Internet of Medical Things (IoMT) for Remote Healthcare Monitoring Using Wearable Sensors

S M Nazmuz Sakib

Graduate of BSc in Business Studies, School of Business And Trade, Pilatusstrasse 6003, 6003 Luzern, Switzerland.
Graduate of LLB (Hon's), Faculty of Law, Dhaka International University, Satarkul Rd, Dhaka 1212.
Graduate of MBA (Human Resources), International MBA Institute, Samstagernstrasse 57, 8832 Wollerau Switzerland.
Phone: +41 78 946 88 86.
sakibpedia@gmail.com

***Abstract*:** In the healthcare industry, the most recent innovations and developments in communication and informational technique play a critical role. These developments paved the mode for the IoMT (Internet of Medical Things), which allows for persistent, distant, and genuine patient monitoring. The capacity, connectivity protocols, big data and volume of data, adaptability, durability, data processing, data acquisition system, data handling, and analytics accessibility, economic viability, privacy and security, and power efficiency are all problems that IoMT architectures confront. The basic aim of his research is to employ remote health monitoring (RHM) and IoMT to identify health monitor easy approach to improve medical residing conditions. Moreover, the use of IoMT and Medical knowledge RHM to strengthen the protection, diagnosis, prognosis, and therapeutic capacities of the Internet of medical things is addressed. The IoMT (Internet of Medical Things) involves a network of health care devices and individuals that exchange medical data via wireless communications. With the rising expansion of the population and the use of advanced technology, medical expenses and medical cost has significantly increased. The coupling of IoMT with medical healthcare has the potential to increase people's lives, deliver effective medical therapy, and establish pocket-friendly approaches. This study discusses the current state of IoT in the medical business, as well as plans for development and innovation strategies and implementations. The adoption of IoT in the medical sector has evolved worldwide, but it still encounters numerous architectural and technological hurdles. To find a solution to the mentioned problems, current research illustrates a basic IoMT design that comprises 3 foundational pillars: data gathering, connection gateways, and servers/cloud. Ultimately, this article examined the possibilities and potential of IoMT in practice, as well as the associated remarkable research concern.

Keywords --- IoMT (Internet of Medical Things), remote health monitoring (RHM), medical, sensor.

1. INTRODUCTION

In the modern era, healthcare and advanced technology industries (Chen, 2020; Gupta et al., 2020b) have captured significant attraction in daily life routines including healthcare setups (Rodrigues et al., 2018). The basic aim is to amalgamating healthcare setups with technology is to facilitate people with a remarkable interfacing capacity between caregivers and patients for the betterment of the accessibility and efficiency of devices of medical importance and various services (Firouzi et al., 2018; Gatouillat et al., 2018). The IoMT, nowadays, is known as medical IoT. IoMT is described as a group of aesculapian devices and utilizations linked by employing various networks. IoMT can also be used for all devices of medical importance and software that are efficiently linked with the help of computers to healthcare information technology setups. A number of healthcare services employ IoMT software for the optimization of treatment, and management of illnesses, to lessen delays, increased the encountering of patients, management of medications, and alleviate costs. The IoMT retail market is expected to hit $117 billion by the start of 2020, as researched by market researchers (Abd-El-Atty et al., 2020).

The medical IoT relies on information technology software to help medical devices communicate with one another; examples of such applications are health-associated devices and medical tracking gadgets between others. Patients can use their mobile phones with Internet connectivity to convey medical data in real-time using such devices. Patients with diabetes and cardiovascular diseases are considered eligible to use mobile apps to check their health and submit findings to their doctors. Infirmaries employ these machines to provide healthcare while avoiding medical visits to the client's home.

Architecture for IoMT

The architecture for medical IoTs comprise of three main layers. These three layers are (i) things layer, (ii) fog layer, and (iii) cloud layer. This is a unique category of architecture. In this structure, healthcare researchers can also collaborate directly via router among the Thing layer and Fog layer and by the general processing servers outside of the fog layer. Each layer is illustrated below:

The things layer comprises patient sensors, monitoring devices, medical records, actuators, nutrition regimen generators and pharmacy controls, etc. The thing layer is directly linked with the ecosystem users. The data gathered by the elements such as remote care data, patient-monitoring data, and wearables is accumulated at top of this layer. The usage of these devices must be securely kept to make sure the integrity of the collection of data. Local routers of the ecosystem are the main reason for linking such kinds of devices with the fog layer. The data is again processed at the fog layer as well as the cloud layer to evolve significant knowledge. Moreover, for the alleviation the delay, experts in healthcare can also acquire the patient information with the help of this router.

The fog layer works between the things layer and the cloud layer. This layer consists of gateway devices and general servers for an evenly distributed fog framework of networking. The general processing potential is saddled with the help of lower layer gadgets for the response in real-time their employers. Such kind of servers are often used to monitor and maintain the system's confidentiality and reliability. This layer's gateway appliances are in charge of routing data from these servers to the cloud layer for some further assessment. Furthermore, healthcare professionals can access patient data using this router to decrease delays.

The cloud layer is made up of computing resources and data storage for analyzing data and generating decision-making processes from it. The cloud also has a broad reach, allowing large medical and healthcare organizations to easily manage their day-to-day operational activities. This layer is made up of cloud systems where the data created by the medical technology will be kept and diagnostic work can be done as needed in the future.

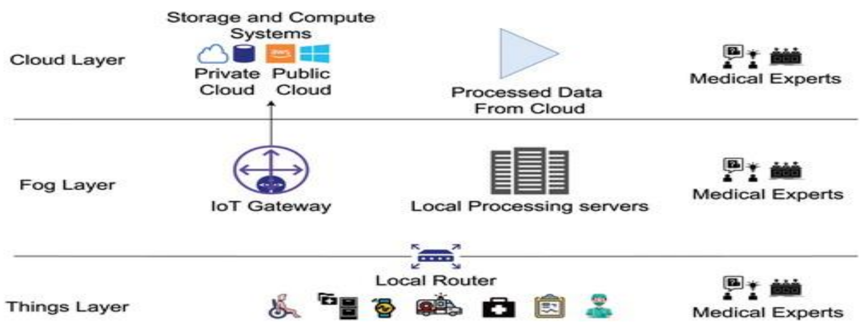

Figure 1. Three layers of IoMT

Currently, IoMT (Internet of Medical Things) (Joyia et al., 2017; Haoyu et al., 2019) played a significant role in remote healthcare monitoring (RHM) [12, 13]. The internet of medical things is employed for the collection of remote information for patient with the help of wearable devices /sensors [14] and keep them in the form of cloud databases. Such kind of informational data is made available for analysis of real time and utilizations by caregivers. The internet of medical things (IoMT) possess three basic stages: Fog layer, device layer and cloud service (Mihovska and Sarkar, 2018; Mallikarjuna and Arun Kumar Reddy, 2019) as shown in Figure 1.

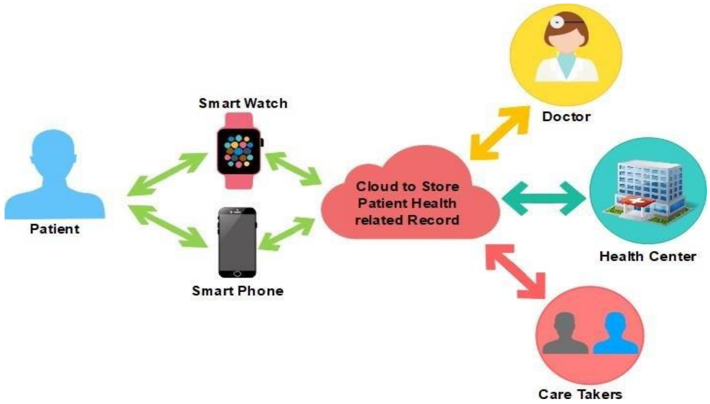

Figure 2. Architecture of IoMT

The basic aim of this device layer (sensing layer) is to maintain an efficient and reliable sensing technology to gather many types of health-oriented information (Qi et al., 2017; AlShorman and Alshorman, 2020). Network services and facilities for the IoMT framework are supported by communication techniques (Mutlag et al., 2019; AlShorman et al., 2020). Nevertheless, communication technologies possess RFID, Bluetooth, WI-FI, UWB, ZIGBEE and IrDA (Mutlag et al., 2019). In the data layer (cloud layer) (Karaca et al., 2019), the data is efficiently progressed and preserved (Farahani et al., 2020). Also, cloud acquire data of patient for the analysis, filtering and storing. By this way, data is supplied for caregivers (Karthick and Pankajavalli, 2020). RHM (Noah et al., 2018; Al-Khafajiy et al., 2019) is a persistant monitoring procedure of the data regarding health care. It comprises: physiologically important monitoring for example temperature, heart rate, physically important evaluation, blood pressure, medical tracking, behavioral evaluation and diet monitoring. The data regarding to health care are wirelessly linked to both the caregivers and patient vi cloud (Benjemmaa et al., 2019). So, Internet of Medical Things (IoMT) favours reliable, real-time, rapid and remote diagnostic evaluation of many types of ailments and increases the decisional processes. By this process, massive amount of data is acquired, processed and evaluated (Depari et al., 2019).

With today's hectic lifestyles, the majority of the population neglect to undergo their routine health screenings. Furthermore, the expense of healthcare is mounting, and state spends a significant amount of expenses on medical care each year. Citizens in Europe and the USA also favour home healthcare than going to hospitals. To solve all of these issues, there is a vital need for distant real-time healthcare surveillance. Wearable sensors and devices that provide continual assessment for sufferers and the older have gotten a lot of interest (Hassanien et al., 2018; Firouzi et al., 2022). The purpose is to provide significant sign assessment, such as temperature, heart rate and blood pressure, which is crucial in modern healthcare environment. In 2014, the WHO (World Health Organization) estimated that 422 million people suffered from type 2 diabetes (T2D). This means that 8.5 percent of the adult population have diabetes. Nevertheless, the WHO estimates that by 2030, the number would have risen to 500 million (Cappon et al., 2017). So, employing RHM can minimize the risk for the people who are more fragile to capture the data of medical importance and deliver this data to the caregivers (AbdulGhaffar et al., 2020). RHM applications include the following (Alfian et al., 2018; Gupta et al., 2020a) Diagnosing ailments

1) Diagnosing diseases

2) Morbidity administration

3) Ailment forcasting

4) Abnormality prediction

5) Inhibition of morbidity

6) Giving the well suited medical treatments and Rehabilitation

As the quantity of IoMT-connected devices grows, ensuring strong security and secrecy becomes more difficult. Privacy and security in the healthcare sector are a difficult subject that continues to worsen as the use of medical devices (MT) becomes more wide spread. Because of the relevance and accessibility of the information in the healthcare domain, the privacy and security of the IoMT require problems to be further complicated. The absence of adequate privacy and security in IoMT will not only compromise client privacy, but it may even endanger patients' existence. As a result, in IoMT, medical informational security is critical.

The basic role of the research is to increase the medical based living services employing IoMT. Patients with some diseases like diabetes require 24/7 critical monitoring (Michaud et al., 2018) which can be efficiently gained with the measurement the level of blood glucose implementing wearable sensors (Usman et al., 2018; AlShorman et al., 2020). The research papers use the IoT and the remarkable informational data analytics for medical applications with the help of cloud evaluation to monitor the sick people in remote areas and give them timely recommendations that could help them to become able for the improvement the medical status.

The paper is provided with the 2. Related researches on the incorporation of the giant data critics and the IoT (internet of things) in medical sector, with their capabilities as well as limitations. 3. Suggested work on IoT and the big data evaluations for medical sector with the help of cloud computing, 4. Results and discussion. 5. Conclusion.

2. LITERATURE REVIEW

The study by Russom et al [1] is all about a research on the development of large amounts of data from many disciplines, as well as the "current and future analytics that may be implemented to the large set of data." [2] Gandomi et al. "The study analyses the fundamental aspects regarding big data and provides a summary of the key elements of big data, as well as the measurements that provide the amount and characteristics of big data, as well as the existing technologies to connect the capability of big data," according to the paper. The writer, Sun et al [3,] elaborates on the growth of smart and big analytics of data and guarantees that smart analytics of big data will lead to improved management, strategic planning, arranging, and regulating. Raghupathi and his colleagues [4] The paper "explains the prospects and promise of big data analytics while also explaining the benefits, design structure, methods, problems, and constraints." Frost and his colleagues [5] The author emphasizes the importance of big data in reducing the intricacies of technology while also lowering costs in the Gill, et al. [6] In this study, the author discusses the use of big data in health care innovation. The research by Sabharwal et al [7] highlights "the critical significance of big data analytics in strengthening person's medical problems and averting serious concerns when handled intelligently." Manogaran et al [8]" the author describes an innovative infrastructure that combines internet of things and big data to provide a reliable national healthcare monitoring and modifying setup." Sun et al [9] propose the "idea of smartly integrated communities by merging internet of things and big data analytics," as per the research. The author of Thota et al [10] proposes a medical wellness setup that incorporate the internet of things and cloud computing, as well as a central fog networking system for securing the services provided. Dubey and colleagues [11] Yassine et al [12], Yassine et al [12], The author of the research, Suma, V et al [13], claims that combining IOT with big data will facilitate excellent decision making, as well as careful planning, coordinating, guiding, controlling, and regulating, hence reducing the use of undesirable raw resources in the company and attempting to make it more sustainable.

(crypto stegno) IoMT is frequently used for tele-healthcare in the contemporary time (Abd-El-Atty et al., 2020).

The health cloud in IoMT may send data to multiple nodes over wireless channel. Despite the fact that IoMTs are the ideal medical system, healthcare IoT devices carry particularly sensitive patient records, hence safe IoMT connection is required (Abd-El-Atty et al., 2020). The ultralight identity-based cryptography (IBE-Lite) technique promises to give availability while maintaining privacy and security. Nonetheless, their technique takes into account a variety of privacy and security risks, as well as concerns. Alarm-net is a smart home automation framework built on the inquiry protocol (Kazeem Moses et al., 2021). This approach was not only subject to adversarial security assaults, which may reveal the whereabouts of the occupant. On the other hand, because it costs a great deal of energy, defensive approach takes longer to accomplish. The BSN-care platform (Abd-El-Atty et al., 2020) provides proper healthcare solutions for medical monitoring. Because external keys have been used, it actually takes extra cycles to generate random keys. The methods for IoMT outlined, use external keys to protect medical data. The basic guidelines of watermarks are explained with as much detail as feasible. In the subsequent, (Abd-El-Atty et al., 2020) gave the concept of watermarking, the functions provided by watermarking, and the criteria and assessment measurements for watermarking systems. Data steganography is an approach for concealing data, such as a coded data, together within a piece of data, such as a cover carrier. It is regarded as a component of data security. Audio steganography is a sort of data steganography in which the confidential message is encoded in sound. Nassrullah, et al., (1988) present an improved LSB-based audio steganography algorithm. By utilizing all messenger data and optimizing the hiding capability and distorting ratio, the suggested approach improves steganography effectiveness.

The employement of the internet to share confidential material is increasing dramatically in this contemporary period. Transmission on the internet, on the other hand, is unreliable and unpredictable. Privacy preservation techniques have been suggested to strengthen the secrecy and security of confidential material as a result of these issues. In addition, Crandler et al.,2017 proposed Code Dependent Steganography, which combines steganography and computer programming (Molaei et al., 2017). It used linear passwords to enforce matrix encoding to improve the graphical significance of the stego image while maintaining high throughput. Molaei et al., (2017) presented a steganography system that used Reed Muller codes and the modulus factor to improve embedding characteristics.

Cyberattacks and confidentiality issues in IoT were explored by Yaqoob et al., (2018). The research proposes a systematic classification by analyzing and evaluating the content in light of essential criteria (e.g., threats, requirements, IEEE norms, sending level, and progression). A few explicit situational studies were also conducted to alert persons about how truly impotent IoT devices are against risks. Several underlying current research challenges were highlighted and addressed in this paper (e.g. data integrity, flexibility and ensure a safe environment, the absence of customization of security programming, fixing of capacity spotlights, and realistic assurance of billions of computers, trustworthiness) (Abd-El-Atty et al., 2020).

Lakshmanaprabu et al., (2018) proposed a multi-level architecture that included the mining of massive data in SIoT using a map-reduced system and a focused classifications monitor. In this regard, a Gabor layer was employed to limit the disruption and disagreeable data from the database, while Hadoop MapReduce was also employed to retrace and decrease big volumes and increase the effectiveness of the new job. Furthermore, the percentage assessment was performed in a different sample group using elephant herds modeling. The proposed architectural system was built utilizing a responsive support vector device dependant to arrange the trends and evaluate the efficacy of the suggested study (Lakshmanaprabu et al., 2018) .

To enhance the safety and excellence of the pictures, Shankar et al., (2017) used symmetric encryption cryptographic techniques. This unique concept was utilized to generate several offers that were linked to elliptic curve cryptography algorithms for encoding and decoding. The mean transceiver ratio is 58.0025, the average - squared blunder prediction is 0.1164, and the association coefficient is 1 for the unencrypted image all with no stretching of the first image, according to the experimental data.

Mahmoud et al., (2018) proposed CoT methodologies and stages of investigations, as well as the application of CoT in the wonderful sector of medicine. As a result, the study confirms numerous key CoT complaints, including a shortage of centralization. It highlights the importance of dynamism when examining the relevant and viable propositions found in the literature from both internal and external perspectives. An evaluation of nearly all the energy generation methods described in this paper indicates that their potential effectiveness needs to be bolstered, specifically regarding quality of service and efficiency (Mahmoud et al., 2018).

One of the most basic prerequisites for individuals to have a better life is health. In any region, improving medical care facilities can enhance person,s quality of life. Numerous medical service staff have recently approved IoT automation to advance medical care processes, enhance transmission of information between individuals, reduce process flaws, regulate drugs and control illnesses, cut costs, and ultimately improve the competency and efficiency of medical processes (Sun et al., 2018). Nevertheless, the rapid proliferation of connected devices and the vast amount of sensory data generated by these devices have created new challenges in terms of information security and privacy. Cyber threats have evolved alongside the rapid adoption of the Internet of Things (IoT), introducing a new avenue for intrusion and risk for the entire healthcare industry. Numerous studies have investigated the various privacy and security vulnerabilities inherent in IoT systems, as well as device vulnerabilities in cloud and fog computing environments related to IoT-based healthcare devices. Privacy and security of patient data are two critical considerations. When we discuss data security, we refer to the secure storage and transmission of data to maintain its integrity, authenticity, and validity. Data privacy, on the other hand, ensures that sensitive information can only be accessed and utilized by authorized individuals. By considering different objectives and requirements, more practical security solutions can be developed. While the widespread use of IoT in healthcare (IoMT) devices enhances patient care, it also places a high demand on data privacy and security (Mutlag et al., 2019).

Table 1. A tabular overview of the surveyed research study.

Topic	Year	Features	Limitations	Results	References
Patient health monitoring	2019	Distant evaluation, emergency alert strategy, KNN categorizer	Costly computation for remarkable informational data sets	98.02% precision on test kit	(Priyadharsan *et al.*, 2019)
IoT based Patient Monitoring [46]	2017	Module for assessing stroke influenced older people, group classifiers	Vitals evaluation restricts stroke prediction precision	Free Forest group classifier acquired	(Ani *et al.*, 2017)
Wearable IoT Enabled Monitoring	2018	distant evaluation pattern in the absence of a gateway	Detectors limit the computation, Diminished quantitative outputs	A portable LCD and RFID reader might be employed as a gateway alternative	(Wan *et al.*, 2018)
Medical IoT-based	2018	Vital potential effectiveness algorithm	No smart decision or prototype forming module	Practically summarized that EEOOA performs in a good way than conventional algorithms	(Pirbhulal *et al.*, 2018)
Novel IoT-based Health Monitoring	2017	Portable system monitoring body fat and heart rate.	No ML approach utilized, no alert system No detection model	Well-established for a physician to observe the person's informational data	(Pereira and Nagapriya, 2017)
IoT based system	2019	Evaluation of a		Cost effective	(Wai *et al.*,

using NodeMCU		large number of physical signs		strategy for solving heart abnormalities	2019)
Edge Cognitive Computing	2018	Health care sector for assessing crucial states as well as emergencies	Absence of prototype	Cognitive analysis employed to establish computing potential to enhance efficacy	(Chen *et al.*, 2018)
IoT based Emergency System	2020	Significant evaluation, data approachable to medical personels	Limited ways to efficiently cope with an emergency	Experts can evaluate, diagnose and suggest individuals distantly	(Ruman *et al.*, 2020)
IoT based Wearable47	2018	Wearable setups to detect vitals & note any abnormality	Restricted sensor information	Decision making employed via threshold factors	(Wan *et al.*, 2018)
Development of Smart Healthcare System	2020	Assessing patient vitals & social conditions	Massive, no ML approach or alert setup	95% accuracy is obtained between actual and observed data	(Islam and Rahaman, 2020)
Multi parameter Patient	2020	Prototype to forecast individual's health condition,	Absence of any webpage for observing trends of data	95% classification precision	(Athira *et al.*, 2020)
System with Nested Cloud	2018	Cardiac abnormality detection system with cloud security, SVM classifier	Lack of quantified outputs or precision	Patient privacy enhanced by privacy algorithm	(Kamble and Bhutad, 2018)

3. COMPARATIVE ANALYSIS

A brief description of comparative analysis of the concerned work is shown in Table 1 with the suggested work. There are a large number of studies (Mohan et al., 2019) on machine comprehension that have been utilized for a large number of medical application such as heart diseases and diabetes. Nevertheless, some studies are present (Nourmohammadi-Khiarak et al., 2020) which significantly employ hybrid metaheuristic technologies. A division of algorithms applied for optimization is given in table.

Table 2. Empirical analysis of various methods and approaches

S.N.	Authors	Use of IoT Device	Mobility	Methodology	Approach	Accuracy	References
1	Al-Makhadmeh	yes	No	Cloud dependent IoT wearable	Higher order Boltzmann(HOB) with deep belief	99.03	(Al-Makhadmeh and Tolba, 2019)

				healthcare gadget	neural network (DNNN)		
2	Vivekanandan, T	No	No	Forecasting of cardiac anomaly	altered DE by using fuzzy AHP FFNN	83	(Vivekanandan and Iyengar, 2017)
3	Uyar,kaan	No	No	Point out a cardiac abnormality	GA oriented recurrent fuzzy platform	97.78	(Uyar and İlhan, 2017)
4	Ahmed, fizar	Yes	No	IoT detector depends cardiac rate sensing	k-approachable ‚ alogrithim	96	(Ahmed, 2017)
5	Nazari, somayeh	No	No	A decision based setup for cardiac anomaly	Fuzzy analytical approach	_	(Nazari *et al.*, 2018)
6	Mohan,S.	No	No	Prophesy of vascular and cardiac abnormality	Hybrid free forest with a simple pattern	88.7	(Mohan *et al.*, 2019)
7	Ali liaqat	No	No	A most likely detection approach architecture of suggestive cardiac abnormality	X2-statistical based pattern and DNN orientation	93.33	(Ali *et al.*, 2019)
8	Haq,amin U.	No	No	Collective smart pattern for the evaluation of cardiac abnormality	A collective smart system	89	(Haq *et al.*, 2018)
9	Nourmohammadi	No	No	Cardiac anomaly detection	ICA having meta heuristic process	94.03	(Nourmohammadi-Khiarak *et al.*, 2020)
10	Rao,MadhuSudana	No	No	collective disease detection	Multiple oriented optimization along with important characteristics	94.05	(Nalluri and Roy, 2017)
11	Proposed	Yes	Yes	IoMT cloud environment for cardiac abnormality prediction	Altered Salp swarm algorithm (SSA) standardization via ANFIS	99.45	

4. RESULTS AND DISCUSSION

Internet of medical things-based approaches have been established and applied in current years in health care sector and this is known as IoMT, however, there are some cases, in which data is preserved in the IoMT-oriented environment with the help of cloud preservation are open to a large number of cyber-attack methdologies to inscribe/recite data utilizing third parties. This is regarded as a remarkable security and privacy risk or limitations to the utilizations of IoMT-related techniques. This has efficiently attracted the modern researches by the implementations of steganography for the betterment of the security of image collaboration in the IoMT technique. A suggested technique is the implementation of IDEA ideology in contrast to steganography approach Matrix-XOR. The Matrix-XOR processes in graphical technique for employing instruction to a specific carrier medium, this transfers the stegano graphic picture having a good-quality entrenching efficacy, reliable security, and alleviated alteration aftermath. A method is suggested to privately deliver informational data in the IoMT-related ecosystem establish on cryptography and steganography approaches. This collective technique gains information security, complete assurance, efficacy, and durability that dipicts successful for the attainment of the approaches. The suggested scheme played excellent in comparison with current state-of-the-art systems, implying that it might be used as a reliable tool for strategic security and privacy of medical data on future IoMT-related knowledge. The suggested hybrid paradigm can be employed on video and audio IoMT-related healthcare information and data acquisition in the cloud in the future. Protection of public and private data and information in IoMT-related approaches are particularly crucial for medical pictures such as positron-emission tomography (PET), ultrasound, X-rays, magnetic resonance imaging (MRI) and radiology among others. Therefore, future utilizations needed to be more effective privacy algorithms to be employed like fully homomorphic encryption, Bcrypt and DNA encryption on cloud, thus increasing the security and privacy of IoMT-related setups. Moreover, massive studies that concentrates on IoMT-related approach security and privacy has implemented AES and RSA on both public and private informational data. In future research, machine learning technologies necessitates the further integration to resolve the issues regarding the constantly emerging and heterogeneous health care data inputs. The suggested research requires minimum time for both encryption as well as decryption processes, thereby facilitate in speedy information recapture form the Internet of medical things-based devices, thus concluding in a reliable as well as dynamic encryption, decryption, and embedding approaches.

5. CHALLENGES AND FUTURE TRENDS

This portion summarizes the challenges of the distant medical assessment of the patients by the usage of wearable detectors (Usman *et al.*, 2018). This comprises:

1) pocket friendly and non- obstructive detecting gadgets (Usman *et al.*, 2018): architecture and assess a non-obstructive sensing devices with reduced cost is a potential problem.

2) Data management [98] and big data issues (Rghioui *et al.*, 2020): big data generated from detecting gadgets in a brief period is difficult to preserve and control if the access to cloud is not available.

3) Privacy and safety(Garg *et al.*, 2020; Mohanty *et al.*, 2020): health care detecting data and electronic person documentation are vitally important and confidential. Although, it is vital to secure this data from vital internet risks.

4) Unrestrained surroundings [103] and Noise impede (De Sarkar *et al.*, 2020): several noise stages can occur.

5) Wireless technique (Pratap *et al.*, 2019; Manjula and Thalapathi Rajasekaran, 2020): No wireless technique and connections parameters for IoT.

6) Accessability and availability (De Sarkar *et al.*, 2020) : various interlinked gadgets, services, networks and consumers are linked that leads to boost the rate of failure.

7) Power planning (Bhardwaj *et al.*, 2019): real period continuous detecting uses the energy.

8) Excellent and smart algorithms utilized for data management uses significant and vast training data. although, laboratory datasets are presented datasets (Schueler *et al.*, 2019).

9) Emerging smart characteristics extraction and categorization algorithms require more computational time period (Stavrinides and Karatza, 2019).

10) Validity and accuracy (Siris *et al.*, 2019): generate healthcare precise devices, modes, algorithms, services is potentially in demand.

11) Wearable sensors adjustment and consumer security (Gaggi *et al.*, 2020): placement of detector and location security problems are key characters in architecture.

12) One sensor modality: data gathering body sensor technologies are to proposed more (Muzammal *et al.*, 2020).

13) Measurements of the wearbale sensing devices should be feasible (Antolín *et al.*, 2017).

14) Wearable gadgets should must be easy to handle (Haghi *et al.*, 2017).

15) Wearable devices should be secured from sweat and water incorporation of several devices and protocols (Panarello *et al.*, 2018; Shah and Bhat, 2020).

6. CONCLUSION

This report provides a comprehensive evaluation of various publications on remote and smart healthcare monitoring systems. The most recent state-of-the-art work in the field of e-healthcare has been reviewed. An assessment of many wearable and non-wearable detectors has been presented in this paper, with a focus on monitoring potential signs such as high blood pressure and high oxygen levels. A comprehensive analysis of various device learning methods used in current health assessment system study is presented. The condition of health status is defined using algorithms of machine learning. Any systems analyst should investigate several machine learning samples and perform comparison their results because they will or will not work for their purpose. Because no single machine learning algorithm usually works excellently for every distant medical setup, it is really critical to figure out which algorithm has the best validity and attributes for a certain architecture. Furthermore, contemporary works that use cloud technology for data retention are evaluated. The significance of the cloud in either IoT-based platform, particularly in medical, is also underscored. In e-healthcare systems, a cloud-based architecture is critical for massive data preservation and data analytics. Various studies have also suggested that a cloud system's high computing capabilities can yield much better data processing than wearable gadgets' along with their limited processing ability. To boost the platform's standard of srvice, bigger activities, such as building machine learning algorithms on archival data, are sent to cloud platforms. But, these studies also highlight the cloud platform's inherent security issues, with many papers proposing light encryption measures as a solution. Finally, this research looked at the Edge computing system as it relates to IoT setups and found that it has a significant influence. Edge computing is not just to increases sustainability by lowering reaction times, but it also provides a variety of other complicated features including data preprocessing, data filtering, data confidentiality of consumer, power preservation, and a local database. Regional judgment modules that inform patients and families in the event of an irregularity can also be utilized edge or fog computing. The machine learning and edge computing features of IoT-depandant smart medical have the most substantial influence, as well as the most space for developments and innovations, according to the extensive literature review. The cloud platform's safety vulnerabilities are also being addressed in terms of bringing it into compliance with medical systems. Edge computing and machine learning are the most significant parts of IoT-based smart healthcare setups, and they are also the least investigated. New scholars are encouraged to develop these elements in order to help the ever-increasing community. As a result, it can be stated that IoMT enables improved real-time establishment of chronic illnesses at a reduced cost, boosts patient and geriatric health wellness programs, and improves the quality of treatment.

7. PERSONAL RECOMMENDATIONS

Internet of medical things (IoMT) in different diseases like heart attacks, diabetes and COVID-19 pandemic regarding technology establishment, possibilities and adoption and illustrates privacy issues linked with IoMT in daily life routine. In pandemic period, a large number of IoMT approaches have been employed particularly to trace and track diseased people as digital inspection, and this has ultimately driven to some issues related to privacy and this issue is needed to be resolve effective to ensure the public safety and security. The other major concern that is needed to be resolve is, the same privacy constraints in internet of medical things would employ to IoMT approaches, but since IoMT gadgets infect human lives, so concerns evolve. However, there are continuous developments in the domain of IoMT privacy have been illustrated broadly, comprising of research based on novel techniques like block chain to minimize privacy concerns for humans as well systems. However, hybrid approaches should be continuously established in the future, consolidating information gathered from the blocks of data mining, artificial intelligence, IoMT-related technologies and giant data evaluations for more accurate and effective solutions in forecasting, automation and simulation. Furthermore, it would also be beneficial if such kind of IoMT approaches possessed privacy as one of major goal in their architecture, thus making sure an increased degree of privacy and safety for mankind.

REFERENCES

[1]. Abd-El-Atty, B., A.M. Iliyasu, H. Alaskar, A. El-Latif and A. Ahmed. 2020. A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. Sensors. 20:3108.

[2]. AbdulGhaffar, A., S.M. Mostafa, A. Alsaleh, T. Sheltami and E.M. Shakshuki. 2020. Internet of things based multiple disease monitoring and health improvement system. J. Ambient Intell. Humaniz. Comput. 11:1021–1029.

[3]. Ahmed, F. 2017. An Internet of Things (IoT) application for predicting the quantity of future heart attack patients. Int. J. Comput. Appl. 164:36–40.

[4]. Al-Khafajiy, M., T. Baker, C. Chalmers, M. Asim, H. Kolivand, M. Fahim and A. Waraich. 2019. Remote health monitoring of elderly through wearable sensors. Multimed. Tools Appl. 78:24681–24706.

[5]. Al-Makhadmeh, Z. and A. Tolba. 2019. Utilizing IoT wearable medical device for heart disease prediction using higher order Boltzmann model: A classification approach. Measurement. 147:106815.

[6]. Alfian, G., M. Syafrudin, M.F. Ijaz, M.A. Syaekhoni, N.L. Fitriyani and J. Rhee. 2018. A personalized healthcare monitoring system for diabetic patients by utilizing BLE-based sensors and real-time data processing. Sensors. 18:2183.

[7]. Ali, L., A. Rahman, A. Khan, M. Zhou, A. Javeed and J.A. Khan. 2019. An automated diagnostic system for heart disease prediction based on ${\chi^{2}}$ statistical model and optimally configured deep neural network. IEEE Access. 7:34938–34945.

[8]. AlShorman, O., B. AlShorman, M. Alkhassaweneh and F. Alkahtani. 2020. A review of internet of medical things (IoMT)–based remote health monitoring through wearable sensors: A case study for diabetic patients. Indones. J. Electr. Eng. Comput. Sci. 20:414–422.

[9]. AlShorman, O.M. and A.M. Alshorman. 2020. Frontal lobe and long-term memory retrieval analysis during pre-learning stress using EEG signals. Bull. Electr. Eng. Informatics. 9:141–145.

[10]. Ani, R., S. Krishna, N. Anju, M.S. Aslam and O.S. Deepa. 2017. Iot based patient monitoring and diagnostic prediction tool using ensemble classifier. In: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, 1588–1593.

[11]. Antolín, D., N. Medrano, B. Calvo and F. Pérez. 2017. A wearable wireless sensor network for indoor smart environment monitoring in safety applications. Sensors. 17:365.

[12]. Athira, A., T.D. Devika and K.R. Varsha. 2020. Design and development of IOT based multi-parameter patient monitoring system. In: 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 862–866.

[13]. Benjemmaa, A., H. Ltifi and M. Ben Ayed. 2019. Design of remote heart monitoring system for cardiac patients. In: International Conference on Advanced Information Networking and Applications, Springer, 963–976.

[14]. Bhardwaj, K.K., A. Khanna, D.K. Sharma and A. Chhabra. 2019. Designing energy-efficient IoT-based intelligent transport system: need, architecture, characteristics, challenges, and applications. In: Energy Conservation for IoT Devices, Springer, 209–233.

[15]. Cappon, G., G. Acciaroli, M. Vettoretti, A. Facchinetti and G. Sparacino. 2017. Wearable continuous glucose monitoring sensors: a revolution in diabetes treatment. Electronics. 6:65.

[16]. Chen, E.T. 2020. Examining the influence of information technology on modern health care. In: Data Analytics in Medicine: Concepts, Methodologies, Tools, and Applications, IGI Global, 1943–1962.

[17]. Chen, M., W. Li, Y. Hao, Y. Qian and I. Humar. 2018. Edge cognitive computing based smart healthcare system. Futur. Gener. Comput. Syst. 86:403–411.

[18]. Depari, A., D. Fernandes Carvalho, P. Bellagente, P. Ferrari, E. Sisinni, A. Flammini and A. Padovani. 2019. An IoT based architecture for enhancing the effectiveness of prototype medical instruments applied to neurodegenerative disease diagnosis. Sensors. 19:1564.

[19]. Farahani, B., M. Barzegari, F.S. Aliee and K.A. Shaik. 2020. Towards collaborative intelligent IoT eHealth: From device to fog, and cloud. Microprocess. Microsyst. 72:102938.

[20]. Firouzi, F., B. Farahani and A. Marinšek. 2022. The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). Inf. Syst. 107:101840.

[21]. Firouzi, F., A.M. Rahmani, K. Mankodiya, M. Badaroglu, G. V Merrett, P. Wong and B. Farahani. 2018. Internet-of-Things and big data for smarter healthcare: From device to architecture, applications and analytics. Futur. Gener. Comput. Syst. 78:583–586.

[22]. Gaggi, O., A. Kolasinska, C.E. Palazzi and G. Quadrio. 2020. Safety first? users' perception of wearable sensor networks for aging. Mob. Networks Appl. 25:986–994.

[23]. Garg, S., K. Kaur, S. Batra, G. Kaddoum, N. Kumar and A. Boukerche. 2020. A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications. Futur. Gener. Comput. Syst. 104:105–118.

[24]. Gatouillat, A., Y. Badr, B. Massot and E. Sejdić. 2018. Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine. IEEE Internet Things J. 5:3810–3822.

[25]. Gupta, D., A. Parikh and R. Swarnalatha. 2020a. Integrated healthcare monitoring device for obese adults using internet of things (IoT). Int. J. Electr. Comput. Eng. 10.

[26]. Gupta, S., L. Goel and A.K. Agarwal. 2020b. Technologies in health care domain: A systematic review. Int. J. e-Collaboration. 16:33–44.

[27]. Haghi, M., K. Thurow and R. Stoll. 2017. Wearable devices in medical internet of things: scientific research and commercially available devices. Healthc. Inform. Res. 23:4–15.

[28].Haoyu, L., L. Jianxing, N. Arunkumar, A.F. Hussein and M.M. Jaber. 2019. An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability. Futur. Gener. Comput. Syst. 98:69–77.

[29].Haq, A.U., J.P. Li, M.H. Memon, S. Nazir and R. Sun. 2018. A hybrid intelligent system framework for the prediction of heart disease using machine learning algorithms. Mob. Inf. Syst. 2018.

[30].Hassanien, A.E., N. Dey and S. Borra. 2018. Medical Big Data and internet of medical things: Advances, challenges and applications, CRC Press.

[31].Islam, M. and A. Rahaman. 2020. Development of smart healthcare monitoring system in IoT environment. SN Comput. Sci. 1:1–11.

[32].Joyia, G.J., R.M. Liaqat, A. Farooq and S. Rehman. 2017. Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. J. Commun. 12:240–247.

[33].Kamble, A. and S. Bhutad. 2018. Iot based patient health monitoring system with nested cloud security. In: 2018 4th International Conference on Computing Communication and Automation (ICCCA), IEEE, 1–5.

[34].Karaca, Y., M. Moonis, Y.-D. Zhang and C. Gezgez. 2019. Mobile cloud computing based stroke healthcare system. Int. J. Inf. Manage. 45:250–261.

[35].Karthick, G.S. and P.B. Pankajavalli. 2020. Architecting IoT based healthcare systems using machine learning algorithms: cloud-oriented healthcare model, streaming data analytics architecture, and case study. In: Incorporating the Internet of Things in Healthcare Applications and Wearable Devices, IGI Global, 40–66.

[36].Kazeem Moses, A., A. Joseph Bamidele, O. Roseline Oluwaseun, S. Misra and A. Abidemi Emmanuel. 2021. Applicability of MMRR load balancing algorithm in cloud computing. Int. J. Comput. Math. Comput. Syst. Theory. 6:7–20.

[37].Lakshmanaprabu, S.K., K. Shankar, A. Khanna, D. Gupta, J.J.P.C. Rodrigues, P.R. Pinheiro and V.H.C. De Albuquerque. 2018. Effective features to classify big data using social internet of things. IEEE Access. 6:24196–24204.

[38].Mahmoud, M.M.E., J.J.P.C. Rodrigues, S.H. Ahmed, S.C. Shah, J.F. Al-Muhtadi, V. V Korotaev and V.H.C. De Albuquerque. 2018. Enabling technologies on cloud of things for smart healthcare. IEEE Access. 6:31950–31967.

[39].Mallikarjuna, B. and D. Arun Kumar Reddy. 2019. Healthcare application development in mobile and cloud environments. In: Internet of Things and Personalized Healthcare Systems, Springer, 93–103.

[40].Manjula, V. and R. Thalapathi Rajasekaran. 2020. Security vulnerabilities in traditional wireless sensor networks by an intern in IoT, blockchain technology for data sharing in IoT. In: Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, Springer, 579–597.

[41].Michaud, T.L., M. Siahpush, R.J. Schwab, L.A. Eiland, M. DeVany, G. Hansen, T.S. Slachetka, E. Boilesen, H.J. Tak and F.A. Wilson. 2018. Remote patient monitoring and clinical outcomes for postdischarge patients with type 2 diabetes. Popul. Health Manag. 21:387–394.

[42].Mihovska, A. and M. Sarkar. 2018. Smart connectivity for internet of things (IoT) applications. In: New Advances in the Internet of Things, Springer, 105–118.

[43].Mohan, S., C. Thirumalai and G. Srivastava. 2019. Effective heart disease prediction using hybrid machine learning techniques. IEEE Access. 7:81542–81554.

[44].Mohanty, S.N., K.C. Ramya, S.S. Rani, D. Gupta, K. Shankar, S.K. Lakshmanaprabu and A. Khanna. 2020. An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. Futur. Gener. Comput. Syst. 102:1027–1037.

[45]. Molaei, A.M., M.H. Sedaaghi and H. Ebrahimnezhad. 2017. Steganography scheme based on Reed-Muller Code with improving payload and ability to Retrieval of Destroyed data for digital images. AUT J. Electr. Eng. 49:53–62.

[46]. Mutlag, A.A., M.K. Abd Ghani, N. al Arunkumar, M.A. Mohammed and O. Mohd. 2019. Enabling technologies for fog computing in healthcare IoT systems. Futur. Gener. Comput. Syst. 90:62–78.

[47]. Muzammal, M., R. Talat, A.H. Sodhro and S. Pirbhulal. 2020. A multi-sensor data fusion enabled ensemble approach for medical data from body sensor networks. Inf. Fusion. 53:155–164.

[48]. Nalluri, M.R. and D.S. Roy. 2017. Hybrid disease diagnosis using multiobjective optimization with evolutionary parameter optimization. J. Healthc. Eng. 2017.

[49]. Nazari, S., M. Fallah, H. Kazemipoor and A. Salehipour. 2018. A fuzzy inference-fuzzy analytic hierarchy process-based clinical decision support system for diagnosis of heart diseases. Expert Syst. Appl. 95:261–271.

[50]. Noah, B., M.S. Keller, S. Mosadeghi, L. Stein, S. Johl, S. Delshad, V.C. Tashjian, D. Lew, J.T. Kwan and A. Jusufagic. 2018. Impact of remote patient monitoring on clinical outcomes: an updated meta-analysis of randomized controlled trials. NPJ Digit. Med. 1:1–12.

[51]. Nourmohammadi-Khiarak, J., M.-R. Feizi-Derakhshi, K. Behrouzi, S. Mazaheri, Y. Zamani-Harghalani and R.M. Tayebi. 2020. New hybrid method for heart disease diagnosis utilizing optimization algorithm in feature selection. Health Technol. (Berl). 10:667–678.

[52]. Panarello, A., N. Tapas, G. Merlino, F. Longo and A. Puliafito. 2018. Blockchain and iot integration: A systematic survey. Sensors. 18:2575.

[53]. Pereira, M. and K.K. Nagapriya. 2017. A novel IoT based health monitoring system using LPC2129. In: 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE, 564–568.

[54]. Pirbhulal, S., W. Wu, S.C. Mukhopadhyay and G. Li. 2018. A medical-IoT based framework for eHealth care. In: 2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI), IEEE, 1–4.

[55]. Pratap, A., R. Gupta, V.S.S. Nadendla and S.K. Das. 2019. On maximizing task throughput in IoT-enabled 5G networks under latency and bandwidth constraints. In: 2019 IEEE International Conference on Smart Computing (SMARTCOMP), IEEE, 217–224.

[56]. Priyadharsan, D.M.J., K.K. Sanjay, S. Kathiresan, K.K. Karthik and K.S. Prasath. 2019. Patient health monitoring using IoT with machine learning. Int. Res. J. Eng. Technol. 6.

[57]. Qi, J., P. Yang, G. Min, O. Amft, F. Dong and L. Xu. 2017. Advanced internet of things for personalised healthcare systems: A survey. Pervasive Mob. Comput. 41:132–149.

[58]. Rghioui, A., J. Lloret and A. Oumnad. 2020. Big data classification and internet of things in healthcare. Int. J. E-Health Med. Commun. 11:20–37.

[59]. Rodrigues, J.J.P.C., D.B.D.R. Segundo, H.A. Junqueira, M.H. Sabino, R.M. Prince, J. Al-Muhtadi and V.H.C. De Albuquerque. 2018. Enabling technologies for the internet of health things. Ieee Access. 6:13129–13141.

[60]. Ruman, M.R., A. Barua, W. Rahman, K.R. Jahan, M.J. Roni and M.F. Rahman. 2020. IoT based emergency health monitoring system. In: 2020 International Conference on Industry 4.0 Technology (I4Tech), IEEE, 159–162.

[61]. De Sarkar, N.R., A. Kundu, M. De and A. Bera. 2020. Agent based noise detection using real time data analysis towards green environment. In: Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications, IGI Global, 539–560.

[62]. Schueler, M., A. Cox, S. Yuan, S. Crouch, J. Graham and W. Hall. 2019. From observatory to laboratory: A pathway to data evolution. In: Living in the Internet of Things (IoT 2019), IET, 1–8.

[63]. Shah, J.L. and H.F. Bhat. 2020. Towards integration of cloud computing with internet of things. In: Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, Springer, 229–260.

[64]. Siris, V.A., N. Fotiou, A. Mertzianis and G.C. Polyzos. 2019. Smart application-aware IoT data collection. J. Reliab. Intell. Environ. 5:17–28.

[65]. Stavrinides, G.L. and H.D. Karatza. 2019. A hybrid approach to scheduling real-time IoT workflows in fog and cloud environments. Multimed. Tools Appl. 78:24639–24655.

[66]. Sun, W., Z. Cai, Y. Li, F. Liu, S. Fang and G. Wang. 2018. Security and privacy in the medical internet of things: a review. Secur. Commun. Networks. 2018.

[67]. Usman, F., J.O. Dennis, A.Y. Ahmed, F. Meriaudeau, O.B. Ayodele and A.A.S. Rabih. 2018. A review of biosensors for non-invasive diabetes monitoring and screening in human exhaled breath. Ieee Access. 7:5963–5974.

[68]. Uyar, K. and A. İlhan. 2017. Diagnosis of heart disease using genetic algorithm based trained recurrent fuzzy neural networks. Procedia Comput. Sci. 120:588–593.

[69]. Vivekanandan, T. and N.C.S.N. Iyengar. 2017. Optimal feature selection using a modified differential evolution algorithm and its effectiveness for prediction of heart disease. Comput. Biol. Med. 90:125–136.

[70]. Wai, K.T., N.P. Aung and L.L. Htay. 2019. Internet of things (IoT) based healthcare monitoring system using NodeMCU and Arduino UNO. Publ. Int. J. Trend Sci. Res. Dev. 3:755–759.

[71]. Wan, J., M. AAH Al-awlaqi, M. Li, M. O'Grady, X. Gu, J. Wang and N. Cao. 2018. Wearable IoT enabled real-time health monitoring system. EURASIP J. Wirel. Commun. Netw. 2018:1–10.

Received: 16 Feb 2024; Accepted: 21 April 2024; Published: 29 April 2024