Multimedia Tools and Applications
https://doi.org/10.1007/s11042-023-17069-z

Revolutionary of secure lightweight energy efficient routing protocol for internet of medical things: a review

Padma Vijetha Dev. B[1,2] · **K. Venkata Prasad**[1]

Received: 21 March 2023 / Revised: 12 July 2023 / Accepted: 14 September 2023

Abstract
Advancements in the Internet of things (IoT) make a way for medical devices to coordinate in an environment that is the Internet of Medical Things (IoMT). In IoMT, some dedicated health monitoring devices are coordinated in an environment to accomplish a specified task. In this sector, patient information is periodically collected for early diagnosis of diseases. Various wearable sensors have been developed for smart sensing in the IoMT meanwhile, the sensed data are forwarded to the smart data collecting devices. Besides the advantages of remote monitoring and lower healthcare cost in IoT-based health monitoring systems, intrusion can occur during data transmission. Moreover, the large energy consumption of devices will result in higher system costs. An energy-efficient data routing protocol is developed in this area to cater to these issues. A swarm intelligence based approach is one of the most prominent methods for energy efficient routing of the data in IoT. The major goal of this paper is to provide deep insight into the lightweight, secure energy efficient routing protocol in IoMT. Furthermore, the limitations of existing methodologies are outlined.

Keywords Internet of Things (IoT) · Internet of Medical Things (IoMT) · Routing protocol · Security protocol · Cloud · Wireless Body Area Network (WBAN) · Sensors · Energy-efficient · Authentication · Swarm intelligence · Lightweight

1 Introduction

The Internet of Things (IoT) is the collection of things connected through the Internet to interact with each other without human intervention. IoT allows the interactions among devices and humans and other devices to communicate each other [1]. The IoT is considered the main part of the future development of the Internet, and it comprises billions of

✉ Padma Vijetha Dev. B
padmavijetha@gmail.com

[1] Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522502, India

[2] Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Kukatpally, Hyderabad, India

intelligent things for communication. The IoT is emerging as a future technology for many applications like industry, medical, business, transportation, mobility, energy, smart city etc. [2]. The development of node-to-node communication with advanced service automation has reduced the human intervention. Escalation of artificial intelligence (AI) and intelligent communication protocols enhance the management and optimization of industrial process. Recent years, the IoT has integrated in several domain for control management [3–7]. The enormous features of IoT make way for healthcare applications referred to as the Internet of Medical Things (IoMT). In medical applications, the medical devices are interconnected in a network to take control measures. The IoMT plays a vital role in medical applications owing to its higher accuracy, reliability and smart communication. The e-health IoMT has taken remarkable growth in recent years to support healthy lifestyle [8]. The advancement of the smart sensor, smart device, and lightweight authentication protocols improves the possibility of connecting medical things in a network. In IoMT, smart devices monitor the patients' biomedical signals without human intervention.

In contrast, conventional healthcare technology uses human management for data collection of the patient case history, medication, drug intake and demographic data etc. [9]. The manual data collection has caused several errors and has led to several errors in the system. However, IoMT eliminates the errors which are made by human that leads to the wrong treatment for the patient. Due to the mobility of the users in IoMT, the topology often changes [10]. The continuous development of electronic devices, communication technology, and sensor technology develop wearable devices for smart monitoring [11]. The wearable sensors are placed in the human body for continuously monitoring the body conditions in real-time, in which the sensed data are shared with the computer and mobile gateway. Information from the computer is forwarded to the hospital for further controlling actions. In recent years, the methods were developed for optimum placement of sensors in the human body [12].

IoMT is a boon technology for patients who cannot visit the hospital [13]. The doctors can easily monitor home treated patients and enable the best treatment for the patient without time delay. Many security issues are rising in the IoMT applications threatening patient information and health. The solutions to security issues in IoMT are classified as cryptographic and non-cryptographic [14, 15]. The emergence of IoMT provides positive changes in healthcare in terms of disease management, diagnosis of disease, improved treatment, reduced healthcare cost, and high security [16]. The security risk in IoMT devices has increased due to the lack of user awareness and attacker intrusion [17]. So it is important to ensure the security of the patient information and the devices used in the IoMT. Secure patient information without compromising device security is challenging in IoMT [18]. It is tedious task to ensure the privacy and security concerns by alleviating the security issues in IoMT [19]. However, it is necessary to have a simple solution for the security and privacy in IoMT that are ensured by energy efficient protocols. The papers reviewed in this survey are distributed in Fig. 1.

1.1 Problem formulation and review objective

The swarm intelligence based algorithms are comes under metaheuristic algorithms, which are inspired by the behaviour of social species. The SI based algorithms are executed through the exploration and exploitation phases. In the exploration, the optimum solution is randomly searched and the exploitation phase has searched the best solution based on the learned skills. The swarm intelligent based approaches are expandable for

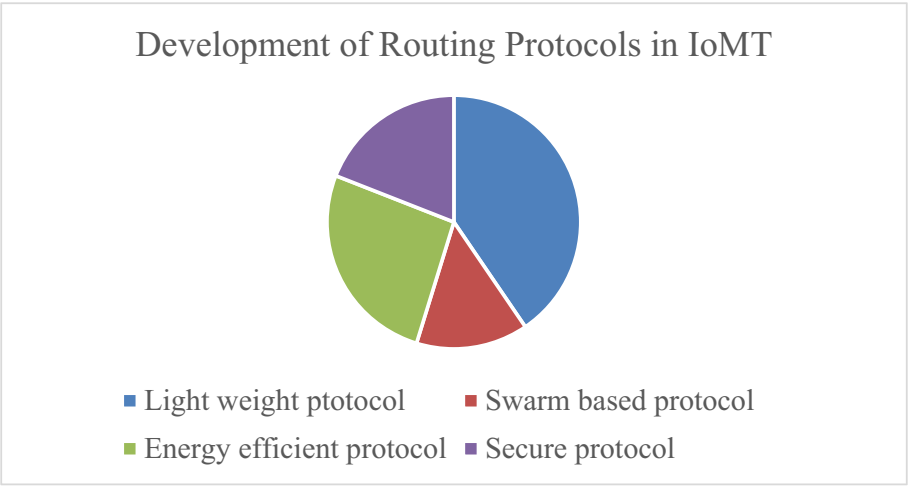

Fig. 1 Reviewed papers

different applications owing to its decision making ability. However, the heterogeneity may be occurs in the system due to the varying decision making ability of the individuals. Moreover, the goal of the algorithm cannot be predicted by examining the individuals. Hence, small varying rules can resulting variations in the system behaviour. Owing to these factors, deep analysis have to be made on the swarm intelligence based routing protocols in the IoMT. Several authors have investigated the development of energy aware secure routing protocol in the IoT. The devices connected to IoT have their own identity to collect data from different regions. The exponential growth of IoT has brought several control approaches to have energy efficient and secure routing protocols. As in the case of IoMT, data routing has played an important role because it has dealt with human lives. The necessity of IoMT is increasing in every phase of the ordinary, especially during the COVID-19 pandemic. As per the current situation, the secure lightweight and energy aware routing protocol in IoMT is an emerging topic. It is risky to maintain secure routing under different attacks in the network. Thus several researches have been made to overcome the drawbacks of data sharing in IoMT. Although numerous reviews have been done on the routing of IoT, only limited surveys are made in the routing protocols of IoMT. The previous survey papers highlight the swarm-based routing protocols and the routing protocols in IoT. But this survey has only provided a deep analysis of the IoMT. This review's major novelty and contribution is to provide deep insight into the security, lightweight, energy aware and swarm based protocols in the IoMT. Here, novelty is added regarding reviewed methodologies from conventional models to advanced methodologies. This review aims to examine the drawbacks of the existing routing protocols and provide a better solution towards an efficient routing strategy with limited energy consumption.

1.2 Contribution of the work

The risk of attackers in the IoMT may threaten the data of patient information like name, id, health status, and medicines. On the other hand, a wide variety of devices in IoMT makes the process complicated. One of the major issue in the routing protocol

is the heterogeneity of devices, frequency breaks in the links and higher bit error rate. Effective routing protocols overcome the security and data transmission issues in IoMT devices. The swarm intelligence based routing protocols are more efficient for dynamic problems; thus, those methods can provide an efficient solution in the routing process. An efficient routing protocol can improve the performance and widen the applications of IoMT. Hence, the systematic review is required in this sector to direct the future researchers to innovate new systems. Previous surveys were focused on the efficient routing protocols in IoT and only limited papers are discussed the routing protocols in IoMT. However, those papers are failed to review recent developments in the routing protocols. Hence, this paper is intended to review an efficient routing protocols in the IoMT. The major contribution of this paper is listed as follows,

- To examine the different attacks and security challenges in the IoMT.
- To provide an insight into the secure energy efficient lightweight routing protocols in IoMT.
- Discuss existing works' limitations and provide a solution to overcome those drawbacks.

This paper does a comprehensive review for the IoMT system, security issues, routing protocols and future scope sequentially. In this paper, section-2 elaborates the review methodology including research queries, searching strategy, inclusion and exclusion of papers. The background of IoT and IoMT with the attacks including malware attack and denial of services are discussed in section-3. The development of different routing protocols including light weight, energy efficient, swarm intelligence based are discussed under section-4. Conclusion of the reviewed methods based on the performance evaluation and the future scope are provided in section-5. The paper organization is shown in Fig. 2.

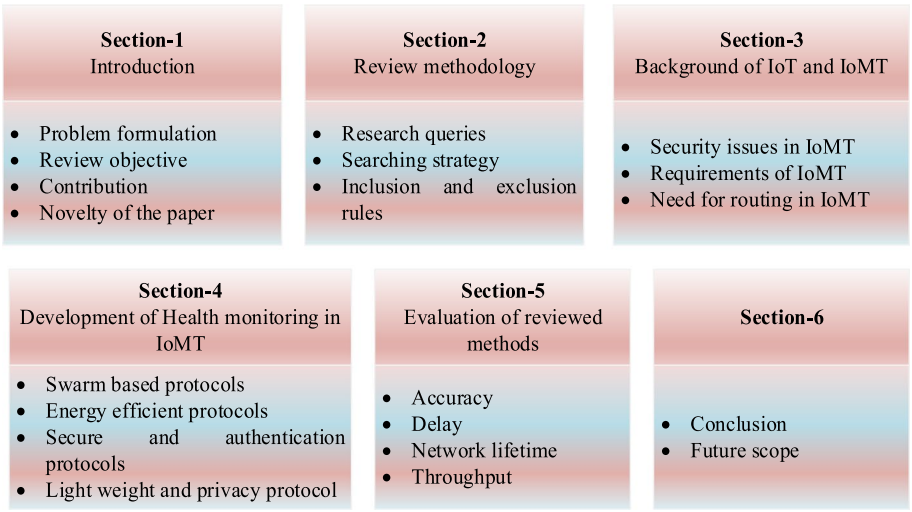

Fig. 2 Organization of the paper

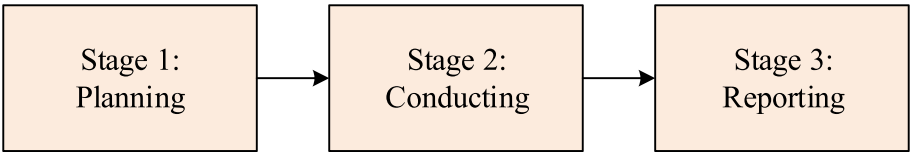

Fig. 3 Systematic review

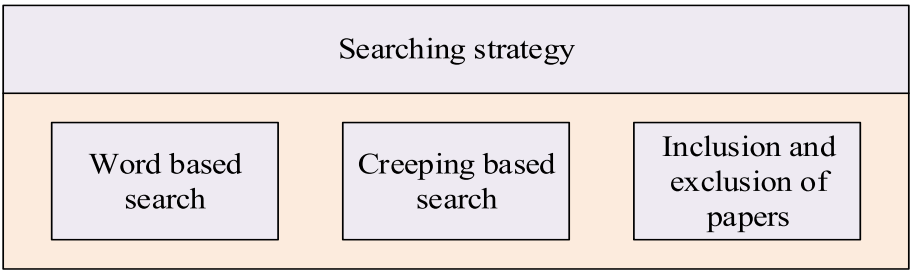

Fig. 4 Searching strategy

2 Review methodology

In this section, the research questions to be answered are given. The systematic review is helpful for literature reviewing of papers. The systematic review has three important stages such as planning, conducting and reporting. The pictorial representation of review methodology is shown in Fig. 3.

In the first stage, the research queries are framed and the responses for these queries must be presented in the document.

2.1 Stage 1: Research queries

Major aim of this review is to answer the following research queries,

- What is the mean by IoT and IoMT ?
- What are the security issues in IoMT ?
- What are requirements for IoMT ?
- How does the routing will affect the data transmission in IoMT?
- What are the recent methods for data transmission in IoMT ?
- How to evaluate the performance efficacy of routing protocols in IoMT ?

2.2 Stage 2: Searching strategy

The searching strategy must be respond to the research queries and other gaols of the paper. The schematic view of searching strategy is shown in Fig. 4. In word-based searching strategy, the papers are gathered by applying the words related to the domain

and the exploration is done by inbuilt sources. Some of the words related to this domain are listed below,

- Security in IoT and IoMT
- IoT based health monitoring
- Routing protocol in IoMT
- Internet of Health Things (IoHT)
- Data transmission in IoMT

In creeping based search strategy, the exploration is carried out based on the previous literatures done in the same domain. At last, the inclusion and exclusion are carried out based on the similarity of the paper domain. The rules in inclusion and exclusions are listed below,

1. Inclusion rules

- Include the literatures in between 2019 to 2023
- Include the literatures for routing protocols only in IoMT
- Include the literatures in the English language

2. Exclusion rules

- Exclude the literatures for routing protocols in IoT
- Exclude the papers having unclear information about the publications

3 Background of IoT and IoMT

The Internet of Things (IoT) is the collection of a wide variety of things connected in a wireless network to interact with each other. The IoT leads a major role in upgrading the hospital to a smart level. The mixture of medical devices with the IoT, called IoMT, enabled cost effective medical solutions for patients. Wearable sensors play a vital role in the IoMT approach. However, tiny physiological sensors are connected to the body area network (BAN) to monitor health. This method is enabled by the wireless technology called Wireless Body Area Network (WBAN). The schematic diagram of IoMT is shown in Fig. 5.

The sensors in WBAN can do the same process as the sensors done in the WSN [20]. The escalating connectivity between remote devices has increased the telemedicine sector. Telemedicine is a way of healing diseases over a distance that uses information and communication technology to diagnose the disease. Telehealth comprises remote clinical services for monitoring and diagnosis. The teleconsultation or the telemonitoring system uses audio and video interactions [21] between the patient and doctors.

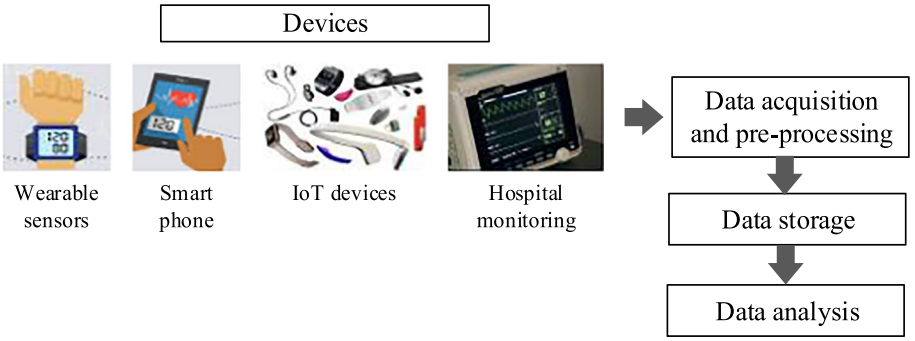

Fig. 5 Process of IoT in healthcare

3.1 Security issues in IoMT

One of the major objectives of this review is to examine different attacks in the IoMT. Some of the most common attacks are listed below,

- **Denial of service (DOS):** It will destroy the availability of devices in the network, and the attackers can access these devices without user permission.
- **Replay attack:** In this attack, the data will be resented due to the fraud delay when the attacker eavesdrops on a secure network.
- **Tampering devices:** The attacker can tamper with the devices to stop their reliable operation, and this can cause wrong data sharing.
- **Tracking of sensor identity:** The GPS device is attached to the patient's equipment to track their location; this could be traced by the attackers. This may threaten the patient's security.
- **Side channel:** In this case, the attacker takes the benefits of data leakage to get the patient's personal information.
- **Malware attack:** This attack may seriously threaten the integrity and confidentiality of the data.

3.2 Requirements of IoMT

Sensors in IoMT deal with sensitive information about the patient's health condition. Hence, a minute error in the IoMT destroys the patient's life, so several requirements are needed for the sensors in IoMT for effective health monitoring and data transfers. The IoT based healthcare system is shown in Fig. 6.

Some of the main requirements of IoMT are listed below,

- IoMT devices must be able to transfer data from lower levels to higher levels of the network. Additionally, the devices have better interconnectivity among them in case of data processing, data transfer, and security.
- IoMT must have the capability of coping with a mass number of devices and device management.

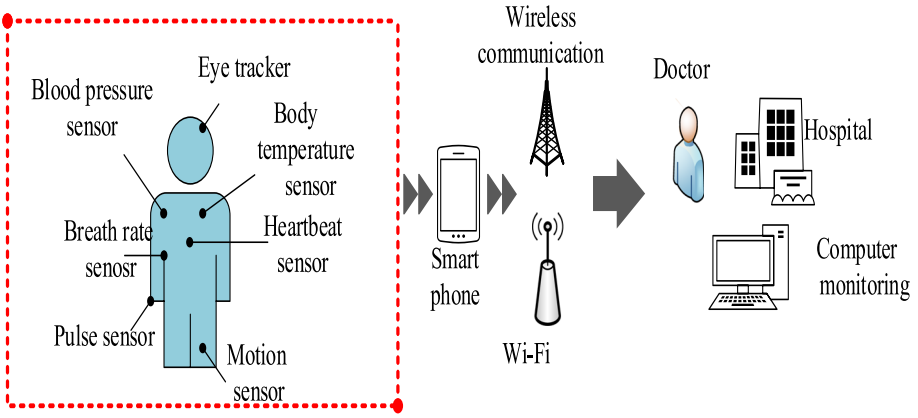

Fig. 6 IoT based health monitoring system

- Most of the critical requirements in IoMT can be accomplished by the Cyber-Physical Systems (CPS).
- Reliability and safety are examined under physical and digital due to the combination of the physical and computational models.
- The hardware of model IoMT must be restricted in hostile environments, and software designing must avoid malfunction.

3.3 Need for routing in IoMT

The number of devices connected to the Internet is due to the rapid development of IoT in every sector. The IoMT utilizes 30% of the IoT device markets, which enables the accessibility of medical services to everyone. At the same time, privacy and secure protocols are important concerns in Internet enabled health care [22]. As discussed earlier, the IoMT has dealt with patient information; hence the unintended exposure of these sector may pose vulnerabilities and security risks. It should be noted that several terms are used for representing the IoMT, like healthcare IoT and healthcare things. However, all these terms represent the IoT devices used in healthcare. One of the major differences between the IoT and IoMT is the sensitivity of data [23]. Thus high priority will be given to the secure and energy efficient routing in the IoMT.

4 Development of health monitoring in IoMT

IoMT is equipped with dedicated devices for the health monitoring of humans by the use of wireless networks. Wireless sensor networks are used in body condition sensing and transfer that data to the destination. Health monitoring in IoMT has become a more challenging task due to the high range of radiation from health monitoring devices that will affect the patient. The health monitoring system is affected due to body sensing devices. Thus efficient health monitoring devices are suggested to overcome these challenges. The types of sensors in health monitoring and different methods are listed below.

Motion trackers are used in the applications of sports, medical and other motion-tracking fields. Thus the movement of the person was easily tracked by the motion trackers; the accelerometer was combined with magnetometers and gyroscopes to improve the data accuracy of the motion tracker. The inter-WBSN cooperation of IoMT is used with the large communication range [24]. In that model, the WBSN was directly attached to the human body or else sewed in the cloth; in some cases, the sensors were embedded within the human body. Two WBSNs consisting of single coordinating nodes were located in the same area as that method used two hops in the IoMT environment.

Health monitoring of the patient is mainly done via sensors placed in the body; hence sensor placement is the initial step of IoMT health monitoring. Manikandan Rajasekaran et al. [25] proposed an autonomous energy charging mechanism for nodes in the IoMT for uninterrupted operation. The proposed method utilizes the Analytical Hierarchical Process (AHP) to distribute energy to the nodes. In that model, the autonomous recharger will supply required power to the SNs. Nodes send their energy status to the base station (BS) that forwards it to the autonomous recharger equipped with a high capacity battery. Hence the system performance was improved with enough energy to the nodes. To overcome the obstacles in healthcare, Peiran Dong et al. [26] proposed an edge computing based decentralized health monitoring in IoMT. In that model, the unique Pareto point was optimized through the Nash bargaining solution. To enhance the patient health monitoring via remote access, a series learning method based dependable gesture recognition (DGR) method was proposed by Nourelhoda et al. [27]. The convergence of that module was improved by continuous monitoring and differentiation of gestures from regular activities. From the above analysis, it is found that the communication through these devices is carried out through Multi-hop communication.

4.1 Swarm intelligence based protocols in IoMT

Data sharing through an optimum path in IoMT is a main consideration for cost effective solutions for data transfer. The swarm intelligent routing protocols provide an effective solution for finding the minimum path to the destination. The movement of swarms inspires Swarm intelligent-based routing during the process of food searching. The different methods of swarm intelligent based routing protocols are listed below.

Indresh Kumar Gupta et al. [28] proposed a hybrid Particle Swarm Optimization (PSO)-Genetic Algorithm (GA) for enhancing the clustering of medical devices. Clustering was the process of grouping medical devices according to their similarity measurements. Each solution of the network was defined as a particle, and the group of particles were a swarm. The fitness function was used to examine the solution for the problem and guide the process. The proposed hybrid algorithm comprises particle initialization, fitness computation and results generation steps. The medical data were clustered using GA, which indicated that individuals with the highest fitness had the highest possibility of participating in the succeeding generations.

Lin Yao et al. [29] developed a comprehensive management system for medical equipment by utilizing the swarm intelligence algorithms of particle swarm optimization (PSO) and chicken swarm optimization (CSO) algorithm. The PSO and the CSO were based on the behaviour of swarms searching for food. Where the improved versions of PSO and CSO were adopted to overcome the time delay during the local search, and the particles are used to solve computing task problems. Here, the proposed methodology was modelled to

reduce the task time and cost of the network. The experimental system module was based on the ASP.NET website technology and the SQL server database.

El-shafeiy et al. [30] had suggested an artificial bee colony (ABC) based routing protocol in the IoMT. In that suggested method, the wheel selection technique was adopted to set the path number for nodes in the network. The ABC choose an optimized path based on the features, and the greedy selection was made between the neighbouring and original path. In that model, the grouping was done based on the node's characteristics. The node characteristics were inputted and grouped based on similarity during the initialization phase.

Jayasankar et al. [31] proposed an Extended Role Based Access Control (ERBAC) model and the Twofish algorithm (TA) on a cloud platform for securing the medical data in the health system. In the EBARC, a special function was introduced, and storage permissions were provided to the consumers. Afterwards, the data access was provided based on the status of membership. In addition to ERBAC, a clustering approach was used to reduce the delay in retrieving medical data. The clustering method on that approach used the PSO and GA and a clustering calculation. After necessary authentication, the RBAC provides the user restricted access based on privileges. Then the Twofish encryption algorithm was used to effectively perform small processor running applications and hardware embedding. The crossover of PSO-GA was used to store the therapeutic knowledge based on progression.

Singh et al. [32] had introduced the genetic algorithm (GA) based protocol for electing the cluster heads (CH) in IoMT. In that suggested model, a multiple mobile sink approach was introduced to minimize the distance between the sink and CH. Four base stations were considered at the separation of 90 degrees. The fitness function of GA has been formulated based on the energy factor, distance, and density. That suggested method had minimized the nearby deployment of nodes having higher energy.

Refaee et al. [33] had improved the security of the data transmission using the butter ant optimization algorithm (BAO) based routing algorithm. Additionally, the fuzzy concept was included in the optimum routing. The k-nearest neighbour (KNN) approach was adopted for filtering the data, and the large dimension of the data has been minimized by principle component analysis (PCA). Moreover, the suggested methodology utilizes distance vector routing protocol to avoid loss networks. The above mentioned methods and their pros and cons are listed in Table 1.

4.2 Energy efficient routing protocol

The lifetime of the network will be degraded if the sensors are energized with minimum energy and consume a higher amount of energy. Energy efficient routing protocols provide sufficient energy to the sensors for long time performance without failure. The energy efficient routing protocols proposed by various authors in IoMT are listed below.

The energy consumption in multi-hop communication is higher; this may degrade the network lifetime. To overcome the higher energy consumption of the nodes, an energy efficient routing protocol must be needed. Yating Qu et al. [34] proposed an energy efficient routing protocol for WBAN to mitigate energy consumption by direct communication. The maximum benefit function was built into that model to normalize the residual energy, transmission efficiency, and available bandwidth. Using those functions, the next hop will be identified for the network.

Table 1 Swarm based routing approaches in IoMT

Author	Method	Objective	Advantage	Limitation
Gupta [28], 2019	Hybrid POS-GA	Clustering	The lower error rate for different datasets	The proposed algorithm future extended into different mathematical problems
Lin Yao et al. [29], 2021	Improved PSO and improved CSO	Data management	Supports large amounts of data support	The degree of load balancing is not improved
El-shafeiy [30], 2021	ABC	Routing	CPU time gets reduced	The method is less significant under the unavailability of large datasets
Jayasankar et al. [31], 2021	TA	Data security	Cloud records are secured by the ERABC model	Encryption speed is not improved
Singh et al. [32], 2022	GA	CH selection	Balancing the load and minimizing the hotspot problem	Unguided mutation of GA does not guarantee an optimization solution
Refaee et al. [33], 2022	BAO	Routing	Network losses are avoided	Categorization is less reliable in the presence of errors in data labelling

Khalid M Awan et al. [35] proposed a Priority-Based Congestion Avoidance Routing Protocol (PCRP) for multi-hop communication. In that method, IoT-based heterogeneous medical sensors achieve energy efficiency with reduced computational complexity. The lowest cost function selected the sensor nodes and forwarded the sensed data to the next-hop node. That process continued until the data reached the sink node. The results from that proposed method were compared with the existing routing protocols of iM-SIMPLE and Optimized Cost Effective and Energy Efficient Routing (OCER). From the analysis of the results, it was evident that the PCRP reduced network traffic, reduced the time for the load transfer, improved lifetime and offered high throughput.

To mitigate the delay, data collision, packet drop, and data re-transmission in the WBAN, Ali Raza Bhangwar et al. [36] proposed Weighted Energy and Temperature Routing Protocol (WETRP). That network comprises bio-medical sensor nodes, relay nodes, and gateway nodes. The relay nodes estimated the temperature rise of the neighbour, and then the biomedical sensors were entered into the routing table in Route Discovery Phase (RDP). The source node broadcasts a route request to the neighbour when the route to the sink node fails to satisfy the temperature and energy threshold. The weight function was assigned to the residual energy, temperature, and link-delay estimation. Relay nodes compare the route request with the routing table and then acknowledge if the route to the sink node already exists or broadcasts to the downstream nodes. The route error packets were used to inform the inactive transmission to the upstream nodes in the route maintenance phase; thus, the source node received the route error packets for an alternative route.

Enas Selem et al. [37] proposed a Temperature Heterogeneity Energy (THE) aware routing protocol for health applications in IoT to overcome the temperature rising of on-body sensors. On that proposed protocol, the sensed data were categorized as an emergency, data priority, critical data priority, and normal data assigned priority for achieving the desired performances. That proposed model comprises a Coordinator Node (CN) separated from the skin and several body nodes placed directly with the skin. The EEG and ECG nodes were classified as critical nodes that transmit the data to CN. The remaining nodes were classified as normal nodes transmitting the data to the parent node (PN), which was selected based on maximizing utility. On THE, the temperature threshold was set as high temperature threshold and set a guard band. The last transmission reaching the highest threshold was not more than the guard band assumed to prevent temperature rise on the skin. After that, the nodes slept until the temperature cooled down, and then the lower temperature threshold was to wake up and resume work, where the node's energy conservation was done during the sleeping mode. That result indicates that the proposed THE protocol improved the network's lifetime and reduced energy consumption.

Muhammad Dawood Khan et al. [38] proposed energy harvested and cooperative enabled routing protocol (EHCRP) for IoT-WBAN to increase efficiency with minimized cost. On that, energy harvesting was the sensor node powering itself with equipped techniques. The overall routing of the EHRCP was divided into data initialization with sensing, node selection, and cooperative efforts. In the initialization phase, the proposed model used 10 heterogeneous sensor nodes (SN) with limited hardware resources, then placed on the human body. The position of the central node coordinator (CNC) was considered for mitigating the line-of-site (LoS) that forwards the data to Personal Digital Assistance (PDA) for processing. After the distance calculation, all the sensor nodes send the BEACON message in the network, including the node's id and destination, residual energy, and node location. After all the nodes were registered, that were scheduled for normal operation, where the CNC assigned time slots to each SN. The methods reviewed in this section are illustrated in Table 2.

Table 2 Energy efficient routing protocol

Authors	Protocols	Objective	Pros	Limitations
Yating Qu et al. [34], 2019	Energy efficient routing protocol	Routing	Adjust the parameter based on data priority	Efficient algorithms should be added for the weight selection of priority data
Khalid M Awan et al. [35], 2019	PCRP	Multi-hop communication	Reduce the time for load transferring	Mobility of nodes should be focused
Ali Raza Bhangwar et al. [36], 2019	WETRP	Temperature and energy efficient routing	Hotspot is reduced	Work will be extended in terms of separating the critical data
Enas Selem et al. [37], 2019	THE	Temperature aware routing	Priority of the node will be supplied with the novel optimization	–
Muhammad Dawood Khan et al. [38], 2020	EHCRP	Extending network lifetime	Delay is reduced	Extension of WBAN with multiple links is not studied
Zeinab Shahbazi and Yung-Cheol Byun, [39]	ATEAR	Secure thermal aware routing	Throughput is increased	The system is not studied under different body postures
Tanzila Saba et al. [40], 2020	Kruskal algorithm based routing	Secure and energy efficient routing	Lower communication overheads	There is no considerable reduction in energy utilization
Khan et al. [41], 2022	AntHocNet	Finding the optimum route in flying IoT healthcare	Reinforcement is improved in flying network	The mobility model could be improved under the unmanned aerial vehicle (UAV)
Roshini et al. [42], 2023	HEASR	Energy aware routing	Data security and encoding are improved	Only network parameters are used to evaluate the system's performance
Natarajan et al. [43], 2023	ECC	Enhancing security and energy efficiency	Higher encryption throughput	Effectiveness cloud be improved further
Zaman et al. [44], 2023	DLAB	Energy and link aware clustering	Lower path loss	Routing is difficult under posture mobility

Analyzing the methods in Table 2, it was found that some of these methods failed to reduce delay in data transfer, and some of the methods were insufficient for improving system stability.

To overcome the deficiencies in WBAN due to the temperature rise of the implanted sensor, Zeinab Shahbazi and Yung-Cheol Byun [39] proposed block chain-based Adaptive Thermal-Energy-Aware Routing (ATEAR) protocol for WBAN was proposed. The blockchain technology on that model offers security, transparency, and a lightweight solution for the cooperation of physiological data with other medical personnel. The blockchain's performance would be evaluated using the 'Hyperledger Caliper' tool. The ATEAR would be examined by using the 'Castalia' simulation tool. The proposed module comprises ATEAR routing protocol and blockchain in addition to inter-BAN, infra-BAN, and beyond-BAN communication. The process would be initiated from the intra-BAN communication, and then the Access Control Rule (ACR) was used for authorization and authentication. By utilizing the composer-rest-server, the restful API for exposing the blockchain services to the client-end. The ATEAR was used for the selection of optimal multi-hop paths.

In order to overcome the energy imbalance of the sensor nodes in a wireless body network, Tanzila Saba et al. [40] proposed an energy-efficient framework. That proposed framework uses two algorithms for biosensor connectivity and secure data transmission utilizing cipher block chaining algorithm. In addition, the Kruskal algorithm was utilized for the section of the hops with minimum cost routing. Using those algorithms, the proposed mode reduces energy consumption and improves the security of the data against malicious nodes. The results indicate that the proposed framework reduced the overall communication overhead.

Khan et al. [41] suggested an AntHocNet to provide an optimum route for data in the flying IoT. That suggested methodology includes both proactive and reactive components to ease communication. An iterative random sampling algorithm improved the adaptability of flying networks. As same as the ant colony optimization algorithm, the ants in the forward direction searched for the optimum route, and the reverse ants maintained the path.

Roshini et al. [42] introduced the hierarchical energy aware secure routing (HEASR) of WBAN. In that model, the nodes were categorized based on the threshold values. The CH was chosen based on energy levels and traffic priority. The data in optimum routing was compressed using the Huffman encoding technique, and the cryptographic algorithm will enhance the data security. The CH was selected based on the LEACH media access control, and the routes were optimized by the body nodes based on the maximal gain function.

Natarajan et al. [43] introduced a unique Elliptic Curve Cryptography (ECC) based routing of healthcare data. In order to minimize the storage limitation, the 186 bit encryption system was designed, and the sensor nodes randomly generated the keys. The key between the sink and sensor nodes was generated through the two party authentication mechanism. The computing algorithm generated the hashing code for ECC.

Zaman et al. [44] introduced a distance, link aware body (DLAB) based clustering mechanism. The CHs were connected with other nodes to facilitate several functionalities. That suggested model was tested on the human body using 9 SNs in different locations. The link aware energy efficient routing estimated the cost function of forwarded nodes.

4.3 Secure and authentication protocol

The authentication protocol in IoMT will improve the data transfer security between the patient and health caretakers. The authentication protocols provide end-to-end secure data transfer. Some of the authentication protocols by different authors are listed below.

Amel Arfaoui et al. [45] proposed a context-aware and lightweight authentication and key agreement scheme for WBAN for emergency and normal situations. That proposed scheme utilizes Real-or Random (ROR) model, Burrow-Abadi-Needham (BAN) logic, and the automatic security protocol verification (Scyther) tool for security. The RoR model comprises the acceptance state, partnering state and adversary state. On that RoR, the adversary must create a real session key from a random one. The BAN logic was adopted for mutual authentication and secure session key establishment among the communication. A Scyther tool was adopted to check the Internet security-sensitive protocols.

Anwesha Mukherjee et al. [46] proposed delay-sensitive fog network for the Internet of Health Things (IoHT) to alleviate high energy consumption. The proposed Fog IoHT comprises BAN, mobile, fog, and cloud servers. The data collected by the BAN were processed inside the fog devices, and the GPS tracked the user's location in the mobile device; that information was the main consideration of Fog IoHT. The access point (AP) and the Road Side Unit (RSU) were selected using the weighted game theory. In that model, the data was fed to fog devices and then forwarded to the cloud storage.

Ankur Gupta et al. [47] proposed a secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN to mitigate the intermediate node capture attacks. At the initial, the system administrator (SA) selects the hub node (HN) then, stored in HN's memory then, the SA registered intermediate node (IN) and the sensor node (SN) by choosing the temporary secret key, after that IN was stored in HN's memory. The authentication phase correction would be interrupted in case of any check failed. The system's security was examined by both formal and informal methods, where the formal analysis and mutual authentication were done via BAN-logic, real-or-random (ROR) model and AVISPA tool. The sensor node (SN), intermediate node (IN) and hub node (HN) were the participants of the proposed method.

To cope with the security of the patient's sensitive information and to enhance the support to the patient during an emergency, Deepak & Fadi Al-Thurjman [48] proposed a smart mutual authentication protocol for cloud based IoMT. That proposed smart service authentication (SSA) framework was implemented using FPGA and motive TMote Skymote. That SSA comprises three stages initialization of the service-authority centre, registration by medical sensors in WBAN, and smart authentication. In the initialization phase, the parameters with random prime numbers were generated by the service authority centre, then select the random integer with less than the prime factor. After that, the registration phase device number with the service authority centre was registered. On smart authentication, the sensed data was transmitted to the cloud services. The Burrows, Abadi Needham (BAN) logic was utilized to examine the security property of mutual authentication.

To ease the deployment of the sensors in IoT, Bander A. Alzahrani et al. [49] proposed an improved lightweight authentication scheme (ILAS). The gateway node selected hash, fuzzy generation, and encryption/decryption on that method. The security of the network was analyzed via the ROR model. Most importantly, the proposed ILAS-IoT provided an access control mechanism widely used in IoT scenarios.

Bander A. Alzahrani et al. [50] proposed a secure and efficient authentication protocol named remote patient-healthcare monitoring protocol (RPMP) for the cloud IoT. The presented protocol concentrates on the smart card attack, session key compromise and impersonation attack. The security feature of that protocol used the BAN logic, which was based on the security analysis and validation done on the ProVerif automated security tool. The RPMP enable a gateway node for mutual authentication and anonymity between the patient and medical professional. That model allows a session key between the medical professional and the gateway node in the protocol session.

Table 3 Authentication protocols in IoMT

Authors	Methodology	Objectives	Findings
Amel Arfaoui et al. [45], 2019	Context-aware and lightweight authentication	Enable the data routing under normal and critical situations	A combination of the protocols examined inter-communication.
Anwesha Mukherjee et al. [46], 2020	Anonymous mutual authentication and key agreement protocol	Minimizing node attacks	Both the indoor and outdoor design of the FogIoHT
Deepak & Fadi Al-Thurjman [48], 2020	Mutual authentication protocol	Improving cloud based IoMT	Enhancing the mutual authentication protocol for telecare medical information system (TMIS) using cloud
Bander A. Alzahrani et al. [49], 2020	ILAS	Easing sensor placement in IoT	Provides high security against various attacks
Bander A. Alzahrani et al. [50], 2020	RPMP	Preventing smart card attacks	It provides accommodation for low end IoT
Minahil et al. [51], 2021	ECC based authentication	Mitigate threats like impersonation, stolen smart card attacks, and offline password leakage.	Reducing the computational and communication cost
Rashmi Singh et al. [52], 2021	Revocable functionality in the authentication protocol	Enable remote authentication	Valid decryption keys were obtained by using the key generation centre (KGC)

To ease the remote access of medical data sharing in a platform of higher security, an ECC-based authentication protocol was presented by Minahil et al. [51]. The security analysis was done by Random Oracle Model (ROM). Rashmi Singh et al. [52] proposed an efficient implementation of revocable functionality in the authentication protocol for the WBAN. The remote authentication was designed by utilizing the Public key infrastructure. In order to overcome the availability of patient information after expired of the service of the client, the authentication was equipped with a revocation function. The methods reviewed in this section are shown in Table 3.

Verifying the methods in Table 3, the delay in data transfer and energy consumption of the devices were not properly reduced. At the same time, energy consumption is the major area to be covered by the IoMT system. Thus in future work, we focused on both drawbacks and produced an effective way to overcome these issues.

4.4 Lightweight security and privacy protocols

Lightweight security protocols in IoMT improve the security of the data that is transferred between the patient and doctors, thus eliminating the possibility of data hackers. Some of the lightweight security protocols are listed below.

To overcome the risk of malicious node intrusion in the IoMT, Venkata P. Yanambaka et al. [53] proposed Physical Unclonable Function (PUF) based device authentication scheme. The integration of the PUF with IoT devices had the advantage of reduced power consumption. The PUF in edge computing was connected with devices like the edge server, edge router, and gateway. The responses gathered from the PUF model were sent to the server after the device entered the server. The device would authenticate based on the similarity with the stored hash values.

To overcome the threat of secrecy share in IoMT, ta et al. [54] proposed a lightweight mutual authentication and key agreement scheme for WBAN. That proposed method guaranteed security to the data shared via wireless sensors. An automatic security verification tool of ProVerif was used for verification and security analysis.

Data privacy is a main security issue in IoMT data transfer that will improve data confidentiality. The privacy of patient information is the main consideration for the IoMT application. Hence, Zhitao Guan et al. [55] proposed an Efficient, Differently Private Data Clustering Scheme (EDPDCS) for privacy. That includes the cluster approach for diagnosis, and the EDPDCS was based on the Map Reduce framework. The iteration of the K-means algorithm was fixed value based on the total privacy budget and minimum privacy budget of each iteration examined by Mean Square Error (MSE).

Ghufran Ahmed et al. [56] proposed a thermal and energy aware routing in WBAN. That proposed method mitigates overheating the IoMT nodes because of the reception of route discovery packets. The proposed models use the transceiver, transmitter, reception, channel, receiving, and thermal computation models. That proposed model offers high throughput. The Received Signal Strength Indicator (RSSI) and Specific absorption rate (SAR) method were used to calculate the thermal changes in the system. The node's transmission power level (TPL) was created during the set-up phase.

Sobhan Esmaeili et al. [57] proposed a priority-aware lightweight sensing model for Body Area Network (BAN) for labelling patient data. In that proposed model, the network topology was designed with four sensors for monitoring the body conditions. A single node can scrutinize, aggregate and prioritize the sensed data; thus, all nodes have 0.3J initial energy. Where the first order radio model has been used, then the single-chip low-powered

transceiver of NORDIC NRF 2401A is utilized. The intervals of activity were assigned to the nodes using Interleaved Division Multiple Access (IDMA) that provide diversity to improve against fading, cost effective receiver, centralized control and optimum capacity. In that proposed method, the sensed data are sampled and measured. In secure sensing, a linear transform was used to map data into space, and useless data was ignored.

Carlos Andres Lara-Nino et al. proposed the lightweight ECC accelerator for IoT applications [58] to enhance security. That proposed model uses the Field Programming Gate Array (FPGA) based acceleration engine for ECC operation with scalar multiplication (kP). The prime finite field and the binary finite field were reported in that paper. The Binary Edward Curves (BEC) had the benefit of completeness in that the addition of the properties was defined, and there was no need for the validation process. Montgomery's ladder scalar multiplication algorithm was used to obtain regularity during the execution.

In order to mitigate various potential attacks due to the data transmission on the public channel, Kisung Park et al. [59] proposed A Mutual Authentication Key Agreement (MAKA) based Lightweight Authentication and Key Agreement without Non-Verification Table (LAKS-NVT) scheme. The proposed LAKS-NVT uses the Real-Or-Random model to verify with the Automated Validation of Internet Security Protocols and Applications (AVISPA) software tool. The practical aspects of LAKS-NVT were carried out by the network simulator 2 (NS2). The MAKA phase starts with generating random numbers and timestamps in the Sensor Node (SN) and is then sent to the access point (AP) after the data is sent with its own identity. The MAKA phase accessed the data, and the network security was analyzed by AVISPA, ROR and BAN logic. Then, the implementation was done using HPLSP.

A lightweight Radio Frequency Identification (RFID) protocol based on Authentication Encryption (AE) was proposed by Masoumeh Safkhani et al. [60]. On that proposed method, FPGA, along with ASCI simulations, was utilized in five different AE from the Competition for Authentication Encryption Security Applicability Robustness (CAESAR) competition for the development of three use cases. The RFID infrastructure comprises highly constrained microchips with limited memory and processing power. That proposed model consists of two phases of initialization and authentication; in the initialization phase, the default values are stored in the parties with the sharing of the encryption key. For each tag, the database was recorded with old and new parameters then the database would be local, integrated with the reader by remote access. In the authentication phase, the reader creates and sends a message to the embedded tag in the kit.

Amal Sammoud et al. [61] proposed a new biometric ElectroCardioGram -based key establishment protocol in WBAN. That proposed protocol was based on the ECG and error correction code with morphing function. An additional node was needed to distribute the symmetric keys between two nodes. That proposed method allowed the node to establish a symmetric key according to the ECG signal that measured the heartbeat over time. The error correcting code of the BCH was used to eliminate the dissimilarities. The AVISPA tool is used for security verification, with the high-level protocol language (HLPSL) of parent-child asymmetric key establishment in that proposed method.

Maria-Dolores Cano & Antonio Canavate-Sanchez [62] proposed an Elliptic Curve Digital Signature Algorithm (ECDSA) for computing the digital signature in medical things and improving security as well as data privacy. That proposed model was mainly based on the ECC. In that model, the dual signature was used to link different types of buyer's order information (OI) and buyer's payment information (PI) in e-commerce. Three participants were vital in that model: transmission device (TD), edge computing device/servers (ECS) and cloud.

Xucheng Huang & Shar Nazir [63] proposed an Analytic Network Process (ANP) method for evaluating the security of IoMT. In the security evaluation, particular phenomena are subparts on a quantitative scale between 0 and 1. The principle eigenvalues and the eigenvector were used to find the relative importance, and then the matrix's consistency was measured.

Maria Papaioannou et al. [8] elaborated on the categorized security countermeasure against threats to the IoMT. To ensure the confidentiality of the patient information, a lightweight encryption protocol was introduced by the specification in ISO/IEC 29192. To ensure the integrity of data transmission, the combination of both symmetric cryptography and attribute-based encryption (ABE) was used in the IoMT edge network. For the purpose of the authentication, the identity based ECC and Lamports One Time Password (OTP) algorithm was used.

Samira Akhbarifar et al. [64] proposed a secure health monitoring model based on cloud IoT. The health monitoring model uses lightweight block encryption technology for security in an IoT environment. Whereas the lightweight, secure block encryption would protect patients' sensitive data. Here the patient's health status was evaluated using data mining methods

To overcome the session-specific temporary information attack, Bander A. Alzahrani et al. [65] proposed an improved lightweight authentication protocol for WBAN. The protocol was based on the secure, efficient, anonymous WBAN authenticated key agreement scheme. The lightweight patient-health monitoring authentication protocol allows users to get authenticated key agreements by hiding their identity. By the validation, the protocol was robust and efficient.

Lightweight security protocols and privacy of the data shared in IoMT are examined in Table 4.

Abdullah M. Almuhaideb & Kawther S. Alqudaihi [66] proposed the anonymity preserving lightweight protocol. The lightweight WBAN authentication would be done by dividing protocol as P-I, which would perform authentication, and P-II would re-authenticate to protect the node's anonymity. The re-authentication scheme would decrease hub communication and thereby reduce the overhead. For mutual authentication and key agreement having informal security, the BAN logic was used. The model was robust in offline and online secret key guessing and is vulnerable to several attacks. The complexity of the model was high due to re-authentication, but the communication cost was low in terms of the reduced overhead.

Chen et al. [67] introduced a lightweight protocol for the Internet of health things (IoHT) to cater to security threats. That suggested model has provided mutual authentication between the user and SNs. Shreya et al. [68] had proposed a fully homomorphic encryption scheme for secured access to patient data.

Zahid et al. [69] had introduced an avant-garde framework (AGF) and Adaptive Transmission Data Rate (ATDR) mechanism for minimizing energy utilization in healthcare devices. That suggested ATDR works based on the average energy consumption, and the regression model was used for examining the channel dynamics. The self-adaptive routing algorithm (SARA) based on dynamic source routing (DSR) was used for data routing.

By analyzing the methods in table 4, it was found that some of these methods failed to cope with the temperature issues in nodes and energy consumption of the devices is not maintained at a minimum level.

Table 4 Lightweight secure protocol and data privacy in IoMT

Authors	Methodology	Objectives	Findings
Venkata P. Yanambaka et al. [53], 2019	PUF based authentication scheme	Overcome intrusion of malicious nodes	Never store the data related to the IoMT devices
ta et al. [54], 2019	mutual authentication and key agreement	Overcome the threat of secrecy sharing	That proposed method improved security without asymmetric encryption.
Zhitao Guan et al. [55], 2019	EDPDCS	Enhancing privacy	The improved initial centroid selection method was used to improve accuracy and efficiency.
Ghufran Ahmed et al. [56], 2019	Thermal and energy aware routing protocol	Minimize the impacts of thermal variations	RSSI and SAR measure the thermal variations in the system
Sobhan Esmaeili et al. [57], 2020	Priority based lightweight protocol	Priority aware routing	Data were prioritized by using the Glasgow Coma Scale (GCS)
Carlos Andres Lara-Nino et al. [58], 2020	FPGA based protocol	Enhancing security	Enhancing security against side channel attack
Kisung Park et al. [59], 2020	MAKA	Minimize the potential attacks	The proposed LAKS-NVT offers the highest security as well as higher communication
Masoumeh Safkhani et al. [60], 2020	RFID	Overcome the leakage of sensitive information of the patient	the reader sends only the generated message to the tag to minimize the cost
Amal Sammoud et al. [61], 2020	ElectroCardioGram based protocol	generation and distribution of cryptographic keys	morphing function minimizes the correlation between the ECG signal and the generated key
Maria-Dolores Cano & Antonio Canavate-Sanchez [62], 2020	ECDSA	Improving security	offers data privacy by hiding the heath data send by the transmission devices from the edge devices
Xucheng Huang & Shar Nazir [63], 2020	ANP	Security enhancement	The pair-wise comparison was applied with alternatives.
Maria Papaioannou et al. [8], 2020	lightweight encryption protocol	Improving the integrity of data transmission	ECC has better performance than the Random Symmetric Key (RSS).

Table 4 (continued)

Authors	Methodology	Objectives	Findings
Samira Akhbarifar et al. [64], 2020	Secure health monitoring model	Health monitoring	Due to the restricted resources, block encryption has a crucial effect on these systems.
Bander A. Alzahrani et al. [65], 2020	Improved lightweight authentication	Prevent session-specific temporary information attack	The protocol is verified by the automated protocol analyzer (ProVerif tool) and random oracle model (ROM).
Abdullah M. Almuhaideb & Kawther S. Alqudaihi [66], 2020	Anonymity preserving protocol	Enhancing security	The model was proved to be robust in the offline and online secret key
Chen et al. [67], 2022	Lightweight protocol	Secure the IoHT	Robust adaptability to future development
Shreya et al. [68], 2022	Homomorphic encryption	Improving data privacy in multi-user	The number of the transmitted message is higher in this model
Zahid et al. [69], 2022	AGF and ATDR	Improving energy aware routing	SARA makes a self-decision to routing

5 Evaluation of reviewed methods

The security and energy provided by different methodologies are estimated through the performance measure. Some of the evaluation metrics are listed below,

- **Throughput:** It is the measure of successfully transmitted from the source and received data at the destination.
- **Encryption throughput:** It is measured by dividing the average amount of data transmitted by the time of encryption.
- **Delay:** It refers to the duration for data to be transmitted across the IoMT devices to take timely action.
- **Energy efficiency:** It measures the amount of energy the network uses to transmit the data among the overall energy utilized.
- **Lifetime:** It is an important measurement to examine the number of available nodes in the network for data sharing. It shows the duration of the nodes that exist in the network based on energy availability.
- **Packet drop:** It measures data packets that fail to reach the destination.
- **Packet Delivery ratio:** It measures the number of successful data forwarded and reaching the destination.

The network lifetime is an important that must be validated for examining the performance efficacy of the system. The nodes in method [34] has sustained for 4980 rounds with the transmission proximity of 95%. The life time of the network can be estimated in terms of power left in the system. In this regard, the multi hop routing protocol in [35] have required amount of power for 3.5×10^4 rounds. In [35] energy harvested routing protocol has improved the ability of 20 nodes to sustain for 18000 rounds. On the other hand, the network lifetime can be estimated in terms of processing time of the system, in this regard, the nodes in [36] is sustained for 630 seconds for processing 1000 data. The improved PSO and CSO methods discussed in [29] has the highest accuracy of 99.8% and the correct rate of 99.4%. At the same time, the two fish algorithm based approach in [31] has lower accuracy of 92.59%. The PSO and GA provided in [28] was validated on 6 datasets while it has provide the error rate of 13.22% and also the running time is higher for this approach. The accuracy of system is affected by the delay in data transmission. In order to examine that the performance of Fog IoHT is estimated in indoor and outdoor conditions. For 200 Mb data the delay is varied as 2.1s and 30s under indoor and outdoor conditions. When compared to this the context aware authentication protocol in [45] has provide lower delay of 9.86ms. Priority-aware Lightweight Secure Sensing Model in [57] has provide the delay of 0.02041s for 0.9150 bits. On the other hand, the delay in LAKS scheme [59] is 0.1s that shows the performance efficacy of the system. From these analysis it is concluded that an efficient method should focus to improve the system accuracy with lower delay and lower energy consumption. The values of evaluation metrics for reviewed methods are shown in Table 5 and Table 6.

6 Conclusion and future scope

The IoMT is an emerging technology in healthcare applications due to its benefits. However, the devices in IoMT are affected by different kinds of attacks and intrusion of malfunction. Hence, the secure lightweight energy efficient routing protocols are reviewed in

Table 5 Performance analysis of reviewed methods

Authors	Accuracy	Correct Rate/ error rate/latency	Time measures
Lin Yao et al. in 2021 [29]	99.8%	Correct rate 99.4%	-
Indresh Kumar Gupta et al. in 2019 [28]	High	Error rate 13.22% for 6 data sets	Running time is 24.54 for 6 data sets
Jayasankar.T et al. in 2021 [31]	92.59% for 30 diseases file	-	Encryption time is 420 ms for 600 files and decryption time is 327 ms for 600 files

Table 6 Analysis of throughput

Authors	Network life time	Throughput
Yating Qu et al. in 2019 [34]	4980 rounds for 10 dead nodes	3550 for 5000 rounds
Khalid M Awan et al. in 2019 [35]	-25 power level in 3.5×10^4 rounds	2.4×10^4 for 2000 rounds
Muhammad Dawood Khan et al. in 2020 [38]	18000 rounds for 20 number of nodes	11×10^4 for 20000 rounds
Zeinab Shahbazi & Yung-Cheol Byun in 2020 [39]	-	88% for 12 nodes
Ali Raza Bhangwar et al. in 2019 [36]	Life time 630 sec for 100 data	62% for 100 data
Anwesha Mukherjee et al. in 2020 [46]	-	Throughput 81000 for 9.126 Mb data
Amel Arfaoui et al. in 2019 [45]	-	Throughput 13.5 bps

this paper. The swarm intelligence based routing algorithms are utilized to get the optimum path for data transfer that improves the system efficiency at a lower cost. But the major issue in swarm based routing protocol is the convergence speed. As the lightweight authentication protocols were improved, system security and some quality issues were found in those models. The quality of health diagnosis and services is enhanced by the authentication protocols that are investigated to overcome the deficiencies. By analyzing the result of the authentication protocols, it was found that performance degrades due to changes in context. This survey investigated several literatures to obtain an effective solution to overcome the deficiencies in IoMT. Then effective solutions towards an energy efficient swarm intelligent based routing protocol are discussed, and the best solutions are suggested. Since the devices in IoMT does not stay at a fixed position, thus mobile SNs are used. Portable devices are preferred for the IoMT application; hence, future work will be focused on portable devices and their security in IoMT. Moreover, some suggestions will be provided for future directions.

By examining the methods suggested by the author, it was found that several risks in the parameters section were found; hence in future works, it is suggested to use an efficient algorithm or better simulation to cope with QoS requirements. Various papers are reviewed to improve the network efficiency that adopts an energy-efficient intelligent-based lightweight routing protocol. Thus in future work, it is suggested to use routing protocols that take care of the mobility of the sensors during body movement. Additionally, to improve the encryption speed, improved algorithms are suggested.

Author's contributions All authors read and approved the final manuscript.

Data availability Data sharing is not applicable to this article.

Declarations

Conflict of interest Authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Consent to participate All the authors involved have agreed to participate in this submitted article.

Consent to publish All the authors involved in this manuscript give full consent for publication of this submitted article.

References

1. Reddy YH, Ali A, Kumar PV, Srinivas MH, Netra K, Achari VJ, Varaprasad R (2022) A Comprehensive Survey of Internet of Things Applications, Threats, and Security Issues. South Asian Res J Eng Tech 4(4):63–77
2. Sadhu PK, Yanambaka VP, Abdelgawad A (2022) Internet of things: Security and solutions survey. Sensors 22(19):7433
3. Khan AA, Laghari AA, Gadekallu TR, Shaikh ZA, Javed AR, Rashid M, Estrela VV, Mikhaylov A (2022) A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Comput Electr Eng 102:108234
4. Khan AA, Wagan AA, Laghari AA, Gilal AR, Aziz IA, Talpur BA (2022) BIoMT: a state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. IEEE Access 10:78887–78898

5. Khan AA, Laghari AA, Li P, Dootio MA, Karim S (2023) The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises. Sci Rep 13(1):1656
6. Khan AA, Laghari AA, Shaikh ZA, Dacko-Pikiewicz Z and Kot S (2022) Internet of Things (IoT) Security with Blockchain Technology: A State-of-the-Art Review. IEEE Access
7. Khan AA, Shaikh AA and Laghari AA (2022) IoT with Multimedia Investigation: A Secure Process of Digital Forensics Chain-of-Custody using Blockchain Hyperledger Sawtooth. Arab J Sci Eng 1-16
8. Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, Lymberopoulos D (2022) A survey on security threats and countermeasures in internet of medical things (IoMT). Trans Emerg Telecommun Technol 33(6):e4049
9. Vishnu S, Ramson SJ, Jegan R (2020) Internet of medical things (IoMT)-An overview. In2020 5th international conference on devices, circuits and systems (ICDCS) IEEE 2020: 101-104
10. Asam M, Jamal T, Adeel M, Hassan A, Butt SA, Ajaz A, Gulzar M (2019) Challenges in wireless body area network. International Journal of Advanced Computer Science and Applications. 2019: 10(11)
11. AlShorman O, AlShorman B, Alkhassaweneh M, Alkahtani F (2020) A review of Internet of medical things (IoMT)–based remote health monitoring through wearable sensors: A case study for diabetic patients. Indonesian J Electric Eng Comput Sci 20(1):414–422
12. Hoareau D, Jodin G, Chantal P-A, Bretin S, Prioux J, Razan F (2022) Synthetized inertial measurement units (IMUs) to evaluate the placement of wearable sensors on human body for motion recognition. J Eng 2022(5):536–543
13. Yaacoub JP, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A (2020) Securing Internet of medical things systems: Limitations, issues and recommendations. Futur Gener Comput Syst 105:581–606
14. Kamalov F, Pourghebleh B, Gheisari M, Liu Y, Moussa S (2023) Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective. Sustainability 15(4):3317
15. Sun Y, Lo FP, Lo B (2019) Security and privacy for the Internet of medical things enabled healthcare systems: A survey. IEEE Access 7:183339–183355
16. Alsubaei F, Abuhussein A, Shandilya V, Shiva S (2019) IoMT-SAF: Internet of medical things security assessment framework. Internet of Things 8:100123
17. Wei K, Zhang L, Guo Y, Jiang X (2020) Health monitoring based on Internet of medical things: architecture, enabling technologies, and applications. IEEE Access 8:27468–27478
18. Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PK (2020) A review on security and privacy of Internet of medical things. arXiv preprint arXiv:2009.05394
19. Alhaj TA, Abdulla SM, Iderss MAE, Ali AAA, Elhaj FA, Remli MA, Gabralla LA (2022) A survey: To govern, protect, and detect security principles on internet of medical things (iomt). IEEE Access 10:124777–124791
20. Liu Q, Mkongwa KG, Zhang C (2021) Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. SN Appl Sci 3:1–9
21. Omboni S, Campolo L, Panzeri E (2020) Telehealth in chronic disease management and the role of the Internet-of-Medical-Things: the Tholomeus® experience. Expert Rev Med Dev 17(7):659–670
22. Chaganti R, Mourade A, Ravi V, Vemprala N, Dua A, Bhushan B (2022) A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. Sustainability. 14(19):12828
23. Rasool RU, Ahmad HF, Rafique W, Qayyum A, Qadir J (2022) Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. J Netw Comput Appl. 103332
24. Abdulmohsin Hammood D, Rahim HA, Alkhayyat A, Ahmad RB (2019) Body-to-body cooperation in Internet of medical things: toward energy efficiency improvement. Future internet 11(11):239
25. Rajasekaran M, Yassine A, Hossain MS, Alhamid MF, Guizani M (2019) Autonomous monitoring in healthcare environment: Reward-based energy charging mechanism for IoMT wireless sensing nodes. Futur Gener Comput Syst 98:565–576
26. Dong P, Ning Z, Obaidat MS, Jiang X, Guo Y, Hu X, Hu B, Sadoun B (2020) Edge computing based healthcare systems: Enabling decentralized health monitoring in Internet of medical Things. IEEE Netw 34(5):254–261
27. Mahmoud NM, Fouad H, Soliman AM (2021) Smart healthcare solutions using the Internet of medical things for hand gesture recognition system. Complex Intell Syst 7(3):1253–1264
28. Gupta IK, Yadav V, Kumar S (2019) Medical data clustering based on particle swarm optimization and genetic algorithm. Intl J Adv Intell Paradigms 14(3-4):345–358

29. Yao L, Shang D, Zhao H, Hu S (2021) Medical equipment comprehensive management system based on cloud computing and Internet of things. J Healthcare Eng
30. El-shafeiy E, Sallam KM, Chakrabortty RK, Abohany AA (2021) A clustering based Swarm Intelligence optimization technique for the Internet of Medical Things. Expert Syst Appl 173:114648
31. Jayasankar T, Bhavadharini RM, Nagarajan NR, Mani G, Ramesh S (2021) Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform. Eur J Mol Clin Med 8(01):1075–1089
32. Singh S, Nandan AS, Sikka G, Malik A, Vidyarthi A (2022) A secure energy-efficient routing protocol for disease data transmission using IoMT. Comput Electr Eng 101:108113
33. Refaee E, Parveen S, Begum KM, Parveen F, Raja MC, Gupta SK, Krishnan S (2022) Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications. Wireless Commun Mobile Comput. 2022
34. Qu Y, Zheng G, Wu H, Ji B, Ma H (2019) An energy-efficient routing protocol for reliable data transmission in wireless body area networks. Sensors. 19(19):4238
35. Awan KM, Ashraf N, Saleem MQ, Sheta OE, Qureshi KN, Zeb A, Haseeb K, Sadiq AS (2019) A priority-based congestion-avoidance routing protocol using IoT-based heterogeneous medical sensors for energy efficiency in healthcare wireless body area networks. Intl J Distrib Sensor Netw 15(6):1550147719853980
36. Bhangwar AR, Ahmed A, Khan UA, Saba T, Almustafa K, Haseeb K, Islam N (2019) WETRP: Weight based energy & temperature aware routing protocol for wireless body sensor networks. IEEE Access 7:87987–87995
37. Selem E, Fatehy M, Abd El-Kader SM, Nassar H (2019) THE (temperature heterogeneity energy) aware routing protocol for IoT health application. IEEE Access 7:108957–108968
38. Khan MD, Ullah Z, Ahmad A, Hayat B, Almogren A, Kim KH, Ilyas M, Ali M (2020) Energy harvested and cooperative enabled efficient routing protocol (EHCRP) for IoT-WBAN. Sensors. 20(21):6267
39. Shahbazi Z, Byun YC (2020) Towards a secure thermal-energy aware routing protocol in wireless body area network based on blockchain technology. Sensors. 20(12):3604
40. Saba T, Haseeb K, Ahmed I, Rehman A (2020) Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. J Infect Public Health 13(10):1567–1575
41. Khan IU, Hassan MA, Alshehri MD, Ikram MA, Alyamani HJ, Alturki R, Hoang VT (2021) Monitoring system-based flying IoT in public health and sports using ant-enabled energy-aware routing. J Healthcare Eng. 2021
42. Roshini A, Kiran KV (2023) Hierarchical energy efficient secure routing protocol for optimal route selection in wireless body area networks. Intl J Intell Netw 4:19–28
43. Natarajan R, Lokesh GH, Flammini F, Premkumar A, Venkatesan VK, Gupta SK (2023) A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. Infrastructures 8(2):22
44. Zaman K, Sun Z, Hussain A, Hussain T, Ali F, Shah SM, Rahman HU (2023) EEDLABA: Energy-Efficient Distance-and Link-Aware Body Area Routing Protocol Based on Clustering Mechanism for Wireless Body Sensor Network. Appl Sci 3(4):2190
45. Arfaoui A, Kribeche A, Senouci SM (2019) Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications. Comput Netw 159:23–36
46. Mukherjee A, De D, Ghosh SK (2020) FogIoHT: A weighted majority game theory based energy-efficient delay-sensitive fog network for internet of health things. Internet of Things 11:100181
47. Gupta A, Tripathi M, Sharma A (2020) A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN. Comput Commun 160:311–325
48. Deebak BD, Al-Turjman F (2020) Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. IEEE J Select Areas Commun 39(2):346–360
49. Alzahrani BA, Chaudhry SA, Barnawi A, Xiao W, Chen M, Al-Barakati A (2020) ILAS-IoT: An improved and lightweight authentication scheme for IoT deployment. J Ambient Intell Humanized Comput. 1-3
50. Alzahrani BA, Irshad A, Alsubhi K, Albeshri A (2020) A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT. Int J Commun Syst 33(11):e4423
51. Ayub MF, Mahmood K, Kumari S, Sangaiah AK (2021) Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. Digital Commun Netw 7(2):235–244
52. Singh R, Joshi A, Mohapatra AK, Jha VN (2021) An efficient implementation of revocable functionality in authentication protocol for wireless body area network. J Inf Optim Sci 42(2):321–331

53. Yanambaka VP, Mohanty SP, Kougianos E, Puthal D (2019) PMsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things. IEEE Trans Consum Electron 65(3):388–397
54. Xu Z, Xu C, Liang W, Xu J, Chen H (2019) A lightweight mutual authentication and key agreement scheme for medical Internet of Things. IEEE Access 7:53922–53931
55. Guan Z, Lv Z, Du X, Wu L, Guizani M (2019) Achieving data utility-privacy tradeoff in Internet of medical things: A machine learning approach. Futur Gener Comput Syst 98:60–68
56. Ahmed G, Mahmood D, Islam S (2019) Thermal and energy aware routing in wireless body area networks. Intl J Distrib Sensor Netw 15(6):1550147719854974
57. Esmaeili S, Tabbakh SR, Shakeri H (2020) A priority-aware lightweight secure sensing model for body area networks with clinical healthcare applications in Internet of Things. Pervasive Mobile Comput 69:101265
58. Lara-Nino CA, Diaz-Perez A, Morales-Sandoval M (2020) Lightweight elliptic curve cryptography accelerator for internet of things applications. Ad Hoc Netw 103:102159
59. Park K, Noh S, Lee H, Das AK, Kim M, Park Y, Wazid M (2020) LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical internet of things. IEEE Access 8:119387–119404
60. Safkhani M, Rostampour S, Bendavid Y, Bagheri N (2020) IoT in medical & pharmaceutical: Designing lightweight RFID security protocols for ensuring supply chain integrity. Comput Netw 181:107558
61. Sammoud A, Chalouf MA, Hamdi O, Montavont N, Bouallegue A (2020) A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis. Comput Secur 96:101838
62. Cano MD, Cañavate-Sanchez A (2020) Preserving data privacy in the internet of medical things using dual signature ECDSA. Secur Commun Netw 2020:1–9
63. Huang X, Nazir S (2020) Evaluating security of internet of medical things using the analytic network process method. Secur Commun Netw 2020:1–4
64. Akhbarifar S, Javadi HH, Rahmani AM, Hosseinzadeh M (2020) A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. Personal and Ubiquitous Computing. 1-7
65. Alzahrani BA, Irshad A, Albeshri A, Alsubhi K, Shafiq M (2020) An improved lightweight authentication protocol for wireless body area networks. IEEE Access 8:190855–190872
66. Almuhaideb AM, Alqudaihi KS (2020) A lightweight and secure anonymity preserving protocol for WBAN. IEEE Access 8:178183–178194
67. Chen CM, Chen Z, Kumari S, Lin MC (2022) LAP-IoHT: A lightweight authentication protocol for the internet of health things. Sensors. 22(14):5401
68. Shreya S, Chatterjee K, Singh A (2022) A smart secure healthcare monitoring system with Internet of Medical Things. Comput Electr Eng 101:107969
69. Zahid N, Sodhro AH, Kamboh UR, Alkhayyat A, Wang L (2022) AI-driven adaptive reliable and sustainable approach for internet of things enabled healthcare system. Math Biosci Eng 19:3953–3971