoMT's long-term goal is to reduce the overall cost of healthcare, which is associated with creating the healthcare IT infrastructure, which is huge. The initial high investment is meant for developing hardware, IT infrastructure and cloud services, while the return on transaction is fixed, but the huge infrastructure behaves as a limitation to IoMT.

5.6. Quality of Services (QoS)

The IoMTNet healthcare system is extremely time-sensitive, which requires QoS assurance with respect to crucial parameters like maintainability, service level and reliability. In this context, the IoMTNet framework can be helpful if these parameters of quantitative scales are satisfied. In addition to this, robustness and system accessibility are essential in providing QoS assurance, because any kind of system adversity can put a patient's life at risk in a clinical environment.

5.7. Regulatory Challenges

A medical-grade clinical device requires permission and authorization from the statutory body to exist in the healthcare market. In front of legislators and regulatory authorities, IoMT devices can bring new threats as well.

6. Conclusion

This paper examines a novel direction for architecture and security of IoMT-based healthcare systems. It also demonstrates different healthcare frameworks and systems that support IoMT backend access and the ability to send and receive clinical data more easily. IoMT-based healthcare systems and technologies have received a lot of research and development attention. This study is beneficial to users who want to learn about various forms of IoMT and cloud networking in healthcare. It offers a full IoT and cloud computing system for healthcare that enables applications to use the IoT and cloud computing backbone, as well as a portal for medical data transfer between medical devices and cloud computing platforms. We then conduct a thorough investigation into cloud computing, especially fog computing, which includes standard architectures and current fog computing research in healthcare applications. Recent cloud-based data storage research was presented, demonstrating that the cloud is the best option for storing and organizing big data in healthcare. Many researchers have also shown that data processing throughout the network is substantially better than data acquisition on wearable devices with their restricted resources. In addition, the paper examines different threats, glitches, and attacks that must be considered, as well as evaluating and describing applicable security mechanisms in order to avoid security risks. The paper discusses security-related challenges and requirements, as well as various research issues in this field. Consequently, a consideration of several IoMT challenges that hamper the progress of IoMT-based health services, such as standardization, network provider, organizational structures, operational efficiency, and clinical data security, is required to help future studies on IoMT-based healthcare systems. In conclusion, the findings of this study could be beneficial to researchers and medical experts active in the sector of IoMT and health developments.

References

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

[2] A. Alabdulatif, I. Khalil, A.R.M. Forkan, and M. Atiquzzaman, "Real-time secure health surveillance for smarter health communities," *IEEE Communications Magazine*, vol. 57, no. 1, pp. 122–129, 2019.

[3] M.S. Rahman, N.C. Peeri, N. Shrestha, R. Zaki, U. Haque, and S.H.A. Hamid, "Defending against the novel coronavirus (COVID-19) outbreak: how can the internet of things (IoT) help to save the World?" *Health Policy and Technology*, 2020.

[4] F.T. Al-Dhief, et al., "A survey of voice pathology surveillance systems based on internet of things and machine learning algorithms," *IEEE Access*, vol. 8, pp. 64514–64533, 2020.

[5] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[6] A. Aldaej, "Enhancing Cyber Security in Modern Internet of Things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)," *IEEE Access*, 2019.

[7] R. Cao, Z. Tang, C. Liu, and B. Veeravalli, "A scalable multi cloud storage architecture for cloud-supported medical internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1641–1654, 2020.

[8] M. Aman, A.H. Yadegaridehkordi, Z.S. Attarbashi, R. Hassan, and Y. Park, "A survey on trend and classification of internet of things reviews," *IEEE Access*, vol. 8, pp. 111763–111782, 2020.

[9] M.H. Homei, E. Salwana, and S. Shamshirband, “An enhanced distributed data aggregation method in the internet of things,” *Sensors*, vol. 19, no. 14, 3173, 2019.

[10]S.M.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, and K. Kwak, “The internet of things for health care: a comprehensive survey,” *IEEE Access*, vol. 3, pp. 678–708, 2015.

[11]T.W. Tseng, C.T. Wu, and F. Lai, “Threat analysis for wearable health devices and environment monitoring internet of things integration system,” *IEEE Access*, vol. 7, pp. 144983–144994, 2019.

[12]K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, and T. Hayajneh, “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring,” *Journal of Medical Systems*, vol. 42, 130, 2018.

[13]T. Yaqoob, H. Abbas, and M. Atiquzzaman, “Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices – a review,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723–3768, 2019.

[14]Y. Miao, G. Wu, C. Liu, M.S. Hossain, and G. Muhammad, “Green cognitive body sensor network: architecture, energy harvesting, and smart clothing-based applications,” *IEEE Sensors Journal*, vol. 19, no. 19, pp. 8371–8378, 2019.

[15]Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, “IOT gateway: Bridging wireless sensor networks into Internet of Things,” in *Proc. IEEE/IFIP 8th Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Dec. 2010, pp. 347–352.

[16]I. Gronbaek, “Architecture for the Internet of Things (IoT): API and interconnect,” in *Proc. Int. Conf. Sensor Technol. Appl.*, Aug. 2008, pp. 802–807.

[17]H. Viswanathan, E.K. Lee, and D. Pompili, “Mobile grid computing for data- and patient-centric ubiquitous healthcare,” in *Proc. 1st IEEE Workshop Enabling Technol. Smartphone Internet Things (ETSIoT)*, Jun. 2012, pp. 36–41.

[18]W. Zhao, W. Chaowei, and Y. Nakahira, “Medical application on Internet of Things,” in *Proc. IET Int. Conf. Commun. Technol. Appl. (ICCTA)*, Oct. 2011, pp. 660–665.

[19]N. Yang, X. Zhao, and H. Zhang, “A non-contact health monitoring model based on the Internet of Things,” in *Proc. 8th Int. Conf. Natural Comput. (ICNC)*, May 2012, pp. 506–510.

[20]R.S.H. Istepanian, “The potential of Internet of Things (IoT) for assisted living applications,” in *Proc. IET Seminar Assist. Living*, Apr. 2011, pp. 1–40.

[21]M. Ahmad, M.B. Amin, S. Hussain, B.H. Kang, T. Cheong, and S. Lee, “Health Fog: A novel framework for health and wellness applications,” *Journal of Supercomputing*, vol. 72, pp. 3677–3695, 2016.

[22]C. Doukas and I. Maglogiannis, “Bringing IoT and cloud computing towards pervasive healthcare,” in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2012, pp. 922–926.

[23]P. Sethi and S.R. Sarangi, “Internet of Things: Architectures Protocols, and Applications,” *Journal of Electrical and Computer Engineering*, vol. 2017, Jan. 2017.

[24]L.A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, “Mobile cloud computing model and big data analysis for healthcare applications,” *IEEE Access*, vol. 4, pp. 6171–6180, 2016.

[25]N. Sultan, “Making use of cloud computing for healthcare provision: Opportunities and challenges,” *International Journal of Information Management*, vol. 34, no. 2, pp. 177–184, Apr. 2014.

[26]A. Darwish, A.E. Hassanien, M. Elhoseny, A.K. Sangaiah, and K. Muhammad, “The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–16, 2017.

[27]B. Negash, T.N. Gia, A. Anzanpour, I. Azimi, M. Jiang, T. Westerlund, A.M. Rahmani, P. Liljeberg, and H. Tenhunen, “Leveraging fog computing for healthcare IoT,” in *Fog Computing in the Internet of Things*, Springer, Berlin/Heidelberg, Germany, pp. 145–169, 2018.

[28]P. Hu, S. Dhelim, H. Ning, and T. Qiu, “Survey on fog computing: Architecture, key technologies, applications and open issues,” *Journal of Network and Computer Applications*, vol. 98, pp. 27–42, 2017.

[29]C.S. Nandyala and H.K. Kim, “From cloud to fog and IoT-based real-time U-healthcare monitoring for smart homes and hospitals,” *International Journal of Smart Home*, vol. 10, pp. 187–196, 2016.

[30]X.M. Zhang and N. Zhang, “An open, secure and flexible platform based on Internet of Things and cloud computing for ambient aiding living and telemedicine,” 2011.

[31]M.M. Noor and W.H. Hassan, “Current research on internet of things (IoT) security: a survey,”

Computer Networks, vol. 148, pp. 283–294, 2019.

[32]P. Verma and S.K. Sood, "Fog Assisted-IoT Enabled Patient Health Monitoring in Smart Homes," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1789–1796, 2018.

[33]T. Aziz and E. Haq, "Security Challenges Facing IoT Layers and Its Protective Measures," *International Journal of Computer Applications*, vol. 179, no. 27, pp. 31–35, 2018.

[34]G. Bouloukakis, et al., "Automated Synthesis of Mediators for Middleware-Layer Protocol Interoperability in The IoT," *Future Generation Computer Systems*, vol. 101, pp. 1271–1294, 2019.

[35]S. Mendhurwar and R. Mishra, "Integration of Social and IoT Technologies: Architectural Framework for Digital Transformation and Cyber Security Challenges," *Enterprise Information Systems*, pp. 1–20, 2019.

[36]I. Lee and K. Lee, "The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[37]J. Miranda, J. Cabral, S.R. Wagner, C. Fischer Pedersen, B. Ravelo, M. Memon, and M. Mathiesen, "An open platform for seamless sensor support in healthcare for the internet of things," *Sensors*, vol. 16, 2089, 2016.

[38]M. Ali, H.S.M. Bilal, M.A. Razzaq, J. Khan, S. Lee, M. Idris, M. Aazam, T. Choi, S.C. Han, and S. Kang, "IoT-based flipped learning platform for medical education," *Digital Communications and Networks*, vol. 3, pp. 188–194, 2017.

[39]P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[40]P. Palandrani, "How Cybersecurity Will Accelerate IoT's Growth," 2020. [Online]. Available: https://www.globalxetfs.com/how-cybersecurity-will-accelerate-iots-growth.

[41]J.P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, and E. Yaacoub, et al., "Securing internet of medical things systems: limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, pp. 581–606, 2020.

[42]A.K. Das and S. Zeadally, "Data security in the smart grid environment," in *Pathways to a Smarter Power System*, A. Taskaraoglu and O. Erdinc, Eds. New York, NY, USA: Academic, ch. 13, pp. 371–395, 2019.

[43]A.K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Generation Computer Systems*, vol. 89, pp. 110–125, Dec. 2018.

[44]T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "Ube-Health: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities," *IEEE Access*, vol. 6, pp. 32258– 32285, 2018.

[45]S. Jabbar, F. Ullah, S. Khalid, M. Khan, and K. Han, "Semantic Interoperability in Heterogeneous IoT Infrastructure for Healthcare," *Wireless Communications and Mobile Computing*, vol. 2017, pp. 1–10, 2017.

[46]P.S. Suryateja, "Threats and Vulnerabilities of Cloud Computing: A Review," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 3, pp. 297–302, 2018.