International Journal of Wireless Information Networks (2021) 28:451–466
https://doi.org/10.1007/s10776-021-00538-3

A Perspective Review of Security Challenges in Body Area Networks for Healthcare Applications

J. Vijitha Ananthi[1] · **P. Subha Hency Jose**[1]

Received: 18 March 2021 / Revised: 16 August 2021 / Accepted: 1 October 2021 / Published online: 18 October 2021

Abstract
Body area network (BAN) connects sensors and actuators to the human body in order to collect patient's information and transmitting it to doctors in a confined space with limited users. wireless body area network (WBAN) is derived from wireless sensor networks (WSN) and enables to transfer of the patient's information with a wide range of communication due to the limitations of the wired body area network. It plays a vital role in healthcare monitoring, healthcare systems, medical field, sports field, and multimedia communication. Sensors and actuators lead to high energy consumption due to their tiny size. WBAN facilitates in securely storing patient information and transmitting it to the doctor without data loss at a specific time. This review examines and summarizes methodological approaches in WBAN relating to security, safety, reliability, and the fastest transmission. Flying body area networks (FBAN) utilizing unmanned aerial vehicles for data transmission are recommended to promote rapid and secure communication in WBAN. FBAN improve the security, scalability, and speed in order to transmit patient's information to the doctor due to high mobility.

Keywords Body area networks (BAN) · Wireless body area networks (WBAN) · Energy consumption · Security limitations · Flying body area networks (FBAN) · Remote healthcare monitoring

1 Introduction

Sensor nodes/actuators represent essentially the wireless sensor network, and the sensor node senses acoustic factors including temperature, pressure, sound, pulse rate, ECG, blood pressure, and heart rate of the human body. In healthcare, this form of sensor network is known as a wireless body area network (WBAN) [1]. These sensor nodes are placed on the cloth and underneath the human body. The data communication in WBAN involves two possible ways. Firstly, there will be communication between Sensors to Personal Device Assistants (PDA) such as Bluetooth or Zigbee. Secondly, there will be communication between PDAs to the base station via the radio interface. The gateway node facilitates the connection of sensors and wearable devices on the human body to the internet. In this way, doctors can access the patient's data online using an internet connection [5]. The most salient issue in wireless body area networks is the consumption of high energy because of the smaller size of the node. It has limited resource devices, and it requires more energy to transmit the data. The possibility of hacking the patient's information while transmitting the data has increased the importance of security concerns. The use of an effective routing protocol and clustering methodology in WBAN might reduce energy consumption and security threats.

Wireless body area networks consist of sensors, biological parameters, body control unit, personal device assistant, transmission factor, and user access. Figure 1 shows that the wireless body area network along with the sensor senses the biological factors continuously in order to obtain the human health information from the body control unit. The electrocardiogram (ECG) sensor records the patient's electric impulse as it passes through the heart muscle. This assists in monitoring the patient's heartbeat, which is used to track various movements such as resting and moving [6]. The temperature of the human body's ears, skin, and forehead are detected by the body temperature sensor. The pressure of blood as it travels through the arteries is measured by blood

✉ J. Vijitha Ananthi
vijithaananthi@karunya.edu.in; vijithaananthij@gmail.com

P. Subha Hency Jose
hency20002000@karunya.edu

[1] Department of Biomedical Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India

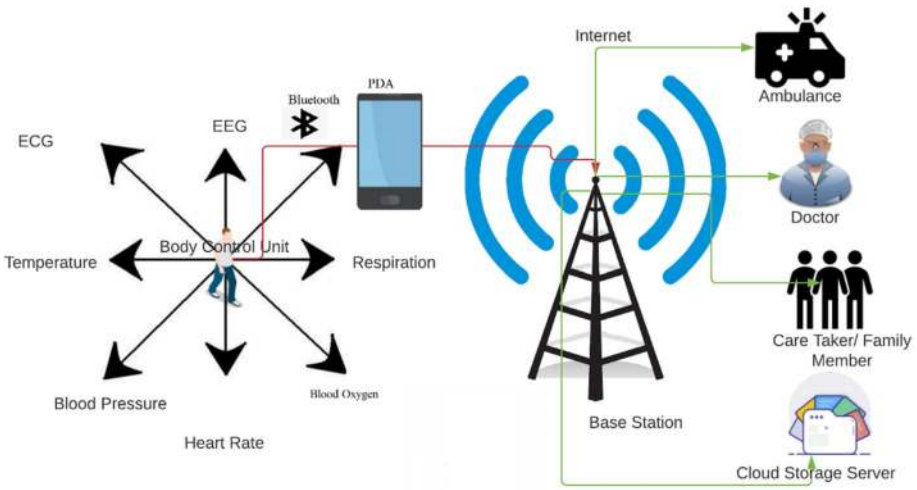

Fig. 1 Wireless body area network architecture

pressure and the pulse wave is measured by the heart rate sensor as it pumps blood through the patient's body. The saturation level of oxygen in the blood is measured with a pulse oximeter. The airflow sensor can be positioned near the human body's nasal to assess the body's respiration. The collected information will be transferred and stored in the personal device assistants (PDA) and later transmitted to the base station. From the base station, the data will be transferred to the respective user applications such as cloud databases, ambulances, family members, and doctors via the Internet [8]. A cloud database's purpose is to store the patient's data on a server so that the doctor can access it and then send the patient's information to the user via the internet. Star topology is used in the body area network. The body control unit acts as a central node and then each sensor will sense and communicate to the center node. The center node interfaces the human body by using Bluetooth or ZigBee or Personal Device Assistants (PDA), and then the patient's information can be accessed by the doctors using the Internet.

1.1 WBAN Architecture

Wireless body area networks can be categorized into three different parts such as intra-WBAN communication, inter-WBAN communication, and beyond WBAN communication [10].

Sensors are connected to a PDA that has restricted coverage within 2 km, a centralized design, and preserves star topology in Intra-WBAN communication. The data transmission between the sensors to PDA is based on Bluetooth or ZigBee. PDA is referred to as a centralized node or coordinator node and acts as a centralized node to collect and transmit the data from sensors to end-users. It maintains the communication between sensors to end-user through the external gateway via Bluetooth.

Inter-WBAN communication connects the PDA to access points along with ad-hoc architecture. Ad-hoc architecture is distributed to communicate directly from one node to another node and does not rely on existing infrastructure; instead, it maintains a random topology. It also connects other wireless devices to the base station within a limited coverage range via a wireless channel.

In Beyond WBAN communication, PDAs are referred to as centralized nodes or coordinator nodes since they use the gateway to connect the various networks. Here, the communication takes place from the base station to the ambulance, doctor, cloud storage server, or family members via the internet. Figure 2 explains the different tier level communication of body area networks.

The wireless body area network is the most important component in the medical field in COVID-19 situations for sharing patient information with the physician. The sensor in WBAN interfaces to the human body via a radio interface to continuously monitor electrocardiogram (ECG),

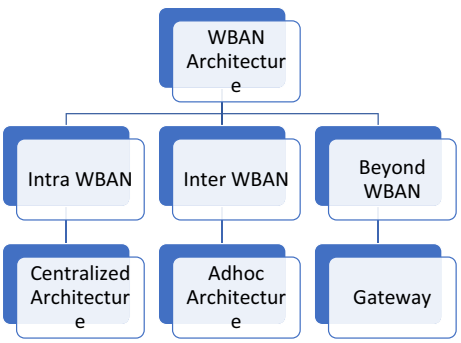

Fig. 2 WBAN architecture

electroencephalogram (EEG), temperature, blood oxygen level, blood pressure, heart rate, motion sensor, and respiration. COVID-19 has drastically changed human lifestyles, and everything has become digital. In order to maintain social distance, humans are severely barred from leaving their homes, and elderly people are not permitted to leave their homes. Body area networks are used to communicate the patient's information to doctors and to receive advice from them over the internet in this circumstance. The patient's quality of life will be enhanced, and hospital costs will be reduced. Even in severe circumstances, continuous monitoring of a patient's health information benefits the treatment of the patient. As a result, the relevant doctors and patient's family members have access to the patient's information that has been saved collectively.

The most salient factors that have to be focused on the development of WBAN [12] are as follows.

- WBAN is used for short-range communication
- Sensors/actuators are smaller in size
- Continuous monitoring of patient
- Patient's information to be stored
- Securely communication to respective doctors and family members
- Immediate action for emergency

1.2 Current Trends in WBAN

Wireless body area networks are utilized in various fields such as medical, entertainment, military, and sports [15]. Wireless body area networks play a significant role in the medical field, both in terms of saving lives and transmitting patient information in the event of an emergency [8]. In WBAN, sensors are placed on the human body and it will continuously monitor the patient's health conditions. If any abnormal changes such as high temperature, low heart rate and so on are found in the patient's health, the data will be transmitted to the doctor for immediate action via internet. The application of a wireless body area network is categorized into two parts as an implantable and wearable sensor. An implantable sensor inserts the sensors into the human body with the help of surgery, and it is not to be removed from the patient's body. A wearable sensor is used whenever the patients need to be monitored and that will be worn by the patient. And this Wearable Sensor node helps to identify the movement and abnormal positions of patients. Wearable sensors can be removed from a patient's body at any time. For instance, wearable personal digital assistant helps to monitor blood glucose, temperature, SpO_2, the functioning of the heart, and blood pressure.

In the entertainment field, this body area sensor network helps to transfer the data streaming operations. The wearable device plays a vital role in the sports field, and that will report the step count, stamina level of the human body, and so on. In military fields, wearable devices help to track the soldier's health condition and the location of the soldiers to provide the medical treatment in case of emergency. Figure 3 shows that the list of applications of wireless body area networks.

2 Security Issues in WBAN

The purpose of network security is to protect data from threats during data transmission. There are two forms of attacks in network security: active and passive attacks, both of which contribute to the detection of malicious data. An active attack is primarily focused on data and has a significant impact on the system's operation. A passive attack damages or modifies data but does not degrade information resources. The security flaws are applied at various levels. Each layer of the TCP/IP layered architecture generates attacks. IP attacks are introduced in the second layer (logic link control), resulting in address spoofing for incorrect communication. Internet Control Message Protocol (ICMP) attacks is generated in the media access control layer, which results in sniffing and man-in-the-middle attacks. In the third network layer, routing attacks such as blackhole and eavesdropping attacks are created. TCP attacks are originated in the transport layer, resulting in high synchronization flooding in data communication. Application layer attacks are generated in the OSI model's application layer, resulting in authentication issues such as accessing the user's username and password [23].

A denial of service (DoS) attack will restrict data from authorized users and prevent them from accessing their resources. Because of the week password, distributed denial of service (DDoS) attacks is generated. The main difference between a DOS and a DDOS attack is that a DOS attack targets a single host at a time, but a DDoS attack targets

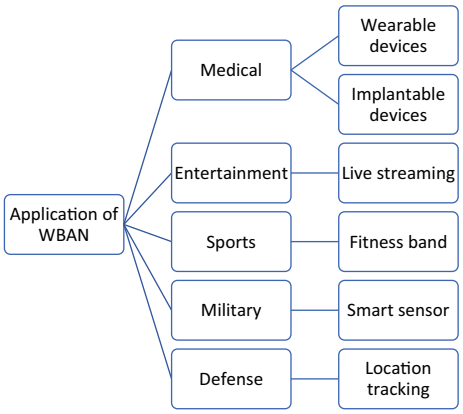

Fig. 3 WBAN applications

numerous hosts simultaneously. These types of attacks will degrade network performance.

Latré et al. [1] describe a detailed survey of wireless body area networks, as well as their limitations and challenges. The author analyzed the process of continuous monitoring and communication between the patients to doctors. To maintain the wireless body area network stability, a cross-layer communication protocol was implemented in a distributed environment. Movassaghi et al. [2] discussed the Micro Electro Mechanical Systems (MEMS) approach in wireless body networks which helps to increase the speed of the data communication, provides reliability and accuracy to users. Here, WBAN is surveyed in all aspects such as insecurity, communication, authentication, link facility, Transmission Control Protocol (TCP) layer, Medium Access Control (MAC) layer, address allocation, dynamic routing, and infrastructure.

Oussama Haddad et al. [3] introduced the new channel impulse model to avoid channel characterization issues in the wireless body area network. The author investigated the patient's movement based on the random waypoint and that will be communicated to the doctor without any inference. The proposed approach improved the channel dc gain, delay spread, and coherence time for the optimal performance of wireless body area networks in telemetry applications. Hussain et al. [4] suggested the lightweight authentication scheme for secure and private data transmission in wireless body area networks. This authentication scheme uses the key hash message authentication with private security keys to transmit the data securely between the patients and doctor. This authentication scheme was designed for wireless body area networks to be implemented in wearable devices with minimal cost. Ramadan et al. [5] proposed the identity-based encryption technique in the RSA algorithm for wireless body area networks. This privacy technique helps to improve the security between the patient's health data transformation. This proposed encryption technique transmits the patient's periodic actions without having to connect to the servers, resulting in security against one-way communication between users. Choudhary et al. [6] discussed the fuzzy-based routing protocol for wireless body area networks to improve security. Biosensor nodes were used to analyze the throughput, latency, and network lifetime of wireless body area networks. Fuzzy logic-based data routing protocol meets the high-quality data standards compared to the existing techniques.

Mehmood et al. [7] suggested reliable cooperative communication in wireless body area networks to improve security and reduces privacy issues. The cryptographic approach was utilized in WBAN benchmarking systems to maintain the key exchange between users and fuzzy logic conditions secure. Fotouhi et al. [8] used the cryptographic hash function scheme with lightweight and forward secure authentication to avoid information attacks and intruders in wireless networks. By using the Real-or Random (ROR) model, the author examined the security level of the wireless networks. Shuai et al. [9] introduced the elliptic curve cryptographic approach with fewer computation for wireless body area networks in order to improve privacy-preserving and authentication. The multi-server architecture was developed without the involvement of any third parties, allowing for more efficient secure data transmission between users as well as high computation efficiency. Haider et al. [10] provides a smart solution for biomedical applications to overcome security issues while transferring the patient's health record data to the doctor. While transmitting data, mitigation of denial of service attacks was introduced, and the user might select an alternate way to avoid such attacks in body area networks.

Kasyoka et al. [11] utilized the elliptic curve cryptographic mechanism for secure data transmission in the wireless body area networks without using the pairing scheme and authentication. This scheme is concentrated on the reduction of computational cost and running time. Shahbazi et al. [12] uses the energy-aware routing protocol for secure communication in wireless body area networks with the support of block-chain technology. This thermal-sensitive routing protocol was designed to combat the high energy consumption and temperature increase in biosensor nodes, and it provided a high throughput, lower delay, and lower routing overhead.

Achour et al. [13] suggested the guaranteed time slots by using a time-division multiplexing scheme for beacon-enabled mode wireless body area networks. This new technique detects malicious attacks by using the guaranteed time slots and helps to overcome the high traffic issues. Selective jamming can be reduced with the assistance of time-division multiple access (TDMA) schemes. This scheme helps to increase the packet delivery ratio and reduces the delay and routing overhead of wireless body area networks. Sridhar et al. [14] discusses the challenges and applications of wireless sensor networks. The most salient applications are as follows:

- *Military Applications* It helps to detect the soldier's health condition while attacks on the battlefield and continuous surveillance. Later, the collected information will be communicated to doctors.
- *Healthcare Applications* It helps to track the continuous health record of patient information, wearable sensor devices, tele-monitoring, integrated patient tracking, and drug distribution.
- *Transportation Applications* It serves to detect real-time live traffic to avoid queuing, jamming, and collision.

- *Environmental Applications* It helps to monitor environmental conditions like heat pressure, moisture conditions in order to take necessary actions.

Jariwala et al. [15] explains the process of adaptable secure data aggregation framework to improve the data integrity, security, and privacy measures in the wearable sensors for the wireless body area networks. This secure data framework improves the homomorphism security approach for the development of data integrity with the help of an aggregation framework. Hasan et al. [16] introduced the software-defined network (SDN) based WBAN for secure data transmission. This technique distributes the patient's health record information based on critical and non-critical patients. Furthermore, by employing the sector-based distance vector (DV) protocol for the earliest contact between patients and doctors, the suggested technique gives non-critical patient communications more priority. Roy et al. [17] explained the security and privacy issues in the wireless body area networks and also suggested adding a cybersecurity mechanism to defend the security challenges. Zhen et al. [18] developed the privacy protection scheme with the cooperation of mobile edge computing for wireless body area networks. Sammoud et al. [19] proposed an innovative routing protocol for secure data communication with the aid of a biometrics-based cryptographic technique. This innovative routing protocol transfers the data with cryptographic keys and also concentrates on minimal power consumption in body area networks. Wang et al. [20] introduced the double hash chains for secure data transmission and it also enables data authenticity and reliability. This proposed scheme supports dynamic conditions and maintains the handover scheme.

3 Security Techniques in WBAN

In wireless body area networks, many security techniques are involved to improve the authentication of data communication between patients and doctors. The most involved techniques are intrusion detection systems and cryptography with key management techniques. Table 1 shows the different security techniques used in the body area network, research issues, and outcomes. Table 2 lists the merits of security-based techniques used in the body area networks.

Table 1 Comparison of security techniques in WBAN

Author[s]	Technique	Research issues	Methodology	Outcome
Bengag et al. [21]	Intrusion detection system	Jamming Attacks	Two MAC Protocols involved (ZIGBEE and TMAC)	Successful packet delivery rate
Arya et al. [22]	IoT based e-health	Data security	Constant monitoring for critical patients	Data authentication and authorization
Al Hayajneh et al. [23]	Cloud-based WBAN	Lesser users	Increased storage level	More users and network lifetime
Thamilarasu et al. [24]	Mobile agent-based IDS	Network-level intrusion attacks	Machine learning and regression algorithms	Accurate results and lesser resource overhead
Umar at.al [25]	Signal propagation-based mutual authentication	Active and passive network attacks	Enables mutual trust and used seed update algorithm	Minimal routing overhead and less computational cost
Dharshini et al. [26]	DMASK-BAN	Vulnerable attacks	Secret key extraction with movement aided from DoS attacks	Minimum power consumption with high QoS
Suchithra et al. [27]	Invariant feature-based approach	High-rate attacks	Maintain the bandwidth conditions in cooperative routing	Low-rate attacks
Kumar et al. [28]	Identity-based anonymous authentication and key agreement	Several security issues	Cloud technology and wireless communication	High storage and low computation cost
Rao et al. [29]	Trust management	High residual power	Fuzzy logic technique	Secure and stable performance
Ali et al. [30]	Enhanced authentication and access control protocol	User impersonation attacks	Bilinear pairing and elliptic curve cryptography	High security

Table 2 Comparison of different security approaches in different aspects

Author[s]	Approaches	Network Utilization	Qualities
Tan et al. [31]	PUF based Cloud assisted Lightweight Authentication	Multi-hop BAN	Lesser storage overhead Lesser resource loss Fewer conflict rates Less channel utilization rate Less packet drop rate High delivery rate
Demir et al. [32]	Cyber-physical systems IWSN Smart Grid WBAN V2X	6G Networks	Security enhancement Multilayer protection High Network lifetime Low latency High reliability Suitable for real-time implementation
Mo et al. [33]	The wearable health monitoring system Known session special temporary information Two-factor authentications Key agreement scheme	Wireless sensor networks	High-security features High efficiency Lesser computational cost Lesser communication overhead Lesser traffic computation
Amel Zendehdel et al. [34]	Telehealth monitoring Bluetooth low energy Wearable device Fingerprinting Vulnerability scanning	Internet of Things	High security High reliability Detection of middleware attacks
Kong et al. [35]	Smart healthcare systems	WBAN	Improves communication security
Jithish et al. [36]	Cyber-physical system Markov Decision Process	WBAN	High Energy efficiency Network longevity Défense the dos and deception attacks
Vyas et al. [37]	Remote health monitoring Health care applications Symmetric key generation Cloud assisted Complex encryption	Wireless communication channels	Intruder identification Improves the security
Damasevicius et al. [38]	Network flow features Different Attack types Cluster Approaches Cybersecurity domain	Wireless sensor network	Network Intrusion detection
Alzahrani et al. [39]	Cloud-based IoT Authentication protocols Remote patient health monitoring Session key	WBAN	Avoiding smart card attacks High secure efficiency
Irshad et al. [40]	Energy internet-based vehicle to grid Cyberattacks The smart grid-based authentication protocol	Wireless network	Lesser computational cost Lesser communication cost

4 Research Issues in Secure WBAN

Table 1 shows the comparison of security techniques in wireless body area networks. Bengag et al. [21] defines the Intrusion detection system techniques to detect jamming attacks in body area sensor networks. In order to enhance the successful packet delivery rate, there are two MAC Protocols are used as ZIGBEE and Timeout Medium Access Control (TMA). Arya et al. [22] discusses the IoT-based e-healthcare systems to improve data security. This e-healthcare technique supports to monitor critical patients continuously and intimate legitimate users for the improvement of data authentication and authorization. Al Hayajneh et al. [23] suggests the cloud-based WBAN for the improvement of storage and the number of users. This approach tends to increase the storage level, the number of users, and network lifetime. Thamilarasu et al. [24] introduces the Mobile agent-based IDS to identify the network-level intrusion attacks. The techniques involved in machine learning and regression algorithms to obtain accurate results and lesser resource overhead. Umar et al. [25] suggested the signal propagation-based mutual authentication scheme to detect active and passive network attacks. Active attacks manipulate the entire content of the data transmission, such as adding extra

characters and spacing between them. Passive attacks are those in which the attackers copy the entire content and reuse it elsewhere. As a result, the mutual authentication technique promotes mutual trust and employs a signal propagation-based seed updating process. This approach minimizes the routing overhead and reduces the computational cost of sensor networks.

Dharshini et al. [26] explains the Denial-of-service proof Movement aided Authenticated Secret Key BAN (DMASK-BAN) scheme to detect vulnerable attacks. This technique helps to extract the secret key to avoid the DoS attacks with minimum power consumption and improves the throughput, delivery rate, and goodput. Suchithra et al. [27] defines the invariant feature-based approach for high-rate network attacks and also maintains the bandwidth conditions of sensor nodes with cooperative routing. Cooperative communication improves the resource nodes and reduces attacks. Kumar et al. [28] suggests the identity-based anonymous authentication and key agreement scheme for several security issues and denial of service attacks. Cloud technology and wireless communication enhances the storage level of the network. High storage levels lead to reduced computational costs with a huge number of users. Rao et al. [29] demonstrates the trust management scheme with fuzzy logic conditions to examine the selfish nodes. The selfish node prevented the user from acting as an intermediary between the two users. Selfish nodes can help to enhance the residual power of wireless body area networks by acting as ideal nodes most of the time. This serves to improve the secure and stable performance of wireless body area networks. Ali et al. [30] proposed the enhanced authentication and access control protocol for the identification of user impersonation attacks along with the bilinear pairing and elliptic curve cryptography to improve the security and sustainability of network architecture. From the Table 1, it is observed that the different techniques were proposed to identify the denial-of-service attacks in order to resolve the security issues in the wireless body area networks. Most of the techniques focused on the detection of intruders, and malicious attackers to avoid the attackers and further improves data security and authenticity.

4.1 Different Security Aspects of Secure WBAN

Tan et al. [31]explained the physical unclonable function (PUF) based cloud-assisted authentication scheme to improve the security performance in multi-hop body area networks. To increase the delivery rate, a lightweight authentication technique is implemented, which results in lower storage overhead, resource loss, conflict rates, channel utilization rate, and packet drop rate. Demir et al. [32] discussed the cyber-physical systems for 6G networks for security enhancement. Smart grid technology is used in the wireless body area network and is adaptable to all applications, including vehicles. The multilayer protection scheme is used to improve the network lifetime, reliability, and low latency which is suitable for real-time applications.

Mo et al. [33] suggested the wearable health monitoring system for known session special temporary information with the two-factor authentications to enhance the security features in a wireless sensor network. A key agreement scheme is involved to improve the security enhancement with high network efficiency and it reduces the computational cost, communication overhead, and traffic computation. Amel Zendehdel et al. introduced the telehealth monitoring scheme with Bluetooth for low energy applications in wearable devices. This scheme involves fingerprinting, biometrics, and vulnerability scanning for high security and high reliability on the internet of things. Kong et al. [35] suggested smart healthcare systems which promotes communication security in wireless body area networks. Jithish et al. [36] discussed the cyber-physical system and used the Markov decision process in wireless body area networks to increase network longevity and energy efficiency, as well as to defend against denial of service and deception attacks.

Vyas et al. [37] discussed the remote health monitoring scheme for health care applications with the help of the Symmetric key generation method. Cloud-assisted technology is involved to improve the storage level in wireless communication channels. Complex encryption techniques are used to identify intruders and strengthen security. Damasevicius et al. [38] explained the network flow features to detect the different types of attackers by using the cybersecurity mechanism in wireless sensor networks. Alzahrani et al. [39] explained the cloud-based IoT scheme for remote patient health monitoring in body area networks. Authentication protocols with session key mechanisms to avoid smart card attacks and improves efficiency. Irshad et al. [40] described how to detect cyber-attacks in wireless networks using a smart grid-based authentication protocol for energy and internet-based vehicle to grid networks. These smart grid networks boost energy efficiency while also lowering computing and communication expenses.

5 Research Challenges in Secure WBAN

Pandey et al. [41] explained the security applications of wireless body area networks and the security improvement of wireless sensor networks. WBAN provides a key ideal solution to improve security enhancement by using biometric and key management schemes. This technique provides authenticity and confidentiality between the patients and doctors. Dhanvijay et al. [42] discussed the IoT-based healthcare application system for high-security enhancement in wireless sensor networks. An Advanced encryption

standard cipher scheme with elliptic curve digital signatory algorithm is utilized to reduce the network and handover delays. Mishra et al. [43] improved the security, privacy issues in the wireless body area networks and also discussed the challenges and research issues. Arfaoui et al. [44] proposed the game-based virtual multiple-input and multiple-output (MIMO) approach to enhance the security application on the internet of things (IoT). Traditional cryptographic techniques are not suitable for this internet of things and biomedical applications. A new proposed scheme enhances the physical layer security in wireless communication channels and this cooperative communication improves the security level. Narwal et al. [45] introduced the Secured, Anonymity Preserving, and Lightweight Mutual Authentication and Key Agreement Scheme (SALMAKA). These techniques improve the security features by using two-hop topologies. This scheme reduces energy consumption, processing cost, computational cost and utilizes the simulation time significantly to obtain high network efficiency.

Khan et al. [46] implemented a key generation scheme for wireless body area networks and communicated via GSM/GPRS from the patient body to the hospital monitoring system. Saif et al. [47] suggested cloud-assisted secure data transmission and provided a cost-effective solution by using advanced encryption standards. This scheme reduces the permissible delay in peak hours for medical applications. Demir et al. [48] proposed the energy scavengers' techniques for biomedical applications to improve security and reduces energy consumption. Batteries are replaced to update the energy reservation with low power systems. Izza et al. [49] explained the security features in wireless body area networks and implemented mutual authentication schemes to increase the patient's privacy. Dodangeh et al. [50] used the biometrics scheme for security applications in wireless body area networks. Biometric uses third-party key exchange protocols, access control mechanisms, and key generation schemes for secure data transmission between the users. Al-Janabi et al. [51] surveyed the security threats and attackers in wireless body networks. Many strategies are explored and suggested as research challenges and issues in wireless body area networks, including cluster-based detection, cloud-assisted intrusion detection, and ad-hoc based communication. Baqai et al. [52] explained the node identification scheme to reduce the inherence rejection in optical-based wireless body area networks. This scheme was implemented by using an energy-efficient security protocol for mobile applications. Salayma et al. [53] explained the fault tolerance issues in wireless body area networks to improve the reliability and reduce the complexity of e-health care applications. Asif et al. [54] explained the applications of wireless body area networks such as medical, electronics, gaming, military, healthcare, emergency services, sports activities, and lifestyle activities. Bhanumathi et al. [55] explained the thermal energy-aware routing protocol to prove the energy efficiency in wireless body area networks. The author suggested a suitable routing protocols such as QoS-centric, reliable routing approach, and data routing in critical situations for healthcare applications.

Al Shayokh et al. [56] proposed the utilization of a time-static energy-efficient clustering algorithm and an encryption scheme in wireless body area networks. This scheme focused on energy consumption and security issues. Khalilian et al. [57] introduced a proposed scheme to prevent spoofing techniques in wireless body area networks. Spoofing attacks will steal the information. Patients' information will be stored in wireless body area networks, and also that data will be transferred to users. Mukhtar et al. [58] proposed the scheme to improve the quality of services (QoS) in the wireless body area networks by using cloud computing technology, software-defined networks, and Kerberos systems for secure and safe communication. Mukhtar et al. [58] introduced human body communication (HBC) to enhance security in wireless body area networks. Ibrahim et al. [59] introduced a new star two-tier topology in wireless body area networks for secure authentication and confidential data transmission. This scheme helps to progress network efficiency and security.

5.1 Evolution of WBAN

Table 3 shows the developments of wireless body area networks in the last five years from the range of 2016 to 2020. In 2016, general techniques such as clustering algorithms, encryption techniques are used to improve network efficiency. In 2017, cloud-based detection and cluster-based detection techniques are utilized to identify the attackers. In 2018, biometrics and key exchange techniques are applied to improve the security and authentication scheme in wireless body area networks. In 2019, advanced techniques such as elliptical curve cryptography techniques are adopted to concentrate on network quality. In 2020, trending techniques are involved to improve network quality and secure communication.

6 Research gap IN WBAN

From this observation, the body area network focused only on security to improve network quality. Wireless body area networks are used in the medical healthcare field to collect the patient's information. Hence, the Patient's emergency needs to be more concentrated when compared to security. The majority of the researchers focused on the successful and secure communication of patient data with the doctor. If the patient is in an emergency, the data must reach the

Table 3 Developments of WBAN

Year	Techniques involved	Network utilized	Merits
2020	Cloud-based IoT Authentication protocols Remote patient health monitoring Session key Key management	WBAN, Wireless sensor networks, Internet of Things, Wireless networks	Detecting intruders High secure efficiency Less computational cost High-Security features High efficiency Less communication overhead Less traffic computation High security High reliability Detection of middleware attacks
2019	Biometrics Key management Advanced encryption cipher Elliptical curve digital signatory Secured, anonymity preserving and lightweight mutual authentication and key agreement scheme (SALMAKA)	Wireless body area networks, Wireless sensor networks, Internet of things, Cooperative communication	Authenticity Confidentiality Fewer handover delays Less energy consumption Less computational cost
2018	Biometrics Third-party key exchange protocol Cloud computing Battery replacement	Sensor network, Body area network, GSM, GPRS	Less energy consumption High security
2017	Cluster-based detection Cloud assisted intrusion Routing protocols Many surveys were involved	Body area networks based on optical and wireless	Less energy consumption Attacker detection
2016	Clustering algorithm Encryption Attack's detection Cloud computing Mutual authentication scheme	WBAN, HBC, Star topology	Network efficiency Less energy consumption High secure communication

doctor without delay, and the critical patient's information must take precedence.

6.1 Observations from Security Issues

For the past five years, the following factors have been identified and focused on wireless body area networks, as illustrated in Fig. 4.

The security measures concentrated on the security and privacy issues and resolve the authentication issues. Energy consumption focused on the reduction of energy utilization in wireless body area networks with the help of clustering and routing protocols. Clustering technology addresses the active nodes to be cluster heads and controls the energy level of cluster members. Network lifetime has been increased by saving energy. The key management scheme introduces the session key, mutual authentication scheme, and implemented in cryptographic techniques. Attacker detection will detect all types of denial-of-service attacks based on the resemblance of the attacks. This is used to find the attacker type based on the working process and outcome of the body area network. Intruder avoidance helps to move the next process of attacker detection. After detecting the attacker type, this intruder avoidance provides the solution and helps to take an alternate path for efficient communication.

6.2 Focusing Factors of WBAN

The following factors need to be implemented in the future for efficient wireless body area networks which is shown in Fig. 5.

Interoperability helps to improve the scalability of the wireless body area networks. Here, patient information need to be transferred to the doctor based on priority. Priority is given to the emergency patients and should be immediately reported to the doctor. Faster and more secure communication aids in the handling of emergency situations, ultimately saving the patient's life. The constrained deployment should not disturb others during deployments. Complexity should be lesser during network installments. The end-user depends on the successful data transmission between the doctor and patient without any interruption.

Table 4 Cryptographic Techniques based on obtained results from existing techniques

Different cryptographic techniques based on obtained results		
Techniques	Reliability (%)	Accuracy (%)
Biometrics techniques [19]	82	78
Key management scheme [41]	79	81
Mutual authentication scheme [25]	89	85
Session key arrangement scheme [39]	83	87
Elliptical curve cryptography [11]	87	89
Lightweight Scheme [31]	82	83
Trust management scheme [29]	70	72

7 Discussions and Recommendations

Al Barazanchi et al. [60] explained a detailed survey between short-range and long-range communications technologies in wireless body area networks. Depending on the frequency requirement and application of transactions, a different range of communication technologies will be used. Ayed et al. [61] discussed the trust management scheme and highlights the trust frameworks in wireless body area networks. Mallavarapu et al. [62] introduced wearable technologies for flexible antennas to improve the gain, bandwidth, and low cost. Sharma et al. [63] focused on secure and efficient data transmission in the body area network which further highlights the glitches of existing techniques. Sultana et al. [64] developed the new routing protocol on the internet of medical things to improve the

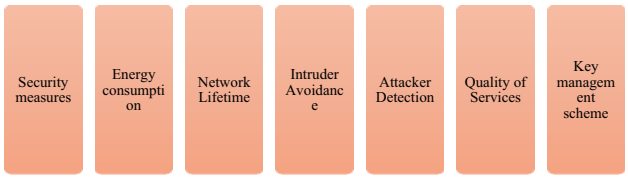

Fig. 4 WBAN factors focused for the past 5 years

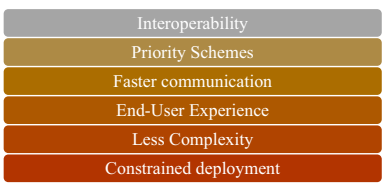

Fig. 5 Future focusing factors of WBAN

throughput and reduce the delay for wireless body area networks. Singh et al. [65] explained the different architectures of wireless body area networks and it concentrates on the less cost and low power device. Sharn et al. [66] discussed the privacy and security issues based on the different biometric techniques. Arora et al. [67] introduced a suitable central node for lesser energy efficiency in the wireless body area networks. Qadri et al. [68] explained how the system changes from wireless body area networks to healthcare internet of things (H-IoT) and this helps to leads future directions in all recent aspects such as blockchain technology, software-defined network, and tactile internet. Latha et al. [69] implemented a Bayesian approach in wireless body area networks for emergencies and a high priority for emergency messages.

7.1 Parameter's Definition

The following parameters are used to analyze the security measures in WBAN such as reliability, accuracy, delivery rate, delay, and throughput. Reliability is calculated based on the performance of nodes and the network lifetime. Equation 1 states that the reliability calculation for the whole network. Where, s denotes the end time of simulation, i denotes the starting time of simulation, L denotes Lifetime, and N denotes Node user. The accuracy calculation for the entire network is given in Eq. 2. Where S(Rs) is defined as the network's selection of a reliable server. Reliable servers are determined by which node has a longer network lifetime than the other node servers after the simulation is completed.

$$R = \sum_{i=1}^{s} L(Ns) \tag{1}$$

$$A = S(Rs)x100\% \tag{2}$$

The delivery rate is defined as the number of data received during transmission which is shown in Eq. 3. Delay is defined as the time taken to transmit the data from the end-users which is shown in Eq. 4. Throughput is defined as the ratio of the number of packets received to the overall network time taken to transmit the data which is shown in Eq. 5.

Table 5 Attacker Detection Techniques based on obtained results from existing techniques

Different attacker detection techniques based on obtained results	
Techniques	Delivery rate (%)
Spoofing attacker [57]	75
Jamming Attack [21]	72
DoS Attacks [36]	82
Vulnerable attacks [26]	84
High and low-rate attacks [27]	89
Different methodologies obtained results using WBAN	
Methodologies	Throughput (Mbps)
Clustering technology [38]	1.8
Efficient routing protocol [6]	1.4
Cloud assisted technology [23]	1.9

$$D(\%) = \frac{D(r)}{D(t)} x100 \tag{3}$$

$$Dy = T(n) - T(i) \tag{4}$$

$$T = D(r)/s \tag{5}$$

where D (%) represents delivery rate in percentage, D(r) denotes the number of packets received, D(t) denotes the transmitted packets. Dy represents the delay, T(n) denotes the time reached nth node and T(i) denotes the time initiated at the ith node. T represents the throughput and s represents the simulation time.

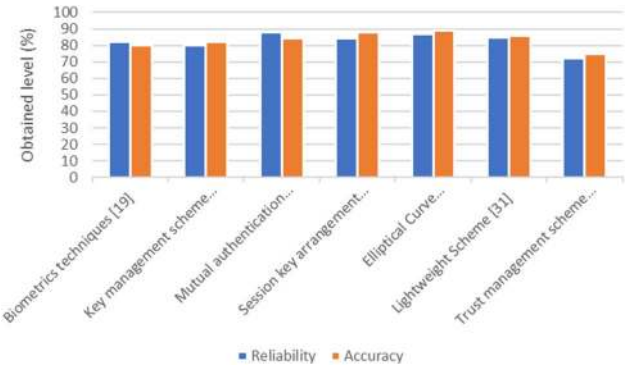

Fig. 6 Comparison of cryptographic techniques

7.2 Discussions

From the discussion of previous sections, this survey realizes the wireless body area networks focused on the security and privacy issues by using cryptographic techniques, attackers' detection techniques, and general techniques. Tables 4 and 5 shows that the different cryptographic and attacker techniques results obtained from the existing technqiues.

The following cryptographic techniques concentrate on the security and privacy issues and obtained efficient results such as high reliability and accuracy.

- Biometrics techniques [19]
- Key management scheme [41]
- Mutual authentication scheme [25]
- Session key arrangement scheme [39]
- Elliptical Curve cryptography [11]
- Lightweight Scheme [31]
- Trust management scheme [29]

Figure 6 shows a comparison of cryptographic techniques. Biometrics techniques [19] obtained the 82% of reliability and 78% of accuracy. The key management scheme [41] obtained the 79% of reliability and 81% of accuracy. Mutual authentication scheme [25] obtained the 89% of reliability of 85% of accuracy. The session key arrangement scheme [39] obtained the 83% of reliability and 87% of accuracy. Elliptical Curve cryptography [11] obtained the 87% of reliability and 89% of accuracy. Lightweight Scheme [31] obtained the 82% of reliability and 83% of accuracy. Trust management scheme [29] obtained the 70% of reliability and 72% of accuracy. When compared to other techniques mutual authentication scheme achieves higher reliability and the elliptical curve cryptographic technique achieves high accuracy in wireless body area networks.

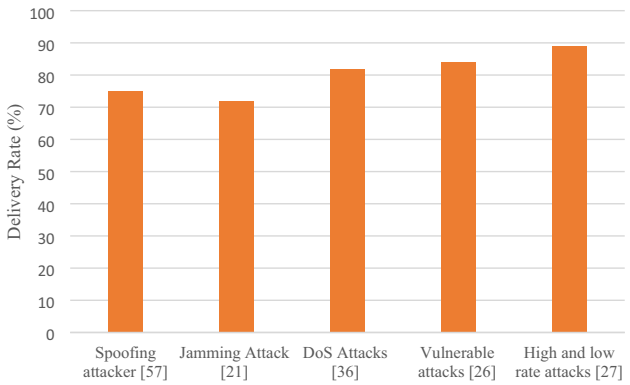

Fig. 7 Comparison of attacker detection techniques

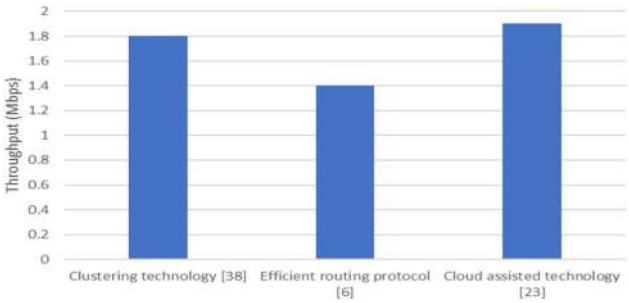

Fig. 8 Comparison of different techniques

The following attacker detection techniques concentrate on the identification of attackers and provide a solution to overcome the attackers. This type of attack concentrates on efficient results such as a high delivery rate and lesser delay.

- Spoofing attacker [57]
- Jamming Attack [21]
- DoS Attacks [36]
- Vulnerable attacks [26]
- High and low-rate attacks [27]

Figure 7 shows the comparison of attacker detection techniques. Spoofing attacker detection method [57] obtained the 75% of delivery rate after detecting the attacks, Jamming Attack detection method [21] obtained the 72% of the delivery rate, DoS attack detection method obtained 82% of delivery rate, Vulnerable attack detection methods [26] obtained 84% of delivery rate and High and low-rate attack detection method [27] obtained the 89% of delivery rate. Here high and low-rate attacks achieve a higher delivery rate and that leads to lesser delay compared to other techniques.

The following general techniques concentrate on the improvement of energy efficiency with secure communication. This provides efficient results such as high throughput and network lifetime.

- Clustering technology [38]
- Efficient routing protocol [6]
- Cloud assisted technology [23]

Figure 8 shows that the comparison of different techniques in wireless body area networks and cloud-assisted technology has high throughput due to high storage server and clustering technology has a high network lifetime due to lesser energy consumption. Clustering technology [38] obtained the throughput of 1.8 Mbps, Efficient routing protocol [6] obtained the throughput of 1.4 Mbps and Cloud assisted technology [23] obtained the throughput of 1.9 Mbps.

7.3 Recommendation

Mucchi et al. [70] suggested the 6G technology for healthcare applications and the adoption of ICT technology produced a drastic improvement in future healthcare systems. The prominent factors included in 6G technology provide the high speed and high communication between the users. Devi et al. [71] provided new insights to the research community with the help of unmanned aerial vehicles in order to monitor the patients and disinfect common areas. Garg et al. [72] explained the advantage of flying ad-hoc networks and the importance of unmanned aerial vehicle transmission. Ali et al. [73] introduced the routing aware mechanism of flying ad-hoc networks. The unmanned aerial vehicle possesses sudden topology changes, fastest data transmission, next-hop selection and also eliminates the dissemination loops with the efficient routing mechanism in Flying AdHoc Network (FANET). Mucchi et al. [74] explained the overview of security threats in WBAN, and this article differentiates the in or on-body architecture. Current trending factors such as secure mobile communication, cross-technology machine, physical layer security, cognitive radio, and block-chain plays a vital role in healthcare applications.

The limitations of flying ad-hoc networks include high node mobility and random topological changes [75], which results in a high drop rate and less security. The advantage of FANET includes a high delivery rate with the fastest communication due to the direct line of sight path between the unmanned aerial vehicles. The process of transmitting patient data using an unmanned aerial vehicle in a flying ad-hoc network is known as a flying body area network.

After summarizing all the above points, this investigation recommends the implementation of body area networks with unmanned aerial vehicles for secure and faster communication. To overcome the limitation of wireless body area networks, the advantage of flying ad hoc networks and flying

body area networks with unmanned aerial vehicles helps to improve the interoperability and constrained deployment in healthcare applications. This will assist the patients to reach the doctor remotely without any interruptions. The speed of data transmission from patient to doctor can be enhanced with the use of flying body area networks. This flying body area network concentrates on the improvement of data speed and data security during data transmission.

8 Conclusion

In the current scenario, WBAN is emerging as a salient approach in the healthcare field. This demanding network helps to transmit the data from the patient to the doctor without any disturbances. Remote e-health monitoring is a demanding scheme in healthcare and biomedical applications. Security, privacy, energy efficiency, network lifetime, computational overhead, packet delivery rate is to be concentrated in wireless body area networks. This investigation summarizes the issues, challenges, developments, and security limitations in a wireless body area network. Various techniques are involved in secure WBAN are cryptography, attacker detection, denial of service attacks, cloud-assisted schemes, clustering schemes, routing protocols and privacy issues. These techniques concentrated on the quality of services such as high throughput, lesser delay, and drop rate. It is observed that the research issues and recommended flying ad-hoc networks for healthcare applications is utilized to obtain faster and secure communication in this COVID-19 situation. Unmanned aerial vehicle transmission leads to make faster communication by using the internet and also without any human interruptions. This contributes to the realization of future possibilities in all domains of biological applications.

References

1. Benoît Latré, Bart Braem, Ingrid Moerman, Chris Blondia and Piet Demeester, A survey on wireless body area networks, *Wireless networks*, Vol. 17, No. 1, pp. 1–18, 2011.
2. Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith and Abbas Jamalipour, Wireless body area networks: A survey, *IEEE Communications surveys & tutorials*, Vol. 16, No. 3, pp. 1658–1686, 2014.
3. Oussama Haddad, Mohammad-Ali. Khalighi, Stanislav Zvanovec and Mouloud Adel, Channel characterization and modeling for optical wireless body-area networks, *IEEE Open Journal of the Communications Society*, Vol. 1, pp. 760–776, 2020.
4. Hussain, Syed Jawad, Muhammad Irfan, N. Z. Jhanjhi, Khalid Hussain, and Mamoona Humayun. Performance Enhancement in Wireless Body Area Networks with Secure Communication. *Wireless Personal Communications*, pp. 1–22, 2020.
5. Mohammed Ramadan, Yongjian Liao, Fagen Li, Shijie Zhou and Hisham Abdalla, IBEET-RSA: Identity-based encryption with equality test over RSA for wireless body area networks, *Mobile Networks and Applications*, Vol. 25, No. 1, pp. 223–233, 2020.
6. Amit Choudhary, M. Nizamuddin and Vibhav Kumar Sachan, A hybrid fuzzy-genetic algorithm for performance optimization of cyber physical wireless body area networks, *International Journal of Fuzzy Systems*, Vol. 22, No. 2, pp. 548–569, 2020.
7. Gulzar Mehmood, Muhammad Zahid Khan, Abdul Waheed, Mahdi Zareei and Ehab Mahmoud Mohamed, A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks, *IEEE Access*, Vol. 8, pp. 131397–131413, 2020.
8. Fotouhi, Mahdi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S. Morteza Pournaghi, and M. A. Doostari. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks* (2020): 107333.
9. Mengxia Shuai, Bin Liu, Yu. Nenghai, Ling Xiong and Changhui Wang, Efficient and privacy-preserving authentication scheme for wireless body area networks, *Journal of Information Security and Applications*, Vol. 52, pp. 102499, 2020.
10. Zeeshan Haider, Tauseef Jamal, Muhammad Asam, Shariq Butt and Aleena Ajaz, Mitigation of Wireless Body Area Networks Challenges Using Cooperation, *International Journal of Security and Its Applications*, Vol. 14, No. 1, pp. 15–30, 2020.
11. Philemon Kasyoka, Michael Kimwele and Shem Mbandu Angolo, Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system, *Journal of Medical Engineering & Technology*, Vol. 44, No. 1, pp. 12–19, 2020.
12. Zeinab Shahbazi and Yung-Cheol. Byun, Towards a Secure Thermal-Energy Aware Routing Protocol in Wireless Body Area Network Based on Blockchain Technology, *Sensors*, Vol. 20, No. 12, pp. 3604, 2020.
13. Achour, M'hammed, M. A. N. A. Mohammed, and Abderrezak Rachedi. On the issues of selective jamming in IEEE 802.15. 4-based wireless body area networks. *Peer-to-Peer Networking and Applications* pp. 1–16, 2020.
14. Sridhar, M., N. Priya, and A. Muniyappan. Wireless body area networks: requirements, characteristics, design consideration, and challenges. In *Incorporating the Internet of Things in Healthcare Applications and Wearable Devices*, pp. 67–85. IGI Global, 2020.
15. Jariwala, Vivaksha J., and Devesh C. Jinwala. AdaptableSDA: secure data aggregation framework in wireless body area networks. In *Wearable and Implantable Medical Devices*, pp. 79–114. Academic Press, 2020.
16. Khalid Hasan, Khandakar Ahmed, Md. Kamanashis Biswas, Saiful Islam and Omid Ameri Sianaki, Software-defined application-specific traffic management for wireless body area networks, *Future Generation Computer Systems*, Vol. 107, pp. 274–285, 2020.
17. Roy, Moumita, Chandreyee Chowdhury, and Nauman Aslam. Security and Privacy Issues in Wireless Sensor and Body Area Networks. In *Handbook of Computer Networks and Cyber Security*, pp. 173–200. Springer, Cham, 2020.
18. Yan Zhen and Hanyong Liu, Distributed privacy protection strategy for MEC enhanced wireless body area networks, *Digital Communications and Networks*, Vol. 6, No. 2, pp. 229–237, 2020.
19. Sammoud, Amal, Mohamed Aymen Chalouf, Omessaad Hamdi, Nicolas MONTAVONT, and Ammar BOUALLEGUE. A new biometrics-based key establishment protocol in WBAN: energy efficiency and security robustness analysis. *Computers & Security*, 101838, 2020.

20. Wang, Weichao, Tuanfa Qin, and Yu Wang. Encryption-free Data Transmission and Hand-over in Two-tier Body Area Networks. *Computer Methods and Programs in Biomedicine*, 105411, 2020
21. Bengag, Asmae, Amina Bengag, and Omar Moussaoui. Effective and Robust Detection of Jamming Attacks for WBAN-Based Healthcare Monitoring Systems. In *International Conference on Electronic Engineering and Renewable Energy*, pp. 169–174. Springer, Singapore, 2020.
22. Arya, K. V., and Rajasi Gore. Data security for WBAN in e-health IoT applications. In *Intelligent Data Security Solutions for e-Health Applications*, pp. 205–218. Academic Press, 2020.
23. Al Hayajneh, Abdullah, Md Zakirul Alam Bhuiyan, and Ian McAndrew. Security of Broadcast Authentication for Cloud-Enabled Wireless Medical Sensor Devices in 5G Networks. *Computer and Information Science* 13, no. 2: 1–13, 2020.
24. Thamilarasu, Geethapriya, Adedayo Odesile, and Andrew Hoang. An Intrusion Detection System for Internet of Medical Things. *IEEE Access* 2020.
25. Mubarak Umar, Wu. Zhenqiang and Xuening Liao, Mutual Authentication in Body Area Networks Using Signal Propagation Characteristics, *IEEE Access*, Vol. 8, pp. 66411–66422, 2020.
26. S. Dharshini and M. Monica Subashini, DMASK-BAN: Improving the security of body area networks, *Computer Fraud & Security*, Vol. 5, pp. 13–19, 2020.
27. Suchithra, M., M. Baskar, J. Ramkumar, P. Kalyanasundaram, and B. Amutha. Invariant packet feature with network conditions for efficient low rate attack detection in multimedia networks for improved QoS. *Journal of Ambient Intelligence and Humanized Computing*, 2020.
28. Kumar, Mahender, and Satish Chand. A Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network. *IEEE Systems Journal*, 2020.
29. J. Durga. Rao and K. Sridevi, Novel security system for wireless body area networks based on fuzzy logic and trust factor considering residual energy, *Materials Today: Proceedings*, Vol. 45, pp. 1498–1501, 2020.
30. Zeeshan Ali, Anwar Ghani, Imran Khan, Shehzad Ashraf Chaudhry, S. K. Hafizul Islam and Debasis Giri, A robust authentication and access control protocol for securing wireless healthcare sensor networks, *Journal of Information Security and Applications*, Vol. 52, pp. 102502, 2020.
31. Xiao Tan, Jiliang Zhang, Yuanjing Zhang, Zheng Qin, Yong Ding and Xingwei Wang, A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network *Tsinghua Science and Technology*, Vol. 26, No. 1, pp. 36–47, 2020.
32. Demir, Mehmet Ozgun, Ali Emre Pusane, Guido Dartmann, Gerd Ascheid, and Gunes Karabulut Kurt. A Garden of Cyber Physical Systems: Requirements, Challenges and Implementation Aspects. *IEEE Internet of Things Magazine*, 2020.
33. Mo, Jiaqing, Wei Shen, and Weisheng Pan. An Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems. *Wireless Communications and Mobile Computing*, 2020.
34. Amel Zendehdel, Ghazale. A semi-automated security assessment framework for wearable health monitoring devices. PhD diss., University of New Brunswick., 2020.
35. Kong, Dehua, Hongyan Dong, Huyuan Li, and Bo Zhang. Research on Data Security of Wireless Body Area Network. In *2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, pp. 132–135. IEEE, 2020.
36. Jithish, J., Sriram Sankaran, and Krishnashree Achuthan. A Decision-centric approach for secure and energy-efficient cyber-physical systems. *Journal of Ambient Intelligence and Humanized Computing*, 2020.
37. Vyas, Avani, and Sujata Pal. Preventing Security and Privacy Attacks in WBANs. In *Handbook of Computer Networks and Cyber Security*, pp. 201–225. Springer, Cham, 2020.
38. Robertas Damasevicius, Algimantas Venckauskas, Sarunas Grigaliunas, Jevgenijus Toldinas, Nerijus Morkevicius, Tautvydas Aleliunas and Paulius Smuikys, LITNET-2020: An Annotated Real-World Network Flow Dataset for Network Intrusion Detection, *Electronics*, Vol. 9, No. 5, pp. 800, 2020.
39. Alzahrani, Bander A., Azeem Irshad, Khalid Alsubhi, and Aiiad Albeshri. A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT. *International Journal of Communication Systems*, p. e4423, 2020.
40. Irshad, Azeem, Muhammad Usman, Shehzad Ashraf Chaudhry, Husnain Naqvi, and Muhammad Shafiq. A provably secure and efficient authenticated key agreement scheme for Energy Internet based Vehicle-to-Grid technology framework. *IEEE Transactions on Industry Applications*, 2020.
41. Pandey, Indrajit, Himadri Sekhar Dutta, and Jyoti Sekhar Banerjee. WBAN: a smart approach to next generation e-healthcare system. In *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 344–349. IEEE, 2019.
42. Dhanvijay, Mrinai M., and Shailaja C. Patil. Optimized mobility management protocol for the IoT based WBAN with an enhanced security. *Wireless Networks*, pp. 1–19, 2020.
43. Mishra, Kumari Sadhana, and Ashish Kumar Sinha. An Overview of Security Issues in Wireless Body Area Network (WBAN) for Healthcare Applications.
44. Arfaoui, Amel, Ali Kribeche, and Sidi Mohammed Senouci. Cooperative MIMO for Adaptive Physical Layer Security in WBAN. In *ICC 2020–2020 IEEE International Conference on Communications (ICC)*, pp. 1–7. IEEE, 2020.
45. Narwal, Bhawna, and Amar Kumar Mohapatra. SALMAKA: Secured, Anonymity Preserving and Lightweight Mutual Au-thentication and Key Agreement Scheme for WBAN. *International Journal Of Sensors, Wireless Communications And Control* Vol. 10: p. 1, 2020.
46. Fozia Hanif Khan, Rehan Shams, Huma Hasan Rizvi and Farheen Qazi, A secure crypto base authentication and communication suite in Wireless Body Area Network (WBAN) for IoT applications, *Wireless Personal Communications*, Vol. 103, No. 4, pp. 2877–2890, 2018.
47. Saif, Sohail, Rajni Gupta, and Suparna Biswas. Implementation of cloud-assisted secure data transmission in WBAN for healthcare monitoring. In Advanced Computational and Communication Paradigms, pp. 665–674. Springer, Singapore, 2018.
48. Süleyman Mahircan. Demir, Fadi Al-Turjman and Ali Muhtaroğlu, Energy scavenging methods for WBAN applications: A review, *IEEE Sensors Journal*, Vol. 18, No. 16, pp. 6477–6488, 2018.
49. Izza, Sarah, Mustapha Benssalah, and Rabah Ouchikh. Security improvement of the enhanced 1-round authentication protocol for wireless body area networks. In *2018 International Conference on Applied Smart Systems (ICASS)*, pp. 1–6. IEEE, 2018.
50. Peyman Dodangeh and Amir Hossein Jahangir, A biometric security scheme for wireless body area networks, *Journal of Information Security and Applications*, Vol. 41, pp. 62–74, 2018.
51. Samaher Al-Janabi, Ibrahim Al-Shourbaji, Mohammad Shojafar and Shahaboddin Shamshirband, Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications, *Egyptian Informatics Journal*, Vol. 18, No. 2, pp. 113–122, 2017.
52. Attiya Baqai, Fahim Aziz Umrani and Bhawani S. Chowdhry, A novel protocol with patient and node identification for optical wban with inherent security and interference rejection, *Wireless Personal Communications*, Vol. 95, No. 4, pp. 4211–4224, 2017.
53. Marwa Salayma, Ahmed Al-Dubai, Imed Romdhani and Youssef Nasser, Wireless body area network (WBAN) a survey on

reliability, fault tolerance, and technologies coexistence, *ACM Computing Surveys (CSUR)*, Vol. 50, No. 1, pp. 1–38, 2017.
54. Asif, Amna, and Irshad Ahmed Sumra. Applications of wireless body area network (wban): A survey. *Engineering Science and Technoogy. International. Research Journal*, pp. 64–71, 2017.
55. V. Bhanumathi and C. P. Sangeetha, A guide for the selection of routing protocols in WBAN for healthcare applications, *Human-centric Computing and Information Sciences*, Vol. 7, No. 1, pp. 24, 2017.
56. Al Shayokh, Md, Abebe Abeshu, G. B. Satrya, and M. A. Nugroho. Efficient and secure data delivery in software defined WBAN for virtual hospital. In *2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, pp. 12–16. IEEE, 2016.
57. Reza Khalilian, Abdalhossein Rezai and Farhad Mesrinejad, Secure wireless body area network (WBAN) communication method using new random key management scheme, *International journal of security and its applications*, Vol. 10, No. 11, pp. 13–22, 2016.
58. Mukhtar, Taha, and Sumit Chaudhary. Energy efficient cluster formation and secure data outsourcing using TEOSCC and ECDH-IBT technique in WBAN. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 596–602. IEEE, 2016.
59. Maged Hamada Ibrahim, Saru Kumari, Ashok Kumar Das, Mohammad Wazid and Vanga Odelu, Secure anonymous mutual authentication for star two-tier wireless body area networks, *Computer methods and programs in biomedicine*, Vol. 135, pp. 37–50, 2016.
60. Al. Barazanchi, Haider Rasheed Israa, M. Safiah. Abdulshaheed and B. Sidek, A Survey: Issues and challenges of communication technologies in WBAN, *Sustain. Eng. Innov*, Vol. 1, No. 2, pp. 84–97, 2020.
61. Samiha Ayed, Lamia Chaari and Amina Fares, A Survey on Trust Management for WBAN: Investigations and Future Directions, *Sensors*, Vol. 20, No. 21, pp. 6041, 2020.
62. Mallavarapu, Sandhya, and Anjaneyulu Lokam. A Critical Survey on Fractal Wearable Antennas with Enhanced Gain and Bandwidth for WBAN. In *Inventive Communication and Computational Technologies*, pp. 737–745. Springer, Singapore.
63. Rajeev Sharma and Sandeep Singh Kang, WBAN For Healthcare Applications: A Survey of Current Challenges And Research Opportunities, *Journal of Critical Reviews*, Vol. 7, No. 17, pp. 2444–2453, 2020.
64. Sultana, Saima, Shamim Akhtar, Sadia Nazim, Pardeep Kumar, Manzoor Ahmed Hashmani, and Syed Sajjad Hussain Rizvi. A Critical Study on Internet of Medical Things for Secure WBAN. In *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital*, pp. 179–197. IGI Global, 2020.
65. Singh, Ritika, Shreya Sinha, Sunidhi Anand, and Mainak Sen. Wireless Body Area Network: An Application of IoT and Its Issuses—A Survey. In *Computational Intelligence in Pattern Recognition*, pp. 285–293. Springer, Singapore, 2020.
66. Sharn, Hari Om, and Nidhi Dubey. An Improved method for Wireless Body Area Network Security and Privacy Issue in E-Healthcare: A Survey.
67. Arora, Neha, Sindhu Hak Gupta, and Basant Kumar. An approach to investigate the best location for the central node placement for energy efficient WBAN. *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–12, 2020.
68. Yazdan Ahmad Qadri, Ali Nauman, Yousaf Bin Zikria, Athanasios V. Vasilakos and Sung Won Kim, The Future of Healthcare Internet of Things: A Survey of Emerging Technologies, *IEEE Communications Surveys & Tutorials*, Vol. 22, No. 2, pp. 1121–1167, 2020.
69. R. Latha and P. Vetrivelan, Wireless Body Area Network (WBAN)-Based Telemedicine for Emergency Care, *Sensors*, Vol. 20, No. 7, pp. 2153, 2020.
70. Mucchi, Lorenzo, Sara Jayousi, Stefano Caputo, Elisabetta Paoletti, Paolo Zoppi, Simona Geli, and Pietro Dioniso. How 6G technology can change the future wireless healthcare. In *2020 2nd 6G wireless summit (6G SUMMIT)*, pp. 1–6. IEEE, 2020.
71. Devi, Manisha, Sunil Kumar Maakar, Deepak Sinwar, Mahesh Jangid, and Poonam Sangwan. Applications of Flying Ad-hoc Network During COVID-19 Pandemic. In *IOP Conference Series: Materials Science and Engineering*, vol. 1099, no. 1, p. 012005. IOP Publishing, 2021.
72. Garg, P. K. Potentials of Network-Based Unmanned Aerial Vehicles. *Cloud and IoT-Based Vehicular Ad Hoc Networks*, pp. 369–397, 2021.
73. Hannan Ali, Saiful Islam, Houbing Song and Kashif Munir, A performance-aware routing mechanism for flying ad hoc networks, *Transactions on Emerging Telecommunications Technologies*, Vol. 32, No. 1, pp. 4192, 2021.
74. Mucchi, Lorenzo, Sara Jayousi, Alessio Martinelli, Stefano Caputo, and Patrizio Marcocci. An overview of security threats, solutions and challenges in wbans for healthcare. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, pp. 1–6. IEEE, 2019.
75. Ananthi, J. Vijitha, and P. Subha Hency Jose. A Review on Various Routing Protocol Designing Features for Flying Ad Hoc Networks. In *Mobile Computing and Sustainable Informatics*, pp. 315–325. Springer, Singapore, 2022.

J. Vijitha Ananthi received her B.E. in Electronics and Communication from the Anna University, in 2010. She received her Master's degree in Communication System from the Karunya University, India. Currently, she is pursuing Ph.D. in Karunya Institute of Science of Technology, India. Her research interest includes overlay in wireless networks, QoS improvement and topology control structures. She has published more research articles in reputed journals and conferences.

P. Subha Hency Jose received her B.E. in Bio Medical Instrumentation Engineering, M.E in Process Control and Instrumentation. She obtained her Ph.D from Karunya University in the field of Electronics and Instrumentation Engineering. At present she is working as Associate Professor in the Department of Biomedical Engineering, Karunya Institute of Technology and Sciences, Coimbatore. Her areas of research include Instrumentation, Process Control,

Biomedical Instrumentation and Control Systems. She has published around 45 articles in reputed journals and has 4 Patents to her credit. She has served in various positions and responsibilities throughout her career. She also has received 3 Project Funding from various agencies.