International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Healthcare Sensors Issues, Challenges & Security Threats in Wireless Body Area Network: A Comprehensive Survey

**M Ragul Vignesh[1], S Sivakumar[2]**

[1]Assistant Professor, [2]Associate Professor,
[1,2]Department of Computer Engineering,
Dhanalakshmi Srinivasan College of Engineering, Coimbatore, Tamil Nadu, India

**ABSTRACT**

In recent events of the pandemic situation there is a heavy surge in the demand for health care applications for monitoring the vitals of the patients through real - time monitoring of the human body. The major concerns which we face in Wireless Body Area Network [WBAN] sensors are security, data privacy, data integrity, confidentiality and dependability. Moreover it has issues such as standardization, energy efficiency, and quality of service. We are more concerned about the security of the data. The main purpose of WBAN sensors is to monitor the patients continuously without any assistance. The sensors are meant to be worn by the patients and the data has to be sent to the Healthcare applications which hold the backend system through a secured network. In this paper we are discussing the various security mechanisms and routing challenges which we are facing and the attacks which could occur over the network and also the summary of certain mechanisms which are present to overcome them. We have analysed the security for the different attack scenarios. This survey is to summarize the major difficulties which we face while designing a network in WBANs which is an emerging field of science in this pandemic situation.

***KEYWORDS:*** *Wireless Body Area Networks (WBANs), Security threats, Security Mechanisms, Attacks based on layers, Security, Quality of service, Health care sensors, Privacy*

***How to cite this paper:*** M Ragul Vignesh | S Sivakumar "Healthcare Sensors Issues, Challenges & Security Threats in Wireless Body Area Network: A Comprehensive Survey" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.989-997, URL: www.ijtsrd.com/papers/ijtsrd42454.pdf

IJTSRD42454

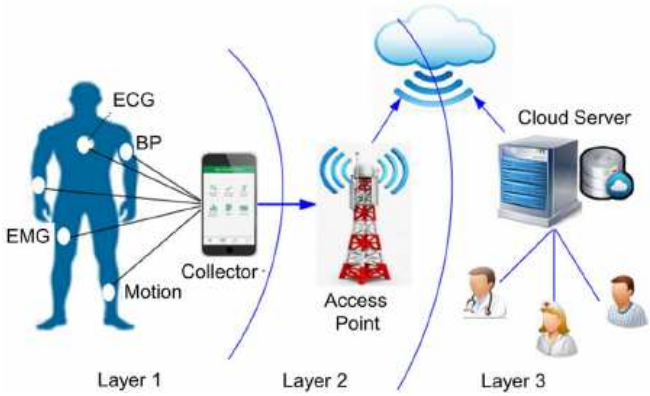


## 1. INTRODUCTION:

The popularity of wearable healthcare devices paired with mobile applications to monitor a person's health has widely become popular in recent days. Considering the recent event of pandemic, we are much more into health and health care self-monitoring applications. The WBANs initially had a scope in hospitals and medical centers where the data of patients are constantly monitored and updated to its nearby monitoring centers where the data are received, processed and maintained. A WBAN majorly consists of sensors attached to the patient, monitoring devices which act as a central data center and a sensor aggregation node. [1]

The WBAN connects sensor nodes which are implanted in the clothes, on the body or under the skin of a person. The sensors are widely placed all over the whole human body and the nodes are connected through a wireless communication channel.[1]

A WBAN offers many promising new applications in the area of remote health monitoring, home/health care, medicine, multimedia, sports and many others, all of which make use of the unconstrained freedom of movement a WBAN offers. In the medical field, for example, a patient can be equipped with a wireless body area network consisting of sensors that constantly measure specific biological functions, such as temperature, blood pressure, heart rate, electrocardiogram (ECG), respiration, etc. The advantage is that the patient doesn't have to stay in bed, but can move freely across the room and even leave the hospital for a while. This improves the quality of life for the patient and reduces hospital costs. In addition, data collected over a longer period and in the natural environment of the patient, offers more useful information, allowing for a more accurate and sometimes even faster diagnosis.[4]




Apart from the major benefits of WBAN health monitoring systems including cost effective and attractive, it provides us with continuous monitoring of vital signal of the patients, which are more essential for elderly people.[2][3]

Security plays a vital role in monitoring centre (MC) networks for medical data processing and health care monitoring systems. WBAN is used for Health care

applications, and also requires proper security mechanisms in order to protect the individual's data and WBAN devices from malicious attackers.[1] The advert of exposing the health issue to the surrounding people will kill a patient faster than the issue itself.

The discussion in this paper covers the various security mechanisms and routing challenges which we are facing and the attacks which could occur over the network and also the summary of certain mechanisms which are present to overcome them. Chapter 2 covers the various security service schemes and security mechanisms for the data and the communication medium. Moving forward with Chapter 3 & 4, the various challenges faced by the sensors itself are reviewed and in Chapter 5 the various attacks which could be performed over it in different network layers is discussed following by the summary and conclusion.

## 2. Design aspect to be considered in WBAN

### 2.1. WBAN Security Services

Whenever we talk about data the term security and privacy plays a very important role. Data security over here means the data which is monitored is securely stored and transferred. Data privacy means the data can be accessed only by the authorized people. Here we discuss the major security concerns such as data security, communication security and data storage.

#### 2.1.1. Confidentiality of data

Confidentiality is the process of protecting medical information so that there is no unauthorized access by malicious users. It prevents data disclosure in the sensor environment when data is transferred among the sensor nodes to the base station and vice versa. It is said that it prevents eavesdropping. On the other hand the major problem for confidentiality is if an authorized node is compromised by the attackers then they can access the highly potential data such as cryptographic keys. With the help of the key the attacker can decrypt the message and access the protected data. [5] Usually the part of the message which contains data is encrypted, the process of encrypting the packet header is used to protect the identity of the node.

#### 2.1.2. Data Access Control

The unauthorized access of the patient's data is prevented by Data access control. It helps in improving privacy policy of the data. The users who could access the data of the patients involve doctors, nurses, pharmacies, insurance companies and other supportive staff and agencies. If an agency gets all the access to the patient's medical report they could exploit them to reduce the premium involved in the policy [6]. So to avoid these things there has to be a strict policy to ensure that different users have different access to the data.

An example of role based access control for health care applications is given in [7]. In WBANs, along with the role based access controls applied to beyond-BAN layer's applications, a comprehensive set of control rules is needed at intra-BAN layer. Authors in [8] discuss some rules on a patient's privacy at home (intra-BAN layer). For instance, who can decide which sensors should collect the data, or whether patients can completely control how much of the data is sent to the central monitoring station, or they only have a partial control? In this case, guidelines need to be defined explicitly[1]. There by giving the total control access to the patient which data to be sent and which should be hidden.

#### 2.1.3. Accountability

The secure data access control in WBANs can be controlled by accountability. When a user without the proper privilege tries to access the unauthorized data of the patients, then the patient should be notified with the act of the user and the user has to be held accountable. Authors in [9] discuss this problem and then propose a technique to defend against it. When an illegal key sharing is happening amongst valid yet unauthorized users.

#### 2.1.4. Integrity

This prevents data from being tampered with throughout the network's data transfer procedure among the WBAN sensors. Lack of integrity is a severe concern since the usage of faulty or incorrect information can have terrible repercussions. Some sensor network applications, such as healthcare or environmental monitoring, rely largely on the integrity issue, and hence the safeguarding of data carried through the network.[5]

#### 2.1.5. Authentication

This technique is used to verify the participants' identities and is primarily used to distinguish between fraudulent users and legal traffic. Every base station and sensor node in a wireless sensor network must be able to determine if the received packet was delivered by an attacker node or a legitimate node. This is due to the fact that an attacker can deceive legitimate nodes into accepting fraudulent data packets. If fake data is fed into the sensor network, unexpected results may occur. The message's MAC can be used to authenticate the source of such misleading information.

#### 2.1.6. Availability

It allows information and services to be accessed at any moment if necessary. Multiple services may become unavailable as a result of denial of service assaults or node compromise, which could have fatal effects for some real-time applications [5]. The WSN protocols used must be strong enough to handle any outages by providing alternative, more secure routes.

#### 2.1.7. Dependability

In the event of individual node failures, sensor intrusions, or malicious alterations, patient-related data must be easily retrievable. Because failure to obtain proper data might result in life-threatening situations, dependability is one of the most important concerns in WBANs. Error-correcting coding approaches can be used to resolve dependability issues [11]. Although WBAN dependability is critical, it has gotten little attention thus far.

### 2.2. Security Mechanisms

#### 2.2.1. Authentication

A mechanism is necessary to determine whether the received data is coming from valid nodes between WBAN devices in order to identify legitimate nodes. There is also a mechanism at the application level to identify the user in order to access the smartphone using various ways such as user ID and password, fingerprint or retina scanning, voice recognition, and so on. Before transmitting data, security methods might provide the authentication procedure. Certificates, digital IDs, biometrics, two-factor authentication, and proximity authentication are only some of the technologies employed. [10]

If a patient misplaces their device, they must be able to reconnect with their sensor devices in a secure manner.

When bringing in a new sensor or processing device, the ability to authenticate the user and securely integrate into the existing network must also be considered. Certificates, for example, can be downloaded from the Certificate Authority (CA) onto the PT, which will also require a password from the application programme to be matched with the replacement unit. The password should never be saved on the smartphone, but rather encrypted and used by the device to verify and authenticate the user using a hash function such as Secure Hash Algorithm 2 (SHA2).[1]

#### 2.2.2. Authorization

Authentication is the process of identifying genuine nodes or users within WBAN, whereas authorization is the process of allowing users such as patients or carers to access the MC database and complete required information. Physicians, for example, may have different levels of access to health data than consumers and health-care providers. Within WBAN, sensors may have varying levels of permission to gather data and send it to certain destinations. Cluster sensors, for example, may have a different authorisation level than the other sensors.

#### 2.2.3. Key Management Protocol

The author in [12] generates the key using hybrid techniques. This involves creating keys using physiological values (PVs) of the human body, which are used for the sensor nodes to calculate keys, rather than the traditional key management methodology of pre-loading created keys. To meet the needs of varied security requirements, key management systems have expanded into several sub-areas. A CA is used to handle public keys in a public key infrastructure (PKI). Asymmetric key methods like Diffie-Hellman and RSA, which demand a lot of resources and electricity, are used in many PKIs [13].

Due to the limited resources available in WSNs, high energy consumption is not desirable, and numerous recommended techniques for implementing PKI with this concern in mind have been offered. While there are many proprietary key management systems available, such as Tiny PK, PKI, and L-PKI, L-PKI is suitable for WSN/WBAN because it provides all of the authentication, confidentiality, non-repudiation, and scalability that are required for resource-constrained platforms like WSN and WBAN, whereas other PKIs only provide a subset of these services.[11]

L-PKI is based on Elliptic Curve Cryptography (ECC) to reduce computational costs and consists of several components, including a Registration Authority (RA), a Certificate Authority (CA), digital certificates, a Certificate Repository, a Validation Authority (VA), a Key Generating Server (KGS), end entities (smartphones), and a Timestamp Server. Compared to RSA, which is not appropriate for resource-constrained networks like WSN, L-PKI with an ECC-based system requires substantially smaller keys, which increases efficiency. For example, 160 bit keys in an ECC based system has the same level of security as those of a 1024 bit keys in an RSA based system [14].

Scalability and power efficiency are the decisive criteria in what level of security mechanisms to apply in WSN and WBAN, therefore scalability and power efficiency are the emphasis of key management systems. Because both networks have distinct hardware abilities, low weight data secrecy and authentication algorithms may be implemented differently in WSN and WBAN [13]. While the number of keys created in WSN is restricted due to power and computational constraints, a full-scale security mechanism can be implemented in smartphones to store and send health data and patient information to MC. A user login and password, as well as other information such as user random salt, fixed salt, and iteration count, are required to generate a master key, which will be used to encrypt health data, patient information, and account information before sending it to MC via a secured channel such as SSL/TLS and IPSec.

#### 2.2.4. Route Discovery Protocol

In a small sensor network, data exchange can be done directly between nodes without the use of a routing protocol, but in a more complex network, routing is required to ensure path redundancy and efficient communication. Within the WSN, route discovery protocols are utilised to communicate with a PT (base station), and intelligent routing is necessary to determine the quickest or better path within the WSN, including cluster header. The Secure and Energy Efficient Multipath (SEEM) Routing Protocol does not take the shortest path to the data source, but rather finds numerous ways and chooses one to utilise [15]. SEEM, on the other hand, lacks cryptographic techniques and solely provides balanced security services. INSENS (Intrusion-Tolerant Routing Protocol for Wireless Sensor Networks) is a multipath routing protocol that uses less processing power and resources. Secure route discovery, secure data transfer, and route management are all steps used by SECMRP. It is a proposed route discovery technique that employs L-PKI and is developed for WSNs. It can provide authentication, confidentiality, integrity, balancing, and scalability security services, whereas SEEM can only provide balancing and INSENS cannot give scalability.

## 3. Constraint & Challenges

### 3.1. Low Power Budget

In terms of power budget, all sensors are constrained, but body sensors are more limited in this regard. Because body sensors rely on energy to conduct all of their tasks, such as sensing, computing, and communication, energy is a valuable resource [1].

Replacing this critical resource is impossible or impractical in many cases, especially for in-body sensors, which are embedded within the human body. As a result, one of the most important considerations in developing WBAN systems and protocols is energy limiting.

### 3.2. Limited Memory

The memory capacity of body sensors is only a few kilobytes. The small size of body sensors is the reason for this constraint. However, while the installation of security mechanisms may not necessitate a large amount of memory, keying material is stored in the sensor's memory and consumes the majority of it.

### 3.3. Computational Capability

Low processing abilities in body sensors is caused by a combination of a low power budget and a lack of memory. Because the primary function of body sensors is conveyance of observed data, there is a limited amount of energy that can be spent on calculation operations [16]. Furthermore, due to memory limitations in body sensors, they are unable to do complex computations.

### 3.4. Low Communication Rate

In WBANs, communication is the most energy-intensive function. It is critical to reduce the amount of communication in these networks in order to save energy. As a result, rather

than transforming actual data, developers have attempted to minimise the overhead transmissions required by other purposes.

### 3.5. Security & Safety

Since the users of WBAN devices are typically non-experts, the devices should be simple and straightforward to operate. Furthermore, WBAN devices are designed to function similarly to plug-and-play devices. Because the data security systems' setup and control are patient-related, they should only require a few simple human interactions [11]. However, in the case of WBANs, security takes precedence above usability, so skipping some manual processes to improve usability is not recommended.

### 3.6. Lack of Standardization

Sensors from various manufacturers could be used in each WBAN. As a result, pre-sharing any cryptographic materials is problematic. It is difficult to design security methods that require the least common settings in such networks that interact with a wide range of devices.

## 4. Routing Challenges

### 4.1. Node Distribution

SNs in WSNs are deployed based on their applications [17]. Deterministic and non-deterministic deployment procedures are the two types of deployment tactics. In the case of a deterministic deployment technique, sensor nodes are manually deployed and data is transmitted via pre-programmed channels. Sensor nodes, on the other hand, are dispersed at random in a non-deterministic deployment methodology with no pre-calculated pathways. When there is a non-uniform distribution of nodes, the routing protocol must be able to execute optimal clustering to improve the wireless network's energy efficiency while also addressing the connection issue.

### 4.2. Data Reporting Model

In WSNs, data reporting and data sensing are based on applications [18]. In WSNs, data reporting and data sensing are based on applications [18]. Data reporting models can be divided into three categories: query-driven, event-driven, and time-driven. In time-driven models, data monitoring and transmission are done on a regular basis after a set time interval. Data is only reported in query or event driven models when the base station generates an event or query. These models have an impact on routing protocol performance in terms of route stability and energy usage.

### 4.3. Defect Resistance

Nodes in WSNs may die out due to environmental interferences, physical damage, or a lack of power supply. The overall operation of the wireless sensor networks must not be harmed by such nodes that have died or failed [19]. Routing protocols must be able to generate alternative routes headed for the base station in the event of node failure or other interruptions [20].

### 4.4. Extensibility & Connectivity

Multiple SNs spread over the sensing region require a routing solution that can handle them. The routing protocols must be flexible enough to encompass the complete range of nodes as the number of nodes grows. Routing protocols must be aware of such topological changes and capable of dealing with them.

### 4.5. Network Dynamics

In wireless sensor networks, sensor nodes can be either mobile or stationary. Because of route stability difficulties, message routing in mobile nodes is more difficult than in fixed nodes. For data to be sent securely to mobile nodes, routing methods must account for route stability [5].

### 4.6. Physical Resources

The restricted battery supply is the primary cause for WSNs' limited uses. As a result, energy waste is a major design concern in protocol development. The sensor nodes also have limited processing and memory capabilities.

## 5. WBAN Attacks

WBANs requirements are vulnerable to various types of attacks. Based on the security in WBANs, these attacks can be categorized as

### 5.1. Physical Layer Attacks

#### 5.1.1. Eave's Drop

Eavesdropping is a precondition for other attacks, an eavesdropping assault is a severe security concern to a wireless sensor network (WSN). Traditional WSNs are made up of wireless nodes with omnidirectional antennas that broadcast radio signals in all directions, making them vulnerable to eavesdropping.

#### 5.1.2. Jamming Attacks

Interference with the radio frequencies of the body sensors is referred to as jamming. The adversary tries to block or interfere with signal reception at the network's nodes in this attack. The attacker does it by sending a continuous random signal on the same frequency as the body sensors. Nodes that are affected will be unable to receive messages from other nodes. In this attack, the adversary can utilise a few nodes to send out radio signals, disrupting the functionality of the transceivers and blocking the entire network. Larger networks, on the other hand, are more difficult to completely block. SNR is a critical factor in successful jamming assaults [21].

#### 5.1.3. Tampering Attacks

An attacker physically tampers with sensors in tampering assaults. An attacker may damage a sensor, replace the entire node or a portion of its hardware, or even electrically interrogate a node in order to obtain patient data or shared cryptographic keys. Sensor devices, in general, have few exterior security protections and are thus vulnerable to physical tampering. The deployed sensors in a WBAN are under the observation of the person carrying these devices, making it impossible for an attacker to physically access the nodes without being discovered. However, there is still the possibility of tampering in WBANs. Patient awareness is an effective deterrent to manipulation. Only approved persons should be permitted to physically handle the gadgets, which might be very beneficial to patients [22].

### 5.2. Datalink Layer Attacks

#### 5.2.1. Exhaustion Attack

Exhaustion of battery resources may occur when a self-sacrificing node always keeps the channel busy. In WSN, rate limitation is used to thwart this attack.

#### 5.2.2. Collision Attack

The jamming technique we just described is known as a collision attack. When the attacker hears the beginning of a communication, he or she listens to the channel and sends out a signal that interferes with the communication. This can result in frame header corruption, checksum mismatches, and, as a result, receiver rejection of sent packets. Because the sole proof of a collision attack is the receipt of wrong messages, this attack is difficult to detect. A frame is dropped

if the Cyclic Redundancy Code (CRC) check fails. Error correcting methods are one of the solutions that can be used to protect WBANs from this assault. Collision attacks in WBANs have a high probability of success, similar to jamming attacks.

### 5.3. Network Layer Attacks

#### 5.3.1. Selective Forwarding

When an attacker adds a compromised node in a routing path, this is known as selective forwarding. When a malicious node receives a packet, it does nothing but ignore it and drops it. The rogue node has the ability to discard packets selectively (just for a specific destination) or totally (all packets). Because the PS is usually in the direct communication range of body sensors in intra-BAN communications, selective forwarding attacks are not applicable to the first communications level (intra-BAN level) of WBAN's architecture. As a result, body sensors can communicate with the PS directory without having to route packets. Body sensors with a short range of communication choose a nearby node to transfer their data to the PS [23]. When numerous APs are placed to assist the body sensors in transmitting information, routing is possible in WBANs at the second level of communications (inter-BAN level). This type of link increases a WBAN's service area and facilitates patient mobility.

#### 5.3.2. Sinkhole Attack

Sinkhole attacks are similar to selective forwarding but are not passive. The compromised or bogus node is used to generate traffic in this attack. In order to prevent packet forwarding, this node drops packets. This attack is similar to the selective forwarding attack in that it can be used in WBANs.

#### 5.3.3 Wormhole Attack

Wormhole attacks use two malicious nodes located far apart to create a wormhole in the target sensor network. There is an out-of-band communication route for both malicious nodes. The sensor nodes are near one malicious node, whereas the base station is near the other. The malicious node near the sensor nodes deceives sensors into believing that it has the shortest path to the sink node via the other malicious node near the sink node. In the target sensor network, this leads to sinkholes and routing confusion. Wormhole attacks, like selective forwarding and sinkhole attacks, can be used in WBANs.

#### 5.3.3. Hello Flood Attack

To introduce themselves to their neighbours, several protocols require nodes to broadcast hello packets. When a node receives such greeting packets, it may believe the sender is one of its neighbours. This assumption may be incorrect in the event of hello flood attacks. An attacker with a powerful antenna can fool sensors into thinking it's in their neighbour's house. Furthermore, the attacker has the ability to claim a high-quality route and establish a wormhole. Although wormhole construction has no effect on WBAN intra-BAN communications, a Hello Flood attack in intra-BAN communications causes body sensors to respond to hello packets, wasting their energy.

#### 5.3.4. Spoofing Attack

The spoofing attack targets the routing information transferred between nodes, attempting to spoof, alter, or replay the data in order to complicate the network [24]. An attacker could, for example, cause network disruption by constructing routing loops, generating phoney error messages, and drawing or repelling network traffic from certain nodes. Spoofing attacks, like selective forwarding, sinkhole, and wormhole attacks, can be used in WBANs.

### 5.4. Transport Layer Attack

#### 5.4.1. DE synchronization Attack

The transport protocols that rely on sequence numbers are targeted by the de-synchronization attack. The attacker alters some messages to include incorrect sequence numbers, resulting in endless retransmissions that waste both energy and bandwidth. WBANs are quite vulnerable to this type of attack. Because body sensors have a limited power budget, retransmissions may quickly deplete the sensor's power and render it unavailable to the network. This attack can be thwarted with authentication.

#### 5.4.2. Flooding Attack

By sending a large number of connection establishment requests, a flooding attack is utilised to drain memory resources. Because body sensors have limited memory space, they are susceptible to flooding attacks.

## 6. Literature Review

### 6.1. AES symmetric key based scheme

A WBAN protocol [24] that is both energy efficient and secure focuses on wearable devices, also known as sensor devices that are implanted into the bodies of patients to monitor their current health status. Through gateway devices, the human body is connected to the internet. Medical specialists use this information to treat disorders such as asthma, diabetes, heart attacks, and high blood pressure in patients. To send the secure BAN, an energy efficient and secure protocol for WBAN is employed, which uses advanced encryption security (AES) based encryption and the SHA-1 hash function. For WBAN, SHA-I is complicated, but a hash chain-based protocol that uses the chaos baker map for security reduces the complexity. Memory space, computation control, and bandwidth are all well-organized in sensor devices. To randomise the data, the authors' protocol uses a chaos baker map, and this technique is also utilised to generate pseudorandom key streams. Implementation of a Lightweight End-to-End Secured Communication System for PMS [26] focuses on a secure end-to-end transportation system for patient monitoring. A wireless link connects the sensor device in the body to the gateway, which sends the patient's medical information.

This paper also looked at data encryption to prevent data theft and data verification to ensure that only authorised individuals have access to data. End-to-end secure PMS concentrating on the security of sensor to gateway wireless connection with encryption protocol, as well as using (MQTT) telemetry transport protocol rather than hypertext transport protocol. AES is used to encrypt data, which is then stored on a server where a legitimate user can retrieve the data for decryption and further activities. The advancement of the internet of things (IoT) brings smart technologies, which have a wide range of applications in healthcare [27].Therefore; these systems are vulnerable to security and privacy. Low power and resource usage are implemented in the secure framework. It uses the AES-CTR mode to set the counter value, which is a variable called the initial vector (IV) value that is incremented by a pseudorandom sequence. The size of the counter value is determined by the encryption algorithm employed, such as AES-128 bits, which employs a basic XOR operation similar to CTR mode. WBAN

needs lightweight and efficient resources to transmit data over the network [28].

Many strategies for security have been presented, and this study study examines group-based cooperation on symmetric key production via physical or link layer received signal strength indicator (RSSI) data collecting. This article [28] proposed cooperative group solution to enhance the variation and size of RSSI data for efficiently key generation. The main advancement is the use of numerous channels between a member hub and a group, or sometimes between two groups, to randomly synthesise RSSI information with better information similarity and fluctuation and multi-overlap information thickness. Similarly, a few bunch models are depicted with protocol design specifics. WBAN is linked to WSN[29]. WBAN is made up of tiny sensors that collect data from the human body and communicate it through a network to biomedical servers. The system's primary goal is to protect the security and confidentiality of data transmitted over a network. To ensure data security and guard against different threats, various security techniques have been devised.

To secure data, this article explores cryptography and key management strategies. The data is kept secure by using strong cryptography and complex calculations. When using encryption techniques for security, execution time and memory consumption should be taken into account. A secure application is designed around the key management protocol. These protocols are used to create and distribute cryptographic keys to network nodes. Confined in server, key pre-distribution, and self-authorizing are the three main types of key management protocols. The trusted server protocol relies on a trusted base station to create the key agreement in the system network. It is viewed as that trusted server protocol are appropriate to networks in the environment of various resources.

WBAN is a new technology that focuses on the medical examination system [30]. It is critical to encrypt and decrypt healthcare data, as well as to produce secret keys on both the source and destination sides. The author suggested a very useful secret key generation methodology that can generate 128 symmetric secret keys to secure communication. The WBAN link must be secured because it consists of many micro sensors that measure the crucial information of patients. It is critical to use cryptographic algorithms in wireless network protocols to ensure secure communication. As a result, complicated algorithms are used to encrypt sensitive information. The suggested High Rate Key Management Technique for WBAN is based on RSS measurements from node A to node B. The RSS measurements of node A and node B are estimated through communication between the two nodes [30]. It can produce 128 symmetric secret keys to keep communication secure. In both static and mobility scenarios, the results reveal that it generates symmetric secret keys with higher effects [31]. Before signal distortion is transferred to the successful quantization process, a filtering procedure is used to reduce bit mismatch.

### 6.2. Hashing algorithm based algorithm scheme

Secure hashing algorithms (SHA) and encryption techniques are used in research reviews to make data transfer more secure and powerful [31]. It generates digital signatures using a hash technique to convey patient data in a more secure and authentic manner. This proposed technique makes use of an asymmetric key generation strategy, which uses a pair of public and private keys, making the processes slower and more complex. Securing Data Communication in WBAN with Digital Signatures [31], the suggested strategy is based on a combination of multiple ways for securing data in WBAN by combining secure keys and digital signatures. Because of the arbitrary keys exchanged with the BNC and the entire sensor node on the network for encryption and decryption, this technique is extremely safe. BNC digitally signs every data packet with SK and sends it to all sensor nodes in the network. It is sent to the medical server after being validated by the BNC. D-sign encrypts data into fixed-size bits known as hash values using the SHA-1 hash function. Digital signatures are created using hash values and the sender's keys, and the hash values are decrypted using the sender's keys. If the new hash values are the same as the old hash values, the data packet has not been changed.

In [32], The Chaos Baker map focuses on a simple hashing work convention in conjunction with the Chaos Baker delineation, which provides highly secure information disclosure and dissemination. In terms of memory space, calculation control, data transfer, and power, the body sensor hubs are source controlled. It employs the hash function protocol, which uses 128-bit text and key sizes. Due to the controlled sources, computationally expensive and control-intensive processes are ineffective for such hubs. The pseudorandom key streams are generated using the Chaos Baker delineate. Every sensor hub receives the data and verifies it by decoding the figure content using the hash bind as an incentive. Chaotic sequences are pseudorandom, and finite is the most important matrix scheme. Chaotic systems use matrices to construct sequences. Patients' data can be encrypted or decrypted using sequences as secret keys. Chaotic compressive sensing is deployed in the body to body network.

### 6.3. Elliptic curve cryptography based scheme

As the population ages, it becomes increasingly difficult to meet the health needs of elderly and patients with available resources. Nano sensors are now available thanks to technological advancements, and they can be used anywhere, just like they may be placed on a human's body to collect health data, therefore data security is critical [34]. To secure the data in this paper, ECC and Diffie Hallman (DH) were utilised. There is a great need to secure vital patient health data, and several strategies are employed to do so. As a result, the asymmetric algorithm ECC was used in this study. To ensure data security, DH is used to generate keys in the system. Because there are two types of users, patients and doctors, this article also focuses on user authentication. To sign up for the system, users must store personal information such as thumb or palm prints in the database. The ECC and DH algorithms are then used to encrypt the biological data. It is initially translated to binary before being assessed using different key sizes such as 128, 192, and 256 bits. Encryption decryption time and key generation time are among the grading criteria.

WBAN is a wireless sensor network that uses small sensors to collect health data from people and send it to the medical community [33]. To ensure security, this data must be encrypted before being sent to the medical server. As a result, for data security in this publication, the hybrid encryption algorithm (HEA) was used. Users must register for a registration number and node ID before using HEA to encrypt and decrypt data. These numbers serve as a key and

are kept private. The sender and receiver then exchange these keys using the Elliptic Curve Diffie Hellman algorithm. To safeguard the data, this study uses a hybrid approach of ECC 128 bit and AES 128 bit encryption. WBAN architecture consist of the intra WBAN and inter WBAN [36]. Intra WBAN uses a personal server (PS) as a gateway to transport signals to the next station, but inter WBAN links to the main network through the internet to receive patients' important health data. Beyond WBAN, there is another critical step of WBAN where the medical environment's database or biomedical server is located. Because WBAN contains very sensitive information, security and privacy are top priorities. To protect the data of the patients, various data security solutions have been offered.

To secure the data, it uses ECC with a very powerful key management mechanism. It takes the points on the curve that will be utilised in cryptography calculations and extracts them. These points are one-of-a-kind to ensure that the values are more random. To accomplish data reliability and security, this technique included registration, verification, and key exchange mechanisms. Technology is rapidly changing. WBAN is a networked healthcare system that sends data. Data transmission with security is a difficult task. For data security, this article uses a three-party authentication mechanism using an ECC technique.

The WBAN was also based on star topology in the research paper. In asymmetric cryptography, two types of keys are used: a public key and a private key, both of which are mathematically connected. There are two purposes in cryptography for achieving security for patient data authentication and encryption. To encrypt and decrypt sensitive data, public and private keys are utilised.

### 6.4. TEOSCC and ECDH-IBT

Various advances in therapeutic inventive work have provided social insurance providers with a new set of tools to improve medical services [27]. As a result, remote checking therapeutic frameworks such as WBAN will become a part of portable human services equipped with continuous checking in the future. In this type of environment, security is a crucial concern, hence a recommended solution based on clustering and encryption is provided. WBAN nodes are grouped into numerous groups in the clustering system, and these groups are in charge of data transmission. As a cluster head, one of the selected groups of nodes contains the cluster node, and the remaining nodes communicate around it. The cluster head is connected to every node in the group and maintains information as well as gathering and sending data from the cluster nodes. Encrypting sensor data using the ECDH Based Iterative Block Transformation (ECDH-IBT) algorithm is the second strategy used in this article [42].

### 6.5. BAN-trust detection

WBAN is an important technology for the healthcare sector [37]. As a result, this profession places a premium on data security and reliability. Although several encryption and decryption mechanisms have been offered for data security, there is still a risk of being subject to a malicious node assault. The malicious node assault in WBAN was detected and dealt with using the BAN trust scheme. BAN trusts consist of two parts one is the data analysis and the second is the trust management. It is difficult for WBAN's nodes to communicate directly, but it is critical to transmit data. To determine whether a node is trustworthy to interact with or not, check to see if it has ever interacted with another node. If it has, the recommendations it receives from others are critical in determining the trustworthiness of that unknown node.

### 6.6. Channel characteristic

WBAN is a biomedical field that transmits critical health information to patients [39]. Tempering attacks, malevolent node attacks, and inserting bogus data attacks may all be possible as a result of the high accessibility of resources. As a result, data security is a major concern in this setting. Other strategies for data security improvements have been presented, however this study used a channel characteristic aware privacy protection system. Encryption methods should be used in this paper [39].To begin, the keys used by two nodes must have the identical sequence, the second key must have a maximum size of 128 to 512 bits, and the third key should encrypt data using statistical randomness. The wireless channel is used to confirm the authentic node-based correlation using the node authentication technique.

### 6.7. Kerberos protocol

The notion of WBAN for a smart healthcare system was sparked by rapid technological progress [38]. As a result, maintaining good security for sensitive data remains a major concern. To secure the data, multiple data security solutions are offered. This article presents the software defined networking (SDN) layout for data transfer and uses the Kerberos networking authentication protocol. This paper [42] explains a flow chart for emergency data delivery, in which the user sends an encapsulated data packet that is inspected by the Kerberos protocol, which grants access to the legitimate user for data retrieval. The SDN controller will analyse the data format and offer a specific data delivery route for data transmission across the SDN.

### 6.8. Block chain

WBAN [40] is a form of technology that continuously monitors and records human health signs. WBAN poses much security and privacy concerns because it stores and develops critical information about patients' health. Block chain technology and digital signatures are used to deal with unwanted access and data manipulation. By employing a chain of hash values to determine the proper values for encryption, block chain protects data from being tampered with. Digital signatures, on the other hand, are employed as a validator, ensuring that data is available to administrators. Users' non-repudiation attacks are likewise mitigated by digital signatures. With the help of aggregation of all the persons' signatures, the DVSSA signature methodology employed in this article makes the size of the signatures on the block chain equivalent to the size of a single-person signature, considerably reducing storage consumption. Users' data is signed using the DVSSA signature mechanism before being transmitted for block chain-based calculations.

## 7. CONCLUSIONS

As a summary, WBAN gathers a patient's vital signs and sends them to any device that is connected to back-end servers and databases that can store the patient's records and make pertinent diagnostic recommendations. In this paper, the health care of patients are taken into consideration and revolves around it, WBANs can also be implemented in the field of elderly care, infant care and monitoring the vitals of eminent sports persons monitoring their vitals and providing proper care. Moreover, in the recent pandemic, we see a lot of people rely on wearable

medical devices to monitor their personal health. The datas inside the wearable devices could be collected, processed and stored for a long term purpose for health benefit. This paper covers the challenges faced by the sensors, routing challenges faced when they try to communicate and security issues. Security plays an important role when it comes to the medical domain. the paper discusses various security threats which could happen on the WBAN and presents a review on the mechanisms which are available to overcome these. As per analysis, to fulfil WBAN's key security needs and thread efficiency, a custom implementation of network coding can be used. WBAN is rapidly expanding, however there is currently no robust and comprehensive security architecture in place for these networks. WBAN data security and privacy research is still in its infancy, and more research and studies are needed in this area.

## 8. ACKNOWLEDGEMENTS

We wish to express our extreme gratitude to the almighty for giving the strength and courage to complete this research work. Thank you.

## REFERENCES

[1] Kang J., Adibi S. (2015) A Review of Security Protocols in mHealth Wireless Body Area Networks (WBAN). In: Doss R., Piramuthu S., ZHOU W. (eds) Future Network Systems and Security. FNSS 2015. Communications in Computer and Information Science, vol 523. Springer.

[2] Bhushan, B., Sahoo, G. Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. Wireless Pers Commun 98, 2037–2077 (2018). https://doi.org/10.1007/s11277-017-4962-0

[3] Li, M., et al.: Data security and privacy in wireless body area networks. Wireless Commun. 17, 51–58 (2010)

[4] Evered, M., Bogeholz, S.: A case study in access control requirements for a Health Information System. In: The Second Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation (2004).

[5] Meingast, M., Roosta, T., Sastry, S.: Security and Privacy Issues with Health Care Information Technology. In: The Proceedings of the 28th IEEE EMBS Annual International Conference (2006).

[6] Info Guide to HIPAA Compliance, Implementation and Privacy, http://www.hipaa-101.com (July 31, 2012)

[7] Krohn, R., Metcalf, D.: mHealth Innovation: Best Practices from The Mobile Frontier, p. 204. HIMSS, Chicago (2014)

[8] Li, M., et al.: Data security and privacy in wireless body area networks. Wireless Commun. 17, 51–58 (2010)

[9] Irum, S., Ali, A., Khan, F.A., Abbas, H.: A hybrid security mechanism for intra-WBAN and inter-WBAN communications. Int. J. Distrib. Sens. Netw. 2013, 1–11 (2013)

[10] Zheng, J., Jamalipour, A.: Wireless Sensor Networks: A Networking Perspective, pp. 1–489. Wiley, Hoboken (2008)

[11] Toorani, M., Shirazi, A.A.B.: LPKI - a lightweight public key infrastructure for the mobile environments. In: 2008 11th IEEE Singapore International Conference on Communication Systems, ICCS 2008, pp. 162–166 (2008)

[12] Nasser, N., Chen, Y.: SEEM: secure and energy-efficient multipath routing protocol for wireless sensor networks. Comput. Commun. 30(11–12), 2401–2412 (2007)

[13] Cherukuri, S., et al.: Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. Presented at the Proceedings of the International Conference on Parallel Processing Workshops (2003)

[14] Raghunandan, G. H., & Lakshmi, B. N. (2011). A comparative analysis of routing techniques for wireless sensor networks. In 2011 national conference on innovations in emerging technology.

[15] Rashvand, H. F. (2012). Smart sensing architectures. In Distributed sensor systems practice and applications.

[16] Ye, W., & Yarvis, M. (2004). Tiered architectures in sensor networks. In the Handbook of sensor networks compact wireless and wired sensing systems.

[17] Tilak, S., et al. (2002). A taxonomy of wireless micro sensor network models. Mobile Computing and Communications Review, 6(2), 28–36

[18] Mpitziopoulos, A., et al.: Jamming in Wireless Sensor Networks. In: Zhang, Y., Kitsos, P. (eds.) Security in RFID and Sensor Networks, pp. 375–397. CRC Press (2009)

[19] Ameen, M., et al.: Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. J. Med. Syst. 36, 93–101 (2010)

[20] Raazi, S.M.K.-U.-R., et al.: BARI+: A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks. Sensors 10, 3911–3933 (2010)

[21] Shah, R.C., et al.: On the performance of Bluetooth and IEEE 802.15.4 radios in a body area network. Presented at the Proceedings of the ICST 3rd International Conference on Body Area Networks (2008)

[22] Gowtham M (2017) Privacy enhanced data communication protocol for wireless body area network. In: International Conference on Advanced Computing and Communication Systems (ICACCS - 2017), Coimbatore, India, p. 5

[23] Li Z, Wang H, Fang H (2017) Group-based cooperation on symmetric key generation for wireless body area networks. IEEE Internet Things J 4(6):1955–1963

[24] Mukhtar T, Chaudhary S (2016) Energy efficient cluster formation and secure data outsourcing using TEOSCC and ECDH-IBT technique in WBAN. In: International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), (p. 17). Chennai, India

[25] Prameela S, Ponmuthuramalingam P (2016) A robust energy efficient and secure data dissemination

protocol for wireless body area networks. In: International Conference on Advances in Computer Applications (ICACA), 978-1-5090-3770-4/16/$31.00©2016 IEEE, p. 14. Coimbatore, India

[26] Alshamsi AZ, Barka E (2017) Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks. In: International Conference on Informatics, Health & Technology (ICIHT), p 7

[27] Econsultancy (2019). The next decade may well see a revolution in the treatment and diagnosis of disease. Xeim, United Kingdom

[28] Anwar M, Abdullah AH, Butt RA, Ashraf MW, Qureshi KN, Ullah F (2018) Securing data communication in wireless body area networks using digital signatures. Tech J Univ Eng Technol (UET) Taxila Pak 23(2):1–6

[29] Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B (2019). HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0. In: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS). Beijing, China, 28–31 Aug 2019

[30] Farooq S, Prashar D, Jyoti K (2018) Hybrid encryption algorithm in wireless body area network (WBAN). In: Rajesh S, Sushabhan C, Anita G (eds) Intelligent communication control and devices. Springer Nature, Singapore, p 10

[31] Rana ES, Kang SS (2019) Implementation of biological key based security technique in wireless body area networks. Int J Innov Technol Explor Eng (IJITEE) 8(8):2156–2163

[32] Khan M, Jilani MT, Khan MK, Ahmed MB (2017) A security framework for wireless body area network based smart healthcare systems. In: Conference: International Conference for Young Researchers in Informatics, Mathematics and Engineering, ICYRIME 2017, (p 6). 80–87

[33] Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S (2016) Survey of main challenges (security and privacy) in wireless body area network for Healthcare Application. Egypt Inform J 18(2):113–122

[34] Li W, Zhu X (2016). BAN-Trust: an attack-resilient malicious node detection scheme for WBAN. In: International Conference on Computing, Networking and Communications (ICNC), (p. 5)

[35] Shayokh MA, Abeshu A, Satrya G, Nugroho MA (2016) Efficient and secure data delivery in software defined WBAN for virtual hospital. In: International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), (p. 5). Bandung, Indonesia

[36] Zhang P, Ma J (2018) Channel characteristic aware privacy protection mechanism in WBAN. Sensors 18(8):2403

[37] Ren Y, Leng Y, Zhu F, Wang J, Kim H-J (2019) Data storage mechanism based on blockchain with privacy protection in wireless body area network. Sensors 19(10):2395

[38] Sivakumar, S., Vivekanandan, P. Efficient fault-tolerant routing in IoT wireless sensor networks based on path graph flow modeling with Marchenko–Pastur distribution (EFT-PMD). Wireless Netw 26, 4543–4555 (2020).

[39] Jabeen, T., Ashraf, H. & Ullah, A. A survey on healthcare data security in wireless body area networks. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-020-02728-y.