International Journal of Engineering & Technology, 7 (4) (2018) 3494-3504

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.16302
Research paper

Wireless body area network revisited

Mustafa Sabah Taha [1, 3] *, Mohd Shafry Mohd Rahim [1, 2], Mohammed Mahdi Hashim [1, 4], Fadil Abass Johi [5]

[1] *School of Computing, Facility of Engineering, University Technology Malaysia, Johor Bahru, Malaysia*
[2] *UTM (IRDA) Digital Media Center, Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia*
[3] *Basrah Oil Training Institute ,Ministry of Oil, Iraq*
[4] *Faculty of Engineering, Uruk University, Baghdad, Iraq*
[5] *Missan Oil Company ,Ministry of Oil, Iraq*
**Corresponding author E-mail: timimymustafa @gmail.com*

Abstract

Rapid growth of wireless body area networks (WBANs) technology allowed the fast and secured acquisition as well as exchange of vast amount of data information in diversified fields. WBANs intend to simplify and improve the speed, accuracy, and reliability of communica-tions from sensors (interior motors) placed on and/or close to the human body, reducing the healthcare cost remarkably. However, the secu-rity of sensitive data transfer using WBANs and subsequent protection from adversaries attack is a major issue. Depending on the types of applications, small and high sensitive sensors having several nodes obtained from invasive/non-invasive micro- and nano-technology can be installed on the human body to capture useful information. Lately, the use of micro-electro-mechanical systems (MEMS) and integrated circuits in wireless communications (WCs) became widespread because of their low-power operation, intelligence, accuracy, and miniaturi-zation. IEEE 802.15.6 and 802.15.4j standards have already been set to specifically regulate the medical networks and WBANs. In this view, present communication provides an all-inclusive overview of the past development, recent progress, challenges and future trends of security technology related to WBANs.

Keywords: *Wireless Body Area Network; Security; ECC; IEEE 802.15.6; E-Healthcare.*

1. Introduction

Over the decades, the population growth worldwide has witnessed several challenges [1-2]. Some of them are the demographic climax involving baby boomers, enhanced life expectation of the aging population and exponential increase in the cost of health care. A study regarding the life expectancy of populace was conducted in Australia, which revealed a considerable increase in the average age from about 70 (during 1960) to 81 years (in 2010) [3]. Similar study on the life expectancy of USA citizens displayed an increase in the average age from 69.8 years (in 1960) to 78.2 years (during 2010) which amounts to 13.5%. Furthermore, the age pyramid of USA showed that the number of adults with age in the range of 60 to 80 in 2050 (81 million) is expected to be doubled than the one existed during 2000 (33 million). Thus, the health care expenses must be increased proportionately to maintain good quality of life. In 2022, the budget for health care can attain 20% of the total gross domestic product (GDP), which may jeopardy the US economy [4], [5]. For instance, the expenses for total health care in USA was raised from 250 billion (in 1980) to 18 trillion (during 2014), wherein 45 million citizens were even uninsured. This statistics clearly indicated that the present healthcare structures of USA must be entirely transformed to well scalable and cost-effective solutions [6] It is well know that, several people dies annually due to cancers, cardiovascular disease, diabetes, asthma, obesity and other chronic diseases. On top, this number will increase exponentially unless inhibited. The primary reasons for such death are due to late diagnosis, proper insurance plan, lack of money, infrastructures, and facilities. Recent studies revealed that most of these deaths can be avoided via early detection of such diseases. Therefore, robust and cost-effective healthcare systems must be developed to detect and prevent such diseases through early diagnoses, wherein WBAN will play a vital role especially in e-Health and m-Health [7]In the past, some inexpensive solutions to the early detection of abnormal diseases or conditions were developed [8]. Such healthcare systems utilized patient-wearable control systems to monitor critical syndromes including heart rate, blood pressure, synapses, etc. This not only led to high-quality life but also allowed the patients to be involved in normal activities without confining at home or in the clinic [9]. All these were attained via the implementation of low-energy smart sensors network, in which a tiny memory was installed or implanted into the patient's body or even into the bloodstream for real time data acquisition [10]. In this spirit, such networks were termed as wireless body area networks so called WBAN in short. Using WBAN in the medical sectors, the healthcare costs can significantly be reduced and the regular monitoring of the patient within the hospital can be avoided [10]. The recent IEEE 802.15.6 international standard for WBAN aspires to provide low-power consumption, short-term installation within the human body and reliable wireless communication in the neighborhood of the body. It supports a broad array of data rates (75.9 kbps) with exceptionally narrow range of up to 15.6 Mbps for different sets of applications [11-12]. WBAN interacts constantly with diverse internet networks and other wireless technologies including ZigBee, WSNs, Bluetooth, WPAN, WLAN, video surveillance systems, cellular networks, etc. Due to its notable benefits, its prospect for marketing in the area of advanced consumer electronics and services has rapidly been grown. This in turn allowed the evolution of a new generation of smart applications, improving the quality of life in terms of human health and hygiene [13]. Indeed, human thinking about health management is going to transform appreciably due to the emergence of WBAN, exactly the same way an Internet has transformed our views towards easy and free communication of vast information quickly [2]. The WBANs are effective for automating the human interaction with varieties of information technologies, where the advantages of smart sensors can be exploited to sample, monitor, process and communicate useful data signals among various body parts swiftly and reliably. Furthermore, doctors and nurses can render real-time feedback to the patient (user) without causing any trouble [2], [14], [15]. WBAN can continuously examine the patient's physiological parameters with extra mobility and flexibility. On top, it renders outsized data intervals from the natural environment of the patient and assists the doctors to achieve a comprehensible outlook of the patient's situation [16]. Nonetheless, scientific acceptance of WBAN in reality requires huge societal and technical challenges. Such challenges may open up many new avenues in terms of system design and implementation. The primary aims of WBAN are to achieve minimum delay, optimum productivity, long network durability, and very low unnecessary energy utilization in communication such as frame and frame collisions plus idle listening. Some of the significant user prerequisites for the WBAN include security, privacy, easy usage compatibility, reliability, and cost [2-17]. Most of the existing reports on WBAN do not provide the details of WBAN standards. It is important to render the latest updates on WBANs in terms their standards, features, major issues, and challenges ahead. Therefore, this paper elucidates the benefits of WBAN by encompassing the following aspects [18]:

i) A comprehensive overview and critical evaluation of the existing work on WBANs
ii) Applications of WBANs
iii) Detail classifications of WBANs in the medical and non-medical fields
iv) Security challenges of WBANs
v) Major limitations of WBANs
vi) Recent progress and future trends in WBANs.

The rest of the paper is organized as follows. In section 2, application of WBAN was discussed while need of IEEE 802.15.6 standard in WBAN is introduced in section 3. section 4, characteristics of WBAN . In section 5, data security and privacy in WBAN. In section 6, Related works are described. Finally, conclusion of paper was given in section 7.

Table 1: Classification of WBAN

WBAN Applications	Medical	Wearable WBAN	Assessing Soldier Fatigue and Battle Readiness
			Aiding Professional and Armature Sport Training
			Sleep Staging
			Asthma
			Wearable Health Monitoring
		Implant WBAN	Cardiovascular Diseases
			Cancer Detection
		Remote Control of Medical Devices	Ambient Assisted Living (AAL)
			Patient Monitoring
			Tele-medicine Systems
			Real Time Streaming
	Non-Medical		Entertainment Applications
			Emergency (non-medical)

2. Applications of WBAN

In the past, WBANs were applied in diverse fields including military, healthcare, sport, entertainment, and so forth. Table1 depicts the categorization of WBAN according to IEEE 802.15.6 standard based on medical and non-medical applications (in consumer electronics). The primary focus of WBAN applications with specific technology requisites is to improve the quality of life [16]. Table 2 presents the in- and on-body applications of WBANs. The following sub-sections underscore the applications of WBANs in various fields.

2.1. Medical applications

Certainly, the WBANs are promising to transform the future of healthcare systems in terms of easy, safe, reliable, and fast detection of diseases. Using WBANs, precarious diseases can be monitored and diagnose in real time to provide valuable feedback to the patient [19]. It was predicted by demographers that people with age above 65 worldwide will be doubled in 2025 (761 million) compared to 1990 (357 million), indicating that by 2050 the medical care for aged populace going to be a major concern. For in stance, the healthcare budget of USA was nearly 2.9 trillion in 2009 and was increased to 4 trillion in 2015 (almost 20% of the GDP). Presently, over 30% of the deaths worldwide that are due to cardiovascular diseases need to be hindered [20-21]. Recent advancement in the microelectronics, sensing, and the Internet plus wireless network technologies and their subsequent implementation in the healthcare services have transformed as well as modernized the living standard. In short, intensive deployment of WBANs will enhance the standard of healthcare systems in terms of better management and detection of diseases and cure [2-21].In the medical field, WBANs help to constantly monitor the physiological condition of patient including body temperature, blood pressure and heart beats. During abnormal situations, the data recorded by the sensors are transferred to a gateway for instance a cell phone. Later, the gateway transmits the collected data to a remotely located emergency center or clinic through cellular or Internet network for taking further action for remedies [22-23]. Briefly, the WBANs provide early solutions to the patient in terms of diagnosis, monitoring, and treatment for several fatal diseases such as diabetes, hypertension, cardiovascular and so on. The subcategories for medical applications of WBANs include the following [24].

2.1.1. Wearable WBANS

For wearable medical applications, WBANs are classified into two groups such as a) Human Performance Management, and b) Disability Assistance, which are briefly discussed underneath.

Soldier Fatigue and Battle Readiness Assessment: Using WBANs, the activity of soldiers in the battlefield can be monitored very closely. It can be accomplished using cameras, biometric sensors, global positioning system (GPS) and wireless networking combined with an aggregation device installed within WBANs for communicating with other soldiers and central monitoring units. Nevertheless, secure communication channels must exist among the soldiers for preventing the ambushes [25]. WBANs have also been utilized by police and firefighters [16]. In the harsh environments, WBANs can be effective to reduce the chance of injury whilst providing superior monitoring and care during injury.

Professional and Amateur Sport Training Assistance: WBANs can be used to control athletes' training programs via monitoring parameters, motion capture, and therapy. Besides, the real-time feedback can be provided to the concerned personnel for further improvement towards the performance and prevention of injuries due to wrong practices [26]. Some examples are:

Sleep Staging: Sleeping being a significant habit and normal physiological action of human consumes about one-third of our life span. Presently, a huge populace (nearly 27% worldwide) [6]. is affected by sleep disorders, which may cause quite severe health problems and lead to cardiovascular diseases, sleepiness at workplace and drowsiness during driving. The estimated loss in the productivity due to sleep disorders mediated work performance was estimated to be 18 billion USD [27]. Thus, monitoring of sleeping is an important area of WBANs application. Sleeping disorders are diagnosed through polysomnography test of the patient by analyzing several biopotentials recorded overnight. Nevertheless, such measurements need several connectors/wires that extend from the patient's head to a box attached to the belt, which disrupts the patient from falling asleep. It also disturbs the movements of patient and instigates artifacts as well noises, thereby reduces the signal quality. Using WBANs, it is possible to remove all connectors/wires and delocalize the intelligence as well the instrumentations in the sensor nodes [28].

Asthma: Sensors attached to the WBAN can monitor the airborne allergic agents and provide real-time feedback to the doctor, which in turn may help numerous asthmatic people [20].

Wearable Health Monitoring: WBANs placed on human body by means of attached sensors and other electronic devices can monitor health in real-time. For instance, a cell phone called Glucophone accompanied by a glucose module can easily monitor the sugar level of diabetic patients, in which the cell phone receives the diagnostics data signal from the glucose module and then stores or sends to a doctor for further analysis [26].

2.1.2. Implant WBAN

This type of applications involves the nodes implanted inside the human body either underneath the skin or within the blood stream, which are effective for the following.

Diabetes Control: In 2010, about 6.4% adult populations worldwide (amounts to 285 million) were suffered from diabetes[14], which is estimated to reach about 438 million by 2030 (nearly 7.8% worldwide) [15]. Recent researches revealed that diabetes treatment is a prolonged medical issue and needs careful monitoring on regular basis [29]. WBANs can be used to monitor frequently the diabetic level to reduce the risk of acute illness, enabling correct doses by eliminating risks of blood circulation, chance of blindness and other complications. Some of them include:

Cardiovascular Diseases: About 17 million people die every year due to cardiovascular diseases alone, a major concern in human health sector [30]. This number can considerably be lowered by undertaking proper healthcare strategies. For instance, the myocardial infarction (MI) cases can remarkably be lessened by screening the episodic events and other atypical conditions via WBAN.

Cancer Detection: The rates of cancer death were estimated to enhance up to 50% (15 million of world population) by 2020[31]. In this regard, WBAN based sensors can be exploited to monitor cancer cells in the human body. This will allow the doctors to frequently diagnose tumors and timely treatment without performing biopsy.

2.1.3. Remote controlled medical devices based on WBANS

The omnipresent Internet facilities allowed the WBANs to connect with assorted devices and services in home care system called Ambient Assisted Living (AAL), wherein every WBAN can communicate wirelessly with a remotely located medical network [32]. Using the AAL, the patient's self-monitored care can be prolonged at home whereby the reliance on intensive personal care and the costs can be reduced with improved quality of life. Actually, the AAL can promote a new generation of IT systems having interesting attributes including anticipatory function, contextual responsiveness, user sociability, and suppleness [33]. This type of WBANs includes:

Patient Monitoring: Screening of the fundamental signals is one of the key functions of WBANs technology. Such monitoring of human health can provide a real-time response and information on the fast recovery procedure. Particularly, acquired crucial signals can be transmitted wirelessly to screen the heartbeats, rates of respiration, body temperature and implant parameters, pressure of blood, and chest echoes. WBANs can be used to administer the drugs preservation in hospitals, monitor the patients physiological conditions remotely, help for treatment and create effective diagnostic interfaces. Constant monitoring of patient conditions and delivering essential medication as per requirement are the central domains of WBANs advancement. Furthermore, WBANs can interconnect diverse devices in- and/or on- the body targeted for hearing supports, digital visions, and so forth. Certainly, applications of WBANs can extend far beyond just patients monitoring and include follow-up after treatment, pharmaceutical drugs development, care for traumatic cases, remote assistance of accidental cases and in-depth research on chronic diseases [34].

Telemedicine Systems: Currently accessible telemedicine schemes either use a power demanding protocol such as Bluetooth (which is openly intervened by other devices functioning in the same frequency) or devoted wireless channels for transmitting signals to remote stations, where long-term monitoring is restricted. Moreover, integrated WBANs in the telemedicine system permit the prolonged screening of ambulatory health without any constraint [34].

2.2. Non-medical applications

The non-medical applications of WBANs are classified into the following five subcategories:

2.2.1. Real-time streaming

It involves videos (2D and 3D) streaming in real-time where clipping are captured by a cellular phone camera, useful for promoting sport goods and latest fashion designs in e-trades. Besides, audio streaming is possible through voice communication wherein one can listen (using headsets) the explanation of art at the museum or the information of bus schedule at the bus stop, multi-casting of conference calls, and musical samples in audio CD store. Such real-time streaming signals are transferred to remote controlled entertainment devices for the recognition/motion of body gesture, vital signs, and body information depending on the entertainment service. It addition, it encloses identification, emotion detection, etc. to scrutinize the forgotten things by transferring an alert to the owner [34].

2.2.2. Entertainment applications

These types of applications are related to gaming, music listening, social networking, etc. With WBANs it is possible to integrate gadgets including microphones, MP3-players, cameras, displays, head-mounted routers and advanced computing devices. These can be utilized for gaming such as controlling game with hand and body motion, virtual reality (virtual world game), tracking personal things, swapping business card related digital profile, exchanging consumer electronics associated information. Some of them are briefly described below.

Emotion Detection: Intensive studies revealed that it is possible to realize effectively various human emotions through the analyses of speech and visual data signal. Particularly, using wearable sensors technology one can detect emotion by inducing physical appearances, leading to the creation of signals to be sensed by arrays of biosensors. For example, increase in the rate of respiration and heartbeats due to fear produce sweating palm, dryness in the throat, etc. Hence, emotional status of human can be observed everywhere consistently by detecting the emotions triggered physiological signals via Electrocardiograph (ECG), Electromyograph (EMG), Electroencephalograph (EEG), Electrodermal Activity (EDA) and so forth [25]. For such monitoring some wearable biosensors can be attached WBANs. These include blood pressure sensors, pressure sensors in earrings or watches, respiration sensors in T-shirts, conductivity sensors deployed in shoes and so on.

Emergency (Nonmedical): Off-body sensors (implanted into house) can detect emergency situations (chances of domestic hazards due to fire or flammable/poisonous gas leakages) to communicate such information immediately to body-worn devices for providing cautions to the wearer (user) in case of urgency [26].

Secure Authentication: In this application of WBANs, the identification both physiological and behavioral biometrics through iris, fingerprints, and facial patterns are made. The duplicability and forgery related to confidential identities can be caught using WBANs, wherein the multi-modal biometrics associated to new behavioral/physical futures of the human body is recognized through gait and electroencephalography [13].

Table 2: Characteristics of W bans Targeted for in and on – Body Application

Application Type	Sensor Node	Data Rate	Duty Cycle (per- device) % per time	Power Consumption	QoS (Sensitive to Latency)	Privacy
In-Body Application	Glucose sensor	Few Kbps	< 1%	Extremely low	Yes	High
	Pacemaker	Few Kbps	< 1%	Low	Yes	High
	Endoscope Capsule	> 2 Mbps	< 50%	Low	Yes	Medium
On-Body Medical Application	ECG	3 Kbps	< 10%	Low	Yes	High
	SpO2	32 Kbps	< 1%	Low	Yes	High
	Blood Pressure	< 10 bps	< 1%	High	Yes	Medium
On-Body Non-Medical Application	Music for Headsets	1.4 Mbps	High	Relatively High	Yes	Low
	Forgotten Things Monitor	256 Kbps	Medium	Low	No	Low
	Social Networking	< 200 Kbps	< 1%	Low	No	High

3. Need of IEEE 802.15.6 standard in WBAN

Lately, it has been realized that IEEE 802.15.6 standard is compulsory in WBANs due to the following reasons [25, 26, 36–40]:

i) WBANs interconnection must support a speed ranging from 10 Kb/s to 10 Mb/s bit rates.
ii) For about 95% of the best performing links the packet error rate (PER) must be below 10% for a 256 octet payload.
iii) WBAN sensor nodes can be removed and added to the network in less than 3 seconds.
iv) Every WBAN must support 256 nodes.
v) Nodes must establish trustworthy communication even in the movement of user. Under acceptable reduction of network capacity that data integrity must be maintained despite of unstable channels. Applications such as walking, twisting, postural body movements respecting sitting, running, turning, arms waving, dancing etc. can produce shadowing effects and channel fading. Although WBAN nodes may move independently respecting each other, movement of WBAN itself may results in interference.
vi) WBAN applications must support optimal jitter (less than 50 ms), latency (<125 ms for medical and <250 ms for non-medical applications), and reliability.
vii) Wearable and implantable WBANs must coexist within range.
viii) Using the physical layer in a 6-m3 topology up to 10 randomly distributed and co-located WBANs must be supported.
ix) All devices in WBAN must transmit at 0.1 mW (-10 dBm) and the utmost radiated transmission power must be below [1] mW (0 dBm). It fulfills the specific absorption rate (SAR) of the Federal Communications Commission's 1.6 W/kg in 1 g of body tissue [35]
x) WBANs must be operational in the heterogeneous setting to receive information, collaborating with other networks of dissimilar standards.
xi) WBANs must be able to integrate ultra-wideband (UWB) technology with a narrow-band transmission for covering diverse settings and supporting large data rates. For example, some medical applications such as ECG monitoring may need a UWB-based WBAN to sustain higher data rates.
xii) To be self-healing, secure and allowance of priority service
xiii) WBANs must include QoS management traits.

WBANs must include power saving systems to function in a power constrained setting.

4. Characteristics of WBAN

4.1. Types of nodes

The node in WBAN are the autonomous devices with communication capacities. A node is classified into three dissimilar groups depending on the function, the execution, and the role that it plays in the network. Furthermore, each of such nodal group in WBANs can be sub-classified into various types. The following classification can be made based on the functionality [20].

Personal Device Node: The physiological responses (data signal) from the medical sensors and actuators are received by the personal server. The node called personal device (PD) or body control unit (BCU) in WBAN interacts with the users, where the user provides the information through an external gateway using PD. A display (LED) on the device or an actuator is used for signal recognition. In some applications, the PD is also known as sink or portable central device [16].

Sensor Node: The role of sensor nodes in WBANs is to measure various internal and external parameters of human body. They respond to data when subjected to physical stimulation and then collect as well as process essential data to provide the information to the wireless routers. These nodes include physiological, ambient or bio-kinetics [16-17]. Such sensors can be attached to wrist watch, mobile phone, or earphone, allowing wireless to monitor the whereabouts of an individual. Presently, WBANs are integrated with several commercially available sensors including temperature, humidity, blood pressure and glucose, thermistor, spirometer, EMG, EEG, ECG, pulse oximetry (SpO_2), CO_2 Gas sensor, plethysmogram, DNA sensor, magnetic and transmission plasmon biosensor, motion sensor (gyroscope/accelerometer/tri-axial accelerometer), and so forth [32].

Actuator: The role of actuator node is to interact with the user immediately after the data is received from the sensors [16]. Actuator provides the network feedback based on data obtained from sensor nodes. For instance, in the healthcare applications it monitors whether the right dose (medicine) is pumped into the body [41]. According to IEEE 802.15.6 standard, other taxonomy for nodes in WBAN can exist depending on their nature of implementation inside the body. Some of the actuator nodes are described underneath [22-42].

Implant Node: As the name suggests, it is implanted in the human body either within the skin or body tissue.

Body Surface Node: It is either positioned on the the human body surface of or at a separation of 2 centimeters from the surface.

External Node: Such nodes are isolated from the human body at a distance ranging from few centimeters to few meters .

Coordinator: Such nodes act as a gateway to the exterior world which may be a WBAN, trust center or access controller. The personal digital assistant (PDA) acts as a coordinator in WBAN, other nodes can exchange information using PDA.

End Nodes: In WBANs, end nodes perform the embedded applications without communicating (relaying) any data information from other nodes.

Relay: These are the intermediate nodes of a parent node having a child node responsible for sensing data and message relay. Essentially, when a node is positioned at a farthest point (such as in the foot) the communicated data must be relayed by other nodes before arriving at the PDA.

4.2. Number of nodes in WBAN

IEEE standards regarding the technical requisites of WBANs are documented [44–47]. It was acknowledged that the number of nodes in WBANs must range from only some (tens to hundreds) actuators or sensors interconnected with portable handset for communication with the Internet. Usually, the WBAN in medical network contains [6] nodes in a scalable design to support about 256 nodes [47]. It is mentioned that an operating range for WBANs is 3 meter [45], 10 piconets per person to support 256 nodes in each network within a cube of volume 6 cubic-meter [40], [48], [49]. WBAN must have at least one hub with number of nodes between [0] to nMaxBANSize (defined as 64 in the IEEE 802.15.6 standard) due to limited transmission policy [50]. However, 2-4WBANs can exist together on the same body (per square meter) [46], wherein maximum number of nodes per network can be 256. Rearguing address allotment, one-octet WBAN identifier (WBAN ID) is used for assigning an abbreviate address to a node or hub for frame exchange [51]. The value of octet varies within 0 to 255. Generally, the number of nodes in a WBAN is unlimited, moreover the limitations associated with the types and the number of network (data transmission protocols and network architectures) can limit the practical applications [16]. The highest number of nodes in a WBAN [11] can be 20 with every super-frame of duration one second is divided into non-overlapping time slots each of 50 ms, thereby allows orthogonal transmission from these nodes. Another study suggested that the maximum number of nodes can be 50 [51], which can be treated as 50 orthogonal channels assigned in every time frame. Actually, the type and nodes number in a WBAN varies depending on the interaction with other WBANs and the environment

4.3. Topology of WBAN

One-hop or two-hop star topologies for WBANs are recommended by the IEEE 802.15.6 standard, where a node exists in the center of the star positioned on a waist-like site [43-52]. Two types [53] of data communication are possible in a one-hop star topology such as transmission from the device to the coordinator and reverse. In such topology, the communication protocols follow beacon mode and non-beacon mode. In the former one, the network coordinator (node at the topology center) controls the data transmission by communicating periodic beacons to characterize the start and the finish of a super-frame. This in turn allows the network connection control and harmonization of the device. The beacon period duration called the duty cycle of the system is specified by the user depending on the standard of WBANs [53-54]. Conversely, in the non-beacon mode a network node sends the data to the coordinator via carrier sense multiple accesses with collision avoidance (CSMA/CA) whenever needed. These nodes require to power up and poll the coordinator for receiving the data. Moreover, the coordinator cannot communicate with the nodes continually because it must stay for invitation for participation [53]. The network is regarded as one-hop star topology when all the network nodes are directly linked to the sink. The coordinator in WBAN is called the sink node to which all other nodes communicate. In contrast, in a multi-hop architecture of WBAN each node is linked to the access points through other nodes. Table 3 compares the multi-hop star topology with the one-hop network configuration [55]. The multi-hop transmission reveals higher delay and lower power than that of one-hop configuration. The multi-hop topology involves overheads together with network operation, where high complexity is achieved with the increase in the number of hops. Particularly, relays in WBANs help to reduce the source to destination transmission power consumption. Distant source and destination require higher transmission power. Using relays, the transmitted heat can be distributed and suitable heat is developed in the proximity of the transmission sensor. Recent IEEE standard of WBANs [11] indicated that only two-hop topology can be supported for compliant communication. Although proprietary systems can support over two-hops, inter-operability may be problematic because they would be devoid of standard-compliant.

4.4. Communication architecture of WBAN

The tires of WBAN communication architecture are classified into three categories such as intra-WBAN communication (Tier-1), inter-WBAN communication (Tier-2) and beyond-WBAN communication (Tier-3). Figure 1 shows the communication tiers in an active typical WBAN, where the devices are dispersed all over the body within central network architecture. Moreover, the exact location of such device depends on specific application [56]. The ideal location of sensor nodes in the body may vary depending on the movement during running, walking, dancing, etc. In short, WBANs are dynamic entities [16]. It is now customary to discuss briefly these communication tiers.

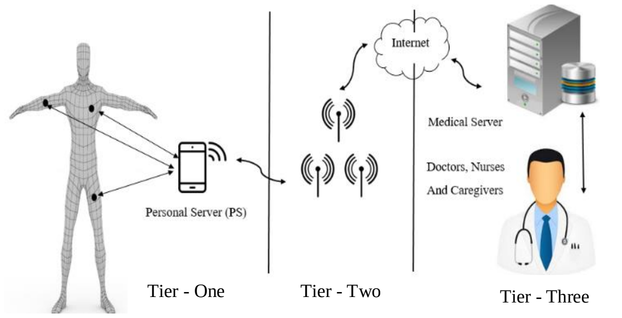

Fig. 1: Tires of Communication in WBANS.

Intra-WBAN Communication (Tier-1): This class presents the network interaction of nodes together with individual transmission ranges (nearly 2 meters) in and around the human body. Figure 1 displays the WBAN communication modes in Tier-1 based on infrastructure, where variable sensors forward the body signals to a personal server (PS) positioned in Tier-1. Later, the processed physiological data is transmitted to an access point (AP) located in Tier-2.

Inter-WBAN Communication (Tier-2): This tier is situated between PS and one or more APs, which are regarded as infrastructural parts or strategic dynamic environment for handling the emergency circumstances. This tier intends to link WBANs with diverse networks for easy access in daily life such as cellular and Internet networks [13]. More the technologies supported by a WBAN, the easier is the process of integration for effective implementations. Tier-2 is further divided into two subcategories as described below.

i) Infrastructure based Architecture: Figure 2 illustrates the communication modes based on infrastructure design. In such modes, WBAN appliances allow dynamic environment in a limited space including hospital and provides central management in terms of security control, where the AP acts as a database server [13].

ii) Ad-hoc based architecture: Figure 3 depicts the ad-hoc based architecture, where multiple APs are used to transmit the information within medical centers. These APs are configured in a mesh-like pattern that allows flexible and fast operation, where the network can easily be expanded. This renders larger radio coverage due to multi-hop distribution and support of patient mobility, where the range of coverage is much wider for movement than infrastructure based design. Actually, this interconnection from WBANs can be extended from a minimum of 2 meters up to 100 meters, suitable for both short and long network systems [13].

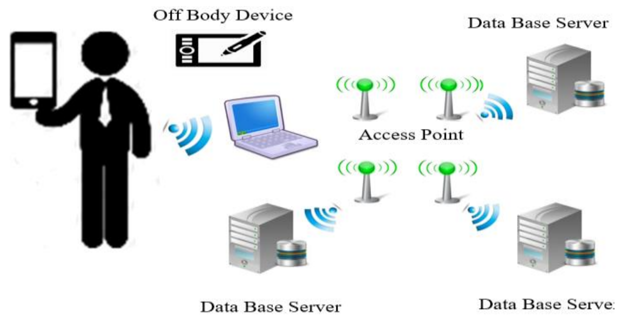

Fig. 2: Communication Modes Based on Infrastructure.

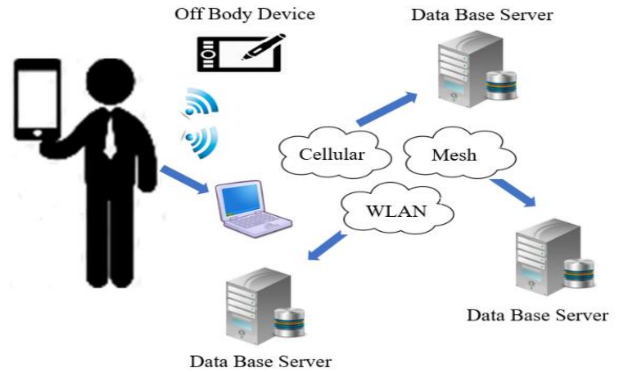

Fig. 3: Communication Modes Based on Ad-Hoc.

Beyond-WBAN Communication (Tier-3): This type is designed for metropolitan areas, where a PDA gateway can be used to interconnect this Tier-2 with the Internet of the medical server (MS) [16]. The Tier-3 architecture is greatly specific to applications. Essentially, a database is the most significant element for Tier-3 in the medical environment where contains the medical records of the patients. Therefore, doctors or patients are notified under emergency either via the Internet or through short message service (SMS) services. Furthermore, Tier-3 design restores all essential information of the patient useful for future treatments [13]. Conversely, the PS in Tier-1 can use GPRS/3G/4G instead of communicating to an AP depending on the specific application.

5. Data security and privacy WBAN

The security and privacy involving patient data are two essential elements for the system safekeeping in WBANs. The confidential data must be securely transferred through the network without falling in unauthorized users hand and then safely stored in a database. Meanwhile, the data can be used only by the authorized personnel in access. Several other requirements are involved in data security and privacy including confidentiality, integrity, authentication, freshness, localization, availability, safe management, etc. The data confidentiality is regarded as significant factor to shield the data from any disclosure or masquerader. Thus, vital information related to the patient must not be disclosed or leaked to exterior or adjacent networks. Data integrity in WBAN implies that the secure information must remain unmodified, where the security system must be robust against any adversaries attack through hash function or MD5 (digital signature). The recurring challenges and issues involving the improved security and privacy in WBAN are discussed below.

5.1. Threats to WBAN

Data storing in WBANs is the foremost challenge. The security of wireless sensor networks is always threatened because the sensor nodes that capture the information are not fully resistant to adversaries attack. Thus, such nodes in the local server can easily be captured by illegal users, thereby remain untrustworthy. Actually, such malicious attack or threat tries to break the security code in local server network. In accidental failure or during malicious activity on network nodes may join or leave the network frequently, allowing the insertion of attackers' forged data as legitimate one by breaking the security code set by the authorized user. Threats emerge from two reasons including device compromising and dynamical networking. It is important to discuss in detail various types of security and privacy in WBANs.

5.2. Types of security and privacy in WBAN

As aforementioned, WBANs offer several applications in civilian and military fields. For instance, WBANs are useful for monitoring environmental pollution, surveillance in the battlefield, homeland security, and human health. For military and commercial applications, WBANs must be protected against malicious attacks, demanding a provision for enhanced security. Thus, security and privacy are the vital issues in the WBANs. Despite the openness of wireless channels the sensitive data must not be fallen into the unauthorized users' hand. With the identical radio frequency band interfacing in a wireless channel, anybody can monitor or join in the communication. This becomes very handy for the adversaries to crack into the wireless network. Effective protection of wireless network involves several security requisites (confidentiality, integrity, non-repudiation, freshness, availability, intrusion detection, key administration, and authenticity) that are carefully accounted during security protocol design. These fundamental concepts of these security services, attacks and remedies in the context of WBANs are discussed hereunder.

Data Security: It deals with secure storing and transfer of data in WBANs.

Data Privacy: It involves the data approval to authorized users only. Disclosure of sensitive and personal medical data to any third party (unauthorized users) is risky. To preserve the data privacy in WBANs non-cryptographic methods are used. A protocol called phantom routing can be used to improve extraordinarily the privacy source location. It expands the source location by initializing a phantom source while narrowly mounting the communication overhead contrast with the single-path routing and flooding.

Data Confidentiality: It is achieved without disclosing the vital data of patient and protecting it from other networks. Data confidentiality in a communication channel is attained via encryption process, where a shared key and security is designed to transfer the patients' private data among the coordinator and the nodes in WBAN.

Eavesdropping: In the WBAN, radio frequency being an open signal source for data transmission the protocol data unit (PDU) is used to collect the information of source and destination header. Then, it passes one intermediary node to another at the moment when the attacker eavesdrop the packet and breaks the privacy.

Node Compromise (NC): It is an active attack where the node fails and the confidentiality is broken, which functions in the following ways:

i) Direct: in this type, an attacker using special tools to acquire the sensitive data captures a node.
ii) Indirect: NC is one of the most detrimental attacks to WBANs. In this kind, the attacker can derive the secret information from a node without capturing it, which is achieved by analyzing the private data collected from other compromised nodes and/or packet PDUs. In this process, a new compromised node under the adversary's control is used to instigate attacks that are more malicious. Generally, a WBAN is installed in an unreceptive setting such as battle fields and health care system. Actually, nonstop monitoring of the network in such settings is not assured, which provides the adversaries a chance to compromise the sensor nodes. In fact, the node compromise in WBANs is rather easy because the sensor nodes are fabricated using inexpensive devices without strong safeguard.

Encryption: To protect the confidentiality of sensitive data in WBANs from misuse encryption algorithm is used. Over the years, encryption techniques such as data encryption standard (DES), advance data encryption standard (ADES) and Rivest Shamir algorithm (RSA) are introduced.

Data Integrity: In WBANs, it assures that the data packets remain unmodified during transmission without falling in the hand of attackers. Errors involving the transmission and processing can modify the transmitted messages that are send from the sender to the receiver, where the error control mechanisms can be used to prevent such modifications. Nevertheless, this task is extremely complicated in WBANs. Data integrity is of two kinds as depicted below.

i) Packet Modifications: In an aggressive setting, an attacker can modify a transmitted data packet in WBANs before reaching to the receiver end, which causes several setbacks. The adversary can simply establish radio interference to some bits in the transmitted packets and modifies their polarities. Consequently, the incomprehensible data packets are dropped at the receiver, leading to a simple denial of service (DoS) attack.

ii) Message Integrity Code: For malicious modification of data packets by attackers the automatic repeat request (ARQ) and forward error correction (FEC) cannot be used in WBANs, because all the error detection and correction codes are openly recognized. Actually, an attacker can modify a frame and re-compute its checksum. Thus, a receiving node is unable to detect the frame modification due to its resemblance with checksum. The message integrity code and digital signature are used to prevent such modifications.

Data Authenticity: It assures the identity of communicating nodes is WBANs, where each node must identify the delivery and reception of data packets from an authorized sender. Otherwise, the receiving node may be deprived of performing the correct functions. It is further classified as:

i) Packet Injection: Sybil attack is a classic example of packet injection in WBANs, where an attacker illegally employs multiple identities via false packets injection that contain spoofed source IP or MAC addresses. This in turn, create serious threats to fair resource allocation, distributed storage, data aggregation, routing protocols, voting, intrusion detection, etc. To foil such attempt various methods are adopted including message authentication code, digital signature, man-in-the middle, and authentication public key.

ii) Data Freshness: It is a significant factor to support the data integrity and confidentiality in WBANs. It guarantees that the data packets are in correct format and not reutilized. Data freshness can be of two types such as strong freshness and weak freshness. The strong freshness assures the frames or packets ordering in terms of delay, where synchronization of WBAN coordinator is necessary during beacon transmission. Conversely, the weak freshness guarantees the ordering of frames or packets when WBAN nodes are in low-duty cycle.

iii) Data Availability: It provides advance assurance involving the maintenance of expected services in WBANs, where it comprehensively relates to all aspect of the network. It is known that the network functionality degrades and results in DoS whenever there is any attack or unforeseen problem. In such situation, data availability can compromise the network to protect the data from being leaked out. Some typical attacks against the availability are discussed hereunder.

Secure Key Localization: It is a key supporting technology for WBANs, in which security and accuracy are the focus. In practice, the localization performance of WBANs is badly affected because of different adverse interfering reasons.

Secure Key Management: In WBANs, data transmission from sender to receiver is performed using a secure cryptographic technique based on generated secret keys. Diverse secure schemes can be used in WBANs including symmetric key management, asymmetric key management, random key material distribution management, location-based key material distribution management, deterministic key material distribution management, key deterministic key material distribution management, key agreement model, group key management. Therefore which provide whole security with cryptography key in wireless body area network is called secure key management.

6. Related works

A survey in the context of Asia [57] revealed that the number of older persons is gradually increasing. The statistics showed that older person in the near future will represent a group of four only, requiring better healthcare to maintain a good quality lifestyle. Besides, elderly people need healthcare services to monitor their health remotely, transferring relevant medical data to doctors or specialists for further diagnoses [58]. Recently, healthcare information communication technology (HICT) made strong impact on the healthcare services in terms of quality of care, management, and safety. Such services include electronic health record (EHR), personal health record (PHR), clinical decision support system (CDSS), electronic medical record (EMR), etc [57]. Healthcare data are of two types, (i) small size containing personal medical records of the patients, and (ii) big size with large storage capacity enclosing medical information of large healthcare institutions such as Hospitals and health centers. The later one needs huge investments for developing infrastructure to handle and store such massive data (records). Additionally, such organizations require trained ICT personnel to maintain such records, which is expensive. The extensive cost of such investment in terms of infrastructures and skilled manpower become a blockade among medical sectors and ICT solutions unless overcome. Of late, cloud computing (CC) has emerged as one of the great solutions, which renders several services to diverse healthcare institutions [59]. In CC data management various parties are involved such as public, private, hybrid and community. The public cloud being the most economic one is often used for data manipulation in a scalable manner. The CC permits the medical institutions to store massive data information without any investment. On top, CC renders easy and free access to the users continuously from anywhere, where only basic computer knowledge is required. However, security, privacy and reliability of CC is a major concern, wherein the confidential and sensitive medical records are always under threat by adversaries attacks [60], [61]. The best part of CC facilities involves the cost effectiveness. These notable features of CC services in terms of freely data access from anywhere worldwide at any time, resource pooling and resource management made it so popular. Certainly, CC has emerged as a promising solution to huge amount for managing healthcare data records. Moreover, existing security problems associated to CC forced reputable medical sectors to refrain from such environment [62-63]. Electrocardiography (ECG), magnetic resonance imaging (MRI) and CT scan are being the key healthcare services need absolute security. For privacy preservation of such records, varied strategies have been adopted. To maintain the medical data integrity, confidentiality and availability the concept of user authentication is introduced so that only the legitimate user can access the data [64]. WBAN sensors being very tiny in size their functionality faces some serious limitations involving the level of energy, memory size and processing capability. Currently, majority of the studies on WBAN focus on the security and energy issues, wherein the energy issues are relevant for the broader area. To tackle such wide area problems, various effective routing protocols are developed such as LEACH, PEGASIS, etc [65], [66].In recent times, various security techniques are proposed for secure data transmission from sensors to base station. Sensors in the WBAN are used to intelligently sense the medical data and transmit to remote controller devices such as cell phone, PDA, etc. Communication among sensors and controllers occurs in a short range of network via Bluetooth, ZigBee, and so on. Furthermore, the controllers transmit the sensed data to base station via internet, intranet, local area network, etc [67], [68]. Base stations may be located either within or exterior to the hospital or in the cloud. Essentially, the security involving the data transmission from sensors to controller devices and then controller devices to base stations is the main concern of WBANs. Presently, the most prominent and effective security system in WBAN is based on asymmetric key cryptography. In asymmetric key cryptography, space and time are the two key features, where a lesser key size is used than symmetric key cryptography [69-71]. On top, shorter processing time and low complexity are the two other significant characteristics of asymmetric key cryptography. Other widely used cryptographic algorithms are RSA and elliptic curve cryptography (ECC) [72]. In short, rapid growth in sensors technology led to solutions of WBANs limitations, resulting wider applications [73]. Diverse sensors nodes in WBANs require secure data transmission, where data transfer either from node to node or from node to base station server must be secured. The healthcare applications require node to base station server [74]. The ECC on mobile healthcare devices has already been implemented, where secure transmission of medical data could be achieved [75]. The main idea was to develop a secure remote patient monitoring system based on mobile devices [76]. However, the medical image compression and video transmission in WBANs remained the major challenges, where complete data must be archived and handled during examination of the patient for improved and secured response [77].

Table 3: Comparison between One –Hop and Multi-Hop Star Topology [55]

Criteria	Star Network	Multi-hop Network
Energy consumption	Lower power is needed for transmission when the nodes are closer to PDA than at farthest locations.	Nodes closer to the PDA consume higher energy because they not only forward their own information from other nodes.
Transmission delay	It offers the least possible transmission delay for any sensor communication to the PDA	Its network configuration dependent. The nodes closest to the PDA receive the information industry without any intermediary relay.
Interference	Sensors located at distant from the PDA need high transmission power, where the amount of interference is high.	The transmission energy is low because each node only transmit to its neighboring nodes, mitigating the interference effects.
Node failure and mobility	Only the failed node is affected without influencing the rest of the network.	The part of the network containing the failed nodes is recognition, involving overhead.

It was acknowledged that the medical data of patients (from rural area to urban area) could be related to physical, behavioral, physiological, psychological, and cognitive data. Most of the healthcare applications must be developed to handle the patients' data from both rural and urban areas with flexibility and security, where data privacy is the major concern in WBANs [78]. Recently, some systems and techniques are proposed to overcome such limitations of WBANs. Healthcare for patients located in the unfriendly remote area [79] became the main focus of WBAN technology. Rural patients are always deprived because of lack of doctors' availability, medical facilities, health centers, clinics, hospitals, etc. A new framework was proposed to resolve diverse issues in remote healthcare systems. In healthcare applications of WBANs, security and privacy are the main issues [80] due to the risks involving devices. Data security limitation can be overcome using various encryption algorithms involving data authentication, key management, etc [81-82]. Besides, issues including legal, political, psychological, and economic are important to look at. These issues can be resolved via appropriate coordination of government and concerned agencies. An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks was introduced [83]. WBANs for healthcare that face DoS attack mediated authentication issues can be resolved via the execution of two-tier authentication scheme. In this scheme, the first tier validates the user via unique identification code and the second tier verifies the legitimate user by passing some parameters and assessing their response. Login requests are validated at the server side based on the saved information during registration. Yes, the proposed security system faced problems related to replay, impersonation, DoS and other network attacks [73].

Another authentication scheme for healthcare security in WBANs was proposed based on passed parameters as identity and random values. The responded values of the users were calculated and examined [84] to determine the success of the developed authentication scheme. Detailed analysis revealed that the users could successfully apply the scheme to access sensitive medical data in a controllable fashion [85]. User authentication is the fundamental requirement of WBANs because sensitive medical data of patient cannot be shared to everyone [56], where only the legitimate user must be able to access the data with proper verification. However, there are some constraints involving the memory, energy and processing capability of sensors in WBANs. Those constraints do not allow mutual endorsement of users in a simple way [87]. Actually, secret keys are required to work securely in any group communication, where the generation and distribution of such keys is the foremost challenge for encryption algorithm developer [88]. The main aim of WBANs technology is to include all the application areas with less time complexity and maximum processing speed [83]. A novel authentication system was developed by combining various parameters (random values, nuances, data and passwords) other than the available conventional algorithms [89]. The effective performance of the proposed scheme was validated and tested using NS2 tool, which revealed better than the previously developed schemes [90]. Satisfactory performance of authentication against DoS attack was achieved. A data transmission and verification scheme based on ECC and symmetric cryptosystem was introduced [69], where data security and transmission performance of the scheme was tested against various known attacks. Proposed scheme was found to be ineffective against mutual authentication and key exchanges. Medical devices in WBANs are of two types including wearable and implantable [68], where both are used for medical data diagnosis, analysis and treatment. The software programmability, liability, and resource constraints are the most significant aspects of WBANs. With ever-increasing risk relating the security and reliability of WBANs the demand of smart medical devices and communication architecture became more prominent. Despite some success of WBANs the ongoing frequent setbacks and malfunctions associated to hardware, software, and attacks posed doubt on the versatility of WBAN devices and their functions. The reliability of WBAN devices must be examined and resolved for effective uses in widespread services. WBANs technology for healthcare applications may lead to a better altitude provided the fault tolerance limit is extended and better security solutions are provided [90]. The most difficult problem in WBANs is the detection of border during medical data transmission [81]. Recent growth of WBANs technology allowed superior solution in different applied areas. Currently, a chemeto measure was introduced that assured the convergence quality of WBANs [91]. Another new method by combining ECC and mutual authentication was proposed [72] for improving the performance of WBAN. Sink node was used to authenticate the base station server and vice versa, wherein hash value for sink ID, registered random number and timestamp value for two-way authentication were implemented to identify the replay attack. Meanwhile, ECC was utilized for key distribution and secure data transmission amid sensor nodes and base station [89], [92], [93]. Table 3 (provided by National Institute of Standards and Technology) compares the various encryption algorithms such symmetric Advanced Encryption Standard (AES), RSA and ECC in terms of their used length of secret keys and attained security.

Table 4: Comparison of Key Length (Bits) of Different Encryption Systems [69]

Symmetric AES	ECC	RSA
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	521	15360

Acknowledgement

This research is a small part of a big research supported by the School of Computing, University Technology Malaysia, Johor Bahru, Malaysia. Mustafa would like to thank the reviewers for their piercing, smart and helpful suggestions for a better research.

7. Conclusion

Present paper comprehensively reviewed various security issues related to WBAN technology. Significant contributions of WBANs in electronic healthcare systems, challenges, and excitements were emphasized. Medical data security in terms of encryption, sensor power, energy, processing speed, and time complexity were considered to be the most relevant aspect in WBANs performance. It was demonstrated that WBANs in healthcare sectors are exceedingly beneficial for uninterrupted monitoring of patient's medical information anywhere and anytime worldwide. It was affirmed that WBANs can easily detect early abnormal conditions of the patient such as heartbeats, blood pressure and sugar, and body temperature useful for subsequent treatment. Undoubtedly, WBANs technology together with cloud computing will contribute to improve the future healthcare systems and quality of life especially for elderly generations in remote areas. Through WBAN mediated health monitoring patients will be engages in normal activities at their work place or home or in nearby specialized medical services instead of taking admission in the hospital for prolonged time. This paper is believed to provide important taxonomy for future navigation into the field of security technologies in WBANs.

References

[1] Milenković, A., Otto, C., & Jovanov, E. (2006). Wireless sensor networks for personal health monitoring: Issues and an implementation. *Computer communications*, *29*(13-14), 2521-2533. https://doi.org/10.1016/j.comcom.2006.02.011.

[2] Otto, C., Milenkovic, A., Sanders, C., & Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of mobile multimedia*, *1*(4), 307-326.

[3] History of life expectancy. (n.d.). Retrieved from http://www.worldlifeexpectancy.com/history-of-life-expectancy

[4] History of life expectancy. (n.d.). Retrieved from http://thesocietypages.org/socimages/2010/03/08/the-graying-of-america

[5] History of life expectancy. (n.d.). Retrieved from http://thesocietypages.org/socimages/2012/06/15/the-graying-of-america

[6] History of life expectancy. (n.d.). Retrieved from http://healthcare-economist.com/2006/01/30/trends-in-health-carespending

[7] Shankar, S. K., & Tomar, A. S. (2016, May). A survey on wireless body area network and electronic-healthcare. In *Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on* (pp. 598-603). IEEE.

[8] Ghatole, S. M., & Dahikar, P. B. (2016). Survey on Wireless Body Area Network for Healthcare Applications. *International Journal of Researches in Biosciences, Agriculture and Technology (IJRBAT)*, *4*(3), 14-17.

[9] Sai Nishita, U., Anusha, K., Ramya SriSai, K., & Mohammed Ali Hussain, D. (2018). Health care monitoring and accident tracking system based on location awareness. *International Journal of Engineering & Technology*, *7*(2.7), 246-248. https://doi.org/10.14419/ijet.v7i2.7.10589.

[10] Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications Surveys & Tutorials*, *16*(3), 1658-1686. https://doi.org/10.1109/SURV.2013.121313.00064.

[11] IEEE Standards Association. (2012). IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks. *IEEE Standard for Information Technology, IEEE*, *802*(6), 1-271.

[12] Smith, D., & Hanlen, L. (2012). Wireless body area networks: Towards a wearable intranet. *ISCIT Tutorial*.

[13] Zhang, J., Cao, Y., Qiao, M., Ai, L., Sun, K., Mi, Q., & Wang, Q. (2018). Human motion monitoring in sports using wearable graphene-coated fiber sensors. *Sensors and Actuators A: Physical*, *274*, 132-140. https://doi.org/10.1016/j.sna.2018.03.011.

[14] Behera, G., Panigrahy, S. K., & Turuk, A. K. (2018). A Biometric based Anonymous User Authentication Technique in Wireless Body Area Networks.

[15] Kwon, H., & Lee, S. (2009, September). Energy-efficient multi-hop transmission in body area networks. In *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on* (pp. 2142-2146). IEEE.

[16] Kaur, N., Singh, E. B., & Student, A. P. (2017). A Survey on Wireless Body Area Network and Human Machine Control. *International Journal of Engineering Science*, *11581*.

[17] Mainanwal, V., Gupta, M., & Upadhayay, S. K. (2015, March). A survey on wireless body area network: Security technology and its design methodology issue. In *Innovations in information, embedded and communication systems (ICIIECS), 2015 international conference on* (pp. 1-5). IEEE.

[18] Kwak, K. S., Ullah, S., & Ullah, N. (2010, November). An overview of IEEE 802.15.6 standard. In *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on* (pp. 1-6). IEEE.

[19] Sharma, S., Tripathi, M. M., & Mishra, V. M. (2017, November). Survey paper on sensors for body area network in health care. In *Emerging Trends in Computing and Communication Technologies (ICETCCT), International Conference on* (pp. 1-6). IEEE.

[20] Dishman, E. (2004). Inventing wellness systems for aging in place. *Computer*, *37*(5), 34-41. https://doi.org/10.1109/MC.2004.1297237.

[21] Barakah, D. M., & Ammad-uddin, M. (2012, February). A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. In *Intelligent Systems, Modelling and Simulation (ISMS), 2012 Third International Conference on* (pp. 214-219). IEEE.

[22] González-Valenzuela, S., Liang, X., Cao, H., Chen, M., & Leung, V. C. (2012). Body area networks. In *Autonomous Sensor Networks* (pp. 17-37). Springer, Berlin, Heidelberg. https://doi.org/10.1007/5346_2012_26.

[23] Khan, R. A., & Pathan, A. S. K. (2018). The state-of-the-art wireless body area sensor networks: A survey. *International Journal of Distributed Sensor Networks*, *14*(4), 1550147718768994. https://doi.org/10.1177/1550147718768994.

[24] Ullah, S., Khan, P., Ullah, N., Saleem, S., Higgins, H., & Kwak, K. S. (2010). A review of wireless body area networks for medical applications. *arXiv preprint arXiv:1001.0831*.

[25] Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., & Kwak, K. S. (2012). A comprehensive survey of wireless body area networks. *Journal of medical systems*, *36*(3), 1065-1094. https://doi.org/10.1007/s10916-010-9571-3.

[26] Lewis, D. (2008). 802.15. 6 call for applications in body area networksresponse summary,"*15–08–0407–05-0006*.

[27] History of life expectancy. (n.d.). Retrieved from http://www.chinadaily.com.cn/china/2013-03/21/content 16320337.htm

[28] Karmakar, N. C., Yang, Y., & Rahim, A. (2018). Wireless Monitoring of Sleep Apnoea Patients. In *Microwave Sleep Apnoea Monitoring* (pp. 25-39). Springer, Singapore. https://doi.org/10.1007/978-981-10-6901-7_3.

[29] History of life expectancy. (n.d.). Retrieved from http://www.worlddiabetesfoundation.org/composite-35.htm

[30] History of life expectancy. (n.d.). Retrieved from http://www.who.int/cardiovascular diseases/resources/atlas.en

[31] History of life expectancy. (n.d.). Retrieved from http://www.who.int/cardiovascular diseases/resources/atlas.en

[32] Lipprandt, M., Eichelberg, M., Thronicke, W., Kruger, J., Druke, I., Willemsen, D. & Hein, A. (2009, May). OSAMI-D: An open service platform for healthcare monitoring applications. In *Human System Interactions, 2009. HSI'09. Second Conference on* (pp. 139-145). IEEE.

[33] Nehmer, J., Becker, M., Karshmer, A., & Lamm, R. (2006, May). Living assistance systems: an ambient intelligence approach. In *Proceedings of the 28th international conference on Software engineering* (pp. 43-50). ACM.

[34] Kwak, K. S., Ullah, S., & Ullah, N. (2010, November). An overview of IEEE 802.15.6 standard. In *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on* (pp. 1-6). IEEE.

[35] History of life expectancy. (n.d.). Retrieved from http://www.fcc.gov/oet/rfsafety/sar.html

[36] Mile, A., Okeyo, G., & Kibe, A. (2018). Hybrid IEEE 802.15. 6 Wireless Body Area Networks Interference Mitigation Model for High Mobility Interference Scenarios. *Wireless Engineering and Technology*, *9*(02), 34. https://doi.org/10.4236/wet.2018.92004.

[37] Lewis, D. 802.15. 6 call for applications-response summary," July 2008. *IEEE802*, *15*.

[38] Smith, D. B., Miniutti, D., Lamahewa, T. A., & Hanlen, L. W. (2013). Propagation models for body-area networks: A survey and new outlook. *IEEE Antennas and Propagation Magazine*, *55*(5), 97-117. https://doi.org/10.1109/MAP.2013.6735479.

[39] Khan, J. Y., Yuce, M. R., Bulger, G., & Harding, B. (2012). Wireless body area network (WBAN) design techniques and performance evaluation. *Journal of medical systems*, *36*(3), 1441-1457 https://doi.org/10.1007/s10916-010-9605-x.

[40] Zhen, B., Patel, M., Lee, S., Won, E., & Astrin, A. (2008). Tg6 technical requirements document (TRD) IEEE p802. 15-08-0644-09-0006. *Tech. Rep*.

[41] Wang, S., & Park, J. T. (2010). Modeling and analysis of multi-type failures in wireless body area networks with semi-Markov model. *IEEE Communications Letters*, *14*(1). https://doi.org/10.1109/LCOMM.2010.01.091719.

[42] Elias, E., Chaumon, M. E. B., & Vacher, M. (2018, July). Methods to Design Home Support for Elders. In *International Conference on Human Aspects of IT for the Aged Population* (pp. 276-289). Springer, Cham. https://doi.org/10.1007/978-3-319-92037-5_21.

[43] Tachtatzis, C., Di Franco, F., Tracey, D. C., Timmons, N. F., & Morrison, J. (2010, December). An energy analysis of IEEE 802.15. Six scheduled access modes. In *GLOBECOM Workshops (GC Wkshps), 2010 IEEE* (pp. 1270-1275). IEEE.

[44] Venkateswarlu, V. T., Naganjaneyulu, P. V., & Rao, D. N. (2017). The Wireless Body Area Sensor Networks and Routing Strategies: Nomenclature and Review of Literature. *Global Journal of Computer Science and Technology*.

[45] Meena, U., & Jha, M. K. (2015, March). An efficiency model for authentication approaches in WBAN. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on* (pp. 476-481). IEEE.

[46] Lewis, D. (2010). *IEEE p802. 15.6/d0 draft standard for body area network* (Vol. 6). 15-10-0245-06.

[47] Bishnu, A., & Bhatia, V. (2018). An IEEE 802.22 transceiver framework and its performance analysis on software defined radio for TV white space. *Telecommunication Systems*, *68*(4), 657-668. https://doi.org/10.1007/s11235-017-0417-x.

[48] Khromov, I. A., & Dvornikov, A. A. (2017, September). The human body as the element of the computer network. In *"Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS), 2017 International Conference* (pp. 378-382). IEEE. https://doi.org/10.1109/ITMQIS.2017.8085838.

[49] Rosini, R., Verdone, R., & D'Errico, R. (2014). Body-to-body indoor channel modeling at 2.45 GHz. *IEEE Transactions on Antennas and Propagation*, *62*(11), 5807-5819. https://doi.org/10.1109/TAP.2014.2352631.

[50] Elhayatmy, G., Dey, N., & Ashour, A. S. (2018). Internet of things based wireless body area network in healthcare. In *Internet of Things and Big Data Analytics toward Next-Generation Intelligence* (pp. 3-20). Springer, Cham. https://doi.org/10.1007/978-3-319-60435-0_1.

[51] Rathour, A. S., & Kumar, R. Performance Analysis of T Slot UWB Patch Antenna for WBAN Applications.

[52] Domingo, M. C. (2014). Sensor and gateway location optimization in body sensor networks. *Wireless networks*, *20*(8), 2337-2347. https://doi.org/10.1007/s11276-014-0745-7.

[53] Sindhu, S., Vashisth, S., & Chakarvarti, S. K. (2016). A review on wireless body area network (WBAN) for health monitoring system: Implementation protocols. *Communication on Applied Electronics, Foundation of Computer Science, Newyork, USA*, *4*(7).

[54] Ullah, F., Abdullah, A. H., Kaiwartya, O., & Cao, Y. (2017). TraPy-MAC: traffic priority aware medium access control protocol for wireless body area network. *Journal of medical systems*, *41*(6), 93. https://doi.org/10.1007/s10916-017-0739-y.

[55] Kwak, K. S., Ullah, S., & Ullah, N. (2010, November). An overview of IEEE 802.15.6 standard. In *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on* (pp. 1-6). IEEE.

[56] Rahim, H. A., Malek, F., Soh, P. J., Hisham, N., Romli, A., Rani, K. A. & Fuad, A. (2017). On body characterization for on-body radio propagation channel using wearable textile monopole antenna. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *nine* (1-4), 7-10.

[57] Cresswell, K., & Sheikh, A. (2013). Organizational issues in the implementation and adoption of health information technology innovations: an interpretative review. *International journal of medical informatics*, *82*(5), e73-e86. https://doi.org/10.1016/j.ijmedinf.2012.10.007

[58] Sukkird, V., & Shirahada, K. (2015). Technology challenges to healthcare service innovation in aging Asia: Case of value co-creation in emergency medical support system. *Technology in Society*, *43*, 122-128. https://doi.org/10.1016/j.techsoc.2015.08.002.

[59] Yousefifard, N., Abbasi, M., & Jourmand, R. (2013). Using Multi-Cloud Approach to Enhance the Protection of Patient Privacy in Electronic Health Records.

[60] Gong, Z., Xiao, Y., Long, Y., & Yang, Y. (2017, July). Research on database ciphertext retrieval based on homomorphic encryption. In *Electronics Information and Emergency Communication (ICEIEC), 2017 7th IEEE International Conference on* (pp. 149-152). IEEE.

[61] Elmogazy, H., & Bamasak, O. (2013, December). Towards healthcare data security in cloud computing. In *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for* (pp. 363-368). IEEE.

[62] Marwan, M., Kartit, A., & Ouahmane, H. (2016). Cloud-based medical image issues. *International Journal of Applied Engineering Research*, *11*(5), 3713-3719.

[63] Bellam, R. B., Coyle, M. P., Krishnan, P., & Rajan, E. G. (2015, September). Issues while migrating medical imaging services on cloud based infrastructure. In *Next Generation Computing Technologies (NGCT), 2015 1st International Conference on* (pp. 109-114). IEEE.

[64] Jees, P., & Diya, T. (2016). Medical Image Protection in Cloud System. *Matrix*, *two*, three.

[65] Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G. & Andreescu, S. (2015, June). Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. In *2015 IEEE international conference on services computing (SCC)* (pp. 285-292). IEEE.

[66] Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. *IEEE Access*, *3*, 678-708. https://doi.org/10.1109/ACCESS.2015.2437951.

[67] Yang, Y., Zhang, S., Yang, J., Li, J., & Li, Z. (2014). Targeted fully homomorphic encryption based on a double decryption algorithm for polynomials. *Tsinghua Science and Technology*, *19*(5), 478-485. https://doi.org/10.1109/TST.2014.6919824.

[68] Zhang, M., Raghunathan, A., & Jha, N. K. (2014). Trustworthiness of Medical Devices and Body Area Networks. *Proceedings of the IEEE*, *102*(8), 1174-1188. https://doi.org/10.1109/JPROC.2014.2322103.

[69] Lee, Y. S., Alasaarela, E., & Lee, H. J. (2014). An efficient encryption scheme using elliptic curve cryptography (ECC) with symmetric algorithm for healthcare system. *International journal of security and its applications*, *8*(3), 63-70. https://doi.org/10.14257/ijsia.2014.8.3.07.

[70] Roček, A., Slavíček, K., Dostál, O., & Javorník, M. (2016). A new approach to fully reversible watermarking in medical imaging with breakthrough visibility parameters. *Biomedical Signal Processing and Control*, *29*, 44-52. https://doi.org/10.1016/j.bspc.2016.05.005.

[71] Sajedi, H. (2018). Applications of data hiding techniques in medical and healthcare systems: a survey. *Network Modeling Analysis in Health Informatics and Bioinformatics*, *7*(1), 6. https://doi.org/10.1007/s13721-018-0169-x.

[72] Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., & Yang, Y. (2016). An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. *Journal of Network and Computer Applications*, *76*, 37-48. https://doi.org/10.1016/j.jnca.2016.10.001.

[73] Bhatia, G., Lala, A., Chaurasia, A., & Rajpal, R. (2013, January). Implementation of Cloud computing technology for the improvement of entire healthcare services in India. In *Advances in Technology and Engineering (ICATE), 2013 International Conference on* (pp. 1-5). IEEE.

[74] Sharma, A., Singh, A. K., & Ghrera, S. P. (2015). Secure hybrid robust watermarking technique for medical images. *Procedia Computer Science*, *70*, 778-784. https://doi.org/10.1016/j.procs.2015.10.117.

[75] Malhotra, K., Gardner, S., & Patz, R. (2007, April). Implementation of elliptic-curve cryptography on mobile healthcare devices. In *Networking, Sensing and Control, 2007 IEEE International Conference on* (pp. 239-244). IEEE.

[76] Arka, I. H., & Chellappan, K. (2014). Collaborative compressed i-cloud medical image storage with decompress viewer. *Procedia Computer Science*, *42*, 114-121. https://doi.org/10.1016/j.procs.2014.11.041.

[77] Elayan, H., Shubair, R. M., & Kiourti, A. (2017, March). Wireless sensors for medical applications: status and future challenges. In *Antennas and Propagation (EUCAP), 2017 11th European Conference on* (pp. 2478-2482). IEEE.

[78] Arsalan, M., Qureshi, A. S., Khan, A., & Rajarajan, M. (2017). Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. *Applied Soft Computing*, *51*, 168-179. https://doi.org/10.1016/j.asoc.2016.11.044.

[79] Noel, A. B., Abdaoui, A., Elfouly, T., Ahmed, M. H., Badawy, A., & Shehata, M. S. (2017). Structural health monitoring using wireless sensor networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *19*(3), 1403-1423. https://doi.org/10.1109/COMST.2017.2691551.

[80] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, *55*(1), 122-129. https://doi.org/10.1109/MCOM.2017.1600267CM.

[81] Singh, J. P., Mishra, M. K., & Khan, M. A. (2017, July). Energy-efficient approach towards video-based sensor networks (wireless) beneath barrier coverage. In *Computing, Communication and Networking Technologies (ICCCNT), 2017 8th International Conference on* (pp. 1-5). IEEE.

[82] Eide, O. W. (2017). *Elliptic Curve Cryptography-Implementation and Performance Testing of Curve Representations* (Master's thesis).

[83] Wu, F., Xu, L., Kumari, S., & Li, X. (2017). A new and secure authentication scheme for wireless sensor networks with formal proof. *Peer-to-Peer Networking and Applications*, *10*(1), 16-30. https://doi.org/10.1007/s12083-015-0404-5.

[84] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*(1), 11. https://doi.org/10.1186/2192-113X-1-11.

[85] Garkoti, G., Peddoju, S. K., & Balasubramanian, R. (2014, December). Detection of insider attacks in cloud based e-healthcare environment. In *Information Technology (ICIT), 2014 International Conference on* (pp. 195-200). IEEE.

[86] Sun, D. Z., Li, J. X., Feng, Z. Y., Cao, Z. F., & Xu, G. Q. (2013). On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. *Personal and ubiquitous computing*, *17*(5), 895-905. https://doi.org/10.1007/s00779-012-0540-3.

[87] Kester, Q. A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., & Quaynor, N. N. (2015, June). A security technique for authentication and security of medical images in health information systems. In *Computational Science and Its Applications (ICCSA), 2015 15th International Conference on* (pp. 8-13). IEEE.

[88] Tomar, A. S., Shankar, S. K., Sharma, M., & Bakshi, A. (2016, September). Enhanced Image Based Authentication with Secure Key Exchange Mechanism Using ECC in Cloud. In International Symposium on Security in Computing and Communication (pp. 63-73). Springer, Singapore. https://doi.org/10.1007/978-981-10-2738-3_6.

[89] Chauhan, R., & Kumar, A. (2013, November). Cloud computing for improved healthcare: Techniques, potential and challenges. In *E-Health and Bioengineering Conference (EHB), 2013* (pp. 1-4). IEEE.

[90] Kester, Q. A., Nana, L., & Pascu, A. C. (2013, November). A novel cryptographic encryption technique for securing digital images in the cloud using AES and RGB pixel displacement. In *Modelling Symposium (EMS), 2013 European* (pp. 293-298). IEEE.

[91] Luarasi, T., Durresi, M., & Durresi, A. (2013, September). Healthcare Based on Cloud Computing. In *Network-Based Information Systems (NBiS), 2013 16th International Conference on* (pp. 113-118). IEEE.

[92] MAHDI HASHIM, M. O. H. A. M. M. E. D., RAHIM, M., & SHAFRY, M. (2017). IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION. *Journal of Theoretical & Applied Information Technology*, *95*(22).

[93] HASHIM, M., RAHIM, M., SHAFRY, M., & ALWAN, A. A. (2018). A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN. *Journal of Theoretical & Applied Information Technology*, *96*(4).