# Security Analysis of Wireless Body Area Networks: Current State and Future Directions

## 1 Introduction

Wireless Body Area Networks (WBANs) have emerged as a revolutionary technology in the healthcare sector, enabling continuous monitoring and remote diagnostics for patients. These networks consist of sensor nodes strategically placed on or within the human body, transmitting crucial physiological data wirelessly to medical servers. This data plays a pivotal role in timely medical interventions and improved patient care. However, the sensitive nature of the information being transmitted raises significant security and privacy concerns. As the integration of WBANs becomes more widespread, ensuring the confidentiality, integrity, and availability of patient data becomes paramount. This research paper delves into the multifaceted realm of WBAN security, thoroughly examining various methodologies, technologies, and protocols that have been developed to safeguard patient information. By meticulously analyzing existing solutions, the paper highlights both their strengths and shortcomings. Furthermore, the research paper presents a comprehensive overview of the challenges posed by security threats in WBANs and proposes possible future directions to address these challenges effectively. With the growing need for secure and reliable healthcare data exchange, this study paves the way for enhancing the security landscape of WBANs, ensuring their potential to revolutionize healthcare remains unhindered.

## 2 Related Works

WIRELESS BODY AREA NETWORK is an advancing solution to meet the needs of local and remote healthcare facilities. As WBANs were easy to use in a variety of applications, it's a popular area for attackers. Asam et al.[2] provided a detailed explanation about various security issues related to WBAN and categorized them into security and cooperation issues. Therefore, proposed a secure cooperative relaying solution for WBAN to solve most of the inheritance problems. And suggested to work on to detect and mitigate different types of DoS attacks, as part of an effective security mechanism. Hasan et al.[7] discussed about the architecture, communication technologies, challenges, and different aspects of WBAN . They also explained the drawbacks of existing WBAN frameworks. They believed that the successful implementation of WBAN would definitely improve the standard of life whether it's a medical or non-medical aspect. It would reduce the prices of hospitalization of patients and helps with early detection of any abnormalities. And as new technologies like SDN and blockchain are advancing rapidly, integrating these technologies with WBAN will bring extraordinary changes within the healthcare sector. They expected that SDN and blockchain could solve some of the most important challenges of WBAN.As the generation in electronics advances, wireless communications, sensor technology, and MEMS have enabled the development of small, low-energy sensors and actuators that can be positioned on, internal, around the human body. One can efficaciously use wireless body area network to deliver sensory data to a relevant server or body coordinator node where the data can be stored, monitored, and analyzed. Hammood et al.[6] discussed that WBAN security implicates some security troubles and provided a survey of WBAN in terms of device architecture, address assignment, routing, chan- nel modelling, PHY layer, MAC layer, security, and applications.

Wireless Body Area Network (WBAN) is an advanced technology for monitoring and record- ing human fitness and health alerts. But due to the sensitive data contained within the WBAN, insecure records can compromise patient privacy and result in inappropriate medical treatment. Usman et al.[19] afforded a complete assessment of Wireless body area network, with a specific focus on security and privacy issues, countermeasures, after which: advised research guidelines and open questions. Firstly, they gave an outline of the WBAN architecture, topol-ogy, and design necessities. In addition, safety requirements and demanding situations have been investigated, and numerous threats and attacks have been identified. Further, different safety features have been taken into consideration in the course of the investigation to fulfil WBAN security necessities and miti-gate potential threats.Taleb et al.[17] aimed to research the wireless technology used in wireless body area network systems.In addition to an in-depth overview of current technologies, they described the need for the recent low-power wide area network (LPWAN) technologies and destiny 5G, B5G, and 6G, and some of those technologies' suitability for WBAN applications. They explained the key capabilities of a WBAN system, which include power consumption, interfer-ence, protection, privacy, reliability, and selecting the proper sensor. They also reviewed the cutting edge of several wireless communication exchange technolo-gies to decide their suitability for scientific WBAN applications, such as new LPWAN conversation technologies, which eventually described the roles of 5G, B5G, and 6G and their effects on the healthcare system.Ayed et al.[3] focused on WBAN's trust management challenges and categorized attacks on trust management models. Firstly, they provided an overview of the existing intra- and inter-WBAN approaches for trust management in WBAN. And Identified some important points to consider as best practices for building a reliable and secure trust management framework. Finally, they concluded by proposing a SWOT diagram of trust management in a WBAN environment.

Usman et al.[20] first proposed a new four-tier architecture for remote monitoring systems and then suggested identifying security requirements and challenges at each tier. They also provided a brief review of the literature aimed at improving the security and privacy of WBAN and outlined the issue. In it, they discussed current and future research trends in WBAN and remote monitoring systems in healthcare. In particular, they focused on the challenge of ensuring confidentiality, integrity, and availability at all levels of WBAN com-munication. Finally, some areas of research are highlighted to ensure end-to-end security.Wireless Body Area Network contains small interconnected sensors for continuous collection of medical data. This data is sent over the network for further processing. However, protection of health data is very important and difficult due to the different numbers of active and passive attacks. There were several references to data security technologies such as digital signatures, ECC, and AES, but they include some security method failures. Therefore, Jabeen et al[8] proposed a new genetic-based cryptographic algorithms to protect data in an untraceable format. In addition, the transmission of encrypted data over the network remains private and is protected using the lightweight telemetry transport protocol.Gomathy B et al.[4] presented a comprehensive and system-atic review of privacy and security challenges in the cloud environment. They have researched and reviewed various articles on all aspects related to security and privacy concepts and identified several tasks such as the architecture of the WBAN in the cloud, cloud-to-cloud privacy and security issues, and optimization strategies to improve security performance. They prepared this investigative survey paper to address various cloud security problems and possible solutions using existing techniques such as cryptography and machine learning-based intrusion detection and prevention. Based on the survey, they suggested that optimization-based patterns are a recent trend in cloud security dealing with different challenges.

WBAN data communication is primarily based on wireless communications and can lead to a variety of security threats and attacks. Anwar et al.[1] focused on key issues and challenges related to WBAN's data security and privacy. Some of the existing methods for backing up WBAN data were described. D-Sign, a hybrid approach that uses a private key and a digital signature to protect the data in a WBAN has been proposed. And that provided better protection for WBAN sensory data. The results showed that the proposed method is more efficient in terms of data security and distinguished use of network resources.Big Data proposes a secure data collection technique that addresses WBAN issues. V. N. Rajavarman et al.[12] firstly, registered the sensor node with CA Connect in a Big Data center network. After preprocessing, the sensor was associated with the big data center by mutual authentication using the Elliptic Curve Digital Signature Algorithm. Sensor nodes were designed with secure distributed storage and aggregate data transmission. They proposed a protocol based on the Elliptic Curve Cryptography Certification Algorithm, ensuring efficient data communication with one-time tokens, efficiently securing cryptographic algorithms, and reducing costs.while WBAN presents a handy manner to acquire patient statistics, it also poses serious challenges which might be basically meditated in the secure storage of gathered data records. Ren et al.[13] raised "Unauthorized access" and "Message tampering" as the major security concerns. And for this reason, they made use of blockchain technology to keep and enhance the security of the collected data statistics. And a sequential aggregate signature scheme using data and a designated verifier (DVSSA) was proposed that ensures that only authorized get access to and overcomes the shortcomings of blockchain. They proposed the integration of these two(blockchain and DVSSA). The integrity of user statistics is assured through the feature safety of the blockchain towards operations. The Experiments by them have additionally confirmed that it makes use of an efficient signature scheme. DVSSA signatures could reap the intention of compressing blockchain space and conserving resources.

Anurag Tewari et al.[18] discussed the features of WBAN . In this review, they provided an assessment of contemporary techniques for designing a whole new dimension of safe and coherent remote eHealth monitoring systems using WBAN. And, they discussed about Some of the shortcomings of WBAN and their possible solutions. They concluded by suggesting that future research must be directed to interdisciplinary connections in order to obtain better and unexplored areas of WBAN-based e-healthcare and also in the direction of IOT to ensure security and privacy of data in WBAN.Deena M. Barakah et al.[5] conducted an extensive survey of WBANs and deployed virtual doctor servers on top of the existing WBAN architectures. The purpose of this review was to explore and identify the role of Wireless Body Area Network in bettering the well-being of human life. This survey sought to scan viable applications of Wireless body network in day-to-day life, the challenges WBAN faces today, and open survey questions. The authors also described Wireless Body Area Network's already existing architecture and proposed a new component, VDS(Virtual Doctor Server). And on the other hand, mHealth security is important in clinical practice to protect and secure the patient user data and WBAN. WBAN and WSN security provides security on a personal-level in contrast to large-scale threats in similar MC networks. James Jin Kang et al.[10] thought that this requires an integrated approach to designing and implementing network security solutions at the public network service provider level. And as low power consumption is an important feature that affects the development and safety of mHealth technology, they felt it was necessary to Provide various levels of mHealth security so that users can choose their level that suits their wants and needs. It Is important.

The numerous security plans for WBAN are discussed and are reviewed indepth by Jabeen et al.[9] .To improve security for transferring patient health data, a number of existing techniques have been examined. They suggested that the best approach for WBAN data security will be evaluated after considering a number of techniques like blockchain, D-Sign, Biometric, RSSI etc. Various existing techniques have been observed in the literature to identify ways to enhance the security of patient health data.Wireless sensor networks(WSN) used in healthcare sector are growing hugely. Many applications such as sphygmomanometers and heart rate monitors are already in use. The use of sensor technology is increasing rapidly in the area of the Wireless Body Area Network (WBAN), nowadays. Security and privacy are very important because the device you use is wireless. Sreeja et al.[16] discussed the problems and analyzed the problems and possible countermeasures. As these wireless applications grow rapidly, their impact will grow. They inferred that it is important to address these issues. Without this, the technology could face major obstacles to future growth and development. Finally, added that Appropriate coordination between various government agencies, manufacturers, and research institutes is needed to overcome these obstacles.Shaheen et al. [14] discussed their thoughts as Wireless Body Area Network is a spectacular revolution in eHealth technology sector that provides physicians with a remote mechanism for monitoring and collecting patient health-related data using wearable sensors. Today, people often have sensor devices embedded in their bodies to provide them with an enhanced and better quality of life. This is an amazing advancement, including information and communication technology (ICT) to maintain normal human living standards, especially by using WBAN to ensure ease of use and convenience, respectively. All of these efforts also involve security and privacy issues. Therefore finally , they described possible solutions to potential security attacks.Qu et al.[11] analyzed the strengths and weaknesses of various routing protocols. They categorized and analyzed in detail the various existing routing protocols proposed by WBAN. Routing protocols have been found to play an important role in the design of energy-efficient, reliable, and cost-effective

WBANs. Based on methods and design goals, WBAN's routing protocols were categorized into attitude-based, temperature-based, cross-layer, cluster-based, and QoS-based routing, by them. In addition, they analyzed a comparison of different protocols so that one could choose the right protocol for their application. This study of theirs benefits researchers to study WBAN's energy-efficient routing protocols in the field of medical systems.Singla et al.[15] have tried to classify a large number of routing protocols from the WBAN literature, such as AES, CSEER, etc., using different cryptographic systems. They analyzed each routing protocol and presented a comparative analysis with different techniques regarding their goals, techniques, strengths and weaknesses, and other characteristics. Symmetric key cryptographic routing protocols have been shown to focus more on the resource-constrained nature of WBAN than on patient data security. On the other hand, they proved that biometric and asymmetric key cryptographic routing protocols emphasize the confidentiality of patient data rather than the resource-constrained nature of WBAN.

| Author, Year | Key contribution | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 |
|---|---|---|---|---|---|---|---|---|---|
| Asam et al. ,2019 | proposed a secure cooperative relaying solution for WBANs to address most of the inherit issues and devised a novel relay selection approach while relying over relays | No | Yes | Yes | Yes | Yes | No | Yes | Yes |
| Jabeen et al. ,202‘ | Various existing techniques are observed to recognize how the security is upgraded for patients' health data. | No | Yes | Yes | Yes | Yes | No | Yes | Yes |
| Usman et al. ,2018 | Divide WBAN into four-tiers and analyzed security requirements and challenges faced by the medical devices at each tier of communications. | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Jabeen , 2020 | A novel genetic-based encryption algorithm is proposed to secure the data in an uncomprehensive form. Besides, the transmission of encrypted data over the network also remains confidential and protected by using a lightweight telemetry transport protocol. | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| singla et al. , | Symmetric key cryptographic routing protocols have been shown to focus more on the resource-constrained nature of WBAN than on patient data security. On the other hand, biometric and asymmetric key cryptographic routing protocols emphasize the confidentiality of patient data rather than the resource-constrained nature of WBAN. | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| B et al. ,2020 | The authors suggest that optimization-based patterns are a recent trend in cloud security dealing with different challenges. | Yes | Yes | Yes | Yes | No | No | Yes | Yes |
| Ayed2020 et al. , | The author proposed a SWOT diagram of trust management in a WBAN environment. | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

**Table 1 continued from previous page**

| Author, Year | Key contribution | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 |
|---|---|---|---|---|---|---|---|---|---|
| Rajavarman et al. , | Proposed a protocol based on the Elliptic Curve Cryptography Certification Algorithm, ensuring efficient data communication with one-time tokens, efficiently securing cryptographic algorithms, and reducing costs. | Yes | Yes | Yes | No | No | No | Yes | No |
| anwar et al. , | proposed a method that is more efficient in terms of data security and distinguished use of network resources. | No | Yes | Yes | Yes | No | No | Yes | Yes |
| Barakah et al. ,2018 | The authors described Wireless Body Area Network's already existing architecture and proposed a new component, VDS(Virtual Doctor Server). | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Kang et al. , | Suggested an integrated approach to designing and implementing network security solutions at the public network service provider level. | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes |
| Tewari Joseph ,2 | Discussed about the data mining algorithms and the techniques that could be employed with the intelligent computing system. | Yes | No | No | Yes | No | No | Yes | Yes |
| Hammood et al. ,2018 | Discussed or analyzed current techniques for disaster prediction, detection and management. | No | Yes | Yes | Yes | No | Yes | Yes | Yes |

**Table 1 continued from previous page**

| Author, Year | Key contribution | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 |
|---|---|---|---|---|---|---|---|---|---|
| Taleb et al. ,2022 | Analyzed agglomerative hierarchical as the optimal algorithm to identify SRL profiles in online learning environments. | Yes | No | Yes | Yes | No | No | Yes | Yes |
| qu et al. ,2021 | Discussed about data mining approaches as well as clustering approaches to analyze accident data of the fifeteen districts of Rome. | No | No | Yes | Yes | Yes | No | Yes | Yes |
| hasan et al. ,2021 | Discussed about suicide<br>bomb attacks by extracting hidden patterns from suicidal bombing attack data For classification, Naïve Bayes, ID3 and J48 algorithms are applied. | Yes | No | No | Yes | No | No | Yes | Yes |

**Table 1 continued from previous page**

| Author, Year | Key contribution | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 |
|---|---|---|---|---|---|---|---|---|---|
| usman et al. ,2021 | Analyzed the challenges faced by previous studies in three aspects and put forward future suggestions on data collection, EDM methods used, and interpretation of prediction model. | No | Yes | Yes | Yes | **Yes** | Yes | Yes | No |
| shaheen ,2020 | Presented a data mining based decision support system using decision tree and artificial neural network as a hybrid approach to estimate the marketing strategies for an organization. | Yes | No | Yes | Yes | No | No | Yes | Yes |
| T. Sreeja et al. ,2021 | Discussed about Stochastic, Statistical and Computer based modeling techniques and Artificial Neural Networks, Fuzzy logic, Support vector machines, Bayesian classifiers, and Cluster algorithms based data mining techniques. | No | No | Yes | Yes | No | No | Yes | Yes |

**Table 1 continued from previous page**

| Author, Year | Key contribution | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 |
|---|---|---|---|---|---|---|---|---|---|
| Anwar et al. ,2021 | proposed a method that is more efficient in terms of data security and distinguished use of network resources. | Yes | No | Yes | Yes | Yes | No | Yes | Yes |

p1 = Data security p2 = Resiliency to known attacks p3= Robustness p4=Saving power p5=Efficient p6=privacy p7=Cost efficient p8=Verification

# 3 METHODOLOGY

## 3.1

### 3.1.1 Definition

A Wireless Body Area Network (WBAN) establishes connections between impartial nodes like sensors and actuators, which could be situated within clothing, on the body's surface, or beneath a person's skin. These nodes utilize wireless communication channels, forming a network that often spans the entirety of the human body.

### 3.1.2 WORKING MECHANISM

WBAN is specifically tailored for application in medical systems and emergency scenarios. In such situations, the compact sensor nodes within the network collect vital bodily data and transmit it to a medical server at a hospital. Medical professionals then review this data to make informed diagnoses. This network maintains the security of communication using private physiological values (PVs), ensuring enhanced medical services. Neglecting security measures could lead to erroneous detections, endangering human lives.

WBAN secures communication via cryptographic keys, employing specialized key distribution schemes. The Diffie-Hellman cryptosystem is utilized to avoid pre-deployment of keys. WBAN sensors differ from regular Wireless Sensor Networks (WSN) due to their limited power and memory. Unlike WSNs, WBAN employs distinct security methods, with unique key management mechanisms. The security strategy utilizes a reliable plug-and-play system, particularly suitable for changing network topologies. However, a potential flaw lies in information leakage during key agreement due to the exchange of excessive data, such as complete feature sets. This could be exploited by a third party possessing these feature sets.

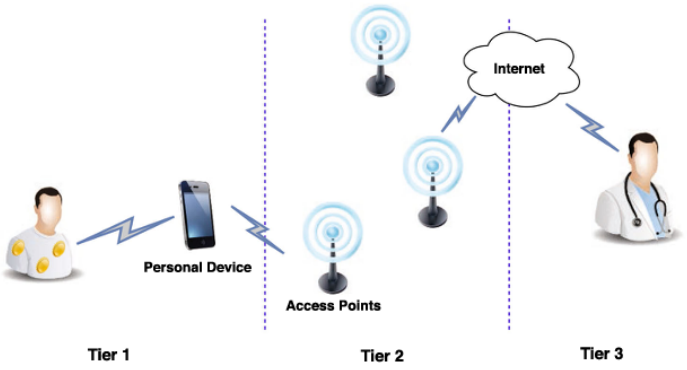
### 3.1.3 Tiers of WBAN:

Sensors in WBANs are in charge of locating physiological data, digitising it, and communicating it to an access point. They can be inserted under the skin, worn close to the body (near-body sensors), or mounted on the body (on-body sensors) (in-body sensors). The first collects and transmits data; the second stores and retrieves data. Actuators of the second type can deliver medication based on the data gathered in addition to measuring and sending data like the first type. Wireless technologies are used to transmit the acquired data to the medical server, where it may be examined and saved. Depending on the system architecture and the technologies being utilized, this can be applied based on 2, 3, or 4 levels. Three levels make up the most common architecture for WBANs: intra-WBAN, inter-WBAN, and beyond-WBAN. Intra-WBAN describes communication first between the sensors and the personal device, and then between the sensors. Some current solutions do not require a wireless network in the first layer by using cables to connect sensors to a personal device directly. Other protocols allow wireless data transmission to a coordinator or master node for further forwarding to the personal device or directly to the personal device, which then forwards the data to an access point after processing. In multi-hop WBAN, where the nodes' range is limited, this type of architecture is used. Therefore, the message delivered from a node may travel through the intermediary nodes in order to reach the personal device. In Single-hop WBAN, the personal device receives the data directly from the nodes in a single-hop design. Although the single-hop design has a lower delay than the multi-hop configuration, the power is higher.

The use of wireless technologies for communication between the personal device and the access point is included in inter-WBAN. WBANs are linked together with other networks via the inter-WBAN tier. Two different types of architecture are utilised for inter-WBAN communication: infrastructure-based architecture, which is used in the majority of WBAN applications and offers more secure communication; and ad-hoc-based architecture, which enables quick and flexible disposition.

The communication between the Access Point and the distant medical centre is referred to as "beyond-WBAN." A gateway is used as a bridge in order to communicate with medical personnel through the Internet or cellular networks. Medical experts are permitted to review the data after obtaining it in order to monitor the patient and offer required medical advice. This level also enables the restoration of patient medical data, which may be required to plan an

### 3.1.4 Typical WBAN Workflow diagram:



### 3.1.5 Technologies available for WBAN Communication:

The WBAN Communication can be categorised into Intra-Body Communication and Inter-Body Communication. Some of the Technologies used for Intra-Body Communication are: IEEE 802.11ax IEEE-802.16n IEEE 802.16.1a Zigbee healthcare 1.0 Some of the Technologies used for Intra-Body Communication are: UMTS 4G 4.5G 5G and beyond.

### 3.1.6 Role of WBAN in Healthcare sector

The wireless body area network is a key technology that can monitor and store human health signals for a considerable amount of time. As part of its first applications, it offered some type of automatic therapy control while continuously tracking and recording patient with chronic illnesses' health characteristics. An extremely recent use of wireless networks is operation assistance. Doctors must keep an eye on the patient's vital signs during a surgery in order to take prompt response. Adhesive electrodes can be applied to the patient to obtain these signals, which are then relayed via wires to display monitors. The usage of so many wires around the operating table restricts access to the patient for the medical staff. Furthermore, a powerful enough impact on the wires can cause the adhesive to come away from the patient. The Smartpad is provided to allow surgeons and medical teams to operate with more freedom. Without glue or cables, a device shows the patient's signals. Despite the fact that real-time patient monitoring is not a brand-new topic in wireless medical applications, researches and businesses are spending a lot of time and money on it. These applications primarily make use of biomedical sensors to track the physiological signals of patients, including electrocardiograms, blood pressure, blood glucose, coagulation, body weight, heart rate, EMG, ECG, oxygen saturation, and others. Home monitoring systems for elderly and chronic patients are expanding quickly in both quantity and quality. Utilizing the system can shorten a patient's stay in the hospital and improve their mobility and safety. Data is continuously and periodically collected by the system, and it then sends that data to a centralised server. Physicians can remotely access patient information. These tools also significantly reduce the amount of time required by doctors and patients too. In contrast to traditional monitoring, which involves the doctors actually seeing the patients, the doctors are able to keep an eye on multiple patients at once. Patients are no longer compelled to visit hospitals on a regular basis. Medical applications can leverage wireless sensor networks to create databases for ongoing clinical usage. It has numerous other uses, including emergency medical care.

## 3.2 3.2 PROBLEM STATEMENT

While WBAN facilitates the collection of patient data, it has significant drawbacks, especially when it comes to secure data transmission or storage. The needs of WBAN users cannot be satisfied by the privacy and security of data stores in WBAN devices. WBAN raises a number of privacy and security issues because it stores and processes sensitive health information. Security is one of the most critical components of a framework. Security is understood as the well-being of the frame. The similarities in the applications of sensor systems in human services are generally distant. This can introduce various security risks to these frameworks. Many people are concerned about healthcare safety issues. These threats and attacks can pose significant problems to the social existence of a person using a remote sensing device. Here and there, for example, the monitoring of the patient area. Privacy is also one of the main issues in wireless sensor networks for healthcare applications. These can be personal beliefs, the social and cultural environment and other public/private causes in general. Sending patient data via wireless means can pose a serious threat to an individual's privacy. Whether the data is collected with or without the individual's consent due to the necessity of the system, abuse or privacy can prevent individuals from taking full advantage of the system.

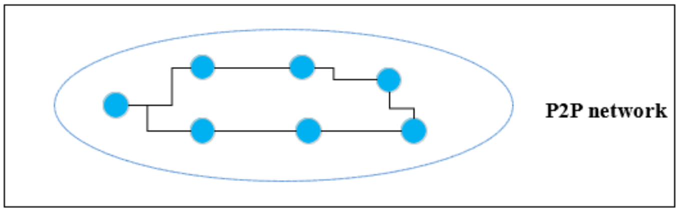
The attacks on WBAN can be roughly mentioned as Confidentiality and authentication attacks through enemy eavesdropping and attempts to reproduce attacks or electronic phishing. Attacking the integrity of the service; Network forced to receive false information. Network availability attacks and Denial of Service (DoS) attacks affect network capacity and performance. And, here raises a question of How to increase data security through WBAN from various attacks while reducing time, cost and memory consumption? The other two main problems of WBAN Communication are: Unauthorized access and data manipulation. Unauthorized WBAN attackers and theft of user information Such attacks violate user privacy. An attacker could sell a user's information to an insurance company. Attackers could change the tokens in the WBAN data collectors to obtain fake user data. This affects security. For example, if the user is a patient and the patient receives the patient data. Doctors are misinformed and can lead to wrong treatment by doctors. There are also many other issues such as energy, mobility, security, communication like networks, QoS, coordination, etc.

## 3.3 3.3 Discussion of Existing Solutions

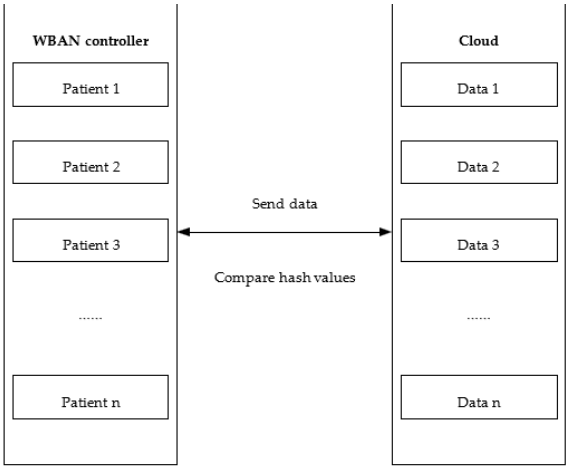
As the security of WBAN data is so crucial, that even it can cost a life if the secure communication between doctor and a patient is interrupted, it is important to take proper countermeasures to all the security issues. First, on system security, in the WBAN situation, if a man uses different tools, internal control tools can be used to transfer information from the entire system. This control tool can also act as a conduit between your internal system and communication with the outside world. Security measures such as authentication, firewalls, and equivalent checks can be attached to page movement at the controller level. Administrative level security implies Effective control of permissions is very important to address the framework. Security efforts should be linked to the investigation of security breaches by employees or those responsible for general framework activities.A customer chain of command characterized by strong authentication measures can prevent security breaches at this level. Security efforts must include some form of access component to ensure only authorized clients can access information. Physical layer security implies Measures at this layer may include controls over access to physical tools and information related to collection or processing. Gadgets are powerless against people with malicious intentions and certain causes like burnout at. In case of a catastrophic event, the framework can fail, causing serious problems with general framework tasks. That's why it's important to take a good look at your devices and manipulate them to configure them. Security at a technical level implies Most devices such as servers, sites and other tools require security controls at a special level. If the ultimate goal of the system is to send information to a central server, then server-based security should be used on the server side and client-based security on the end-client side. This is especially important for secure data sharing. This can result in a stack backhaul to the client-side sensor, increasing the overall cost in that regard. For the Information security, The WBAN application includes medical data in addition to personal data. Safety and security are key to all parts. Either way, when you install important sensitive data extensions on your device, you put your data at real risk of theft, corruption, misuse and control. There are several security risks associated with healthcare services using sensor organizations. Data encryption implies Your data will be encrypted so that it cannot be shared while travelling. The benefit of data encryption is privacy protection from spying attacks. Data integrity implies Data integrity benefits include data integrity checks and data initialization.The reliability of the information allows interested parties to verify that the information has not been altered. Data lineage validation indicates to the beneficiary that the declared sender initiated the data. Authentication implies The authentication service consists of the communication process between nodes. This is an effective method against phishing attacks. To achieve a maximum level of security and to barricade from any type of attack, many models are proposed based on these factors: Lightweight: A proposed security solution should be computationally lightweight to meet resource constraints (Polai et al., 2019). Confidential : increasing privacy by ensuring that outsiders cannot learn the identity of the two parties during the authentication process (Shen et al., 2018b). Both parties involved should verify each other: This means that the parties can mutually authenticate each other. Therefore, the authentication process is protected against impersonation attacks (Xiong and Qin, 2015). No Association: ensures that even if an adversary can intercept two outgoing messages belonging to the same node, the hidden identity of the node is still preserved. (Lee et al., 2017a). Session key generation: After a successful authentication process between two nodes, a secure session key must be generated and securely exchanged to protect subsequent communications (Xiong and Qin, 2015). Transmission confidentiality: ensures that session keys are protected even if one or both parties to the communication are compromised. Moreover, even if the adversary has one or both private keys (He and Zeadally, 2015). NON-executable : the ability to effectively neutralize a misbehaving node (Xiong and Qin, 2015). Non-repudiation: It is essential that the messages sent through the WBAN are non-repudiable. Therefore, senders cannot reject the messages they send (Shen et al., 2018b). Resistance against known attacks: A proposed security solution should be resilient against known attacks. For example, resilience against replay attacks, resilience against spoofing attacks, resilience against verification attacks, resilience against modification attacks, and resilience against man-in-the-middle attacks (Chala et al., 2017). Many different schemes were proposed to ensure absolute security to the discussed problems in Wireless Body Area Networks. Those include: Mo0del Based on Hashing algorithms: A research review uses Secure Hash Algorithm (SHA) along with cryptographic techniques to make data transmission more secure and robust (Anwar et al. 2018). A hashing method creates a digital signature to transfer patient data in a more secure manner. The proposed algorithm uses an asymmetric key generation approach including a public-private key pair, which reduces the speed of the algorithm and adds complexity. D-sign uses the SHA-1 hash function to encode data into fixed-size bits called hash values. It uses a hash function protocol and uses 128-bit text and key sizes. Model Based On Advanced Encryption Scheme: A low-power and secure WBAN protocol focuses on implanting wearable devices, also called sensor devices, inside patients to monitor their current health status. The human body connects to the Internet through a gateway device. Medical professionals use this data to treat patient diseases such as asthma, diabetes, heart attacks and high blood pressure. WBAN is a developing technology focusing on health screening systems. Encrypting and decrypting medical information is very important, and it is necessary to generate private keys on both the source and destination sides. Model Based On Kerberos protocol: Rapid changes in technology led to the idea of WBAN for smart healthcare systems (Jabeen 2021). Therefore, high security of sensitive data is still a big challenge. Several data security techniques are in place to protect your data. This article introduces the design of Software Defined Networks (SDN) for data transfer and the names of network authentication protocols used such as Kerberos. This article provides a flowchart for emergency data delivery. This means that the user send the encapsulated data packet. This data packet is checked by the Kerberos protocol and the authorized user is granted access to retrieve the data. When data is sent through SDN, the SDN controller examines the data format and suggests specific paths for data transmission.

Model Based On BAN Trust model: WBAN is a key technology that supports the healthcare system. Therefore, data security and reliability are important in this context. Various encryption and decryption techniques have been proposed for data security, but they can still be vulnerable to malicious node attacks. This paper used the BAN trust scheme to detect and mitigate the attacks of malicious nodes against WBAN. BAN Trust consists of two parts: data analysis and trust management. Direct communication is not easy for WBAN nodes, but sending data is very important. So to understand whether a node can be trusted, first check if the node has interacted with another node before. Recommendations obtained from others are important to determine the reliability of this unknown node. Model Based on 802.15.4/ZigBee : 802.15.4/ZigBee WBAN includes recent methodologies in design (Tariq 2017) that prevent migration to certification, management, and detectable medical stimulation systems (Tariq 2017). Physical temperature, voice, heart rate, blood pressure. The ZigBee guardband is inconsistent in two important angles of symmetric key cryptography: bearing and dispersion.

Model Based on Blockchain: WBAN is a technology that monitors and records health signals for a long time. Because WBAN stores and develops critical patient health information, it raises various security and privacy concerns. It uses blockchain technology and digital data signature to combat unauthorized access and manipulation. Blockchain is used to prevent data manipulation by using a chain of hash values to select the appropriate value to use for encryptionA successful scripted attack by a hacker on a centralized database gives the hacker access to a large amount of data. But with blockchain and distributed ledger technology, cracking is much more difficult. The goal of many blockchain projects is to secure data storage. The potential benefits for end users are revolutionary. Blockchain projects not only have the potential to create architectures for data storage systems that are inherently more secure, but also empower individual users. Blockchain projects often use native digital currencies as part of their tokenization model. This allows users to monetize third-party data while avoiding identity theft and other problems caused by massive data breaches in recent years.

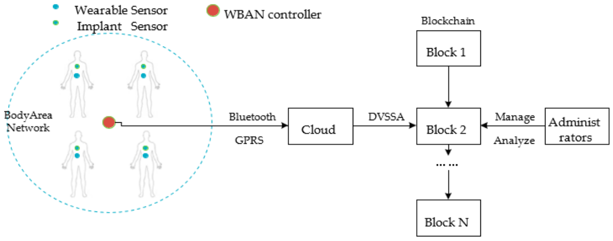


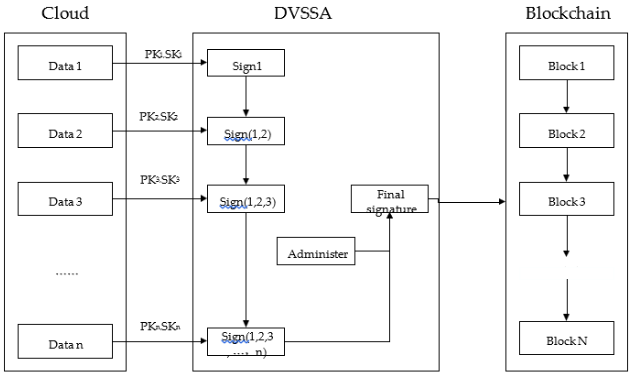
Model Based on Digital Signature: A digital signature is used as a verifier. This means ensuring that administrators have access to data. Digital signatures also ensure that users cannot deny attacks. The DVSSA signature technique used in this paper aggregates all individual signatures to match the size of signatures in the blockchain to the size of individual signatures, greatly reducing memory consumption. User data is signed by the DVSSA signature process and submitted for blockchain-based computation. Traditional Data storage solutions rely heavily on central databases to maintain security.



# 4 FUTURE WORKS

WBAN is an advanced medical technology for healthcare services. Continuous monitoring provides early diagnosis and prevention of various diseases. In addition, it helps to reduce medical expenses. However, security and privacy concerns have prevented its successful implementation. Since the patient's physiological information is very sensitive, security mechanisms should be an integral part of the WBAN routing protocol for patients worldwide. confirm. However, due to limited resources, designing a secure and energy-efficient routing protocol is a difficult task. This document has attempted to categorize the routing protocols in the WBAN literature based on different cryptographic systems. After analyzing each routing protocol, we provide a comparative analysis with other different schemes in terms of objectives, techniques, strengths and weaknesses, and other characteristics. Different security challenges and limited resources are considered by different protocol classifications. Symmetric-key encrypted routing protocols emphasize the resource-constrained nature of WBANs on patient data security. On the other hand, cryptographic routing protocols that use biometric and asymmetric keys emphasize patient data security more than the resource-constrained nature of WBANs. Mixed key encryption routing protocols try to balance both aspects. An extensive literature review suggests that future work should focus on network optimization to reduce power consumption, path loss, and delay. To meet the strict security requirements of WBAN, advanced encryption techniques and low overhead are recommended. Lossless compression techniques are recommended to reduce network traffic and achieve high performance. This study also points out that as a future challenge, it aims to propose a secure cooperative relay solution for WBAN to solve more of the traditional problems. Similarly, we identify and mitigate various types of DoS attacks as part of an effective security mechanism. It solves the problem of unauthorized access to WBAN using blockchain and DVSSA scheme, allowing only designated verifiers to view and analyze WBAN user data. In addition, we discussed various techniques for storing WBAN user data to address the data tampering issue and ensure data integrity based on strong cryptographic anti-tampering properties. DVSSA signature scheme is proposed in this document By concatenating each person's signatures sequentially, the blockchain becomes the size of one person's signature and saves a lot of storage space. Personal data received from each user is stored in separate data blocks in the cloud and stored in the cloud as linked lists. User data in the cloud is signed using the DVSSA signature scheme and sent to the blockchain. The study also concludes that the combination of blockchain and DVSSA digital signature scheme is a very suitable solution to solve data manipulation and unauthorized access. As I said before, I think future work should be more towards this goal.





## References

[1] M. Anwar, A. H. Abdullah, R. A. Butt, M. W. Ashraf, K. N. Qureshi, and F. Ullah. Securing data communication in wireless body area networks using digital signatures. *Technical Journal*, 23(02):50–55, 2018.

[2] M. Asam, T. Jamal, A. Ajaz, Z. Haider, and S. A. Butt. Security issues in wbans. *arXiv preprint arXiv:1911.04330*, 2019.

[3] S. Ayed, L. Chaari, and A. Fares. A survey on trust management for wban: Investigations and future directions. *Sensors*, 20(21):6041, 2020.

[4] G. B, R. Sm, and S. G. Challenges and issues in cloud security for wban applications - a systematic survey. *Innovations in Information and Communication Technology Series*, 2020.

[5] D. M. Barakah and M. Ammad-uddin. A survey of challenges and applications of wireless body area network (wban) and role of a virtual doctor server in existing architecture. *2012 Third International Conference on Intelligent Systems Modelling and Simulation*, pages 214–219, 2012.

[6] D. Hammood and A. Alkhayyat. An overview of the survey/review studies in wireless body area network. In *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*, pages 18–23. IEEE, 2020.

[7] K. Hasan, K. Biswas, K. Ahmed, N. S. Nafi, and M. S. Islam. A comprehensive review of wireless body area network. *Journal of Network and Computer Applications*, 143:178–198, 2019.

[8] T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band, and A. Mosavi. A lightweight genetic based algorithm for data security in wireless body area networks. *IEEE Access*, 8:183460–183469, 2020.

[9] T. Jabeen, H. Ashraf, and A. Ullah. A survey on healthcare data security in wireless body area networks. *Journal of ambient intelligence and humanized computing*, 12(10):9841–9854, 2021.

[10] J. J. Kang and S. Adibi. A review of security protocols in mhealth wireless body area networks (wban). In *FNSS*, 2015.

[11] Y. Qu, G. Zheng, H. Ma, X. Wang, B. Ji, and H. Wu. A survey of routing protocols in wban for healthcare applications. *Sensors*, 19(7):1638, 2019.

[12] V. N. Rajavarman and R. Shobarani. A secured data retrieval architecture for wban using elliptic curve digital signature. *VOLUME-8 ISSUE-10, AUGUST 2019, REGULAR ISSUE*, 2019.

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

[14] N. Shaheen, R. Mughal, and M. R. Shafique. Survey of security and privacy in wireless body area networks for healthcare applications.

[15] R. Singla, N. Kaur, D. Koundal, and A. Bharadwaj. Challenges and developments in secure routing protocols for healthcare in wban: A comparative analysis. *Wireless Personal Communications*, 122(2):1767–1806, 2022.

[16] S. Sreeja and M. Bharathi. A survey on security and privacy issues in wireless sensor networks for healthcare application. *International Journal of Recent Trends in Engineering & Research*, 4(03), 2018.

[17] H. Taleb, A. Nasser, G. Andrieux, N. Charara, and E. Motta Cruz. Wireless technologies, medical applications and future challenges in wban: A survey. *Wireless Networks*, 27(8):5271–5295, 2021.

[18] A. Tewari and P. Verma. Security and privacy in e-healthcare monitoring with wban: A critical review. *International Journal of Computer Applications*, 136:37–42, 2016.

[19] M. Usman, M. R. Asghar, I. S. Ansari, and M. Qaraqe. Security in wireless body area networks: From in-body to off-body communications. *IEEE Access*, 6:58064–58074, 2018.

[20] M. Usman, M. R. Asghar, I. S. Ansari, and M. Qaraqe. Security in wireless body area networks: From in-body to off-body communications. *IEEE Access*, 6:58064–58074, 2018.