CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

On the Design of Efficient and Secure Heterogenous Generalized Signcryption for Wireless Body Sensor Networks

by

Tabarak Matloob

A thesis submitted in partial fulfillment for the
degree of Master of Science

in the

Faculty of Computing
Department of Computer Science

2023

I dedicate my dissertation work to my parents, supervisor, and all other teachers. A special feeling of gratitude is for my father, the most unswerving man I have ever known in this world

CERTIFICATE OF APPROVAL

On the Design of Efficient and Secure Heterogenous Generalized Signcryption for Wireless Body Sensor Networks

by

Tabarak Matloob

(MCS203053)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Suban Ullah	FAST NUCES, Islamabad
(b)	Internal Examiner	Dr. Amir Qayyum	CUST, Islamabad
(c)	Supervisor	Dr. M. Siraj Rathore	CUST, Islamabad

Dr. M. Siraj Rathore
Thesis Supervisor
April, 2023

Dr. Abdul Basit Siddiqui
Head
Dept. of Computer Science
April, 2023

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
April, 2023

Author's Declaration

I, **Tabarak Matloob** hereby state that my MS thesis titled "**On the Design of Efficient and Secure Heterogenous Generalized Signcryption for Wireless Body Sensor Networks**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MS Degree.

(Tabarak Matloob)

Registration No: MCS203053

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**On the Design of Efficient and Secure Heterogenous Generalized Signcryption for Wireless Body Sensor Networks**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS Degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Tabarak Matloob)

Registration No: MCS203053

Acknowledgements

Allah (S.W.T), the creator of all universes, deserves all thanks. First and foremost, I thank ALLAH (S.W.T.) for giving me the power, wisdom, and blessings to finish this research. My sincere appreciation to my renowned ex-supervisor, Dr. Jawaid Iqbal, I genuinely thank him for his research support, encouragement, and guidance. He helped me understand the subject. He has taught me, consciously and intuitively, how-to do-good experiments. I am really grateful to my family and friends for their help, encouragement, and support during this Master of Science degree. Additionally, this endeavor would not have been possible without the generous support from the Mr. Qaisar Manzoor, who assisted my research. I pray ALLAH (S.W.T.) for true prosperity in all fields and knowledge for the benefit of mankind.

(Tabarak Matloob)

Abstract

In Wireless Body Sensor Networks (WBSNs) various biosensor nodes i.e., ECG, EMG, EEG, BP, SpO2, respiratory rate, and body temperature are deployed on patient body for real time monitoring of patient health records. Furthermore, the collected patient information is stored in a centralized server and then communicated using a public network with various stockholders such as doctors and researchers for further diagnoses and treatment. WBSNs face a variety of challenges due to their constrained nature environment such as patient data security and privacy across a public network, high computational cost and communication overhead along with high energy consumption. To resolve the above-mentioned issues in a desirable way we have proposed an efficient and secure heterogenous generalized signcryption that can adaptively work as an encryption mode, a signature mode, or a signcryption mode with a logical single cipher that consumes fewer resources by using shorter keys size. Signcryption is a cryptographic technique that combines both encryption and digital signature functionalities into a single operation. The main idea behind signcryption is to provide confidentiality, authenticity, and integrity in a more efficient way than performing encryption and digital signature operations separately.it has commonly three techniques like Hash and Encrypt, Encrypt and Sign and Hybrid. In our proposed scheme each biosensor node may now securely transmit patient data by calculating its whole private key using just its partial private key and a random integer. Biosensor nodes implanted on a patient's body in a hospital ward may use IEEE 802.15.6 standards to continuously monitor vital signs and securely transmit them to a base station. After receiving encoded patient data, the BS used 3G/4G Internet services to send the data to the centralized server in a general signcrypted format. The patient information stored on the central server is only accessible to licensed medical professionals and approved researchers. In order to treat their patients, medical professionals examine medical data. Moreover, in our proposed heterogeneous approach, biosensor nodes put on a patient's body may operate in the CLC domain, while a PKI-based environment is employed on the MS side to improve scalability. In order to preserve the balance between security and cost, our suggested architecture employs the notion of generalized signcryption. However, the sender selects only one mode at a

time such as encryption mode, signature mode, and signcryption mode according to their security requirements. The acquired findings demonstrate the effectiveness of our suggested system in comparison to existing state-of-the-art methods described in the literature in terms of processing cost, transmission overhead, and energy consumption. Scenario of our work is if we required data form multiple sensors along with multiple security standards or requirements then our system provides choice for data transmission with fulfillment of security requirement with better performance in terms of communication overhead, computational cost and energy consumption. We used a statistical method of comparison to provide outcomes that were more visually appealing and straight forward. Our contribution led to a 36% decrease in computational cost, a 16.36% decrease in transmission overhead, and a 17% decrease in energy consumption, ultimately leading to an increased overall performance of the system. Overall, our proposed architecture provides an effective and efficient solution for secure data transmission with multiple security requirements.

Keywords: Encryption, Digital Signature, WBAN, Inside keyword guess attack, Heterogeneous signcryption, healthcare

Contents

List of Figures

List of Tables

Abbreviations

$\mathbf{A}_{CK}$	Acknowledgment
BS	Base Station
BSN	Body Sensor Network
CLC	Certificate less cryptography
$\mathbf{C}_{ST}$	Certificate
$\mathbf{CU}_{A}$	Control Unit A
$\mathbf{CU}_{B}$	Control Unit B
$\mathbf{F}_{PK}$	Full Private Key
KGC	Key Generation Centre
$\mathbf{K}_{pu}$	Public Key
MS	Medical Server
$\mathbf{P}_{id}$	Patient Id
PKI	Public key infrastructure
$\mathbf{P}_{PK}$	Partial Private Key
TP	Type
WBSN	Wireless Body Sensor Network
WSN	Wireless Sensor Network

Chapter 1

Introduction

Healthcare networks are networks of devices, sensors, and other technologies used in the healthcare industry to monitor, diagnose, and treat patients. These networks allow healthcare professionals to collect, store, and analyze health-related data and communicate with other healthcare providers and patients.

1.1 Wireless Body Sensor Network

There are several types of healthcare networks, WBAN is a wireless network of sensors and devices worn by patients to collect and transmit data about their physiological and medical conditions. These networks are essential to enhancing the standard of care provided to patients and lowering healthcare costs without compromising quality.

1.1.1 Wireless Sensor Network

In order to keep tabs on the world around them, Wireless Sensor Networks (WSN) use a network of small, low-power devices called sensor nodes to conduct environmental monitoring and data collecting. Sensors, processors, and wireless communication capabilities allow these nodes to collaborate and send collected data to a control hub for further analysis. WSNs are used for a wide range of

purposes, from industrial process control and environmental monitoring to military surveillance. Together, a network of wireless sensor nodes can keep tabs on the state of the world around them [1-4]. These nodes, which can be small and battery-powered, are equipped with sensors and a wireless communication module, and are typically deployed in large numbers to cover a specific area or region [5]. The data collected by the nodes is then typically sent to a central location for processing and analysis. WSNs have a wide range of applications, including environmental monitoring, industrial control, and military surveillance [6].

1.1.2 WBSN Background

The term 'Wireless Body Sensor Network' (WBSN) refers to a network that wirelessly collects and processes data on physiological parameters such a person's heart rate, blood pressure, and body temperature [7]. It consists of a huge number of cheap, miniature sensor nodes that are wirelessly linked to one another. You may stick these sensor nodes anywhere on or in a person. The sensor nodes wirelessly exchange data with a central hub or gateway, which then transmits the information to a distant monitoring station. WBSN have a broad range of application, including healthcare, fitness, and sports performance monitoring. Also, it can be used for monitoring the elderly in their homes, in hospitals or other care settings, and for tracking the health status of individuals in remote or dangerous environments, such as firefighters or soldiers in the field. The technology for WBSN is advancing quickly, with researchers developing new types of sensors, new networking protocols, and new data analysis methods to improve the performance and reliability of these systems [8]. The goal is to create a system that is accurate, durable, and comfortable to wear, and that can provide actionable information to help improve the health and well-being of the people who use them.

Essentially, it's a group of gadgets that may be worn or implanted and communicate with one another and a main device through a wireless network [9]. Vital signs and other biometric information are only some of the examples of medical data that these networks are designed to gather, transmit, and evaluate. People with chronic diseases including heart disease, diabetes, and obesity may benefit from using

WBSNs at a hospital, at home, or at a community health center to better monitor and enhance their health and well-being. They can also be used for fitness tracking and remote patient monitoring. WBSN typically composed of several sensor nodes that are placed in different parts of the body, such as on the chest, wrists, ankles, and abdomen [10]. Data collected by the sensor nodes is sent wirelessly to a hub device, which may be a smartphone, tablet, or other device. The data is sent from the hub device to a distant server, where it may be evaluated by medical personnel or specialized software. There is a lot of effort being put into improving the WBSN technology, which is still in its early stages of development. The standardization of the communication protocols, security and privacy concerns are being addressed by researchers and industry. Additionally, WBSN can be used for non-healthcare related application such as industrial process monitoring, Environmental sensing, and tracking. As it is wireless, it enables to track people or assets in real-time, improve safety, and optimize operations. Moreover, WBSN can be integrated with other wireless systems such as wireless mesh networks and wireless sensor networks, enabling data to be transmitted over long distances and in challenging environments. However, developing and deploying WBSN can be quite challenging [11]. They require a deep understanding of human physiology, sensor technology, wireless communications, and data analysis. Furthermore, they need to comply with strict regulatory and privacy standards, which can vary widely depending on the application and the location. Security is also a big concern for WBSN, to prevent unauthorized access and tampering of the sensitive data.

1.1.3 Architecture of WBSN

The WBSN architecture is a network of wireless sensor nodes that are positioned on or inside the human body to monitor a variety of physiological data. These nodes may be put either externally or internally. The basic components of a WBSN architecture include:

1. **Sensors:** Heart rate monitors, temperature trackers, and blood pressure cuffs are all examples of such gadgets.

2. **Wireless transceivers:** These gadgets are the conduits through which sensor data is sent to the network. In order to communicate with one another, they may use Zigbee or Bluetooth, two of several possible wireless protocols.

3. **Network gateway:** This is the device that connects the WBSN to a wider network, such as the Internet. It may also perform data processing and storage functions.

4. **Data server:** This is a centralized server that stores and manages the data collected from the WBSN.

5. **Client applications:** These are the software programs that allow users to access and analyze the data collected by the WBSN. These applications can be accessed via mobile devices or web browsers Sensors are devices that gather data from the body, such as heart rate, temperature, and blood pressure. These devices are also known as biosensors.

6. It is the wireless transceivers that connect the sensors to the network. Users may then access this data if they so want. They could make use of any number of wireless communication protocols, like Zigbee or Bluetooth, for example.

7. **Network gateway:** This is the piece of hardware that establishes a connection between the WBSN and a more extensive network like the Internet. It is also possible for it to execute duties related to the processing and storage of data.

8. **Data server:** This refers to a centralized server that stores and maintains the data that has been acquired from the WBSN.

9. Client apps are the software packages that provide users the ability to access and examine the data that has been gathered by the WBSN. These programmers may be accessed by web browsers on desktop computers as well as mobile web browsers.

The diagram of WBSN architecture can be illustrated as:

Sensor node(s) <—> Gateway <—> Data Server <—> Client Application(s)

Note that there are many variations of WBSN architecture, depending on the specific application and system requirements. We use an architecture showing in figure 1.1 below:

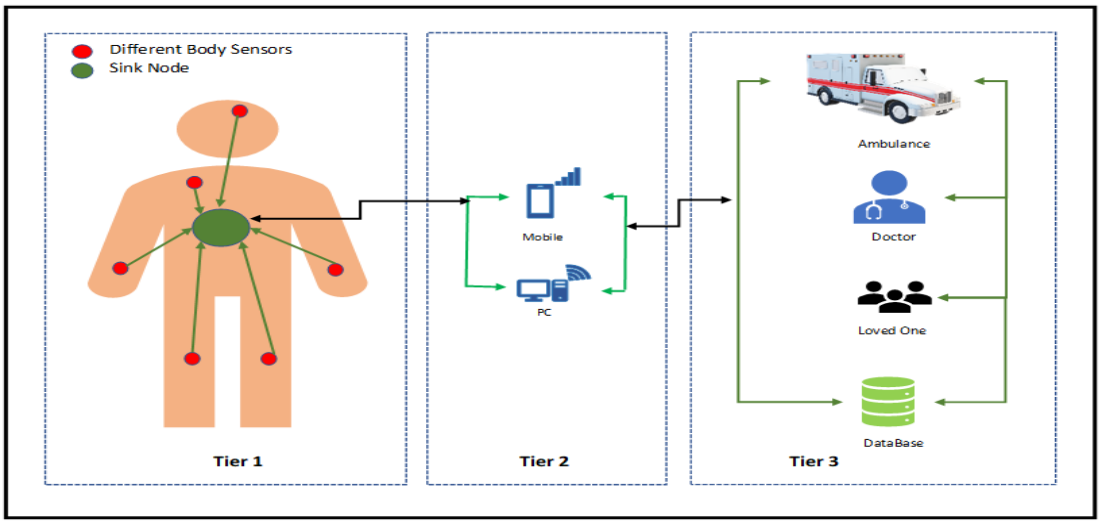


FIGURE 1.1: Architecture of WBSN

1.1.4 WBSN Applications

By allowing for continuous tracking of a patient's vitals and other health metrics, WBSNs may prove to be a game-changer in the healthcare sector [12]. WBANs have several potential uses in the healthcare sector, including:

1. **Telemedicine:** WBANs can be used to provide remote monitoring and telemedicine services, which can improve access to healthcare for patients in remote or underserved areas.

2. **Ambulatory monitoring:** WBANs can be used to monitor a patient's vital signs and other health-related data while they are moving around, which can be used to detect early warning signs of a health problem.

3. **Chronic disease management:** Patient monitoring using WBANs has the potential to enhance the diagnosis and management of chronic illnesses including diabetes, heart failure, and asthma.

It's important to note that while WBANs have many advantages in healthcare domain, security and privacy should be a top priority. Additionally, it's important to consider and comply with regulatory requirements and standards, such as HIPAA, to ensure that the use of WBANs is compliant with laws and regulations.

1.1.5 Sensors Used for Health Care Domain

Several different sensor technologies have use in healthcare monitoring and data collection. When it comes to healthcare [13], some of the most popular sensor types utilized in WBANs are:

1. **Temperature sensors:** These sensors can be used to measure body temperature, which can be used to detect fever and other signs of illness.
2. **Heart rate sensors:** These sensors can monitor your heart rate and its variability, which doctors may use to spot early warning symptoms of cardiovascular illness.
3. **Blood pressure sensors:** These sensors can be used to measure blood pressure, which can be used to detect hypertension and other cardiovascular conditions.
4. **Respiratory rate sensors:** These sensors can be used to measure breathing rate, which can be used to detect signs of respiratory disease and other respiratory conditions.
5. **Oxygen saturation sensors:** These sensors can be used to measure the oxygen saturation of the blood, which can be used to detect signs of hypoxia and other respiratory conditions.
6. **Glucose sensors:** These sensors can be used to measure glucose levels in the blood, which can be used to detect and manage diabetes.
7. **Gait analysis sensors:** These sensors can be used to analyze the way a person walks, which can be used to detect signs of mobility issues and other physical conditions.

8. **Accelerometer sensors:** These sensors can be used to measure acceleration and movement, which can be used to detect falls, physical activity level and sleep patterns.

It's important to note that the selection of sensors should be done considering the power consumption, cost, size, and also the accuracy of the sensor. Furthermore, the sensor data should be integrated with other sources of data to provide more accurate and meaningful insights. It's also important to note that the selection of sensors should be done considering the power consumption, cost, size, and also the accuracy of the sensor. Furthermore, the sensor data should be integrated with other sources of data to provide more accurate and meaningful insights.

1.1.6 Body Sensor Network Standards

Body Sensor Network (BSN) standards are guidelines and protocols that are used to ensure compatibility and interoperability between different BSN devices and systems. Some commonly used BSN standards include:

1. **Bluetooth Smart** (also known as Bluetooth Low Energy or BLE): This is a wireless communication protocol that is commonly used in BSN devices.
2. **Zigbee:** This is a wireless communication protocol that is also commonly used in BSN devices. It is designed for low power consumption and is suitable for small, low-cost devices.
3. **UWB:** In order to transmit data across relatively small distances, UWB (Ultra-Wideband) makes use of a broad frequency band. It uses the IEEE 802.15.4a standard and is developed for high-bandwidth, precise location-based services.

It is important to note that standards are constantly evolving, so it is important to stay up to date with the latest developments in this field.

1.1.6.1 Bluetooth

Bluetooth, short for 'Bluetooth wireless technology,' is a system for wirelessly connecting and exchanging data between electronic devices over relatively short distances. It is based on the IEEE 802.15.1 standard and is commonly used in a wide range of consumer and industrial applications, such as wireless headsets, smartphones, laptops, and home automation systems [14]. Bluetooth is designed to be low-power and low-cost, making it well-suited for small, portable devices. It also has a relatively low data rate, which makes it suitable for applications that require only small amounts of data to be transmitted. Bluetooth devices can be configured in different topologies, such as point-to-point, point-to-multipoint, or star. This allows devices to be organized in a variety of different ways, depending on the specific requirements of the application. It also includes a set of security features that help to protect against unauthorized access and data tampering. You can protect your inter-device communication with the help of technologies like encryption and authentication. It has several versions, such as Bluetooth Classic and Bluetooth Low Energy (BLE), also known as Bluetooth Smart. Bluetooth Classic is designed for applications that require a high data rate, such as streaming audio, while BLE is designed for applications that require low power consumption, such as fitness trackers and smart watches. When it comes to wireless communication, Bluetooth is often used since it is widely supported by most devices and platforms and has a high degree of compatibility.

1.1.6.2 Zigbee

Zigbee is a wireless communication protocol that is based on the IEEE 802.15.4 standard. It is designed for low-cost, low-power wireless networks and is often used in applications such as home automation, smart lighting, and wireless sensor networks. Zigbee networks can be composed of a variety of different devices, including routers, coordinators, and end devices [15]. Routers and coordinators are responsible for relaying data within the network, while end devices are typically sensors or other types of devices that collect and transmit data. One of the key features of Zigbee is its low power consumption, which makes it well-suited

for battery-powered devices. Zigbee devices can operate for several years on a single set of batteries. Zigbee also offers a high degree of flexibility in terms of network topology. Star, tree, and mesh topologies are all viable options for network configuration, with the choice ultimately coming down to the needs of the application. Zigbee is a popular standard for wireless sensor networks, including BSN. It is also used in other applications such as smart homes, lighting control and industrial automation. The Zigbee Alliance, an organization that promotes the use of Zigbee technology, provides a set of specifications and guidelines to ensure interoperability between Zigbee devices from different manufacturers.

1.1.6.3 UWB

UWB (Ultra-Wideband) is a wireless communication technology that uses a wide frequency band to transmit data over short distances. It is based on the IEEE 802.15.4a standard and is designed for high-precision location-based services and high-bandwidth applications. One of the key features of UWB is its ability to transmit large amounts of data over short distances with high precision [16]. This makes it well-suited for applications such as indoor positioning, asset tracking, and high-definition video streaming. UWB also offers a high degree of security, as the wide frequency band makes it difficult for an attacker to intercept and decode the signal. Additionally, UWB is capable of operating in the presence of other wireless technologies, such as Wi-Fi and Bluetooth, without causing significant interference. UWB devices can operate in different modes, such as time-of-flight (TOF) and angle-of-arrival (AOA) mode. These modes allow for precise location and direction determination, which is useful for asset tracking, and indoor positioning.

1.1.6.4 IEEE 802.15.6

IEEE 802.15.6 is a wireless communication standard that is being developed by the IEEE 802.15 Working Group for Wireless Body Area Networks (WBANs). This standard defines the physical layer (PHY) and the medium access control (MAC) layer for wireless communication between devices that are worn or implanted on

or in the human body [17]. The IEEE 802.15.6 standard is designed to provide low-power, low-cost, and low-data-rate communication for medical and healthcare applications, such as wireless monitoring of vital signs, and drug delivery systems, among others. The standard also addresses the specific requirements of WBANs, such as the need for low-power consumption, high reliability, and robustness against interference and multi-path fading. This standard includes several PHY and MAC options to support different applications and environments. The PHY options include: UWB-IR (Ultra-Wideband-Impulse Radio) and Low-rate 2.4 GHz. The standard also includes security and privacy features such as secure key management, data confidentiality, and integrity, to protect the sensitive information transmitted by the devices. The IEEE 802.15.6 standard is still under development and not yet fully approved, and the devices that conform to this standard are not yet commercially available.

1.1.6.4.1 Applications of IEEE 802.15.6

IEEE 802.15.6 is a wireless communication standard that is being developed specifically for wireless body area networks (WBANs) and it has the potential to be used in a wide range of medical and healthcare applications. Some examples of potential applications include:

1. **Wireless monitoring of vital signs:** IEEE 802.15.6-compliant devices can be used to monitor a patient's vital signs such as heart rate, blood pressure, and body temperature wirelessly and in real-time.
2. **Drug delivery systems:** IEEE 802.15.6-compliant devices can be used to control and monitor the delivery of drugs to patients through wireless communication.
3. **Rehabilitation and physiotherapy:** IEEE 802.15.6-compliant devices can be used to monitor a patient's progress during rehabilitation and physiotherapy, and to provide feedback to the therapist in real-time.
4. **Implantable medical devices:** IEEE 802.15.6-compliant devices can be used to communicate with implantable medical devices such as pacemakers

and cochlear implants, allowing for remote monitoring and control of the device.

It is important to note that the standard is still under development and the actual applications that will be implemented are yet to be seen [18]. However, the potential of this standard in the medical and healthcare industry is promising and it will likely to be adopted in various other applications as well. It is specially designed for Sensor Networks.

1.2 Wireless Body Sensor Network Security

In WBSN, a heterogenous domain refers to a network that includes different types of devices with varying capabilities and requirements. This can include wearable devices, sensors, and medical devices that use different communication protocols, have different battery life requirements, and operate at different frequencies. The heterogeneous nature of the network presents challenges in terms of network management, security, and data integration, but also offers a greater range of possible applications and services.

1.2.1 Certificate-Less Cryptography

Certificate Less Cryptography (CLC) is a technique used in WBANs to optimize the overall performance of the network. CLC is a type of public-key cryptography that eliminates the need for trusted third-party certificate authorities (CA) to issue and manage digital certificates.

The CLC protocol requires that users broadcast both their public key and an associated identification hash. The privacy and safety of the user is increased since they no longer need to depend on a third party to verify their identification [24].

The design of a CLC model in a WBAN typically involves several key components:

1. **Cross-layer design:** The CLC model integrates information from different layers of the network protocol stack, such as the physical, MAC, and network layers.

2. **Channel state information:** The CLC model uses channel state information (CSI) from the physical layer to optimize the operation of other layers.

3. **Energy efficiency:** The CLC model aims to improve the energy efficiency of the WBAN by reducing the power consumption of the nodes and prolonging the battery life.

4. **Quality of Service (QoS):** The CLC model takes into account the QoS requirements of different applications and services running on the WBAN. For example, it can prioritize the transmission of real-time data over non-real-time data.

It is important to note that there is no unique design of CLC model, and different designs may have different trade-offs depending on the specific requirements of the WBAN.

1.2.1.1 CLC Key Steps

The working mechanism of CLC on base stations in a WBAN typically involves several key steps:

1. **Channel state information (CSI) collection:** The base station collects CSI from the wireless body area nodes (WBANs) through a feedback mechanism. This information can include the channel gain, noise power, and interference level.

2. **Resource allocation:** The base station uses the CSI to allocate resources, such as transmission power and bandwidth, to the WBANs. This can be done through techniques such as power control, rate adaptation, and scheduling.

3. **Quality of Service (QoS) management:** The base station uses the CSI and resource allocation information to manage the QoS of the WBANs. This can include prioritizing the transmission of real-time data over non-real-time data, and allocating more resources to nodes that have high QoS requirements.

4. **Security management:** The base station uses the CSI and resource allocation information to secure the network. This can include encrypting the data and authenticating the nodes.

5. **Network control and coordination:** The base station uses the CSI and resource allocation information to control and coordinate the network. This can include forming clusters of nodes, managing handovers, and adjusting the transmission power of the nodes to avoid interference.

6. **Adaptive mechanism:** The base station uses the CSI and resource allocation information to adapt the network to changing network conditions. This can include adjusting the transmission power, rate, and scheduling based on the channel conditions. It is important to note that the specific working mechanism of CLC on base stations may vary depending on the specific design of the network and the requirements of the application.

CLC is a way of organizing these sensor nodes into clusters, with one node acting as a cluster head. The cluster head is responsible for coordinating the activities of the other nodes in the cluster and for relaying data to the base station.

1.2.1.2 Benefits to Using CLC in a WBSN

Increased energy efficiency: By grouping the sensor nodes into clusters and having one node act as a cluster head, CLC reduces the number of nodes that need to communicate directly with the base station. This reduces the overall energy consumption of the network, as fewer nodes need to be active at any given time.

1. **Improved scalability:** CLC allows for the easy addition or removal of sensor nodes to the network, as the clusters can be dynamically reconfigured to accommodate changes in the number or location of nodes.

2. **Increased reliability:** CLC allows for the detection and isolation of failed or malfunctioning nodes, so that they can be replaced or repaired without affecting the overall operation of the network.

3. **Improving security:** CLC can improve the security by authenticating the cluster head as a legitimate sender of data.

It is important to note that, Clustering can be a challenging task in WBSN due to the mobility of the nodes and the dynamic nature of the wireless communication environment. The creation of CLC should also account for the unique qualities of the sensor nodes and the physiological data they gather, so that the clusters are ideally designed for the desired use case.

1.2.2 Public Key Infrastructure

Public Key Infrastructure (PKI) which is a set of technologies and policies that are used to secure communications and transactions over a network. In a WBSN, PKI can be used to secure the communication between the sensor nodes and the hub or base station, as well as the transmission of data to remote servers [25]. PKI works by using a pair of keys, a public key and a private key, to encrypt and decrypt data. The public key is used to encrypt data, and the private key is used to decrypt it. A sender encrypts data using the public key of the intended recipient, and the recipient then decrypts it using their private key. This ensures that the data can only be read by the intended recipient.

1.2.2.1 Application of PKI

1. Authenticate sensor nodes and hub or base station

2. Secure communication between the nodes and the hub

3. Ensure the privacy and integrity of the data that is transmitted

4. PKI can be implemented in WBSN in multiple ways, some examples include:

5. **Using a pre-shared key:** Here the key is preloaded into the nodes and hub before deployment.

6. **Using digital certificates:** Each node and hub will have a unique certificate that can be used for authentication and encryption.

7. **Using a Public Key Encryption (PKE) based scheme:** Here instead of a pre-shared key or certificate, a public-private key pair is generated by each node and hub during the initialization.

It's important to note that PKI has a lot of overheads, especially in terms of computation and communication requirements. That makes it hard to implement on low-power, low-memory and low-bandwidth devices such as WBSN nodes [26]. However, with the recent advancement in cryptography and optimization techniques, it's becoming more practical to implement PKI on such devices.

As WBSN is still an emerging field, the standardization of the PKI protocols, security and privacy concerns are being addressed by researchers and industry.

1.2.3 Identity-Based Cryptography

Identity-Based Cryptography (IBC) is a form of public-key cryptography where the public key of a user is derived from their unique identity, such as an email address, instead of being randomly generated. In IBC, a trusted third party known as a Private Key Generator (PKG) generates a private key for each user and manages the mapping between their identity and public key [27]. This simplifies key management, as users don't have to manage their own keys, but it also means that the security of the system is dependent on the security of the PKG.

1.2.3.1 Pros and Cons of IBC

1. **Simplified Key Management:** As the public key of a user is derived from their identity, users do not have to manage their own keys, making key management easier.

2. **Ease of Use:** IBC eliminates the need for users to generate their own public-private key pairs, making it easier for users to adopt and use cryptography.

3. **Scalability:** IBC can be used to manage the keys of a large number of users, making it a scalable solution for organizations with many users.

1.2.3.2 Cons of IBC:

1. **Security Dependent on PKG**: Attacks against the Private Key Generator (PKG) may compromise the whole system.

2. **Privacy Concerns**: Since a user's identity is utilized as their public key, it is potentially less private than other kinds of public-key encryption.

3. **Complexity:** Implementing and managing IBC can be complex, as it requires a trusted third party (PKG) to manage the mapping between identities and public keys.

4. **Vulnerability to Compromised PKG:** If the PKG is compromised, the security of all users in the system may be at risk.

1.2.4 WBAN Security Need or Requirements

Wireless Body Area Networks (WBANs) are vulnerable to security threats, just like any other wireless network.

Therefore, it is important to consider security when designing and implementing WBANs. Some of the key security needs and requirements for WBANs include:

1. **Confidentiality:** WBANs transmit sensitive medical information, such as vital signs and medical history, which needs to be protected from unauthorized access.

2. **Authentication:** WBANs need to be able to verify the identity of devices and users to prevent unauthorized access to the network and data.

3. **Integrity:** To prevent data from becoming inaccurate or unreliable during transmission, WBANs must prevent any kind of data modification.

4. **Access control:** WBANs need to be able to control access to the network and data, to prevent unauthorized access and data leakage.

5. **Non-repudiation:** WBANs need to be able to provide evidence of the origin and authenticity of data, to prevent denial of data transmission or receipt.

6. **Data protection:** WBANs need to protect data from being lost or stolen, and ensure data recovery in case of device failure or loss.

7. **Secure updates**: WBANs need to be able to securely update devices and software, to ensure that the network and devices are kept up to date and secure.

8. **Secure communication:** WBANs need to be able to securely communicate between devices, to protect data during transmission.

9. **Compliance:** WBANs need to comply with relevant regulations and standards, such as HIPAA for healthcare.

It's important to note that security threats to WBANs are constantly evolving, and it is important to keep the security measures up to date and to conduct regular security assessments to identify and mitigate potential vulnerabilities.

1.2.5 Symmetric Cryptography and Asymmetric Cryptography

Symmetric cryptography and asymmetric cryptography are two main branches of cryptography, which are used to secure communications and protect data from unauthorized access.

1. **Symmetric cryptography**, also known as secret key cryptography, uses a single shared secret key to encrypt and decrypt data. The sender and

the receiver use the same key to encrypt and decrypt the data, so the key must be kept secret and shared securely between the sender and the receiver [19]. Examples of symmetric encryption algorithms include the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES).

2. **Asymmetric cryptography**, also known as public key cryptography, uses a pair of keys: a public key and a private key. The public key is used to encrypt data and the private key is used to decrypt data. Anyone can use the public key to encrypt data, but only the holder of the private key can decrypt it. This is made possible by the mathematical properties of the encryption algorithm. Examples of asymmetric encryption algorithms include RSA, ECC and El Gamal. One of the major advantages of asymmetric cryptography over symmetric cryptography is that it enables secure communications without the need to share a secret key. The public key can be freely distributed and used to encrypt data, while the private key is kept secret by the holder [20]. As a result, symmetric cryptography is often used to encrypt large amounts of data, while asymmetric cryptography is used to encrypt the symmetric key and the small amount of data [21]. Both symmetric and asymmetric cryptography play important roles in securing communications and protecting data, and are often used in combination to provide a higher level of security.

1.2.5.1 Pros of Symmetric Cryptography

1. Faster and more efficient than asymmetric cryptography
2. Simplicity in its design and implementation

1.2.5.2 Cons of Symmetric Cryptography

Key distribution is a major problem, as both sender and receiver must have a copy of the same key

1. Key management is difficult in large systems

1.2.5.3 Pros of Asymmetric Cryptography

1. Key distribution is more straightforward, as the public key can be freely shared
2. Greater security, as the private key must be kept secret
3. More secure key management

1.2.5.4 Cons of Asymmetric Cryptography

1. Slower and less efficient than symmetric cryptography
2. More complex design and implementation

In summary, symmetric cryptography is typically used for bulk encryption and decryption of data, while asymmetric cryptography is used primarily for key exchange and authentication [22]. Both have their own advantages and disadvantages and are used together in many systems, such as Transport Layer Security (TLS) and Secure Shell (SSH).

1.2.6 Asymmetric Using Generalized Signcryption

Asymmetric cryptography can also be used in a technique called 'generalized signcryption.' This method allows for a message to be encrypted with a public key and then decrypted with a different private key. This can be useful in situations where multiple parties need to be able to decrypt a message, but not all parties should have access to the same private key. For example, let's say Alice wants to send a message to Bob and Carol, but she doesn't want either of them to be able to read the message without the other's permission. Alice could encrypt the message with Bob's public key, then encrypt the result with Carol's public key. Bob and Carol would then use their own private keys to decrypt the message, but neither would be able to read the message without the other's help [23]. Generalized signcryption is an extension of the classic public-key encryption and can be useful

in situations where multiple parties need to be able to decrypt a message, but not all parties should have access to the same private key. However, it is a relatively advanced technique and is not widely used in practice.

1.3 Research Gap

The increasing demand for secure communication in various domains has led to the development of various signcryption schemes. However, the heterogeneous nature of these schemes makes it difficult for users to choose the appropriate one that meets their specific requirements. This has resulted in a choice issue, where users struggle to determine the best scheme for their needs based on factors such as security strength, computational efficiency, and compatibility with existing infrastructure.

1.4 Problem Statement

The objective of this problem statement is to develop a unique heterogenous generalized signcryption solution that can address the choice issue by allowing users to dynamically select the appropriate signcryption scheme based on their specific requirements, without compromising security or performance. The solution should provide a unified framework for the evaluation and comparison of computational cost, communication overhead and energy consumption as well, making it easier for users to make informed decisions.

1.5 Research Questions

To solve the problem, as indicated in the problem statement, we need to address at least following questions:

1. How to design efficient and secure heterogeneous (CLC/PKI) generalized signcryption to reduce the cost while maintaining the desired security?

2. What is impact of proposed generalized signcryption scheme in terms of computational cost, communication overhead and energy consumption.

1.6 Purpose

The purpose of this research question is to guide the development of a solution that addresses the challenge faced by users in selecting the appropriate signcryption scheme for their secure communication needs. The research question focuses on the development of a heterogenous generalized signcryption solution that considers multiple factors such as security strength, computational efficiency, compatibility with existing infrastructure, computational cost, communication overhead, and energy consumption. The ultimate goal of this research is to provide a unified framework for the evaluation and comparison of different signcryption schemes, making it easier for users to make informed decisions and find the best solution for their specific requirements without compromising security or performance.

1.7 Scope

In the Healthcare Wireless Body Area Network (WBAN) domain, there is scope for using cost-effective and efficient communication schemes to support the transmission of medical data and patient information. The following are some of the ways in which these schemes can be used Low-power wireless communication can help reduce the cost and power consumption of WBAN devices, making them more affordable and practical for widespread use in healthcare [28]. Data compression algorithms can be used to reduce the size of medical data being transmitted, making it more efficient to transmit and store. This can help reduce the cost of data storage and transmission, as well as improve the performance of WBAN devices [29]. Overall, the use of cost-effective and efficient communication schemes in the Healthcare WBAN domain can help improve the quality and reliability of medical data transmission, while reducing the cost and complexity of WBAN devices. This

can help drive the widespread adoption of WBANs in healthcare and support the development of new and innovative healthcare solutions.

1.8 Significance

The use of less cost and efficient communication schemes in the Healthcare Wireless Body Area Network (WBAN) domain is significant for several reasons:

1. **Improved Accessibility:** By reducing the cost and complexity of WBAN devices, less cost and efficient communication schemes can help improve accessibility to medical data and patient information, particularly in resource-limited settings.

2. **Enhanced Patient Safety:** By improving the reliability and accuracy of medical data transmitted over WBANs, less cost and efficient communication schemes can help enhance patient safety by reducing the risk of errors and inaccuracies in medical data.

3. **Improved Patient Comfort:** By reducing the power consumption and size of WBAN devices, less cost and efficient communication schemes can help improve patient comfort by reducing the weight and size of wearable medical devices.

4. **Increased Adoption:** By making WBAN devices more affordable and practical, less cost and efficient communication schemes can help drive the widespread adoption of WBANs in healthcare, improving access to medical data and information for patients and healthcare providers.

5. **Better Health Outcomes:** By enabling real-time monitoring and analysis of medical data, WBANs can support better health outcomes by providing early detection of potential health issues and enabling more accurate and timely diagnoses.

Overall, the use of less cost and efficient communication schemes in the Healthcare WBAN domain is significant because it can help improve the quality and reliability

of medical data transmission, reduce the cost and complexity of WBAN devices, and drive the widespread adoption of WBANs in healthcare, supporting the development of new and innovative healthcare solutions.

1.9 Contribution

Our major contribution is to provide a desirable, efficient and secure way of heterogenous generalized signcryption that can adaptively work as an encryption mode, a signature mode, or a signcryption mode with a logical single cipher that consumes fewer resources by using shorter keys size. Scenario of our work is if we require data form multiple sensors along with multiple security standards or requirements then our system provides choice for data transmission with fulfillment of security requirement with better performance in terms of communication overhead, computational cost and energy consumption. We used a statistical method of comparison to provide outcomes that were more visually appealing and straight forward. Our contribution led to a 36% decrease in computational cost, a 16.36% decrease in transmission overhead, and a 17% decrease in energy consumption, ultimately leading to an increased overall performance of the system. Overall, our proposed architecture provides an effective and efficient solution for secure data transmission with multiple security requirements.

Chapter 2

Literature Review

To gain a thorough understanding of the current state of the field, a review of the literature on generalized signcryption in Wireless Body Sensor Networks (WBSNs) is necessary. Signcryption is a cryptographic technique that provides both confidentiality and authentication by merging digital signatures and encryption. In the context of WBSNs, secure communication between sensor nodes is crucial to safeguard sensitive data.

[30-35] Studies have shown that traditional signcryption schemes are not suitable for WBSNs due to their high computational and communication overhead. To address this issue, researchers have proposed several generalized signcryption schemes specifically designed for WBSNs. These methods are developed to keep data safe and private while cutting down on unnecessary processing and transmission. One such example is the WBSN-oriented generalized signcryption (WOGS) scheme, which is based on elliptic curve cryptography and provides a compact signcryption solution for WBSNs. Another example is the lightweight generalized signcryption (LGS) scheme, which uses a hash-based approach to minimize the overhead in both computation and communication. Additionally, researchers have proposed various optimizations and enhancements to existing signcryption schemes to improve their efficiency and security in WBSNs. This includes the use of smart cards and hardware accelerators to reduce computation overhead and the integration of key agreement protocols to enhance security.

2.1 Overview of Literature

Overall, the literature suggests that generalized signcryption schemes are a promising solution for secure communication in WBSNs. However, there is still room for improvement, and further research is needed to address the challenges and limitations of these schemes in real-world WBSN deployments. In 2009, Saleem et al. [32] described the fundamental security needs of WBANs in addition to the challenges associated with Denial of Service (DDoS). Additionally, the authors highlight the current multi-layered risks that are posed to WBANs and give an in-depth discussion of the principles of security. The authors conclude by rating the state of security in WBAN. In their 2011 publication, Zhang et al. [33] attempted to investigate potential resource-constrained WBANs risks and offer a study of communication protocols, cryptographic algorithms, and key management procedures that are important to WBANs security. Furthermore, the authors examine issues with existing solutions and potential avenues for the development of future research in the area of WBANs security. In 2013, Aqeel et al. [34] published their research in an attempt to provide a critical examination of various authentication processes for WBANs. The IEEE 802.15.6 standard serves as the foundation for all of the research and conversation. The writers Javadi et al. [35] analyze the significant threats to security and privacy that are posed by WBANs. In addition, they talk about a problem with the Quality of Service (QoS) in WBANs that hasn't been handled yet and might lead to major security risks. In the last section, the authors provide potential research areas that may be pursued in the future.

2.2 Wireless Body Sensor Network

Saha et al. [36] provided a synopsis of the present state of WBAN security in their article published in 2014. In addition to this, the writers bring out a number of very serious safety issues. Pathania et al. [37] provide an overview of WBANs as well as associated problems, with a particular emphasis on the difficulty of the security issue. In addition to a vulnerability assessment, the authors examine security

threats and WBAN-specific security needs. Kang et al. [38] conducted research on the safety precautions taken by application and communication protocols in the year 2015. The writers also analyze the design, as well as potential flaws, prospective threats, and potential improvements in the future. In their paper [39], Mainanwal et al. evaluated the benefits and drawbacks of various security and privacy procedures that are applied in WBANs. We also discuss the risks and constraints that WBANs face. Possible future paths of research are then explored. Usha and Priya cover attack types, defense tactics, and simulation tools for WBANs [40].

2.3 Wireless Local Area Network

In order to strengthen the safety of wireless local area networks (WLANs), Masdari et al. [41] carried out an exhaustive research project on the many authentication techniques that were presented in the 2016 academic literature. The writers also investigate both the positive and negative aspects of each authentication system and compare the characteristics and functionalities of each option. In conclusion, the authors provide some suggestions for potential next steps. An in-depth investigation of WBANs and WSNs is presented by Naik et al. [42]. In addition to this, the writers examine both the positive and negative aspects of various WBAN security solutions. In 2017, Al-Janabi et al. [43] conducted an analysis of the communication architecture of WBANs utilizing latest research and suggestions. In addition, they investigated the potential hazards, problems relating to privacy and security, and other concerns that are connected to the use of networks of this sort. In addition to that, the most recent security precautions and research findings pertaining to WBANs are included in the paper. In the last step of this process, we evaluate possible subjects for further investigation and innovation. Sawaneh et al. [44] did a survey research study on the topic of developing and implementing WBANs in healthcare systems. [44] The need of protecting users' privacy and data when using WBAN is also briefly discussed. Zou et al. [45] analyze the feasibility of various different secure communication mechanisms that might be used

inside WBANs as well as between WBANs and external organisations. In their study, the fundamental security requirements that must be satisfied in order to ensure safe transmission at both levels are highlighted. The principal emphasis of Aman and Shah's [46] extensive evaluation of relevant research is on the issues that are presented by routing and security in mobile, ubiquitous, and WBANs.

2.4 Security Assaults

In 2018, Narwal and Mohapatra [47] carried out an exhaustive investigation on a wide variety of authentication procedures. The authors give not only a thorough description of each scheme but also an in-depth examination of each scheme with regard to security assaults, security measures, and other elements that are relevant. The information included in Usman et al [48].'s introduction to WBAN security is summarized. The authors recommend developing a taxonomy as a means to simplify the process of classifying items used inside healthcare systems. Each layer of the WBAN architecture has been examined to look for any security flaws.

The writers did a fantastic job of locating engaging themes and plausible study approaches, Malik et al. [49] offer an overview of the most significant security needs and possible dangers in WBANs at different levels. The authors base their analysis on the OSI model, which serves as a framework. The paper begins with an introduction of WBANs as a tool for healthcare monitoring, and then continues on to a discussion of cryptographic techniques that may be utilized to address issues about security and privacy. Both the writers Kompara et al. [50] lay a significant emphasis on the importance of necessary agreement in addition to the safety of intra-BAN communication. It offers a comprehensive analysis of the many different key agreement processes that are now in use, labelling them as 'traditional,' 'secret key,' and 'hybrid key,' accordingly. In addition to this, we provide a description of the characteristics of each category and an analysis of how well WBANs can withstand potential dangers.

2.5 Security Services

In 2019, Morales et al. [51] presented a detailed review of security services and several ideas for enhancing the WBAN architecture. The study's ultimate objective is to provide a thorough picture of the security of the WBANs system. Zhang et al. [52] provide an overview of WBANs, their uses, and security issues. The most current research and publications shed light on the multiplicity of security flaws that plague WBANs and the many approaches used to remedy them. Luo et al. [53] perform a comprehensive literature study on the privacy and security risks of electronic healthcare record systems used by WBANs. As Li et al. [54] have pointed out, there are issues with the design of authentication mechanisms for WBANs. The authors also give the scientific community with potential future directions. To address security and privacy concerns with WBANs, Chaudharyet al. [55] studies these challenges, suggests solutions, and discusses the authentication technique employed. In addition to a variety of authentication kinds and methodologies, Hussain et al. [56] present a summary of the features of WBANs.In addition, it examines and contrasts a variety of authentication techniques, expanding on their relative advantages and disadvantages, grading their overall performance, and evaluating their resilience to certain security breaches. In their conclusion, the authors offer probable future measures. The article by Asam et al. [57] provides a comprehensive overview of the problems associated with WBANs from the points of view of communication and security. Unfortunately, the authors only present a superficial evaluation, neglecting important issues about security in the process. Sen et al. [58] investigate the fundamental safety needs of WBANs as well as their concerns with DoS.

In 2020, Roy et al. [59] conducted a comprehensive analysis of the security and privacy concerns connected with WSNs and WBAN. The authors evaluate and contrast the two systems by analyzing their fundamental characteristics, design, and performance measures, as well as their actual applications. Researchers are presented with open research challenges as a last phase. Sharma et al. [60] analyze and evaluate the routing, security, energy, and cost-cutting aspects in WBAN in their study and assessment.

2.6 Analysis of WBANs Evolutions

Hajar et al. [61] present a thorough analysis of the technology behind WBANs in 2021, concentrating on security and privacy issues, possible remedies, future research topics, and unanswered concerns. In contrast, the authors were only concerned with non-authentication approaches. WBANs face a variety of security procedures and routing issues, which Vignesh et al. [62] explain in depth. Moreover, they discuss potential network-based assaults and analyze some of the protections in place to thwart them. Numerous potential vectors for assault are also dissected by the writers. The study continues by outlining the key difficulties users have while establishing a connection in WBANs, a brand-new scientific field developed in response to the epidemic. An extensive literature evaluation of the various WBAN security approaches is conducted by Jabeen et al. [63]. With memory constraints in mind, the authors choose study areas in which to evaluate the effectiveness of various assaults. The schemes are checked for quality and applicability to the research topic. What's more, the projects we're talking about span the years 2016-2020, albeit we're going to be focusing on the more recent ones first. Several methods are explored in the research literature to determine how the privacy of patients' healthcare information transfers might be enhanced. The data encryption methods Message Authentication Code (MAC), Secure Hash Algorithm 1 (SHA-1), and hybrid encryption are ranked according to their respective strengths and weaknesses. In conclusion, the authors evaluate safety under various assault conditions. The several methods of authentication and security are discussed by Narwal et al. [64]. This study used a more comprehensive approach to security and authentication in WBANs than previous research had taken. In addition to a full discussion of the security procedures in WBANs, this article provides an in-depth study of the most crucial security elements, including the dangers involved, the sorts of attackers that may target these networks, and the existing remedies. In addition, the authors examine WBAN applications, outstanding research concerns, ideas for more research, and potential future developments. In a broader perspective, the study examines the use, technology, and components of WBANs as well as their security and authentication.

2.7 Signcryption Schemes Survey

WBANs have been thoroughly investigated for a considerable amount of time. This has led to the publication of several papers that offer a high-level overview of the field and analyze the current literature on various issues within it. The aforementioned surveys mostly examine authentication, architecture, security, and impediments. This paper covers various aspects related to sign encryption schemes, including security requirements, applications, and classification based on cryptography and algorithm [65]. Additionally, it offers brief overviews of recently introduced schemes, a list of their security characteristics, and techniques for assessing both their performance and security. Some of them are: The goal of this research is to categorize, examine, and rate WBAN signcryption techniques.

2.7.1 Attribute-Based Signcryption Scheme

It is only feasible to divulge the information linked with a particular public key if a small number of persons know the master key. Obtaining a certificate of public-key authenticity is unnecessary. By presenting and implementing key policy attribute-based encryption, Barbosa et al. [66] introduced a breakthrough concept (KP-ABE). This research's encrypted material is associated with a set of attributes. However, the encrypted data can only be decrypted by users whose credentials match those in the key's access tree. Because the private keys necessary to decrypt the data are created by the access tree, which is also used to build the user access strategy, this is the case. The four components of the proposed method are the encipherment, key generation, decryption, and initialization cyphers. This research provides a dynamic access policy that avoids the challenges caused by a single authority by using many authorities. Boneh et al. [67] identified unauthorized access and manipulation with a patient's vital signs as two significant security issues of wireless body area networks (WBAN). This study leverages blockchain technology to prevent unauthorized modifications to patients' personal information, and the sequential aggregate signature scheme with a designated verifier (DVSSA) approach may prevent unauthorized persons from having access to patients' vital

signs. Even the tiny storage problem of blockchain was resolved by data compression. If necessary, the permissions of the users might be revoked. By employing ABE bilinear pairings, Boneh et al. [68] introduced a unique method for encrypting data. To prevent unauthorized access to critical patient data, this study identifies a set of user characteristics in advance. Tan et al. [69] relied on a KP-ABE-based secure data transfer technique while relaying sensitive data from biosensor nodes to a sink node. Hohenberger and Waters [70] proposed online/offline ABE as a solution to the problem of high computational costs (encryption and key generation) in ABE. The first part of the suggested strategy is implemented online, while the second phase is implemented in the real world. In the offline phase, the costliest procedures are calculated, while the other activities are computed online. It works nicely in BSNs environments. Liu et al. [71] have developed a unique authentication methodology with their suggestion of a certificate-less signing method. With this strategy, both the sender and the recipient remain anonymous throughout communication. Tan et al. [72] proposed identity-based encryption (IBE) to protect the confidentiality of patients' medical information during transmission utilizing BSNs. The sensor nodes in experiment encrypt the data using the identity characteristics that the revoked users do not possess. With this additional degree of security in place, only users who have not been blacklisted may decode the data. All attributes required to produce a secret key are managed by a centralized authority (CA), in case a patient needs to be transported from one hospital to another for specialist testing, such as the usage of an electronic medical record (EMR) in the diagnostic process. As a consequence, the physician at the other hospital will only be privy to incomplete information regarding the patient's confidential medical history. Patients' medical data may be securely exchanged over a public network, due to the many blockchain-based security and privacy protections stated by Jin et al. [73]. Moreover, the merits and limitations of each blockchain-based solution are highlighted. A novel mechanism for limiting who may access what information was proposed by Li et al [74]. On this project, we employ ABE to encrypt personal information about persons before storing it in the cloud.

Advancements in technology, including the rise of cloud computing and the Internet of Things, have greatly improved medical treatment. Nevertheless, concerns

regarding data security and privacy persist, hindering progress in smart health. Zhang et al. [75] proposed security and privacy measures for patient data in the 4 International Journal of Distributed Sensor Networks utilizing the CP-ABE approach. The Privacy-Aware Smart Health (PASH) standard model, according to the study's authors, is more secure and produces better results than other methods now in use.

2.7.2 Identity-Based Signcryption Scheme

The rapid advancement of Attribute-Based Encryption (ABE) has led to the expansion of Identity-Based Signature (IBS) notation and the introduction of the concept of Attribute-Based Signature (ABS), both of which are consequences of the swift progress of ABE. In the ABS concept, a private key holder uses a signing predicate to generate a signature for data, which can only be verified by a third-party verifier. The verifier can confirm that the signing predicate has been satisfied, but cannot access any information about the signer's attributes. By utilizing a unique signing predicate with their private key, the signer creates a signature.

2.7.3 CLC-Based Signcryption Schemes

Yang et al. [76] have proposed using CLC to enhance the security of WBANs. In terms of lowering processing expenses and transmission overhead, as well as boosting general network security, there is still potential for improvement.

This research not only lowers costs but also satisfies a fundamental cryptographic security criterion. It may still show improvement in BSNs settings. Access trees are defined using AND, OR logic gates with additional parameters in the attribute-based signcryption (ABSC) scheme introduced by Ma et al. [77]. The encoded message is of a fixed length. The system provides a cost savings compared to previously proposed methods in the literature. based on consortium blockchain. It seeks to address a key problem with the present emergency system: obtaining the patient's permission to access their private

medical records in the event of an emergency. In addition, it lays out the smart contract-based criteria for regulating medical emergencies and determining how long sensitive patient data should be kept secure from intrusion. Given the novelty of ABSC research, we suggest a new ABSC method using blockchain technology and fixed-size encoded text to reduce overhead and increase privacy and security. In addition, we boost the BSNs' overall effectiveness to increase the average patient lifespan. The literature presents a number of methods for securing the BSNs environment based on IBE, CLC, ABE, ABS, and ABSC. Despite their widespread use, all of these methods suffer from serious security flaws and inefficiency in both processing time and data transfer.

2.7.4 PKI-Based Signcryption Schemes

In the limited resources of BSNs, our suggested approach excels. According to the public key cryptosystem, PKI signcryption, iD-based signcryption, and certificate-less signcryption are the three distinct variants of signcryption. PKI signcryption is the most common kind. PKI is often used to safeguard a huge network, such as the Internet. The literature provides a plethora of reliable PKI-based signcryption techniques. [78] Registration authority, certificate authority, verification authority, and a certificate revocation list are all part of the PKI basic system. PKI is primarily used to verify the integrity of public keys between sending and receiving nodes. Certificate distribution and revocation are resource-intensive operations, making the PKI method inappropriate for resource-constrained environments like BSNs. Various iD-based sign-encryption algorithms were presented as a solution to the PKI certificate management issue. [76-78] The users of these systems submit requests to a private key generator, who then generates the necessary keys (PKG). When a request is sent to the PKG, it includes the sender's ID, phone number, and email address. The PKG generates private keys for secure communication by using the master secret key and other system characteristics it has stored. All private keys are generated by PKG, therefore an assault on it would compromise the security of the whole system. ID-based signcryption solves the issue of public key authenticity without certificates, but it still has the key escrow problem. Using

certificate-less sign encryption, scientists have finally solved the key escrow and certificate management issues.

EMRs may also be transferred on the blockchain, although in an encoded form. To prevent unlawful actions and boost network performance, participants in this research only shared their data's decryption keys with authorized medical personnel. The suggested approach was shown to scale well using simulation findings. Previous research has suggested a few other certificateless signcryption based systems. The user's entire private key in these schemes is created in two stages, the first by an external entity known as a key generating center (KGC), and the second by the user. Certificate-less sign-encryption is, thus, the best option in the resource-Iqbal et al. [79] restricted setting of BSNs. In this research, Amin et al. [80] presented the idea of online/offline signcryption, which merges the use of encryption and signatures to protect the privacy and authenticity of sensitive information. Therefore, for the resource-constrained context of BSNs, mobile phones, smart cards, and radio-frequency identification, online/offline signcryption is a very optimal option (RFID). In order to reduce the burden on devices with limited resources, difficult and time-consuming computations might be performed in the offline phase by more robust machines. This allows signcryption to do its data processing in the shortest possible time by making use of pre-computation. When it comes to online/offline signcryption, most of the published approaches focus on Public Key Infrastructure (PKI) implementations. [58–60]. Thwin et al. [81] came up with the idea of combining the blockchain with the proxy re-encryption method in order to securely transmit personal health information (vital signs). This was done in order to address issues with network performance, privacy and security, sensor storage restriction, revocation of permission, and scalability (vital signs). It continues to be impenetrable despite the onslaught of enemy attack.

2.8 Comparative Analysis of Literature Review

Signcryption is a cryptographic primitive that combines the functionalities of digital signatures and encryption in a single step. It is designed to provide both

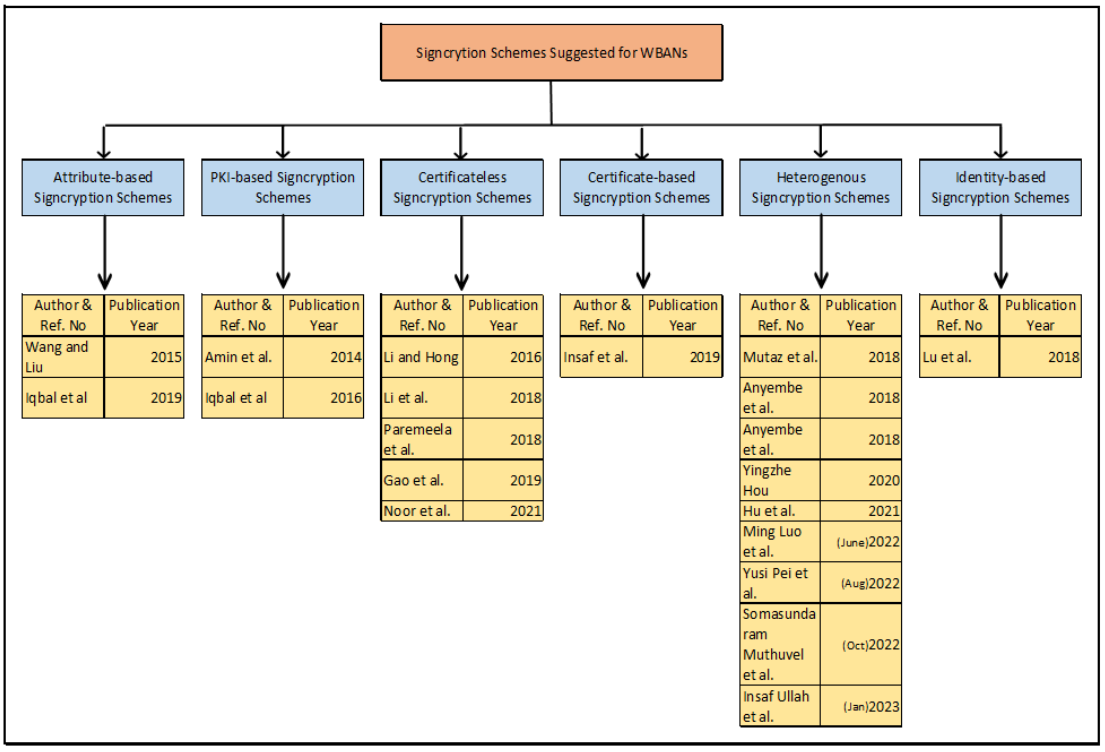


FIGURE 2.1: Comparative Analysis

confidentiality and authenticity for messages in a more efficient and streamlined way than using separate digital signature and encryption mechanisms. Some signcryption mechanism are discussed in figure 2.1 above.

There are several signcryption schemes that have been proposed in the literature. Here are some details about a few of them:

RSA-based Signcryption: This scheme is based on the RSA public-key encryption algorithm. It combines RSA signature and encryption operations in a single step. The sender generates a signature on the plaintext message using their private key and then encrypts the message and the signature using the recipient's public key. The recipient can verify the signature using the sender's public key and then decrypt the message using their own private key.

Elliptic Curve Cryptography (ECC)-based Signcryption: This scheme is based on the use of elliptic curve cryptography. It uses a hybrid encryption approach where the message is first encrypted with a symmetric key algorithm and then the key is encrypted using the recipient's public key. The sender generates a signature on the ciphertext and the encrypted symmetric key using

their private key. The recipient can verify the signature using the sender's public key and then decrypt the symmetric key and use it to decrypt the message. Here are brief descriptions of some common types of cryptographic schemes as discussed in figure 2.1 above.

Attribute-Based Encryption (ABE): A type of encryption that allows access control policies to be defined based on attributes of users, such as age or job title, rather than just their identity. ABE is useful in situations where access control needs to be more granular than just user identities.

Public Key Infrastructure (PKI) based Signcryption: A cryptographic technique that combines digital signature and encryption functionalities into a single operation. PKI based Signcryption uses a trusted third party, known as a Certificate Authority (CA), to issue digital certificates that verify the identity of users and their public keys.

Certificateless Signcryption: A type of encryption that uses a hybrid approach of PKI and Identity-Based Encryption (IBE) techniques. In certificateless Signcryption, a user's public key is generated based on a combination of their identity and a random number, eliminating the need for digital certificates. This scheme is a variation of identity-based signcryption that does not require a trusted authority to generate private keys. Instead, it uses a public key infrastructure (PKI) based on the recipient's email address or other identifier. The sender generates a signature on the plaintext message and encrypts both the message and the signature using the recipient's identifier. The recipient can then decrypt the message and verify the signature using a public key obtained from the PKI.

Certificate-based Signcryption: A type of encryption that relies on digital certificates issued by a trusted third party. Certificate-based Signcryption uses a user's public key, which is included in their digital certificate, to encrypt data.

Heterogeneous Signcryption: A type of encryption that supports multiple cryptographic algorithms and key lengths in a single operation. Heterogeneous Signcryption is useful in situations where different levels of security are needed for different types of data.

Identity-based Signcryption: A type of encryption that uses a user's identity, such as their email address, as their public key. Identity-based Signcryption eliminates the need for public key distribution, simplifying the key management process. This scheme is based on identity-based encryption (IBE). It allows a sender to encrypt a message for a recipient using their email address or other identifier as the public key. The sender generates a signature on the plaintext message and encrypts both the message and the signature using the recipient's identifier. The recipient can then decrypt the message and verify the signature using their private key, which is generated by a trusted authority.

Chapter 3

Proposed Network Model

For the proposed network's workflow, we took into account not only the sensors themselves, but also the base station, the medical server (MS), and the stakeholders. The following sections elaborate on the function of the various players involved.

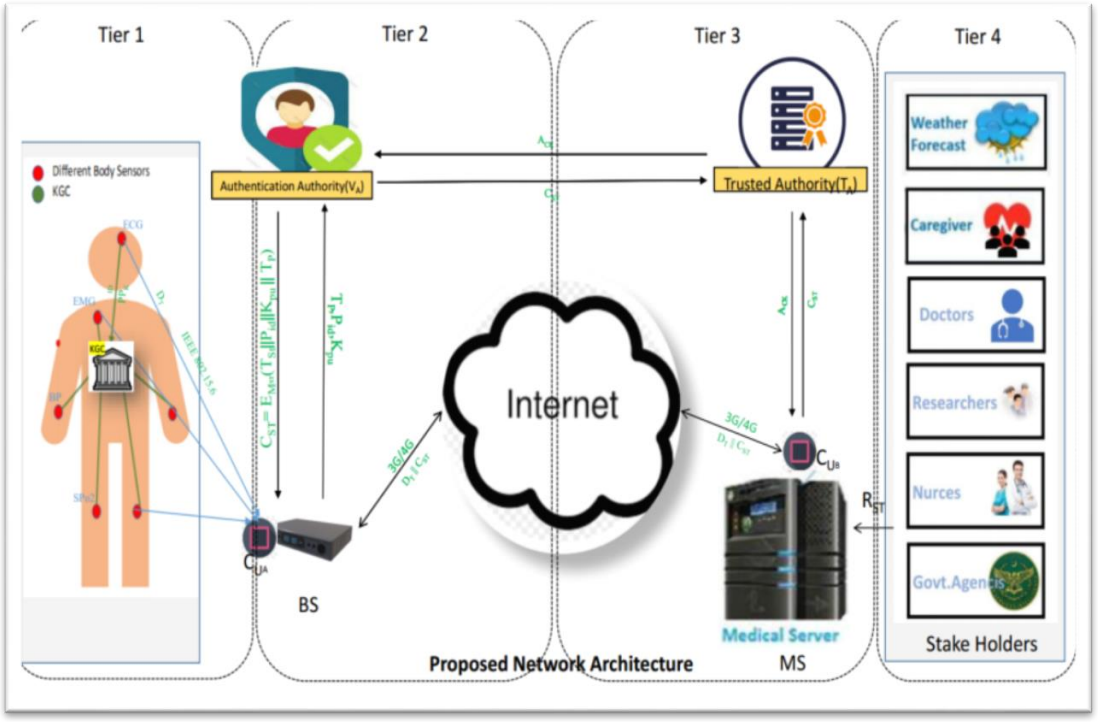


FIGURE 3.1: Proposed Network Architecture

This methodology has three modes of data transmission and four tiers. Three modes of data transmission detailed diagram show in figure 3.1.

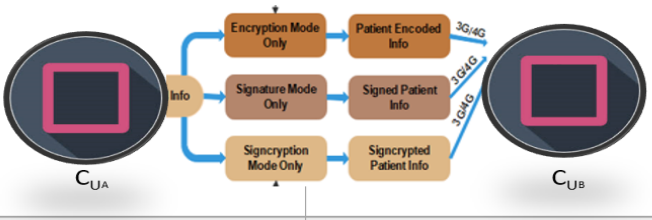
TYPE		
Type 1:	C= $\mathcal{E}_{Pu\ CU_B}$ (M)	T=$D_{Pr\ CUB}$ ($\mathcal{E}_{Pu\ CUB}$ (M))
Type 2:	S= $\mathcal{E}_{FPK_{Sid}}$ (M)	T=$D_{Pu\ CUA}$ ($\mathcal{E}_{FPK_{Sid}}$(M))
Type 3:	Sign= $\mathcal{E}_{Pu\ CU_B}$($\mathcal{E}_{FPK_{Sid}}$(M))	T= $D_{Pu\ CUA}$ ($D_{Pr\ CUB}$ ($\mathcal{E}_{Pu\ CU_B}$($\mathcal{E}_{FPK_{Sid}}$(M))))

FIGURE 3.2: Modes of Data Transmission

It has three types of modes

1. Encryption mode only
2. Digital Signature mode only
3. Signcryption mode only

All formulae will be discussed in detail in corresponding Tiers and generically shown in figure 3.2.

3.1 Tier 1

This tier has three major components

1. Sensor
2. Key generation center (KGC)
3. Control Unit A (CU_A) / Base Station

First of all, when sensor sense data from environment then if data meet any of its threshold either minimum or maximum. Then sensor send its ID to KGC for Generation of Partial Private key (P_{Pk}), KGC receives ID and generate a P_{Pk} pass

it to sensor, sensor generate a random no itself multiply random no with partial private key generated from KGC to generate its Full Private Key (FPK) as shown in figure 3.3 below.

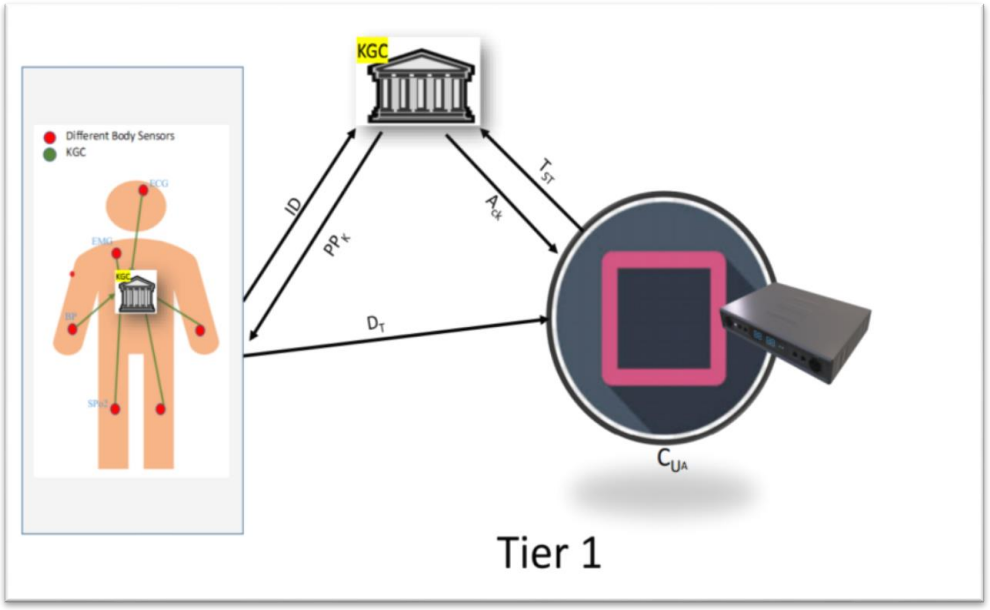


FIGURE 3.3: Tier 1 of Proposed Architecture

On the basis of sensor type, selected at the time of implantation or initialization one of scheme is selected from our three proposed schemes either encryption, digital signature or signcryption as mentioned below.

3.1.1 Encryption Mode (Type 1)

If sensor required encryption mode only then apply formula below before transmitting its data.

$$\mathbf{C} = \varepsilon_{\mathbf{PuCU_B}}(\mathbf{M})$$

3.1.2 Digital Signature Mode (Type 2)

If sensor required digital signature mode only then apply formula below before transmitting its data.

$$\mathbf{S} = \varepsilon_{\mathbf{FPK_{Sid}}}(\mathbf{M})$$

3.1.3 Signcryption Mode (Type 3)

If sensor required signcryption mode only then apply formula below before transmitting its data.

$$\mathbf{Sign} = \varepsilon_{\mathbf{PuCU_B}}(\varepsilon_{\mathbf{FPK_{Sid}}}(\mathbf{M}))$$

After successful data compilation data will send to CU_A / BS in the cover of D_T for further processing CU_A / BS receives data from sensor and sent sensor id with timestamp to KGC for verification. On receiving acknowledgment from KGC, CU_A / BS proceed data further in Tier 2.

3.2 Tier 2

This Tier has three major responsibilities.

1. Authentication Authority
2. Trusted Authority
3. Internet connection

In Tier 2 CU_A / BS send Sensor Type T_P Patient id P_{id} and Public Key K_{pu} of sensor to an Authentication Authority (V_A). V_A compile a certificate C_{St} and send to Trusted Authority (T_A) for record.

T_A send acknowledgment to V_A. V_A send a certificate C_{St} encrypted with master secret key M_{ST} having Time Stamp (T_{St}), T_P, P_{id}, K_{pu}. Then CU_A / BS transmit D_T and C_{St} over the network using 3G/4G internet connection as shown in figure 3.4 below.

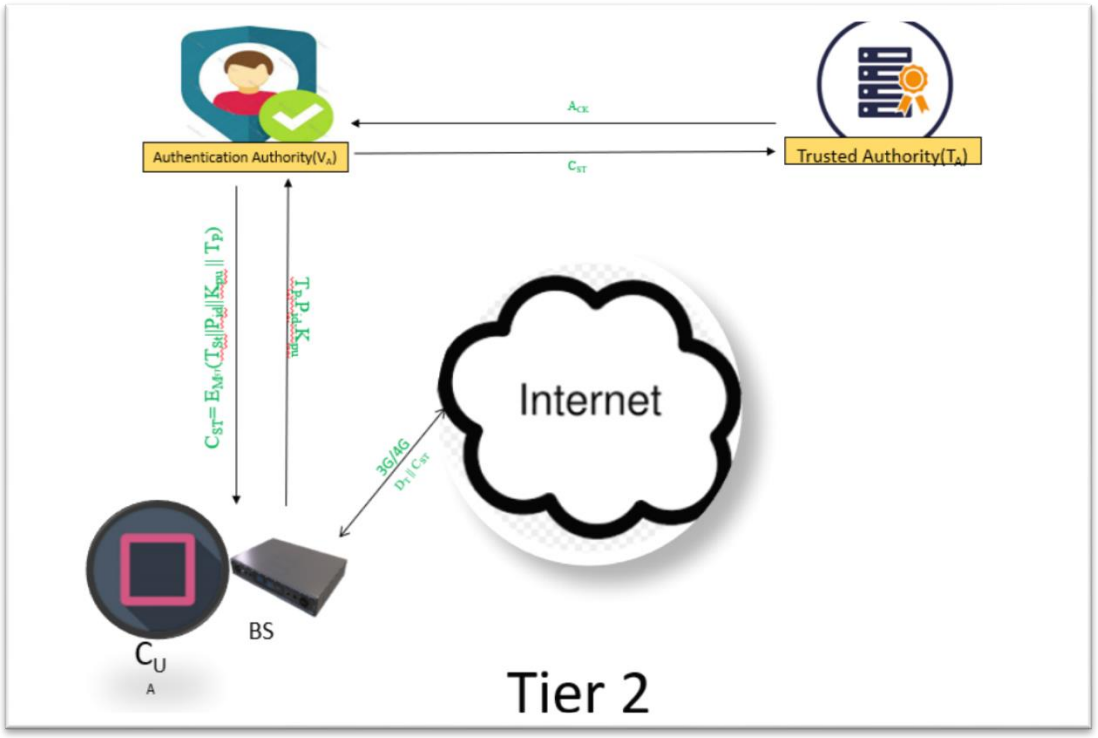


FIGURE 3.4: Tier 2 of Proposed Architecture

3.3 Tier 3

This Tier has one component and two major responsibilities.

Component

1. Medical Server (MS)

Responsibilities

1. Receive Data from Internet Through 3G/4G Internet connection.
2. Verify its certificate from T_A.

First of all, MS receives Data from internet having D_T and C_{ST} from internet through 3G/4G internet connection. Send C_{ST} to T_A for verification of C_{ST} and sensor type. When acknowledgment receives medical server decrypt data according to sensor type and store it flow is describe in figure 3.5 below.

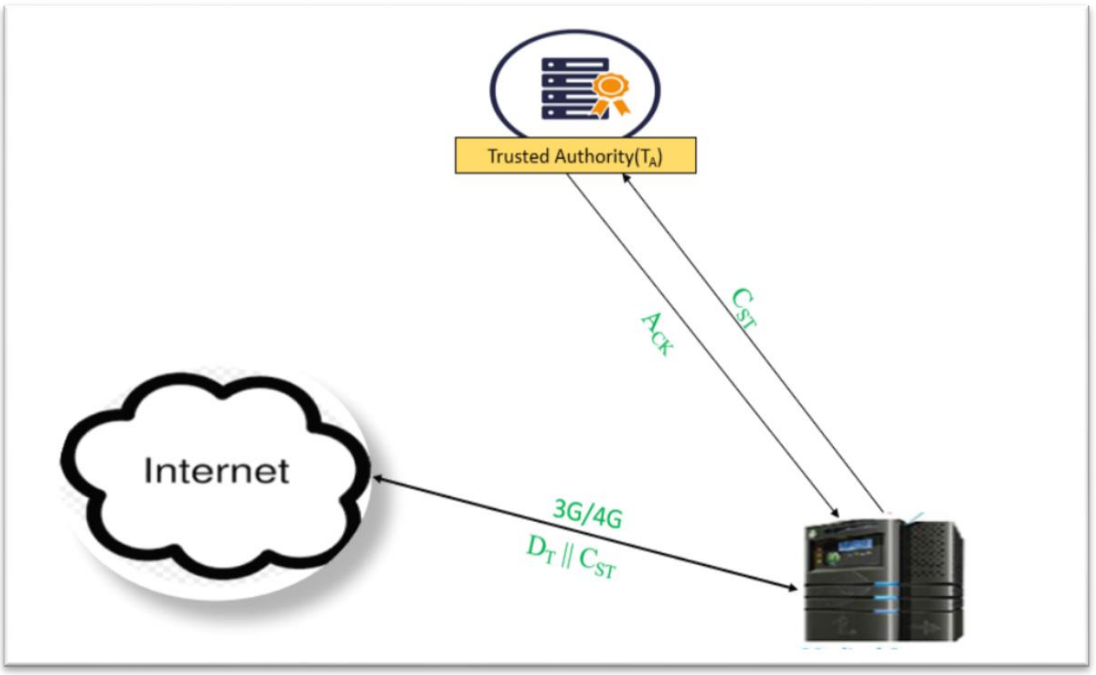


FIGURE 3.5: Tier 3 of Proposed Architecture

As we described in tier 1 data is compiled according to sensor type same scenario over here data is extracted according to sensor type and stored MS.

3.3.1 Encryption Mode (Type 1)

If sensor required encryption mode only then apply formula below for extracting its data.

$$\mathbf{T} = \mathbf{D}_{\mathbf{Pr\,CUB}}(\varepsilon_{\mathbf{PuCUB}}(\mathbf{M}))$$

3.3.2 Digital Signature Mode (Type 2)

If sensor required digital signature mode only then apply formula for extracting its data.

$$\mathbf{T} = \mathbf{D}_{\mathbf{Pr\,CUA}}(\varepsilon_{\mathbf{FPK_{Sid}}}(\mathbf{M}))$$

3.3.3 Signcryption Mode (Type 3)

If sensor required signcryption mode only then apply formula below before transmitting its data.

$$\mathbf{T} = \mathbf{D}_{\mathbf{PuCUA}}(\mathbf{D}_{\mathbf{PrCUB}}(\varepsilon_{\mathbf{PuCU_8}}(\varepsilon_{\mathbf{FPK_{Sid}}}(\mathbf{M}))))$$

3.4 Tier 4

This Tier has three components and one major responsibility.

Component

1. Certificate Authority
2. Verification Authority
3. Registration Authority

Responsibilities

1. Request to registration authority for verification
2. Stakeholder verification of certificates from Verification authority

First of all, MS send Key and data to Registration Authority (R_A), R_A send confirmation to certificate Authority (C_A) for certification then C_A sent a certificate to Verification Authority (V_A) for record and later confirmation. And at same time C_A reply to MS with key and generated certificate. Then MS send Data, key and certificate to Stake holders. Stake holders sent key and certificate to V_A for confirmation. V_A reply acknowledgment if confirms else denied. In case of confirmation successful communication starts between MS and stake holders.

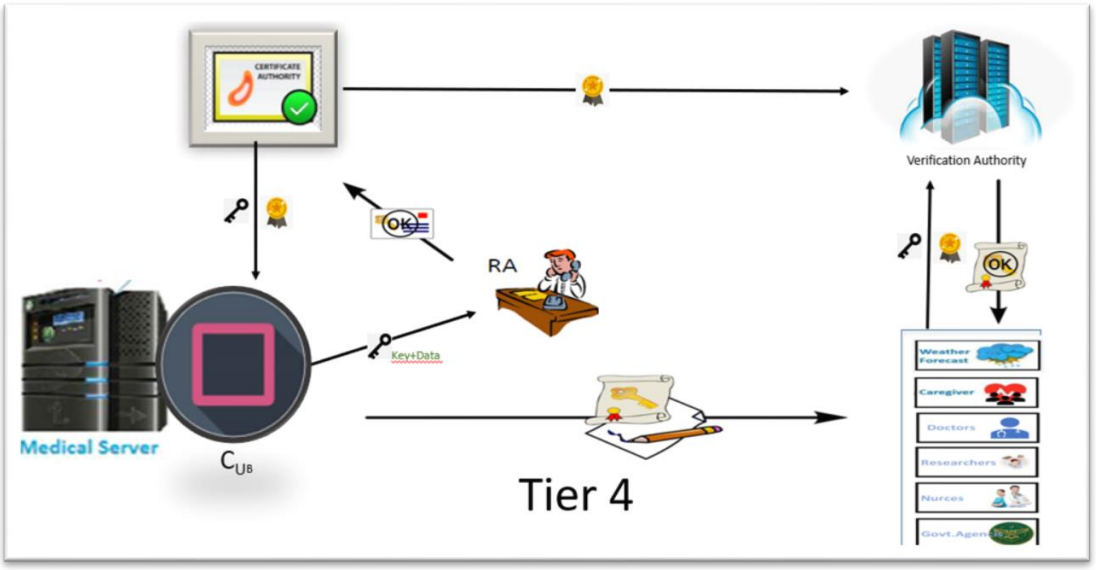


FIGURE 3.6: Tier 4 of Proposed Architecture

3.5 Proposed Scheme

The proposed scheme in the field of Wireless Body Area Networks (WBANs) is a cutting-edge solution. This scheme leverages the latest advancements in wireless technology to create a seamless and unobtrusive network of wearable sensors that can monitor and transmit vital health data in real-time.

Setup Phase:

The security parameter 's' is chosen by the Key Generation Centre (KGC) who selects a cyclic addition group |G1| and a cyclic multiplication group |G2| with the same prime order 'q1'. The generator 'P1' is selected for group 'G1' and a bilinear pairing 'bp' is confirmed. The master secret M_{ST} key is computed using 'α' and the public key P_U is obtained as '$P_U = \alpha P1$'. Three hash functions 'H1', 'H2', and 'H3' are also confirmed. The system parameters 'PParams' for the Certificateless Cryptography (CLC) system are determined. Similarly, the Certificate Authority (CA) determines the system parameters 'PParams' 'for the Public Key Infrastructure (PKI) system, where 'G1' is a subgroup of 'G1' 'and 'P2' is the generator for 'G1''.

Partial Key Extraction Phase:

In the Certificateless Public Key Encryption (CL-PKE) process, the KGC inputs the sender's identity 'IDi' and a random number 'R_{ND}', computes 'Di = R_{ND} * P1', 'ti = H1(IDi)', and outputs the partial private key $P_{PK} = \alpha + R_{ND} + T_{st}$ and the partial public key 'ti + Di'.

Secret Value Generation Phase:

The secret value 'di' is randomly selected by the sender in the Certificateless Secret Value Generation (CL-SVG) process, and the full private key is interpreted as 'SKi = (ui, di)'.

Full Private Key Generation Phase:

In the Certificateless Public Key Generation (CL-PKG) process, the sender computes the remaining part of the public key 'P_{PKi} = dP1' and the full public key is set as FPKi = (Ti, P_{PKi}).

Public Key Generation Phase:

1. **Receiver Side:**

In the PKI Key Generation (PKI-KG) process, the receiver selects a random private key 'dj' and sets the public key as 'Pj = dP2'.

1. **Sender Side:**

The sender's private key 'SKs', and the receiver's public key (P_U). The sender computes a random number R_{ND}, computes 'h = H2(w)', 'R = h (R_{ND} * P_U, 'h = H3(ID, SKs, R)', and outputs the ciphertext 'σ = (R, y)' where 'y = h + s (w - u) (mod q)'.

PKI-Trapdoor Generation Phase:

The Public Key Infrastructure Trapdoor Generation (PKI-TG) involves the receiver computing the trapdoor 'T_D' using the keyword 'w', system parameters 'PParams1', and private key 'P_K'.

The steps are:

1. Compute h = H2(w)
2. Compute T_D = h-1dPwr.

Finally, the test involves the cloud server verifying the equation

e (PPKs, Pw, Pr) = e (T, R, h)

The cloud server uses the trapdoor to test the validity of the equation

e (PPKs, T) = e (P_U, R) * e (P, Tw)

If the verification is successful, the corresponding data is returned, otherwise, nothing is returned. Finally, the correctness of the scheme is verified.

3.6 Public Key Cryptography

There are two main types of public key cryptography, which are:

RSA (Rivest–Shamir–Adleman): RSA is a widely used public key cryptography algorithm named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on the difficulty of factoring large integers and involves generating a pair of keys, one public and one private, to encrypt and decrypt messages. RSA is used in many applications, including secure web browsing, email encryption, and digital signatures.

Elliptic Curve Cryptography (ECC): ECC is another type of public key cryptography that uses the properties of elliptic curves over finite fields to generate and manipulate keys. ECC provides the same level of security as RSA, but with

smaller key sizes, making it more efficient for mobile devices and other applications where resources are limited. ECC is used in many applications, including secure messaging, mobile payments, and internet of things (IoT) devices.

Other less common types of public key cryptography include:

DSA (Digital Signature Algorithm): DSA is a digital signature algorithm that was proposed by the US National Institute of Standards and Technology (NIST) in 1991. It is used to sign and verify digital documents and messages and is based on the difficulty of solving the discrete logarithm problem.

Diffie-Hellman Key Exchange: Diffie-Hellman is a key exchange algorithm that allows two parties to securely exchange cryptographic keys over an insecure channel. It is based on the difficulty of computing discrete logarithms in a finite field.

Overall, public key cryptography provides a secure and efficient way of encrypting, decrypting, signing, and verifying digital information. The choice of algorithm depends on the specific application requirements, such as security level, key size, and computational efficiency. In our proposed it is open ended choice for user to adopt any one as per their requirements. Open ended means user can adopt any one who's with already familiar or using in any other similar environment.

3.7 Proposed Algorithm

An algorithm is a step-by-step process for solving a problem or achieving a specific task. When describing a proposed algorithm, it is important to provide clear and concise steps for how the algorithm will operate. Some key points to consider in describing a proposed algorithm include:

1. **Input:** What data or information is needed for the algorithm to run?
2. **Output:** What is the expected result of running the algorithm?
3. **Data structures:** What data structures will the algorithm use to store and manipulate information?

4. **Key operations:** What are the key operations or steps that the algorithm will perform in order to achieve its goal?

5. **Special cases:** What special cases or edge cases should the algorithm handle, and how will it handle them?

Our proposed algorithm is given below.

3.8 Security Analysis

Wireless nature of WBANs also poses significant security challenges, as the sensitive health information transmitted through these networks is vulnerable to interception and tampering.

3.8.1 Game 1

Initialization phase: CU_A and CU_B performing the Setup algorithm and generating the secret key $\{P_{Pk}, R_{ND}\}$. It outputs the cryptographic parameters CGP_1, CGP_2.

Phase 1: CU_A maintains five lists (Li) to keep track of Hi queries and two lists (PLK and CLK) to keep track of private key queries from PKI and CLC, respectively.

H1 queries: Given P_{Pk} as input, B checks if the tuple (P_{Pk}) is in L1. If it is, B returns to E1. If not, B selects Z* and adds the tuple (P_{Pk}) to L1, then returns E1. The same process applies to the other H queries (H2, H3, H4, H5).

CLC queries: Given ID_i as input, B searches CLK for the tuple (IDi, P_{Ku}, PP_K, S_{ID}, T_{ST}). If found, B returns the public key (PP_K, T_P). If not, B generates x, computes F_{PK} and P_{PK}, adds the tuple (IDi, P_{Ku}, PP_K, S_{ID}, T_{ST}). to CLK and returns the public key F_{PK} and P_{PK}.

PKI queries: CU_B searches PLK for the tuple ($D_T||C_{ST}$) and returns the private key (P_{ID}, P_{KU}).

Algorithm 1: Key Agreement and communication

Pre load (M_{SK}, P_{id}, S_{ids}, K_{pu} and T_p) on BS and Biosensors
Sent ID to KGC and Get PP_K from KGC
Generate a Random No R_{ND}
Calculate Full Private Key FP_K= R_{ND}*PP_K
Computes D_T
If (Sensor_type = type1)
Then
D_T= $?_{Pu\ CUB}$ (V_t)
Else If (Sensor_type = type2)
Then
D_T= $?_{FPK}$ (V_t)
Else If (Sensor_type = type3)
Then
D_T=$?_{Pu\ CUB}$ ($?_{FPK}$ (V_t))
Else
Discarded
Send D_T to BS/ C_{UA}
Base Station
If S_{id} =pre stored id So Grant Permission
Else
Black listed
If Authentication Granted
Send (T_P, P_{ID}, K_{PU}) to V_A
Authentication Authority (V_A)
If P_{id} =pre stored patient Ids so grant Authentication
Send Certificate C_{ST}=$?_{Mst}$ (T_{st} || T_P || P_{ID} || K_{PU}) to BS and T_A As well for Record
Base Station
Send D_T, C_{ST} to MS/C_{UB}
Medical Server
Sent C_{ST} to T_A for Verification
If (Ack=1)
Then
D $_{MST}$ C_{ST}
If (T_P = type1)
Then
T= $D_{Pr\ CUB}$(D_T)
Else If (T_P = type2)
Then
D_T= $D_{Pu\ Sid}$ (D_T)
Else If (T_P = type3)
Then
D_T= $D_{Pu\ Sid}$ ($D_{Pr\ CUB}$ (D_T)
Else
Discarded
End

V_A queries: B updates the tuple (IDi, P_{Ku}, PP_K, S_{ID}, T_{ST}) in CLK with ($D_T||C_{ST}$).

Stakeholder's queries: CU_B generates an identity IDq and given IDi as input, if IDi = IDq, B sets x=PP_K. If IDi $\neq$ IDq, B checks LK for (IDi, T_{ST}, PP_K). If not found, B generates x and calculates pk, then adds the tuple (IDi, T_{ST}, PP_K) to LK and returns the public key.

T_A queries: B searches LK for (IDi, T_{ST}, PP_K) and returns the private key xi. Finally, for SC queries, given the sender and receiver IDs, and a plaintext m, B performs a secure computation as specified in the protocol.

Game describes a protocol for secure communication between two entities, CUA and CUB, and their interactions with other entities, including PKI, CLC, and various stakeholders. The protocol has several phases, including an initialization phase where CUA and CUB generate a secret key and output cryptographic parameters, and several query phases where different entities make requests for information. During the query phases, CUA maintains several lists to keep track of queries, and responds to queries based on the input provided. For example, CUB may search a list for a specific tuple or generate a new tuple and add it to the list. Different types of queries are handled differently depending on the entity making the query and the information requested. Game also describes several specific actions taken during the protocol, such as generating an identity, performing a secure computation, and updating tuples in lists. Overall, the text provides a detailed description of the protocol and its various components. The text describes a cryptographic protocol that involves two entities, CUA and CUB, as well as other entities such as PKI, CLC, and various stakeholders. The protocol consists of several phases, including an initialization phase and several query phases.

During the initialization phase, CUA and CUB perform the Setup algorithm and generate a secret key {PPk, RND}. The cryptographic parameters CGP1, CGP2 are outputted as a result of this phase. During the query phases, CUA maintains five lists (Li) to keep track of Hi queries and two lists (PLK and CLK) to keep track of private key queries from PKI and CLC, respectively. The text describes how queries are handled based on the input provided.

For example, during H1 queries, CUB checks if the tuple (PPk) is in L1. If it is, CUB returns to E1. If not, CUB selects Z* and adds the tuple (PPk) to L1, then returns E1. The same process applies to the other H queries (H2, H3, H4, H5). During CLC queries, CUB searches CLK for the tuple (IDi, PKu, PPK, SID, TST). If found, CUB returns the public key (PPK, TP). If not, CUB generates x, computes FPK and PPK, adds the tuple (IDi, PKu, PPK, SID, TST) to CLK and returns the public key FPK and PPK. During PKI queries, CUB searches PLK for the tuple (DT||CST) and returns the private key (PID, PKU). For Stakeholder's queries, CUB generates an identity IDq and given IDi as input, if IDi = IDq, CUB sets x=PPK. If IDi $\neq$ IDq, CUB checks LK for (IDi, TST, PPK). If not found, CUB generates x and calculates pk, then adds the tuple (IDi, TST, PPK) to LK and returns the public key.

For TA queries, CUB searches LK for (IDi, TST, PPK) and returns the private key xi. Finally, for SC queries, given the sender and receiver IDs, and a plaintext m, CUB performs a secure computation as specified in the protocol.

Overall, the text provides a detailed description of the various actions taken during the protocol and how different entities interact with one another. It highlights the importance of secure communication and cryptography in ensuring the privacy and integrity of information.

3.8.2 Game 2

Initialization: B runs the Setup procedure and transmits CUA the cryptographic parameters CGP1 and CGP2.**Probing:** They're the same as in the first game.**Forgery:** A sends identities (IDi, TST, PPK) and ? * to CUB. If the following conditions are hold, A wins.**The game**:

1. The USC query of (P_{KU} CU_A, P_{PK} sid) σ * * * $P_{UK,}$ Idi, s, r does not return.
2. No attempt is made to run the CL-SKG query on IDs *.
3. The SC query of σ * is not performed.

4. Sender uses CLC to encrypt plaintext m and sends it to a PKI recipient in this fashion:

5. Choose (ID_i, P_{Ku}, PP_K, S_{ID}, T_{ST})

6. Compute ID_i, T_{ST}, PP_K P_{sk}

7. Output = C_{ST}.

The Perspective of the User. In PKI, the receiver decrypts the ciphertext given the cypher state text (CST). In case the ciphertext is correct, this procedure will return m in plaintext. If the input is invalid, the algorithm will produce a failure sign $\perp$.

1. Compute M_{ST}.

2. Compute (ID_i, P_{Ku}, PP_K, S_{ID}, T_{ST})

3. Verify that Sid has the authentication value. In such case, the plaintext value of m would be shown. If it doesn't work, the error symbol is shown.

4. Trapdoor. In PKI, receiver chooses but does not have full private key and not computable due having multiplication of random no with it.

5. Computes the trapdoor current timestamp. Otherwise, the failure symbol $\perp$ is output.

Game 2 describes a protocol involving several phases and parties, such as CUA, CUB, PKI, and CLC. In the Initialization phase, B runs the Setup procedure and transmits the cryptographic parameters to CUA. Then, the Probing phase is performed, which is the same as the first game. Next, the Forgery game is played, where A sends identities and a signature to CUB, and if certain conditions are met, A wins the game.

The game includes several queries such as USC, CL-SKG, and SC, and A needs to meet specific criteria to win the game. Additionally, the text describes the perspective of the user in PKI, where the receiver decrypts the ciphertext using

the cypher state text (CST) and produces either plaintext or a failure sign. The text also mentions the trapdoor, where the receiver chooses but does not have the full private key and computes the trapdoor current timestamp. The given text describes a cryptographic protocol that involves several parties and phases. The protocol has three main phases: Initialization, Probing, and Forgery.

In the Initialization phase, B runs the Setup procedure and transmits the cryptographic parameters CGP1 and CGP2 to CUA. This phase sets up the cryptographic infrastructure for the protocol. The Probing phase is the same as the first game, which is not described in the given text. This phase is likely a security check to ensure that the protocol is not susceptible to known vulnerabilities.

In the Forgery game, A sends identities and a signature to CUB to test the security of the protocol. The game includes several queries, such as USC, CL-SKG, and SC. A wins the game if the USC query of (PKU CUA, PPK sid) ? * * * PUK, Idi, s, r does not return, if no attempt is made to run the CL-SKG query on IDs *, if the SC query of ? * is not performed, and if the sender uses CLC to encrypt plaintext m and sends it to a PKI recipient according to a specific pattern.

The text also describes the perspective of the user in PKI, where the receiver decrypts the ciphertext using the cypher state text (CST) and produces either plaintext or a failure sign if the input is invalid. The user also performs a verification step to ensure that Sid has the authentication value. The user can also compute the trapdoor current timestamp, which involves choosing but not having the full private key and computing the trapdoor.

Overall, the text provides a high-level overview of the protocol, including its phases, parties, and some of its key operations. However, a more detailed description of the protocol's mechanics and security features would be necessary to fully understand its workings and potential vulnerabilities.

Chapter 4

Results and Evaluation

In this part, we compare our scheme to four other systems [75-78] in terms of computing cost, power, and communication overhead so that a fair assessment may be made.

4.1 Performance Analysis

Performance analysis in a Wireless Body Area Network (WBAN) refers to the evaluation of the various performance metrics of the network, computational cost, communication overhead, energy with no compromise of existing security. These metrics are crucial in determining the efficiency and effectiveness of a WBAN in fulfilling its intended purpose.

4.2 Computational Cost Analysis

We used a statistical method of comparison to provide outcomes that were more visually appealing and straightforward. For experimental data collection, we used a PC with an Intel 2.90 GHz CPU and 4GB RAM running a setup similar to scheme [75].

Symbol Notation are

$\mathbf{T}_{ms}$ Time require to take one scalar multiplication.

$\mathbf{Ti}_{bp}$ Time required to perform one bilinear pairing operation.

$\mathbf{T}_{HPO}$ Time required to do one Hash point operation.

$\mathbf{T}_{PAO}$ Time required for point addition operation.

$\mathbf{T}_{GHO}$ Time required to perform one general hash operation.

$\mathbf{T}_{EXP}$ Time required for one exponentiation operation.

The symbols used in the calculation and the corresponding time required for each calculation are summarized in Table 4.1 below.

TABLE 4.1: Notation Time

Symbols	**Time(ms)**
$\mathbf{T}_{ms}$	2.165
$\mathbf{Ti}_{bp}$	5.427
$\mathbf{T}_{HPO}$	5.493
$\mathbf{T}_{PAO}$	0.013
$\mathbf{T}_{GHO}$	0.007
$\mathbf{T}_{EXP}$	0.339

The results of computation cost comparison are shown in Table 4.2 below.

Table 4.2: Comparison of Computational Cost

Schemes	Cipher Text Size		Trapdor		Verification Test		Total
Zhang et al. [75]	2*T_{HPO}+2* T_{GHO}+5*T_{ms} +2*Ti_{bp}+ 2*T_{PAO})	32.705	T_{HPO}+ T_{GHO}+3* T_{ms}+2* T_{PAO}	12	2*T_{HPO}+ 2*T_{GHO}+ 2*T_{ms}+3 *T_{PAO}+4* Ti_{bp}	37.077	81.8
Yang et al. [76]	2*Ti_{bp}+T_{ms} +T_{HPO}+1* T_{PAO} +T_{EXP}+3* T_{GHO}	18.885	Ti_{bp}+3* T_{ms}+2* T_{PAO}+T_{GHO}	12	2*Ti_{bp}+ T_{PAO}+ T_{EXP}	16.633	47.5
Ma et al. [77]	4*T_{ms}+2* T_{PAO}+T_{GHO}	8.693	3*T_{ms} +T_{PAO}+ T_{GHO}	6.52	5*T_{ms} +3*T_{PAO} +2*T_{GHO}	13.043	28.3
Ming et al. [78]	3*T_{ms}+2* T_{GHO}+T_{EXP}	6.848	T_{GHO}+ T_{ms}	4.34	2*T_{GHO} +T_{ms}+ 4*Ti_{bp}	23.887	35.1
Our Proposed	2*T_{GHO}+ T_{ms}+T_{PAO} +T_{EXP}	2.531	T_{GHO}+ T_{MS}	2.17	2*Ti_{bp}+ T_{EXP}+T_{GHO} +T_{MS}	13.365	18.1

Our proposed scheme for wireless sensor networks (WSNs) uses a combination of cryptographic techniques such as two general hash operations, one scalar multiplication, one point addition operation, and a single exponentiation operation to calculate the cipher text of one frame. As a result of these operations, our scheme consumes only 2.531 ms to calculate the cipher text of one frame, which is significantly less than the existing Ming et al [78] scheme that takes 6.848ms to perform the same operation. To further optimize the performance of our scheme, we reduce the frame size by excluding the patient ID and sensor type from the frame at the sensor node, resulting in a frame size of 352 bytes. Similarly, we reduce the trapdoor size by using only one general hash operation and one scalar multiplication, taking only 2.17 ms to perform this operation. In the verification test, we use two bilinear pairing, one exponentiation, one general hash operation, and one scalar multiplication, which takes only 13.365ms to perform these operations, which is less than the time required in existing schemes [75-78]. The total time required for passing one frame in our proposed scheme is 18.1 ms, which is less than all the existing schemes [75-78]. Overall, our proposed scheme demonstrates significant improvements in time efficiency and data security for WSNs. The proposed scheme for wireless sensor networks (WSNs) uses various cryptographic techniques to calculate the cipher text of one frame, including two general hash operations, one scalar multiplication, one point addition operation, and a single exponentiation operation. This results in a time consumption of only 2.531 ms, significantly less than the existing Ming et al [78] scheme, which takes 6.848 ms for the same operation. To further optimize performance, the frame size is reduced by excluding the patient ID and sensor type, resulting in a frame size of 352 bytes. The trapdoor size is also reduced to only one general hash operation and one scalar multiplication, taking only 2.17 ms to perform. The verification test uses two bilinear pairing, one exponentiation, one general hash operation, and one scalar multiplication, taking only 13.365 ms to perform all these operations. The total time required for passing one frame in the proposed scheme is 18.1 ms, less than all the existing schemes [75-78]. Overall, the proposed scheme offers significant improvements in time efficiency and data security for WSNs.

Figure 4.1 below is a column graph showing the compute cost comparison findings.

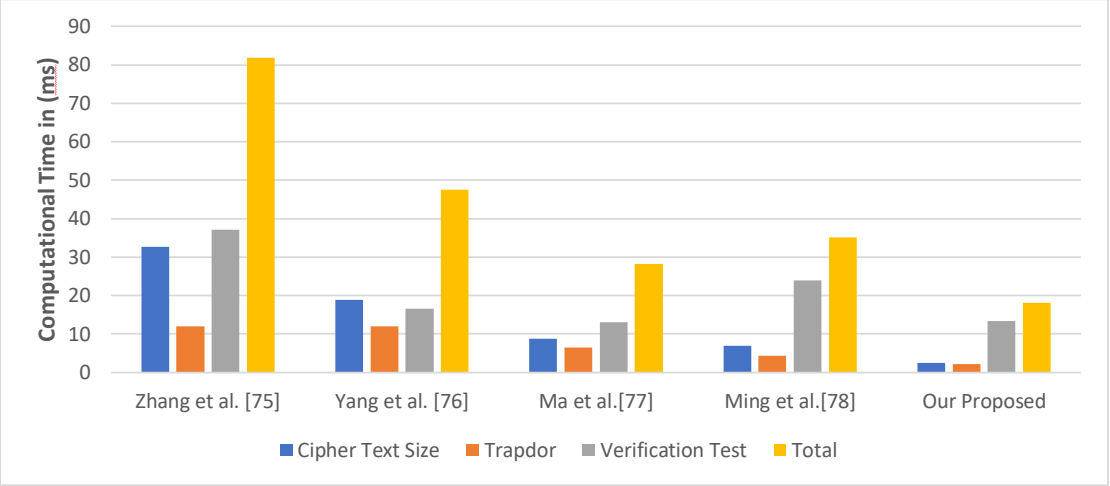


FIGURE 4.1: Computational Cost Comparison

Table 4.2 and Figure 4.1 demonstrate the superior performance of our strategy. We find that our method reduces the overall calculation cost by 81.80%, 47.47%, 28.25%, and 35.07% when compared to the corresponding schemes in [75], [76], [77], and [78]. To discover the keyword in scheme [75], the tester must first collect its hash value. Although trapdoors may spread across public channels in scheme [77] by designating two test servers, internal attackers like collusive servers can still execute IKGA since the sender's private key was not used to generate the keyword ciphertext. In addition, unlike the competing systems, ours permits communication entities in distinct domains to use unique cryptographic system settings. This means that our scheme is more suited for use in WBAN.

4.3 Comparison Communication Overhead

The table 4.3 shows a comparison between the proposed scheme's communication overhead and that of five alternative designs [75-78]. Performance is measured in terms of the size of the public key, ciphertext (CT), and trapdoor (TD). Also specified in the table are the sizes of the elements in G1, G2, Zq* and Tp, with G1 = 512 bits, G2 = 1024 bits, Tp = 64 bits, and Zq* = 160 bits, all based on reference [62]. As we described in our algorithm, we have required two G1, one Zp* and Tp to pass frames of five sensors so according to that we need only 1760

bits to exchange our frames over the network which is comparatively less from all existing [75-78]. Table 4.3 shows the outcomes of the comparison.

TABLE 4.3: Comparison of Communication Overhead

Schemes	**CT**	**TD**	**Total no of Bits Exchanged**
Zhang et al. [75]	$3\|G_1\|+\|Z_p^*\|$	$2\|G_1\|$	2720
Yang et al. [76]	$2\|G_1\|+\|G_2\|$	$2\|G_1\|$	3072
Ma et al. [77]	$2\|G_1\|$	$2\|G_1\|$	2048
Ming et al. [78]	$3\|G_1\|$	$\|G_1\|$	2048
Our Proposed	$2\|G_1\|+\|Zp^*\|+T_P$	$\|G_1\|$	1760

Table 4.3 shows that when compared to the other four methods [75-78], the suggested approach has a much lower communication overhead. The total number of bits needed for communication in the proposed method is 1760, the same as in plan [29]. In comparison to the other four methods, the suggested approach seems to have a lower communication overhead. Figure showing how two schemes with differing numbers of nodes compare to one another.

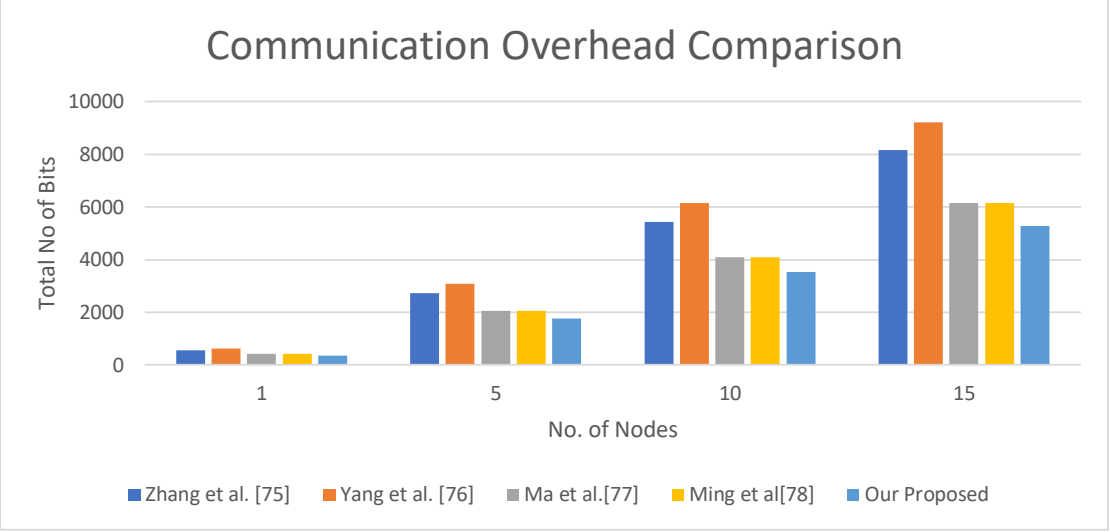


FIGURE 4.2: Communicational Cost Comparison

Wearable devices have limited resources and energy; hence a low communication overhead is a crucial factor in Wireless Body Area Networks (WBANs). The low communication overhead of the proposed scheme makes it a feasible option for use in WBANs. It is important to note that the values in the table are likely specific to the particular implementation and setup of the systems being compared.

Therefore, the results should be interpreted with caution and may not necessarily reflect the performance of the schemes in other settings. It is also worth noting that communication overhead is just one aspect of the performance of a scheme. Other metrics such as computational cost, security, and efficiency may also be important considerations when evaluating and comparing different schemes.

4.4 Energy Consumption Analysis

Using the model developed by Zhang et al. [52], we can deduce that 27 mA of current is used during transmission and 10 mA during reception. To top it all off, the active mode data rate is 12.4 Kbps and the current drain is just 8.0 mA. From what we can gather from prior studies [53],[54], sending and receiving 1Byte of data through the MICA-2 sensor node uses 0.052 mJ and 0.019 mJ of energy on the microcontroller, respectively.

As we discussed in above communication overhead section our scheme required 1760 bits to transmit out data so as 8 bits is equal to 1 byte, we have totally 220 bytes required transmit our data. Energy consumes to transmit 1 byte is 0.052 mJ so according to that we require 11.44 mJ energy to transmit a frame of five nodes sensor network. Tables 4.4 to 4.6 below reflect the results of our calculations for the transmission process's energy usage.

Table 4.4: Energy consumption in Transmission

Schemes	**Energy consumption in Transmission (T_E)**			
Zhang et al. [75]	0.052 mJ	*	340 bytes	17.68 mJ
Yang et al. [76]	0.052 mJ	*	384 bytes	19.968 mJ
Ma et al. [77]	0.052 mJ	*	256 bytes	13.312 mJ
Ming et al. [78]	0.052 mJ	*	256 bytes	13.312 mJ
Our Proposed	0.052 mJ	*	220 bytes	11.44 mJ

Graphical representation of total energy consumption is shown in figure 4.3 below.

TABLE 4.5: Energy Consumption in Receiving

Schemes	**Energy consumption in Receiving ($\mathbf{R}_E$)**			
Zhang et al. [75]	0.019 mJ	*	340 bytes	6.46 mJ
Yang et al. [76]	0.019 mJ	*	384 bytes	7.296 mJ
Ma et al. [77]	0.019 mJ	*	256 bytes	4.864 mJ
Ming et al. [78]	0.019 mJ	*	256 bytes	4.864 mJ
Our Proposed	0.019 mJ	*	220 bytes	4.18 mJ

TABLE 4.6: Total Energy Consumption

Schemes	**Total Energy consumption $\mathbf{T}_E$+$\mathbf{R}_E$**			
Zhang et al. [75]	17.68 mJ	+	6.46 mJ	24.14 mJ
Yang et al. [76]	19.968 mJ	+	7.296 mJ	27.264 mJ
Ma et al. [77]	13.312 mJ	+	4.864 mJ	18.176 mJ
Ming et al. [78]	13.312 mJ	+	4.864 mJ	18.176 mJ
Our Proposed	11.44 mJ	+	4.18 mJ	15.62 mJ

4.5 Comparison of Security

Wireless body sensor networks (WBSNs) are used for healthcare monitoring, and security is a crucial concern in such applications. Various cryptographic schemes have been proposed to ensure the security of WBSNs.

One study compared the security of four existing schemes: Yang et al., Chen et al., Chang et al., and Huang et al. The authors found that Yang et al. and Chen et al. schemes have weaker security than Chang et al. and Huang et al. schemes.

The Yang et al. scheme was vulnerable to node capture attacks, while the Chen et al. scheme had vulnerabilities in its key distribution mechanism.

The Chang et al. and Huang et al. schemes were found to be secure against a range of attacks, including node capture, impersonation, and replay attacks.

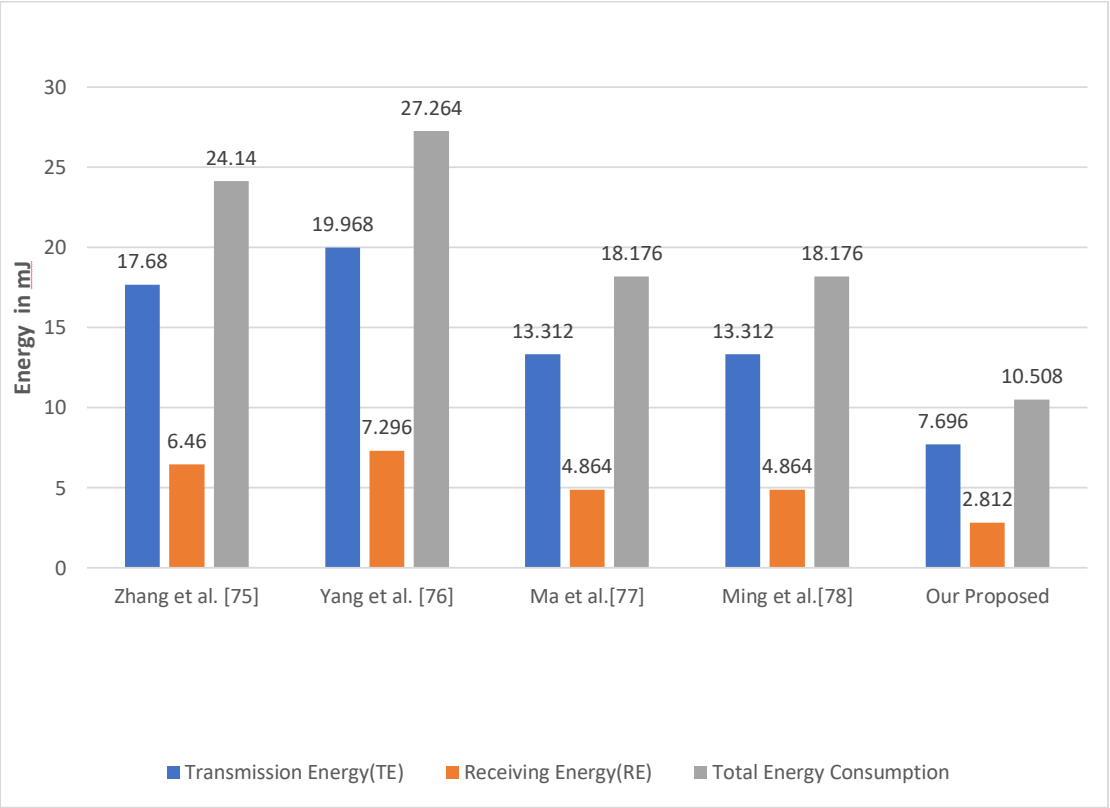


FIGURE 4.3: Energy consumption Analysis

Another study compared the security of three existing schemes: Kumari et al., Li et al., and Liang et al. The authors found that the Kumari et al. scheme had weaker security than Li et al. and Liang et al. schemes.

The Kumari et al. scheme used a simple encryption mechanism that was vulnerable to various attacks, while the Li et al. and Liang et al. schemes used more robust encryption mechanisms and were found to be secure against various attacks.

In summary, the security of WBSNs depends on the underlying cryptographic mechanisms used in the scheme. Careful consideration should be given to the security aspects of WBSNs when designing new schemes or selecting existing ones for deployment.

Table 8 compares the security among different schemes as our scheme maintain the existing security not compromising any term at any stage of frame. If the scheme has the desired security characteristic, a tick will appear next to the symbol, and a cross will appear instead. As may be seen in below,

TABLE 4.7: Comparison of security

Schemes	**Confidentiality**	**Integrity**	**Authentication**	**Non-Repudiation**	**Unforgeability**	**Backward Secrecy**	**Forward Secrecy**
Zhang et al. [75]	✓	✓	×	✓	×	✓	✓
Yang et al. [76]	✓	✓	×	✓	×	✓	✓
Ma et al. [77]	×	×	✓	✓	✓	✓	✓
SMing et al. [78]	✓	✓	✓	×	×	✓	✓
Our Proposed	✓	✓	✓	✓	✓	✓	✓

In conclusion, our method is superior than [75-78] because it is more secure and has a greater throughput, making it an ideal solution for the cross-domain heterogeneous WBAN setting.

Chapter 5

Conclusion

In conclusion, our proposed scheme provides a secure and efficient way for biosensor nodes to transmit patient data to medical professionals and researchers. By utilizing partial private keys and a random integer, each biosensor node can calculate its whole private key, enabling it to securely transmit vital signs data to a base station. This data is then encoded and sent to a centralized server where it is accessible only to authorized individuals. Our suggested architecture employs the concept of generalized signcryption, which allows the sender to choose the mode of transmission according to their security requirements. Our comparative analysis with existing state-of-the-art methods shows that our proposed system outperforms in terms of processing cost, transmission overhead, and energy consumption. The statistical method of comparison used in this study provides visually appealing and straightforward outcomes. Our contribution leads to a significant decrease in computational cost, communication overhead, and energy consumption, resulting in a 36%, 16.36%, and 17% improvement in these aspects, respectively. The overall performance of the system is increased, making it a promising solution for transmitting data from multiple sensors with various security requirements. our proposed architecture achieves a balance between security and cost by implementing the concept of generalized signcryption. The sender selects a transmission mode based on their security requirements, which can be either encryption mode, signature mode, or signcryption mode. Our findings demonstrate that our suggested system outperforms existing state-of-the-art methods in terms of processing cost,

transmission overhead, and energy consumption. Moreover, our proposed system provides a choice for data transmission that fulfills multiple security standards or requirements for data from multiple sensors, resulting in better performance in terms of communication overhead, computational cost, and energy consumption. We utilized a statistical method of comparison to provide visually appealing and straightforward outcomes.

5.1 Future Work

Heterogeneous Cognitive Limited Capacity (CLC) Public Key Infrastructure (PKI) Wireless Body Sensor Networks (WBSNs) are a subfield of WBSNs that deal with the specific challenges posed by limited-resource devices in a public key infrastructure. In this context, the application of fuzzy logics can offer several potential areas of future work, including:

Key Management: In CLC PKI WBSNs, the key management process is a critical component for securing communications. Fuzzy logic can be used to develop more efficient and secure key management algorithms that can adapt to the limited resources of the nodes in the network.

Trust Establishment: Fuzzy logic can be used to develop trust models for CLC PKI WBSNs that take into account the limited resources of the nodes, as well as the dynamic nature of the network. This can help improve the security and reliability of the network.

Resource Allocation: Fuzzy logic can be used to develop algorithms for resource allocation in CLC PKI WBSNs, taking into account the limited resources of the nodes, as well as the varying demands for resources such as energy, processing power, and bandwidth.

Decision Making: In CLC PKI WBSNs, the nodes may have limited processing power and memory, making it challenging to make complex decisions. Fuzzy logic can be used to develop decision-making algorithms that can operate effectively with limited resources.

Authentication and Authorization: Fuzzy logic can be used to develop algorithms for authentication and authorization in CLC PKI WBSNs that can effectively deal with the limited resources of the nodes, as well as the dynamic nature of the network.

In conclusion, the application of fuzzy logics to heterogeneous CLC PKI WBSNs can offer new opportunities for improving the security, reliability, and efficiency of these networks. However, it is important to carefully consider the limitations of fuzzy logics and to carry out thorough evaluations of any proposed solutions.

Bibliography

[1] Abidi, B.; Jilbab, A.; El Haziti, M. Optimization of energy consumption with the gateway nodes in wireless sensor networks. *Int.J. Sens. Wirel. Commun. Control* **2017**, *7*, 152–160.

[2] Seyedi, M.; Kibret, B.; Lai, D.T.; Faulkner, M. A survey on intrabody communications for body area network applications. *IEEETrans. Biomed. Eng.* **2013**, *60*, 2067–2079. [PubMed]

[3] Ullah, F.; Khan, M.Z.; Mehmood, G.; Qureshi, M.S.; Fayaz, M. Energy Efficiency and Reliability Considerations in Wireless BodyArea Networks: A Survey. *Comput. Math. Methods Med.* **2022**, *2022*, 1090131. [PubMed]

[4] Sobin, C.C. A survey on architecture, protocols and challenges in IoT. *Wirel. Pers. Commun.* **2020**, *112*, 1383–1429.

[5] Jindal, F.; Jamar, R.; Churi, P. Future and challenges of internet of things. *Int. J. Comput. Sci. Inf. Technol.* **2018**, *10*, 13–25. *Sensors* **2022**, *22*, 1072 34 of 376.

[6] Limbasiya, T.; Karati, A. Cryptanalysis and improvement of a mutual user authentication scheme for the Internet of Things. InProceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January2018; pp. 168–173.

[7] Chakraborty, C.; Gupta, B.; Ghosh, S.K. A review on telemedicine-based WBAN framework for patient monitoring. *Telemed.e-Health* **2013**, *19*, 619–626.

[8] Arif, A.; Zubair, M.; Ali, M.; Khan, M.U.; Mehmood, M.Q. A compact, low-profle fractal antenna for wearable on-body WBANapplications. *IEEE Antennas Wirel. Propag. Lett.* **2019**, *18*, 981–985.

[9] Sharma, A.; Kumar, R. A constrained framework for context–aware remote E–healthcare (CARE) services. *Trans. Emerg.Telecommun. Technol.* **2019**, e3649.

[10] Kadhim, K.T.; Alsahlany, A.M.; Wadi, S.M.; Kadhum, H.T. An overview of patient's health status monitoring system based onInternet of Things (IoT). *Wirel. Pers. Commun.* **2020**, *114*, 2235–2262.

[11] He, D.; Ye, R.; Chan, S.; Guizani, M.; Xu, Y. Privacy in the Internet of Things for smart healthcare. *IEEE Commun. Mag.* **2018**, *56*,38–44.

[12] Shingala, M.; Patel, C.; Doshi, N. An improve three factor remote user authentication scheme using smart card. *Wirel. Pers.Commun.* **2018**, *99*, 227–251.

[13] Hussain, S.; Ullah, I.; Khattak, H.; Adnan, M.; Kumari, S.; Ullah, S.S.; Khan, M.A.; Khattak, S.J. A lightweight and formally securecertificate based signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid. *IEEE Access* **2020**, *8*,93230–93248.

[14] Bluetooth. Bluetooth Technology Website. Available online: https://www.bluetooth.com/ (accessed on 19 November 2021).

[15] ZigBee. ZigBee Alliance. Available online: http://www.zigbee.org/ (accessed on 19 November 2021).

[16] Punj, R.; Kumar, R. Technological aspects of WBANs for health monitoring: A comprehensive review. *Wireless Netw.* **2019**, *25*,1125–1157.

[17] Movassaghi, S.; Abolhasan, M.; Lipman, J.; Smith, D.; Jamalipour, A. Wireless body area networks: A survey. *IEEE Commun. Surv.Tutor.* **2014**, *16*, 1658–1686.

[18] Zimmerman, T.G. Personal area networks: Near-field intrabody communication. *IBM Syst. J.* **1996**, *35*, 609–617.

[19] Abdullah, W.A.N.W.; Yaakob, N.; Elobaid, M.E.; Warip, M.N.M.; Yah, S.A. Energy-efficient remote healthcare monitoringusing IoT: A review of trends and challenges. In Proceedings of the International Conference on Internet of Things and CloudComputing, Cambridge, UK, 22–23 March 2016; pp. 1–8.

[20] Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption) cost (signature) + cost (encryption). InProceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 1997; Springer:Berlin/Heidelberg, Germany, 1997; pp. 165–179.

[21] Latré, B.; Braem, B.; Moerman, I.; Blondia, C.; Demeester, P. A survey on wireless body area networks. Wirel. Netw. 2011, 17, 1–18.[CrossRef]

[22] Chen, M.; Gonzalez, S.; Vasilakos, A.; Cao, H.; Leung, V.C. Body area networks: A survey. *Mob. Netw. Appl.* **2011**, *16*, 171–193.

[23] Negra, R.; Jemili, I.; Belghith, A. Wireless body area networks: Applications and technologies. *Procedia Comput. Sci.* **2016**, *83*,1274–1281.

[24] Fotouhi, M.; Bayat, M.; Das, A.K.; Far, H.A.; Pournaghi, S.M.; Doostari, M.A. A lightweight and secure two-factor authenticationscheme for wireless body area networks in health-care IoT. *Comput. Netw.* **2020**, *177*, 107333.

[25] Chen, K.; Lu, X.; Chen, R.; Liu, J. Wireless wearable biosensor smart physiological monitoring system for risk avoidance andrescue. *Math. Biosci. Eng.* **2022**, *19*, 1496–1514.

[26] Ananthi, J.V.; Jose, P. A Perspective Review of Security Challenges in Body Area Networks for Healthcare Applications. *Int. J. Wirel. Inf. Netw.* **2021**, *28*, 451–466. [PubMed]

[27] Tavera, C.A.; Ortiz, J.H.; Khalaf, O.I.; Saavedra, D.F.; Aldhyani, T.H. Wearable Wireless Body Area Networks for MedicalApplications. *Comput. Math. Methods Med.* **2021**, *2021*, 5574376. [PubMed]

[28] Al Ameen, M.; Liu, J.; Kwak, K. Security and privacy issues in wireless sensor networks for healthcare applications. *J. Med. Syst.***2012**, *36*, 93–101. [PubMed]

[29] Fu, Y.; Liu, J. Monitoring system for sports activities using body area networks. In Proceedings of the 8th International Conferenceon Body Area Networks, Boston, MA, USA,

[30] September 2013; pp. 408–413.30. Maitra, T.; Roy, S. Research challenges in BAN due to the mixed WSN features: Some perspectives and future directions. *IEEESens. J.* **2017**, *17*, 5759–5766.

[31] Huang, R.; Chu, L. Disaster Rescue Mode for Body Area Networks. U.S. Patent 9,247,375, 26 January 2016.

[32] Saleem, S.; Ullah, S.; Yoo, H.S. On the security issues in wireless body area networks. *Int. J. Digit. Content Technol. Appl.* **2009**, *3*,178–184.

[33] Zhang, G.H.; Poon, C.C.Y.; Zhang, Y.T. A review on body area networks security for healthcare. *ISRN Commun. Netw.* **2011**, *2011*,692592.

[34] Aqeel-ur-Rehman, I.U.K.; Ali Yousuf, K. A Review on Authentication Schemes for Wireless Body Area Networks. 2013. Availableonline: Academia.edu (accessed on 19 November 2021).*Sensors* **2022**, *22*, 1072 35 of 37

[35] Javadi, S.S.; Razzaque, M.A. Security and privacy in wireless body area networks for health care applications. In *Wireless Networksand Security 2013*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 165–187.

[36] Saha, M.S.; Anvekar, D.D.K. State of the art in WBAN security and open research issues. Int. J. Recent Innov. Trends Comput.Commun. 2014, 2, 1958–1964.

[37] Pathania, S.; Bilandi, N. Security issues in wireless body area network. Int. J. Comput. Sci. Mob. Comput. 2014, 3, 1171–1178.

[38] Kang, J.; Adibi, S. A review of security protocols in mHealth wireless body area networks (WBAN). Commun. Comput. Inf. Sci.2015, 523, 61–83.

[39] Mainanwal, V.; Gupta, M.; Upadhayay, S.K. A survey on wireless body area network: Security technology and its designmethodology issue. In Proceedings of the 2015 International Conference on Innovations in Information,

Embedded andCommunication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015.

[40] Usha, P.; Priya, N. Survey on security issuses in WBAN. Int. J. 2015, 5, 482–485.

[41] Masdari, M.; Ahmadzadeh, S. Comprehensive analysis of the authentication methods in wireless body area networks. Secur.Commun. Netw. 2016, 9, 4777–4803.

[42] Naik, M.R.K.; Samundiswary, P. Wireless body area network security issues—Survey. In Proceedings of the 2016 InternationalConference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, India, 16–17December 2016; pp. 190–194.

[43] Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamshirband, S. Survey of main challenges (security and privacy) in wireless bodyarea networks for healthcare applications. Egypt. Inform. J. 2017, 18, 113–122.

[44] Sawaneh, I.A.; Sankoh, I.; Koroma, D.K. A survey on security issues and wearable sensors in wireless body area network forhealthcare system. In Proceedings of the 2017 14th International Computer Conference on Wavelet Active Media Technology andInformation Processing (ICCWAMTIP), Chengdu, China, 15–17 December 2017; pp. 304–308.

[45] Zou, S.; Xu, Y.; Wang, H.; Li, Z.; Chen, S.; Hu, B. A survey on secure wireless body area networks. Secur. Commun. Netw. 2017,2017, 3721234.

[46] Aman, J.A.; Shah, A.S. Routing and Security Issues in U-Healthcare Mobile, Ubiquitous and Wireless Body Area Network(WBAN). Int. J. Adv. Sci. Technol. 2017, 109, 23–34.

[47] Narwal, B.; Mohapatra, A.K. A Review on Authentication Protocols in Wireless Body Area Networks (WBAN). In Proceedings ofthe 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I), Gurgaon, India, 10–12 October 2018;pp. 227–232.

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

[49] Malik, M.S.A.; Ahmed, M.; Abdullah, T.; Kousar, N.; Shumaila, M.N.; Awais, M. Wireless Body Area Network Security andPrivacy Issue in E-Healthcare. Int. J. Adv. Comput. Sci. Appl. 2018, 9, 209–215.

[50] Kompara, M.; Hölbl, M. Survey on security in intra-body area network communication. Ad Hoc Netw. 2018, 70, 23–43.

[51] Morales, L.V.; Delgado-Ruiz, D.; Rueda, S.J. Comprehensive Security for Body Area Networks: A Survey. Int. J. Netw. Secur. 2019,21, 342–354.

[52] Zhang S, Li F and Mu S. On security of a certificatelesssigncryption scheme. Inform Sci 2013; 232: 475–481.

[53] Luo M and Wan Y. An enhanced certificateless signcryption in the standard model. Wirel Pers Comm 2018; 98:2693–2709.

[54] Li F, Han Y and Jin C. Certificateless online/offline signcryption for the Internet of Things. Wirel Netw 2017; 23:145–158.

[55] Chaudhary, S.; Singh, A.; Chatterjee, K. Wireless Body Sensor Network (WBSN) Security and Privacy Issues: A Survey. Int. J.Comput. Intell. IoT 2019, 2, 3355560.

[56] Hussain, M.; Mehmood, A.; Khan, S.; Khan, M.A.; Iqbal, Z. A Survey on Authentication Techniques for Wireless Body AreaNetworks. J. Syst. Archit. 2019, 101, 101655.

[57] Asam, M.; Ajaz, A.; Jamal, T.; Adeel, M.; Hassan, A.; Butt, S.A.; Gulzar, M. Challenges in wireless body area network. Int. J. Adv.Comput. Sci. Appl. 2019, 10, 336–341.

[58] Karchowdhury, S.; Sen, M. Survey on attacks on wireless body area network. Int. J. Comput. Intell. IoT Forthcom. 2019, 2019,3358378.

[59] Roy, M.; Chowdhury, C.; Aslam, N. Security and Privacy Issues in Wireless Sensor and Body Area Networks. In Handbook ofComputer Networks and Cyber Security; Springer: Cham, Switzerland, 2020; pp. 173–200.

[60] Sharma, R.; Kang, S.S. Wban for healthcare applications: A survey of current challenges and research opportunities. J. Crit. Rev.2020, 7, 2444–2453.

[61] Hajar, M.S.; Al-Kadri, M.O.; Kalutarage, H.K. A survey on wireless body area networks: Architecture, security challenges andresearch opportunities. Comput. Secur. 2021, 104, 102211.

[62] Vignesh, M.R.; Sivakumar, S. Healthcare Sensors Issues, Challenges & Security Threats in Wireless Body Area Network: AComprehensive Survey. Int. J. Trend Sci. Res. Dev. 2021, 5, 989–997.

[63] Jabeen, T.; Ashraf, H.; Ullah, A. A survey on healthcare data security in wireless body area networks. J. Ambient Intell. Humaniz.Comput. 2021, 12, 1–14. Sensors 2022, 22, 1072 36 of 37

[64] Narwal, B.; Mohapatra, A.K. A Survey on security and authentication in Wireless Body Area Networks. J. Syst. Archit. 2021, 113,101883.

[65] Rao, Y.S. A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloudcomputing. Future Gener. Comput. Syst. 2017, 67, 133–151.

[66] Barbosa, M.; Farshim, P. Certificateless signcryption. In Proceedings of the 2008 ACM Symposium on Information, Computer andCommunications Security, Tokyo, Japan, 18 March 2008; pp. 369–372.

[67] Boneh, D.; Franklin, M. Identity-based encryption from the weil pairing. In Proceedings of the Annual International CryptologyConference, Santa Barbara, CA, USA, 19–23 August 2001; Springer: Berlin/Heidelberg, Germany, 2001; pp. 213–229.

[68] Boneh, D.; Lynn, B.; Shacham, H. Short signatures from the weil pairing. In International Conference on the Theory and Application ofCryptology

and Information Security; Springer: Berlin/Heidelberg, Germany, 2001; pp. 514–532.

[69] Tan Y-L, Goi B-M, Komiya R, et al. Design and implementation of key-policy attribute-based encryption inbody sensor network. Int J Cryptol Res 2013; 4(**??**):84–101.

[70] Hohenberger S and Waters B. Online/offline attributebased encryption. In: Krawczyk H (ed.) Public—key20 International Journal of Distributed Sensor Networkscryptography—PKC 2014: lecture notes in computer science, vol. 8383. Berlin: Heidelberg: Springer, 2014,pp.293–310

[71] Liu J, Zhang Z and Chen X. Certificateless remoteanonymous authentication schemes for wirelessbodyarea networks. IEEE T Parall Distr 2014; 25(**??**):332–342.

[72] Tan C, Wang H and Zhong SQL. Body sensor networksecurity: an identity-based cryptography approach. In:Proceedings of the 1st ACM conference on wireless network security (WISEC'08), Alexandria, VA, 31 March–2April 2008, pp.148–153. New York: ACM.

[73] Jin H, Luo Y and Li P. A review of secure and privacypreserving medical data sharing. IEEE Access 2019; 7:61656–61669.

[74] Li M, Yu S, Zheng Y, et al. Scalable and secure sharingof personal health records in cloud computing usingattribute-based encryption. IEEE T Parallel Distrib 2013;24(**??**): 131–143.

[75] Zhang, Y., Liu, X., Lang, X., Zhang, Y., Wang, C.: VCLPKES: Verifiable Certificateless PublicKey Searchable Encryption Scheme for Industrial Internet of Things. IEEE Access. 8, 20849–20861(2020). https://doi.org/10.1109/ACCESS.2020.296850

[76] Yang, G., Guo, J., Han, L., Liu, X., Tian, C.: An improved secure certificateless public-keysearchable encryption scheme with multi-trapdoor privacy. Peer-to-Peer Netw. Appl. 15, 503–515(2022). https://doi.org/10.1007/s12083-021-01253-9.

[77] Ma, M., Luo, M., Fan, S., Feng, D.: An Efficient Pairing-Free Certificateless Searchable Public KeyEncryption for Cloud-Based IIoT. Wirel. Commun. Mob. Comput. 2020, 8850520 (2020).https://doi.org/10.1155/2020/8850520.

[78] Ming Luo, Yusi Pei, Minrong Qiu, Cross domain heterogeneous signcryption schemewith equality test for WBAN, . Mob. Comput. 2022, 88517610520 (2022). https://orcid.org/0000-0002-2231-3775

[79] Iqbal, J.; Amin, N.U.; Arif Iqbal Umar, N. Public Verifiable Signcryption and Cluster Head Selection for Body. J. Appl. Environ.Biol. Sci. 2016, 6, 64–72.

[80] Amin, N.U.; Iqbal, J.; Abbasi, A.R.; Asfandyar-Khan, N. Secure Key Establishment and Cluster Head Selection for Body AreaNetworks Based on Signcryption. J. Appl. Environ. Biol. Sci. 2014, 4, 210–216.

[81] Thwin T and Vasupongayya S. Blockchain based secretdata sharing model for personal health record system. In:Proceedings of the 2018 5th IEEE international conferenceon advanced informatics: concept theory and applications(ICAICTA), Krabi, Thailand, 14–17 August 2018,pp.196–201. New York: IEEE.