AN AUTHENTICATION TECHNIQUE FOR ENHANCING SECURITY IN HEALTHCARE MONITORING SYSTEMS USING WIRELESS BODY AREA NETWORKS (WBANs)

A Thesis submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY
IN
COMPUTER SCIENCE AND ENGINEERING

By

Mr. C. RAMESH KUMAR
Registration Number - 17SCSE301039

Supervisor

Dr. T. GANESH KUMAR
Associate Professor

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY
UTTAR PRADESH, INDIA
MAY 2023

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis, entitled "**AN AUTHENTICATION TECHNIQUE FOR ENHANCING SECURITY IN HEALTHCARE MONITORING SYSTEMS USING WIRELESS BODY AREA NETWORKS (WBANs)**" in fulfillment of the requirements for the award of the degree of Doctor of Philosophy in the department of computer science and engineering and submitted in Galgotias University, Greater Noida is an authentic record of my own work carried out during a period from July 2017 to Oct 2022 under the supervision of **Dr. T. GANESH KUMAR**.

The matter embodied in this thesis has not been submitted by me for the award of any other degree of this or any other University/Institute.

Mr. C. RAMESH KUMAR

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Dr. T. GANESH KUMAR
Supervisor
School of Computing Science and Engineering

The Ph.D. Viva-Voice examination of _____ Research Scholar, has been held on _____.

Sign of Supervisor Sign of External Examiner

ABSTRACT

In Health-Care Monitoring (HCM) applications, the Wireless Sensor Network (WSN) gives an important benefit for the subsequent evaluation. The development of a specialized biological network named Body Sensor Networks (BSNs) or Body Area Networks (BANs) are been provoked by the major advancements in WSN algorithms along with applications. WSBN is a kind of WSN, which is particularly associated with healthcare applications. In HCM, for checking the useful parameters exactly, the Biosensors Nodes (BN) are located above the human bodies' surface or implanted into the human body tissues. Sensing a patient's significant signs, processing, along with communicating data are the three important tasks presented by the sensors in WBANs. The human body's essential physiological parameters like blood pressure, ECG, and pulse are gathered by BN. Through Body Sensor Units (BSUs), these biosensors collect physical data and for further assessment, the biosensor transmits the physical data to its final destination (personal display assistant, gateway, Base Station (BS). Since the WBAN collects the profits of continuous progress, it can save human lives by employing it not just in medicine but also in military applications and sports activities. Security together with privacy in WBANs based HCM services has constantly been a critical problem, even though WBANs enhance the value of health care services. However, any abuse of the patient's sensitive health-related and personal information transmitted over an open channel could mislead the doctor to make an inaccurate diagnosis and treatment, which can lead to fatal reverberations to the patient. Therefore, it is prudent to protect the data sensed by the sensors so as to maintain its integrity, and prevent it from attacks by the adversary. Apart from this, the sensor nodes surrounding the human body and sensing the physiological data have inadequate resources

concerning battery life, memory space, processing capabilities. Therefore, with the given resource constraints and issues of security and privacy in WBAN, it is necessary to come up with a stronger solution.

In this thesis, a novel authentication using an identity-based group signature (IBGS) protocol has been proposed to provide security to the WBSN. This protocol uses an identity-based group signature algorithm between biosensors and Group Manager (GM) with full anonymity to authenticate the message. Here, the base station or access point is considered the trusted authority and it generates the secret key for the biosensor based on group id and transmits the generated secret key to the biosensor manager. The GM is responsible for generating a signature on the message that has been sent to it by one of its group members and broadcasts the message to the base station whether it is verified. Upon successful verification, the message is accepted. Besides, sound informal security evaluation has been performed to demonstrate that IBGS attains necessary security properties and is safe from sundry attacks. In the end, to exhibit the practical applications of IBGS, it has been compared with the existing related schemes and the outcome reveals that IBGS optimizes energy consumption, computation cost, packet ratio, average delay, key mismatching ratio, data privacy rate, and information loss rate significantly and performs efficiently concerning measurement of security on patient health information.

Next, in this thesis, an energy-efficient secure data transmission mechanism is proposed in WBSN using a novel authentication id-based group signature model (IDGS) and Secret key induced Elliptic Curve Cryptography SECC technique. At first, the Group Manager (GM) is selected from the sensors in the remote body sensor system using Normalized Opposition Based Learning BAT Optimization Algorithm (NOBL-BOA). Afterward, clustering with Information Entropy induced K-Means Algorithm

(IEKMA) takes place to improve energy efficiency. Next, to provide security to the WBSN, message authentication is carried out based on novel authentication ID-based group signature protocol. the formal security proof for IDGS has been provided using necessary security properties. Finally, the SECC is used to encrypt the message for secure data transmission. In the end, a comparative performance analysis with other relevant schemes manifests that IDGS achieves better performance and shows promising results while providing more robust security, energy efficiency and privacy.

Keywords: *Wireless Body Sensor Network (WBSN), Security, Authentication, Energy efficiency, BAT Optimization Algorithm (BOA), K-Means Clustering (KMA), ID-based Group Signature Model.*

ACKNOWLEDGEMENT

I Mr. Ramesh Kumar C Working as an Assistant Professor and doing research for the degree of Ph.D. at Galgotias University was a quite magnificent and challenging experience for me. In all these years, many people directly or indirectly contributed to shaping my career. It was hardly possible for me tocomplete my doctoral work without the precious and invaluable support of these personalities.

I would like to give my small tribute to all those people. Initially, I would express my sincere gratitude to my supervisor Dr. T. GANESH KUMAR Associate Professor, School of Computing Science and Engineering for his valuable guidance, enthusiasm, and over-friendly nature that helped me a lot to complete my research work promptly.

I must owe a special debt of gratitude to Hon'ble Chancellor Mr. Suneel Galgotia Mr. Dhruv Galgotia, CEO, and Hon'ble Vice-Chancellor Dr. K. Mallikharjuna Babu, Galgotias University for their valuable support throughout my research work.

I express my sincere thanks to Dr. Munish Sabharwal, Dean School of Computing Science & Engineering, and Dr. R. Rajesh Kannan, Head, Ph.D. Programme for their guidance and moral support during my research work and to all faculties of the School of Computing Science & Engineering who helped me a lot in my course of research work and all those who stood behind me.

I express my heartfelt gratitude to my parents for their moral support and encouragement. I am thankful to my family members, friends, and well-wishers who have been constantly motivating me throughout the progress of this work.

C.RAMESH KUMAR

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATION		FULL FORM
WBANs	-	Wireless Body Area Networks
WLANs	-	Wireless Local Area Networks
BSUs	-	Body Sensor Units
BCU	-	Body Control Unit
PDAs	-	Personal Digital Assistants
PS	-	Personal Server
AP	-	Access Point
QoS	-	Quality Of Service
ADC	-	Analog To Digital Conversion
MEMS	-	Micro-Electromechanical Systems
ECG	-	Electrocardiography
EEG	-	Electroencephalography
EMG	-	Electromyography
PIR	-	Passive Infrared Motion Sensor
RFID	-	Radio Frequency Identification
CH	-	Cluster Head
PER	-	Packet Error Rate
PRR	-	Packet Reception Ratio
WPANs	-	Wireless Personal Area Networks
ISM	-	Industrial, Science And Medical
IoT	-	Internet Of Things
BLE	-	Bluetooth Low Energy
UWB	-	Ultra-Wideband
HBC	-	Human Body Communication
MAC	-	Message Authentication Code
HIPAA	-	The American Health Insurance Portability and Accountability Act
DoS	-	Denial Of Service
WEP	-	Wired Equivalent Privacy

WPA	-	Wi–Fi Protected Access
ECC	-	Elliptic Curve Cryptography
PKI	-	Public Key Infrastructures
BSN	-	Biosensor Node
GM	-	Group Manager
IBGS	-	Identity-Based Group Signature Algorithm
IDGS	-	Novel Authentication ID-Centric Group Signature
SECC	-	Secret Key Induced Elliptic Curve Cryptography
NOBL-BOA	-	Normalized Opposition Based Learning Bat Optimization Algorithm
IEKMA	-	Information Entropy Induced K-Means Algorithm
RQ	-	Research Questions
CA	-	Certificate Authority
DCS	-	Digital Certificate Scheme
PTK	-	Pairwise Temporal Key
MK	-	Pre-Defined Master Key
GTK	-	Group Temporal Key
PPG	-	Photoplethysmogram
PSKA	-	Physiological Signal Key Agreement Technique (PSKA)
IBAAKA	-	Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement
MQTT	-	Message Queuing Telemetry Transfer
ROM	-	Random Oracle Model
ET	-	Encryption Time
AD	-	Average Delay
DT	-	Decryption Time

LIST OF PUBLICATIONS

INTERNATIONAL JOURNALS

1. **Rameshkumar, C**., and **T. Ganeshkumar**," An Energy Efficiency Based Secure Data Transmission in WBSN Using Novel Id-Based Group Signature Model and SECC Technique", Journal of Internet Technology, Vol. 24, no. 3, pp.683-696,ISSN: 1607-9264, 2023. DOI: 10.53106/160792642023052403014 (**SCI – Impact Factor: 1.140**)
2. **Rameshkumar, C**., and **T. Ganeshkumar**., "A novel authentication scheme of identity-based group signature algorithm for wireless body sensor network (WBSN)". International Journal of Health Sciences, 6(S1), 3448–3463, 2021. (**Scopus**)
3. **C.RameshKumar** et al, "A Novel of Multi-Agent Based Architecture Design for Wireless Body-Area Network Monitoring System", international journal of scientific & technology research, volume-8, issue-09, September 2019, ISSN:2277-8616. (**Scopus**)
4. **C.RameshKumar** et al, "An Efficient Elliptic Curve Cryptography (ECC) Encryption Scheme for Wireless Body Area Network Healthcare System", Journal of Adv Research in Dynamical & Control Systems, Vol. 11, Issue-08, 2019, ISSN: 1943-023X. (**Scopus**)
5. **Rameshkumar** et al, "A Novel Group Digital Signature Authentication Protocol for Wireless Body Area Network", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), ISSN:2394-2320, Vol 5, Issue 4, April 2018. (**UGC**).
6. **C.RameshKumar** et al, "A Novel of Encryption Design for WBAN Healthcare System Using Elliptic Curve Cryptography (ECC)", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), ISSN:2394-2320, Vol 5, Issue 4, April 2018. (**UGC**).

INTERNATIONAL CONFERENCES

1. **Rameshkumar**, C., and **T. Ganeshkumar**. "A Novel of Survey: In Healthcare System for Wireless Body-Area Network." In Applications of Computational Methods in Manufacturing and Product Design, Lecture Notes in Mechanical Engineering, pp. 591-609. Springer, Singapore, 2022. DOI: 10.1007/978-981-19-0296-3_55 **(Scopus).**
2. **Rameshkumar** et al." An Efficient Distributed Energy and Consumption Method for Ensuring Wireless Sensor Network (WSN) Coverage Using the Firefly Algorithm." In Applications of Computational Methods in Manufacturing and Product Design, Lecture Notes in Mechanical Engineering, pp. 591-609. Springer, Singapore, 2023. DOI: 10.1007/978-981-99-1665-8_7 **(Scopus).**

CHAP TER I

INTRODUCTION

1.1 WIRELESS BODY AREA NETWORKS (WBANS)

Recent advances in the technology of integrated electronic devices, wireless communications and digital electronics have enabled the development of small, inexpensive, and low power devices called sensors that can be incorporated into items, clothing and accessories [1]. They even can be worn comfortably and easily deployed on the human body. The sensors are networked together to form the so-called Wireless Body Area Networks (WBANs) that offer advanced monitoring applications without interfering with the daily activities of the wearers [2]. The most important uses of such a network are applications that measure different parameters of the person, control the environment surrounding his body and send the collected data to a node referred to as the main node. The main node(s) can send data to remote location using any available ambient networks (GSM, WIFI, satellite, 3G). In more common terms, a WBAN can be defined as a self-autonomous network at the human body scale which consists of a collection of smart, low-power, hardware-constrained, miniaturized and heterogeneous wireless devices attached to (or implanted into) a moving/fixed body [3]. IEEE 802 has established the IEEE 802.15.6 standards for WBAN for communication standard optimized for low-power in-body/on-body nodes to serve a variety of medical and non-medical applications [3, 4]. The security structure for IEEE 802.15.6 has been taken from IEEE standard 802.15.4 with modifications. The IEEE 802.15.4 standard is a low-power standard designed for low data rate applications. It intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) focusing on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end-user-oriented approaches, such as Wi-Fi). However, there are still open security issues in IEEE 802.15.6 specific to WBAN which are to be addressed [5].

The small size and the low cost of individual sensors are the key factors for the expanse of WBAN's applications including, but not being limited to, unobtrusive health monitoring, WBANs are a type of WSNs where sensors are positioned on the human body to compute specific physiological factors of a person [6]. This is done through the Internet or a cellular network, personal digital assistants (PDAs) or

cellular phones as intermediary devices. The use of WBANs for medical and non-medical applications strongly requires the security requirements, because, patient's private health data transmits in the open nature, typically in a wireless channel, to achieve the intermediate device and then the monitoring station [7, 8]. Security is based on diverse applications ranging from medical (heart monitoring) to non-medical (listening to MP4) applications. In case of medical (i.e., health care) applications, the security risks may cause a patient to an unsafe condition, and sometimes to death [9]. A secure WBAN comprise confidentiality and privacy, reliability and verification, key establishment and trust set-up, secure group administration and data aggregation [10]. Therefore, an efficient and scalable security and privacy approach is needed to avoid malicious action with a WBAN. But, the combination of a high-level security approach in a low-power and limited resource sensor improves the computational, communication and management costs. In a WBAN, security and privacy performance are important and thus, designing a low-power and secure WBAN system is a primary concern to the designers.

The bio-sensors are positioned on human's body for transmitting the sensing data through a safe channel to small body area network gateway. The gateway handles the data and again transmits in a secure channel for identifying health condition of a patient using medical server in the hospital. The results are observed and analyzed using medical staff/doctors charged with monitoring patients. A patient wears a number of bio-sensors. A centralized control device is used to send the data in and out of the network. The control device is employed as a gateway connecting the internal network and base station. The base station is linked with an external network. The communication of healthcare data between sensors to the medical servers in WBAN is private and secure.

Authenticated medical data transmission plays an essential role for WBAN as false or unauthorized medical information result in inaccurate treatments or diagnoses for patients. The transmitted information is encrypted to preserve the patient privacy. The medical staff of hospital gathers confidential data that are unchanged and certainly originate from the specified patient. The main demands in WBAN are security, scalability, reliability and robustness. The size and resource limitations of bio-sensors are essential in success and reliability of WBAN. Health care organization accesses the data from BAN of the patient after successful authentication. Scalability with a

number of sensors and patients is an essential factor in all networks. User access control is an important requirement in presenting the security and data privacy for WBAN. User access control is significant for the complete operation and large acceptance of wireless body area network services [11]. The security framework for WBAN comprises of the user authentication, user authorization, and user accountability to manage the user access and avoid many kinds of attacks. User access control recognizes and requires many access benefits for many users. In WBAN, doctors and company agents are essential users to access medical data of a patient that does not essential for all users.

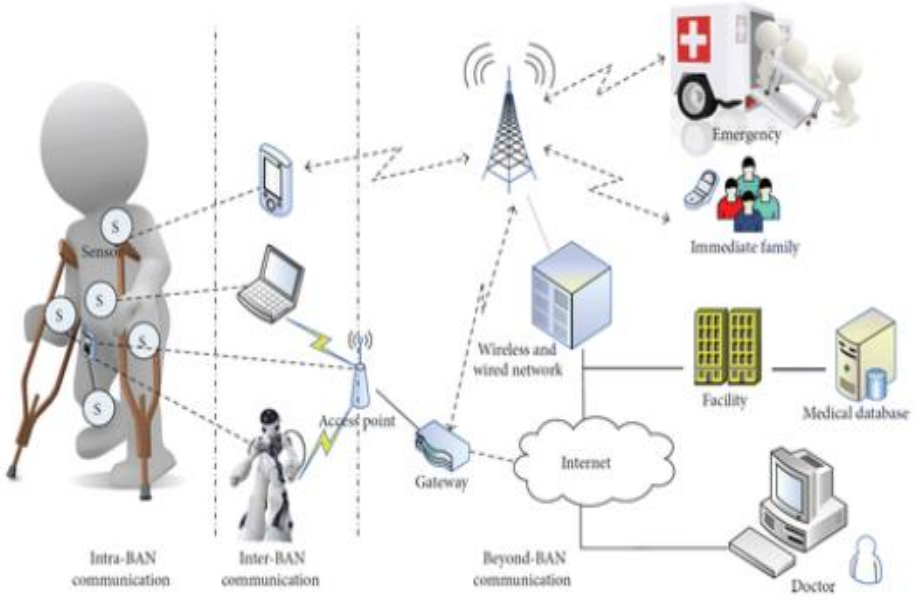

Figure 1.1 Health monitoring system based on WBANs

Figure 1.1 explains the health monitoring system depending on the WBANs by [12]. The WBANs communication architecture is divided into three parts: the intra-BAN communication, the inter-BAN communication, and the beyond-BAN communication [13]. The intra-BAN communication refers to wireless communication within 2 meters around the person. It is possible to realize the communication between the sensors and make the body sensor and personal server communicate. The WBANs are different from WSNs; they are less likely to work independently, so the inter BAN communication refers to the communication between a PS (personal server) and an AP (access point). That is, the interconnection between

BANs is realized by a common network, such as Internet and mobile communication network. The beyond-BAN communication is mainly used in the implementation scope of metropolitan area connectivity. The communication is designed according to the concrete application and the user's specific requirements.

This chapter gives a presentation of the background information needed to understand the WBAN issues along with the important challenges that must be addressed in data security and critical applications and solved within the scope of this thesis. For this, we present in the next section the major challenges that should be faced by the engineering tasks in WBANs and we provide a comparison between WSNs and WBANs. Then, we show the major differences between WBANs and WSNs and we give a comparison between the characteristics of these two networks. We, also, discuss the two fundamental functions of all sensor networks which are sensing and communicating. Subsequently the current standards for WBAN's communication are presented and compared. In addition, we describe the state of the art related to the research domains that are addressed within the scope of this thesis.

1.1.1 Wireless Body Area Network (WBAN): Challenges

Wireless Body Area Network (WBAN) has been developed mainly as an interdisciplinary area that allows inexpensive and continuous monitoring applications with real-time updates of sensors records using any ambient network (e.g., Bluetooth, Wi-Fi, UMTS, 3G, and 4G). The challenges faced by WBANs are in many ways similar to those faced by wireless sensor networks (WSNs) [14]. However, there is a consensus among researchers that there are intrinsic differences between the two networks due to the complexity of human body's internal environment and the characteristics of the external environment surrounding the human body, which requires special attention. Some of these differences and properties are illustrated in Table 1.1 and summarized in the following.

First of all, the deployment of WSNs allows to monitor large-scale areas while with WBANs only an area limited to a few meters is used. In fact, due to concerns on health hazards, the transmit power should be limited and, consequently, the communication and transmission coverage of the WBAN would be limited. Second, the density and the number of nodes deployed in WSNs is higher than that in WBANs, where devices' redundancy are commonly not applied [15]. Third, due to their limited battery life, the body sensors in a WBAN are constrained by energy requirements.

Therefore, they should be small in size to be comfortably wearable without constraining users' mobility. In addition, the data generated by WBANs contains in general medical information having stringent temporal and Quality of Service (QoS) requirements when compared to WSNs. Fifth, the replacement and charging of implanted and wearable sensor nodes is generally difficult since it can lead to some human body discomfort. The monitoring of human body may be achieved by placing heterogeneous wireless devices strategically on the body [16]. These sensors will be used to monitor either specific human body parameters such as body temperature, blood saturation, oxygen level and localization or information related to user's surrounding environment such as the ambient temperature, the daily exposure to airborne pollutants, and the oxygen level. The WSN nodes are homogenous and deployed in order to perform similar sensing functions [17]. Compared to WSNs where the human intervention is, mostly, not possible, in WBAN such a task is possible rather unavoidable in some cases.

Table 1.1 Comparison between WBAN and WSN

Challenges	Wireless Sensor Network	Body Area Network
Scale	The monitored environment is a large-scale area (meters/kilometers)	The monitored environment is limited to the human body (centimeters/meters)
Number of nodes	Many redundant nodes for wide area coverage	Fewer, limited in space
Result accuracy	Large number of nodes provide accuracy	Few nodes, need to be robust and Accurate
Node tasks	Sensor nodes are homogeneous and perform a dedicated task (e.g., vibration sensors, multimedia sensors, etc.)	Nodes are heterogeneous and performmultiple tasks
Node size	Small is preferred	Small is essential
Network topology	Very likely to be fixed or static. Theycan be also integrated into unmanned items	More variable due to the human bodymovement and activity
Data rates	Most often homogeneous	Most often heterogeneous
Node replacement	Nodes are deployed in tight and unreachable areas that may not beeasily accessible by maintainers	Nodes are placed on the human body, hidden under clothing, or even implanted
Node lifetime	Several years or months	Several years or months, (smaller battery Capacity compared to WSNs)

Power supply	Accessible and can be replaced easilyand frequently	Inaccessible and difficult to replace if sensors are deployed based on an implantable setting
Impact of data loss	Likely to be compensated by redundant nodes	More significant, may requireadditional measures to ensureconstraining QoS and real-time data delivery
Human intervention	Not possible in most cases	Possible rather inevitable in some cases
Channel	Air, water, on ground, under ground	Air, vicinity/inside human body

1.1.2 Sensing Activity

Wireless sensor nodes are, in general, designed to perform specific activities in terms of sensing, data collection, processing, and wireless transmission. The architecture of a typical wireless sensor node with its sub-systems is illustrated in Figure 6. A power generator can potentially be used to autonomously power the sensor node or to harvest energy from the environment surrounding the sensor (e.g., solar energy).

Sensing is a fundamental task to all sensor networks that mainly consists of sensors and an analog to digital conversion (ADC) unit that is responsible for converting the physical sensed phenomena into digital signal form [18] as in shown in the figure 1.2. The quality of sensing depends heavily on technological advances in signal conditioning, micro-electromechanical systems (MEMS), and nano-technology. The sensors respond to a physical stimuli event (e.g., vibration, high temperature, shortness of breath or decreased heart rate), gather data on this event, process the data (if necessary) and then report wirelessly this information to a remote destination.

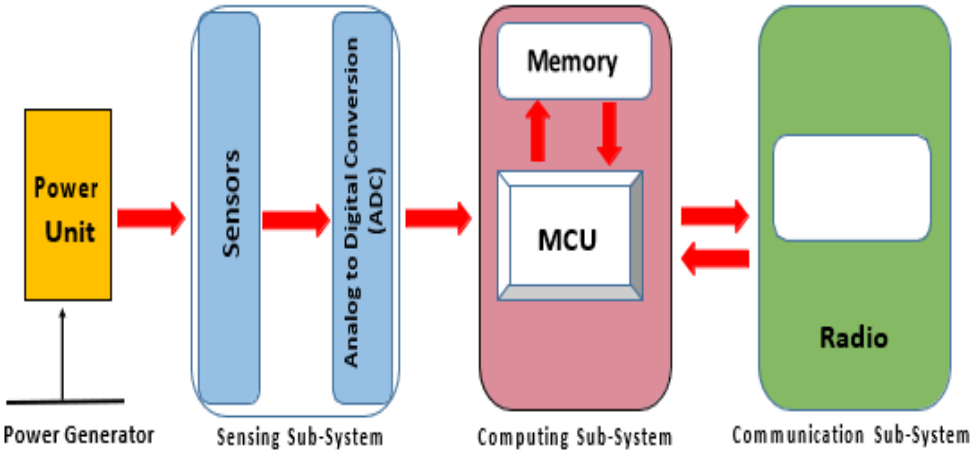

Figure 1.2. Sensing Compounds

The sensors used in WBANs are in general physical sensors which capture physical data regarding the human body functions, body environment, and even objects of interest to the body. These sensors are organized into three main categories, namely Physiological sensors, Motion (Bio-kinetic) sensors, and Environmental sensors. Following, the description of these three types is given:

- The physiological sensors: They include temperature sensors, microphones, touch sensors, light sensors, and biosensors [19]. They are used for measuring the human body's functions (e.g., blood pressure, body temperature, electrocardiography (ECG), electroencephalography (EEG), and electromyography (EMG).
- The Bio-kinetic / Activity sensors focus on measuring the location, the number of footsteps, the acceleration, the length of walked distance, and the angular rate of rotation derived from a moving object or person. Bio-kinetic sensors range from economical devices (e.g., pedometers) to complex implementations including gyroscopes and accelerometers that are attached on specific parts of the body (e.g., arm, thigh, ankle, and waist)
- The Environmental / Ambient sensors measure physical phenomena related to their surrounding environment, such as humidity, vibration, light, sound pressure level, and ambient temperature. These sensors can be either integrated into items and clothes, or terrestrially deployed (on the ground or in underground) to detect sudden environmental phenomenon.

The combination of physiological, activity and environmental sensors is of great interest in monitoring applications to provide a complete protection for both

individuals and environments. For example, when monitoring first responders and firefighters in their workplaces, one would be interested in using: (i) environmental sensors to measure the level of toxic gases in the air and the presence of hazards; (ii) physiological sensors to monitor vital signs and stress levels; and (iii) activity sensors to track motion and human behaviors. Some of the most widely used ambient and environmental sensors used in smart environment monitoring applications are summarized in Table 1.2.

Table 1.2. Ambient Sensors used in Smart Environment Monitoring

Sensor	Measurements	Data formats
Passive Infrared Motion Sensor (PIR)	Motion	Categorical
Active Infrared	Motion / Identification	Categorical
Radio Frequency Identification (RFID)	Object information	Categorical
Pressure	Pressure on mat, chair, etc.	Numeric
Magnetic Switches	Door/Cabinet (Opening/Closing)	Categorical
Ultrasonic	Motion	Numeric
Camera	Activity	Image
Microphone	Activity	Sound

1.2 WBAN ARCHITECTURE

This section explores architectural issues related to WBAN systems. To this end we describe the main activity of such technology, which is sensing performed by the set of sensors devices attached to the human body and we explain how communication between those devices is achieved.

1.2.1 Sensor nodes classification

WBANs will facilitate the early identification, monitoring and management of potentially hazardous phenomena including diseases of many types in healthcare applications, fire detection during a firefighting mission, loss and disorientation of first responders during a disaster-aid intervention. The elementary sensor nodes can be further classified into three subcategories; namely, the implanted medical sensor, wearable medical sensors, and wearable non-medical sensors. These subcategories are described in the following and some examples are provided in Table 1.3.

The several sensors are elementary devices that communicate with each other

through wireless or wired media and send their readings to the WBAN coordinator node. The latter forwards the data towards sink nodes to their destination (e.g., the terminal base station). The sink node is considered as a gateway that enables the relaying of sensors' readings to other networks such as a WSN and the internet. In some applications, the sink is part of the network; whereas in others it is an external element that enquires and requests information from the network. Figure 1.3 illustrates a simplified architecture of a WBAN in which several types of sensors are used including environmental sensors, physiological sensors and activity sensors.

Table 1.3. Characteristics of implanted/wearable sensors

Sensor Type	Sensor Node	Power Consumption	QoS (Stringent Delay)	Privacy
Implanted (Medical Sensors)	Glucose Sensor	Extremely Low	Yes	High
	Pacemaker	Low	Yes	High
	Endoscope Capsule	Low	Yes	Medium
Wearable (Medical Sensors)	ECG	Low	Yes	High
	SpO2	Low	Yes	High
	Blood Pressure	High	Yes	Medium
Wearable (Non-Medical Sensors)	Music for Headsets	Relatively High	Yes	Low
	Forgotten Things Monitor	Low	No	Low
	Social Networking	Low	No	High

1.2.2 Communication architecture

The WBANs have a particularly hierarchical communication nature. A typical WBAN encompasses multiple elementary sensor nodes that are deployed on the human body and can be either implanted or wearable devices. The WBAN also includes a main node (i.e., a coordinator) that is responsible for controlling the network and collecting all the sensor data from the elementary sensors. The collected data should then be relayed to its destination (i.e., the network control center) via a gateway in a prompt and reliable way. The deployed sensors capture continuously large quantities of data, which must be properly processed to extract the required information. Data processing must be hierarchical to exploit the asymmetry of resources, preserve system efficiency, and ensure that data is available when needed.

In general, WBANs support three types of communication; namely, intra-WBAN communication, inter- WBAN communication, extra-WBAN communication. These different levels for communication are illustrated in Figure 1.3 and Figure 1.4.

- The Intra-WBAN communications refers to the communication between the different sensors implanted or attached to the human's body and/or between body sensors and the WBAN coordinator. The latter is also attached to the human's body in order to locally process the collected data and manage the elementary sensing devices. Often, a WBAN is organized into a star network where sensors nodes send their collected data to the coordinator WBAN node [20].
- The Extra-WBAN communications is used in order to enhance the reliability performance of the application and the coverage range of the system [21]. To enable prompt and reliable transmission and relaying of data collected from the WBANs to a remote data center, the WBANs interact with the external environment through a plethora of technologies, such as a personal digital assistant (PDA) device or a mobile phone equipped with wireless personal area networking, wireless sensor network (WSNs), vehicular networks (VANET), wireless local area networking (Wi-Fi) capabilities, or cellular data services (GPRS, 3G, and 4G).
- The Inter-WBAN communications refers to the communication between two or more WBANs [22]. In every WBAN, the main node plays the role of a cluster head (CH), which is responsible of collecting all the data from elementary sensor nodes and forwarding this data to the remote-control center, through any ambient network (e.g., WIFI, 3G, and 4G). However, due to users' mobility and the incomplete availability of communication infrastructure in hazardous environments and rural areas, relaying the collected data in a reliable way is hard to achieve. Inter-WBAN communication includes the communication between CHs and exploits cooperative and multi-hop communication to provide reliable end-to-end data transmission in case of out-of-coverage or unavailable network infrastructures [23].

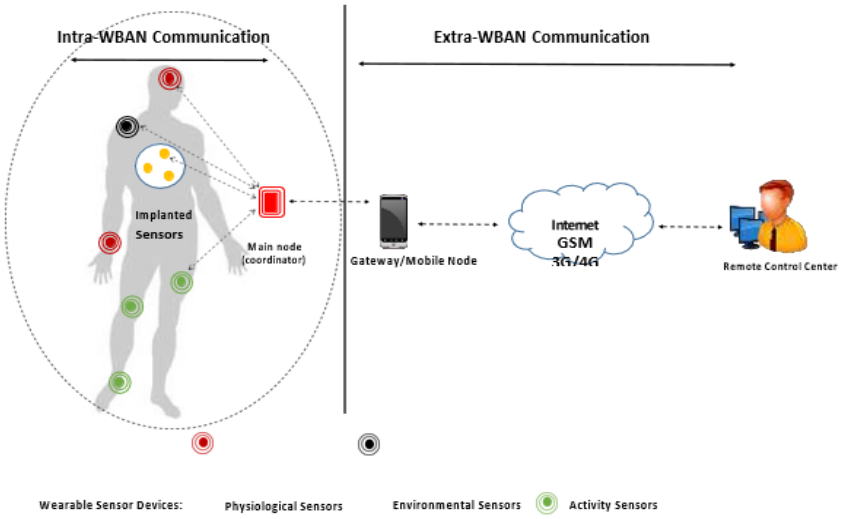

Figure 1.3. Intra-WBANs and Extra-WBANs Communication Architecture

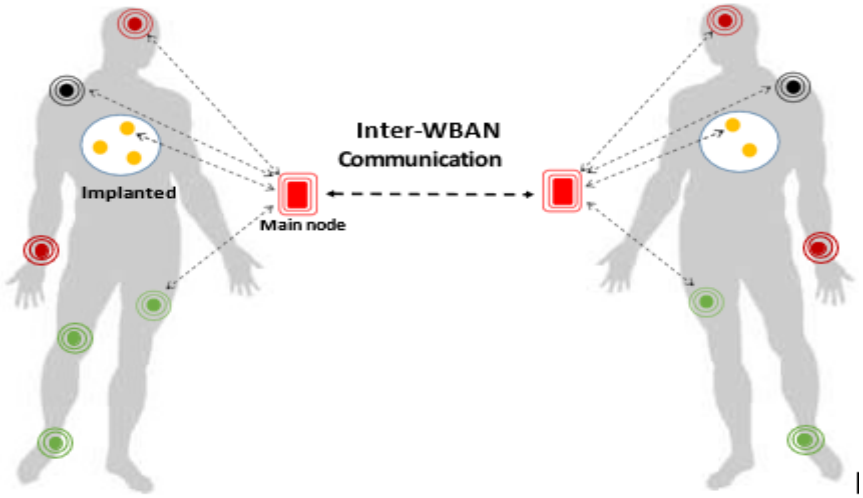

Figure 1.4. Inter-WBAN Communication Architecture

1.2.3 Toward the Need of a Cluster-based Network Organization

The deployment of WBANs in large-scale monitoring applications faces many limitations in terms of data reliability, constrained sensors' energy, and the users' mobility. The need for efficient data collection and aggregation in such circumstances necessitates the organization of a network topology that enables the extension of the network lifetime as shown in the Figure 1.5. Network clustering approaches has proven to be an effective solution for organizing energy constrained sensor networks by minimizing the energy consumption and reducing the communication costs. Clustering techniques aim at gathering data among groups of elementary sensor nodes, which elect their leaders (the cluster head node) among themselves. The latter is mainly a powerful node compared to elementary sensors that is in charge of performing data aggregation and communication to the terminal base station (BS).

A data flow scenario in a clustered network is illustrated in Figure 9. WBAN nodes are partitioned into groups called clusters. Each cluster has a number of member nodes and a main coordinator, referred to as a cluster head (CH). WBANs in the same cluster may work independently (i.e., organized in a star topology) or cooperate together (i.e., organized in an Ad-Hoc network) to collect periodic or streamed data about the phenomenon of interest. The WBANs (i.e., member nodes) send their collections (e.g., temperature and humidity) in a real-time manner to the CH. The CH aggregates the collected data and sends it to the terminal base station directly or using multi-hop communications.

Since WBANs have limited bandwidth, the performance of the monitoring system may suffer and be degraded when multiple WBANs coexist in close vicinity and occupy the same channel at the same time [24]. This also causes received signal strength to decrease reducing channel capacity. In addition, the WBAN may suffer from severe channel interference that degrades the communication performance of each WBAN. Consequently, the ratio of the number of incorrectly transferred data packet and referred to as packet error rate (PER) increases and the total number of successfully transmitted packets, and referred to as packet reception ratio (PRR) decreases. Therefore, the coexistence problem increases packets retransmissions and delay [25], which decrease the channel utilization rate. Thus, it is important to implement predictive mechanisms that allow to avoid and minimize the impact of WBAN coexistence problem.

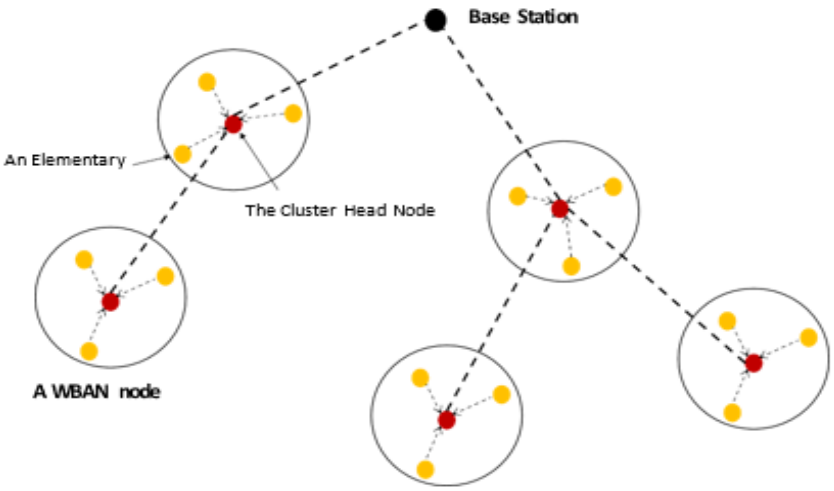

Figure 1.5. A Cluster-based Network Topology

1.3 CURRENT STANDARDS FOR WBANS COMMUNICATION

Current candidate technologies for BANs in the field of wireless short-range connectivity include IEEE 802 family of wireless personal area networks (WPANs) and wireless local area networks (WLANs), Bluetooth, and ZigBee. These technologies are covered and discussed in this section and a comparison between them in Table 4 is provided. The comparison is built over a set of common criteria, such as: frequency bands, bandwidth, data rate, Transmission power, communication range, and network cost as shown in the Table 1.4.

IEEE 802.11 - WLAN/Wi-Fi: is a set of low tier, terrestrial, network technologies for data communication. The WLAN standards operates at the 2.4 GHz and 5 GHz Industrial, Science and Medical (ISM) frequency bands [26]. The IEEE 802.11 operates on three main bands. A low band that has a maximum transmission power of 50 mW, the middle with a maximum of 250 mW, and the high band with a maximum of 1 W. The wireless standards such as 802.11a, 802.11b, and 802.11ac have their own pros and cons that make the use of Wi-Fi inadequate to support real-time monitoring and large-scale BANs. For example, while the 802.11a provides a fast maximum speed and regulated frequencies to prevent interference from other devices, it is characterized by a high cost and a small range that can be easily obstructed. Also, although the 802.11b has a low cost and provides a good signal range, it frequently suffers from interference with WLAN transmissions. The low-power Wi-Fi is another wireless technology that has been recently investigated in wireless sensors applications. It was modified from the original IEEE 802.11 standard in order to include lower cycling operation, transmission power, and other energy-saving options [27]. The huge number of devices using the Wi-Fi technology, which are frequently used at home, work, hospitals, smartphones, and enterprises has promoted the advances in low-power Wi-Fi. A reason for promoting the use of low-power Wi-Fi in integrated and wearable sensing technologies is to empower the concept of Internet of Things (IoT) [28], which makes it also a promising technology for WBANs applications [29].

Bluetooth / IEEE802.15.1: The second wireless option is the IEEE 802.15.1 (Bluetooth) standard [24]. Bluetooth technology was designed as a short-range wireless communication standard, and later widely used for connecting a variety of individually carried devices to support data and voice applications. It was mainly

adopted in the implementation of healthcare and telemedicine applications [19, 22, and 24]. Bluetooth devices operate in the 2.4 GHz ISM band, utilizing frequency hopping among 79 1 MHz channels at a nominal rate of 1,600 hops/sec to reduce interference [22]. The major drawback of the Bluetooth technology consists in the fact that its properties including the high bandwidth requirement and small size networks are not appropriate to support high-speed data transfers, long functioning time for sensor devices and multi-hop communication. Such a drawback makes Bluetooth standard unsuitable for WBANs applications. Bluetooth Low Energy (BLE) [30] is a derived option of the Bluetooth standard. It was introduced as a more suitable solution for WBANs applications where less power consumption is enabled using low duty cycle operation. Unfortunately, additional challenges are added when low duty cycle is improperly used to save energy. This makes BLE inappropriate for critical monitoring applications (i.e., healthcare) that require frequent data reporting.

Table 1.4. Comparison of the existing wireless technologies for WBANs

	IEEE802.15.6	**ZigBee IEEE802.15.4**	**Bluetooth IEEE802.15 .1**	**WLANs IEEE802.11 b/g**
Frequency bands	3-10 GHz	2.4 GHZ	2.4 GHz	2.4 GHz and 5 GHz
Bandwidth	>500MHz	2 MHZ	1 MHZ	20 MHZ
Data rate	100-500 Mbps	250 kbps	1 Mbps	11 and 54 Mbps
Transmission power	- 41dBm	0 dBm	4 dBm 20 dBm	250 mW
Coverage	3m	70-100m	10m	100 m
Power Requirements	Low	Low	Medium Low (for BLE)	High
Network topology	Point-to-Point	Ad-hoc, peer-to-peer, star or mesh	Ad-hoc, very small network	Infrastructure (point-hub)

ZigBee / IEEE802.15.4: Currently the most widely used radio standard in WBANs is IEEE 802.15.4 (ZigBee). When compared to Bluetooth, ZigBee standard offers larger coverage area and better performance under interference. It targets low-data-rate and low-power-consumption applications.

Specifically, ZigBee/IEEE 802.15.4 devices can operate in the ISM bands, with data rates from 20 Kbps to 250 Kbps [20]. ZigBee supports three types of topologies-stars, cluster tree and mesh topology. ZigBee offers some advantages such as

supporting different network topologies, providing multi-hop routing in either a cluster tree topology or a mesh topology. Also, it consumes less power, processing and memory resources. It also provides security services. The maximum speed in ZigBee standard is 250 Kbps at 2.4 GHz to increase the batteries life. In addition, it has a low cost due to wide industry acceptance and adoption. However, the 250 kbps (data rate) is inadequate to support real-time monitoring for large- scale WBANs since it causes larger delivery delays [22]. Such a problem is critical in applications carrying urgent data (e.g., medical and firefighting applications). Also it can suffer from interference with WLAN transmissions. Therefore, ZigBee is not scalable in terms of power consumption and does not provide adequate QoS for all WBANs applications.

IEEE802.15.6: Given limitations reported for the aforementioned standards (i.e., WLAN, Bluetooth and Zigbee), there was a need to develop new standards that match the requirements of WBANs and operate properly with the targeted applications. In this context, the IEEE 802.15.6 WBAN standard was proposed as a promising wireless technology for low power WBAN devices. It provides short-range communications around or inside a human body, nonetheless it is not limited to humans. It also defines interferences awareness mechanisms what gives an improved coexistence with other wireless communication standards. The proposed standard uses different frequency bands for data transmission, namely the Narrowband (NB), the Ultra-Wideband (UWB), and the Human Body Communication (HBC): (i) The NB contains the 400, 800, 900 MHz and the 2.3 and 2.4 GHz bands; (ii) The UWB implements the 3.1–11.2 GHz; and (iii) The HBC includes the frequencies within the range of 10–50 MHz The IEEE802.15.6 is applicable in medical applications (Wearable only BAN, Human performance management, and Implant BAN) and non-medical applications (Real Time Video /audio Streaming, Data file transfer & Stream transfer, and Entertainment) [24]. The shorter range of UWB technology, compared to the previously introduced standards proves to be an advantage, as shorter transmission has lower power requirements, the equipment can be of smaller size and misuse is limited. In addition, it considers the minimization of the specific absorption rate (SAR) into the human body and the optimization of the battery life by allowing sensing devices to operate on very low transmit power for safety. However, some of the supported frequency bands are not suitable for WBANs applications since they do not support voice or video (e.g., HBC) or their use is only eligible by authorized users

(e.g., UWB). In addition, IEEE 802.15.6 is currently only draft standard and certain details may change when it is published.

1.4 SECURITY AND PRIVACY REQUIREMENTS OF WBANS

WBAN systems require certain security measures to guarantee security, privacy, data integrity and confidentiality of a patient's health records at all the times. A supporting WBAN infrastructure must implement specific security operations that guarantee all of these features [31]. Security and privacy of patient information are the two crucial features for within each WBAN system. Security implies data is protected from unauthorized users when being transferred, collected, processed and remains safely stored. On the other hand, privacy suggests the authority to control the gathering and usage of one's personal information. For instance, a patient may require his details to not be shared among insurance companies who could use this information to restrain his/her from the coverage. More specifically, mission-critical data within a WBAN system is extremely sensitive, that if leaked to unauthorized personnel could lead to several consequences for the patient such as losing the job, public humiliation and mental instability. Another example, when the intruders access information, through physically capturing the node and change the information; and therefore, false information will be passed to the physician that may result in a patient's death. Someone can use the individual's medical data to seek out the personal rivalries with the patient [32]. Consequently, more attention should be given and taken to protect this sensitive and critical information from unauthorized access, use and changes [33]. Figure. 1.6 illustrates a secure mechanism of the data collection and various points of the networking including the final where the data can be retrieved by only the authorized person and through personal identification means of decryption.

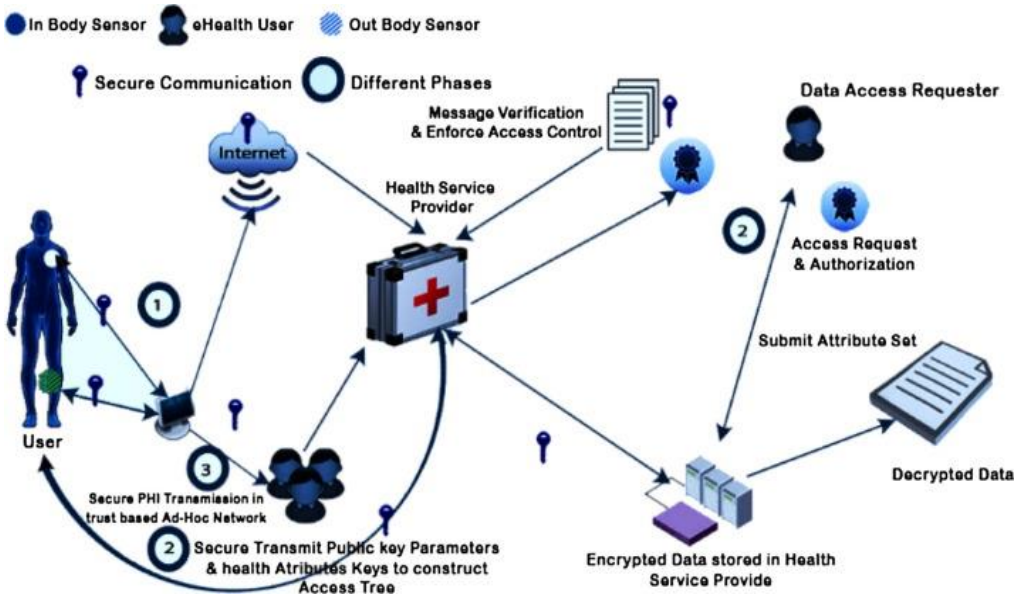

Figure 1.6. Security and privacy in a WBAN system.

The major security and privacy requirements to ensure the safety of a WBAN system and its extensive acceptance by its users are outlined as follows:

1. Data Confidentiality: Data confidentiality denotes the protection of a confidential data from exposure that is considered as the vital issue in a WBAN. Since WBAN nodes applied in medical situations are expected and relied upon to transmit delicate and private information about the status of a patient's well-being, hence their data must be protected from unauthorized access that could be hazardous to the patient's life [32, 33]. This important, transported data can be "overheard" during transmission that can either damage the patient, the provider, or the system itself. Encryption can provide better confidentiality for this sensitive data by providing a shared key on a secured communication-channel between secured WBAN nodes and their coordinators [34, 35].

2. Data Integrity: Data integrity refers to the measures taken to protect the content of a message, its accuracy and consistency. It applies to both single messages as well as streams of messages [36, 37]. However, data confidentiality does not protect data from external modifications, as information can be illicitly changed when data is transmitted to an insecure WBAN as an adversary that can easily moderate the patient's information before reaching to the network coordinator. More specifically, modifications can be simply made by integrating some fragments, manipulating data within a packet, and then forwarding the packet to the PS. This

interception and modification can lead to serious health concerns and even death in extreme cases. Consequently, it is imperative that the information not be accessible and altered by a potential adversary by applying authentication protocols.

3. Data Freshness: Data freshness techniques can effectively make certain that the integrity and confidentiality of data are protected from recording and replaying older data by an adversary and confuse the WBAN coordinator. It ensures that old data is not recycled and that its frames are correct. There are two types of data freshness are currently in use: Strong freshness promises delay in addition to frame ordering; and weak freshness which is limited to frame ordering, but does not provide any delay guarantees. Strong freshness is required for synchronization when a beacon is being conveyed to the WBAN coordinator and weak freshness is used for WBAN nodes with a low-duty cycle [32, 33].

4. Availability of the network: It insinuates a medical practitioner with efficient access to a patient's information. Since such a system carries important, highly sensitive and potentially lifesaving information, it is paramount that the network is available at all the times for patients' usage in case of an emergency [36, 37], For this, it is essential to switch the operations to another WBAN in case of availability loss occurs [31].

5. Data Authentication: Medical and non-medical applications may require data authentication. Thus, nodes within a WBAN must be capable to verify that the information is sent from a known trust center and not an imposter. Therefore, the network and coordinator-nodes for all data calculate Message Authentication Code (MAC) by sharing an undisclosed key. Accurate calculation of a MAC code, assures the network coordinator that the message is being conducted by a trustworthy node [38, 31].

6. Secure Management: To deliver key distribution to a WBAN, the decryption and encryption operation requires secure control by the coordinator. The coordinator role is to add and remove WBAN nodes in a secure way during node association and disassociation [38].

7. Dependability: The system must be reliable and dependable. A failure in retrieving the correct data represents another critical concern in WBANs as it may become a

life-threatening matter for the patient [39]. In order to address this issue, error-correcting code techniques can be used [40].

8. Secure Localization: Most WBAN applications need correct estimation of the patient's location. Lack of tracking methods could let an attacker to transmit improper details such as, by replying with a fake signal about the patient's location [38, 37]. Authors in [41] discussed about localization systems and their attacks.

9. Accountability: In the medical field, it is necessary for healthcare providers to safe guard patient health information [43]. If a provider does not secure this information, or worse, abuses his or her responsibility for it then he or she should be made accountable for this to discourage additional abuses [42]. The author in [44] discussed the accountability problem and proposed a technique to defend against it.

10. Flexibility: The patient needs to have the flexibility of designating AP control of medical data within a WBAN. For instance, in the case of an emergency, authorization to interpret patient's data could be given on demand to a different physician who is not necessarily listed as having permission [44]. In other example, if a patient changes the hospital or a physician it should be possible to transfer the access controls.

11. Privacy rules and compliance requirement: The need to secure private health information is a global concern. One of the most important privacy measures is to set out rules/polices for whom have the right to access patient's sensitive data to protect the patient's privacy. Several regulations and acts are enlisted in health care provisions. Currently there are different sets of regulations/polices for privacy all over the world. The American Health Insurance Portability and Accountability Act (HIPAA) is comprised of a set of directions to for doctors, healthcare providers, and hospitals and is designed to ensure that an individual's health and medical records are secure [45, 46]. HIPAA outlines detailed precautions that must be taken to safe guard patient data when used for administrative or communication needs. The Act provides for both civil and criminal consequences, including a fine as much as $250,000 and/or imprisonment for 10 years if a provider shares private information for monetary gain [37].

Medical health providers are obligated under the Act to ensure that their systems and their associates pursue the following rules and guidelines [45]:

- That the system is secure and confidential and that patient's health information is secured and properly formatted.
- Provides protection against any infrequent of security, confidentiality and integrity when they occur.
- Provide protection against unauthorized access to or usage of the patient's health information. HIPPA Act additionally regulates some other critical areas like:
  - ✓ Securing patients health records, in particular from those who do not need the information.
  - ✓ Establish systems that need user identification from both consumers and medical staff.
  - ✓ Only authorized person has the right to access sensitive data and applications.
  - ✓ Ensure integrity of patient health information throughout its life cycle within the system.

The HITECH Act, or Health Information Technology for Economic and Clinical Health Act, expands on how information technology can safely be used to collect, store, share and use sensitive patient information. The Act notes that those who are custodians of patient health information must contact the person affected if a security issue arises [47]. All this is a good example of how such rules and regulations should be enacted at a larger scope if any country adopts the WBAN technology. There are special conditions, for example a disaster or medical emergency that may require the divulging of patient health information to first responders [46]. Table 1.5 shows the major security threats, security requirements and the possible security solutions when using a WBAN.

Table 1.5. Security threats and possible security solutions in WBAN.

Security threats	Security requirements	Possible security solutions
Unauthorized access	Key establishment and trust setup	Random key distribution and public key cryptography
Message disclosure	Confidentiality and privacy	Link/network layer encryption and Access control
Message modification	Integrity and authenticity	Keyed secure hash function and Digital signature
Denial of Service (DOS)	Availability	Intrusion detection systems and redundancy
Compromised node	Resilience to node compromise	Inconsistency detection and node revocation and Tamper – proofing
Routing attacks	Secure routing	Secure routing protocols
Intrusions and malicious activities	Secure group management, Intrusion detection Systems and secure data aggregation	Secure group communication
		Intrusion detection systems

1.5 WBAN SECURITY THREATS

WBANs are vulnerable to a huge number of attacks and threats. WBAN are frequently open to several external threats and intrusions, which could hack into the network as shown in Fig. Thus, security and privacy issues should be addressed very well, attacker may target the availability of a WBAN by capturing or incapacitating a particular node, which sometimes results in loss of a patient's life [36]. For example, the adversary can capture or incapacitate an EEG sensor and sends the false information to the physician. This could result in a hazardous life-threatening situation or even a death. An adversary can also use jamming and tampering. Jamming (radio frequency interference) can be used by an adversary on a few nodes to block the entire network [34]. This method cannot block large networks, but since WBANs are generally small networks, not only chances of network blocking are quite high, but also lead to packet loss. In fact, an adversary sometimes physically tampers WBANs. It is possible that an attacker could electronically interfere, damage, or supplant the WBAN to acquire a patient's personal health information. It can also use a flooding technique to exhaust the memory by repeatedly sending extra unnecessary packets,

which the system is unable to handle. This prevents the legitimate users of the network to access the services or the resources [32]. It can be done through Denial of Service (DoS) attack that is meant not only to disrupt, subvert and destroy the network, but also to diminish the network's capability of providing the necessary emergency services [31], [33]. Table 1 typically shows the security threats and possible security solutions that can be used in WBAN.

1.5.1 The Current Security Measures

Security in WBAN is important and should not be ignored. This is sensitive medical information is sensitive and must be protected and kept same at all times from unauthorized people who may use the data that may be harmful to the individual. Several security solutions for WBAN have been proposed and they are as follows.

1.5.2 TinySec

TinySec represents as a solution to attain link layer encryption and authentication of the data in biomedical sensors networks. This technique is link-layer security architecture for WSNs and is officially part of TinyOS release. In this system, a group key is used between sensor nodes, with secure encrypted data packets and a MAC being calculated for the entire packet. It relies on a single key by default, which is manually programmed into the sensors nodes before they are deployed. This provides a minimum level of security and cannot protect against physical node capture, since it is shared [42].

1.5.3 Biometrics

This method is widely used to secure communication in biomedical sensor networks using biometrics. The method advocates employing of self-body as a way to manage cryptographic keys for sensors that are attached to the user's body. If the measuring value such as EEG is same from using two different sensors of the body, it will generate a key that can be used distribute the symmetric key securely, either encrypted or decrypted [34], [35].

1.5.4 IEEE 802.15.4 and IEEE 802.15.6 security protocols

Under this system, security suites are implemented under the IEEE 802.15.4. The security suites are categorized into two essential modes: secured and unsecured mode. Unsecured mode means that no security suite has selected. The standard defines 8 unique security suites. The first one is the Null suite that gives no security, while the others are categorized according to the different security levels. A detailed description

of this standard can be found in [36]. Further, in 2012, the better version, IEEE 802.15.6 standard was approved [37]. This most current standard strives to provide an international norm for reliable low power, short range wireless communication in and around a human body. It supports a wide range of rates varying from narrow band (75.9 Kbps) to ultra-wide band (15.6 Mbps), depending on the need [48].

1.5.5 ZigBee security services

ZigBee came together as conglomerate of industry players to give a new meaning to ultra-low power wireless communication. The (NWK) ZigBee network layer defines supplementary security services including processes for authentication and key-exchange in addition to IEEE802.15.4. The ZigBee standard identifies a trust center of which some of the coordinator responsibilities are, to allow nodes to join the network and distribute keys [49].

1.5.6 Bluetooth security protocols

It comprises of various protocols such as Baseband, Link Manager Protocol (LMP) and Logical Link Control and Adaptation (L2CAP). The baseband enables the link between Bluetooth devices and exchange the data in form of packets. LMP is responsible for security issues like encryption, authentication, and exchanging the encryption keys. The L2CAP can support higher level of multiplexing and packets reassembly which can help in providing quality of service communication [50].

1.5.7 Wireless security protocols

Various security protocols are developed to protect the wireless network such as Wired Equivalent Privacy (WEP), Wi–Fi Protected Access (WPA) and Wi–Fi Protected Access version 2 (WPA-2). The original encryption protocols that was developed for wireless network was WEP. It was having many security flaws so WPA and WPA-2 replaced it. WPA use a pre-shared key (PSK) and a temporal key Integrity Protocol (TKIP) for data encryption. The advanced version WPA-2 uses Advanced Encryption Standard (AES) for encryption that is more secure and reliable.

1.5.8 Hardware encryption

Rather than using a software-based encryption as in TinySec, hardware encryption is implemented by use of a ChipCon 2420 ZigBee compliant RF Transceiver. The CC2420 is capable of executing IEEE 802.15.4 security operations with AES encryption by utilizing 128-bit keys. The operations utilize a counter called, CTR, mode of decryption and encryption [47].

1.5.9 Elliptic curve cryptography

This method has appeared as a feasible choice for public key cryptography in WBAN. The primary use of using Elliptic Curve Cryptography (ECC) lies in its features offering high computation, small key-size, and compact signatures. Although the energy requirements are still significant then the other contemporary system provides an alternative for high system security [51].

1.5.10 Encryption techniques

WBAN can be provided the necessary security by deigning the network to encrypt the whole data with different keys. It offers high form of security by three different mechanisms following which an effective encryption can be achieved, Symmetric key encryption, Conventional Public Key Encryption and Identity Based Encryption [50].

1.6 AUTHENTICATION WITH DIGITAL SIGNATURES

One of the most well-known and widely used cryptographic authentication mechanisms is a digital signature. It is often viewed as a cryptographic analog of a handwritten signature and belongs to mechanisms that use techniques of asymmetric or public-key cryptography. We will give a short introduction to digital signatures, highlight their use in public key infrastructures, and discuss some privacy limitations.

1.6.1 Digital Signatures

The basic concept of digital signatures involves a signer and potentially many verifiers. The signer is given the ability to sign arbitrary messages or documents. For this purpose, the signer is in possession of some secret information, his private key sk, which is usually bound through some strong mathematical relationship to the signer's public key pk. This public key uniquely identifies the signer amongst other parties, i.e., pk serves as a cryptographic identity of the signer and is used by verifiers to check the validity of digital signatures that were generated by the signer. A digital signature scheme is represented by three main algorithms:

Key generation. The key generation algorithm Kg is executed by the user initially to setup own private/public key pair (sk, pk). The private key sk is kept secret by the user, whereas the corresponding public key pk is made public, for example distributed to all potential verifiers.

Signature generation. A user in possession of a key pair (sk, pk) can apply the

signature generation algorithm Sign to produce a digital signature σ on some message m.

Signature verification. Through the verification algorithm Vrfy any verifier can check the validity of a signature σ on the given message m using the public key pk of the purported signer. This algorithm decides whether σ is valid or not.

Digital signatures are already widely used today to ensure authenticity of the signer and his data for example to establish authenticated channel to some web server over a public network, or as a tool for enforcing access control to a distant service, network, or any other resource, or as an authorization mechanism for securing the patient data transactions, e.g. in healthcare sector, or simply for ensuring the integrity and proving the source of origin for digital documents created and distributed by the signer.

1.6.2 Public Key Infrastructures

The most prominent application domain of digital signatures is in the construction of modern public key infrastructures (PKI), where the primary goal of digital signatures is to establish an authentic link between the cryptographic identity (i.e. public key) of some entity, possibly of a human user or some digital device, and other (non-cryptographic) identities (or attributes) of this entity, such as the real name, email address, role within some organization, domain name, etc. This link can be established by the means of certification that reflects the existing trust relationship between the issuer of the digital certificate and the certified entity.

1.6.3 Digital Certificates

In its very basic form, a digital certificate certA→B is a signature generated by A in possession of the key pair (skA, pkA) on a message containing (B, pkB), i.e., the non-cryptographic identity B and the public key of B. Whenever B presents (B, pkB, certA→B) to some third party (verifier) V, the latter can verify, whether certA→B is a valid signature of A on the message (B, pkB) using the public key of A. The underlying idea is that A is trusted by V not to certify invalid links between non-cryptographic identities and public keys. In this case valid certificate certA→B would convince V that B is the owner of pkB, or, in other words, that pkB is the cryptographic identity of B. This trust put into the digital certificate of B can further be limited in time, for example if A includes some expiration time t and thus signs the message (B,

pkB,t). A may also exclude the non-cryptographic identity of B from the signed message, in which case the issued certificate certA→B becomes anonymous.

1.6.4 Certification Authorities

In traditional public key infrastructures, the role of certificate issuers is exhibited by trusted certification authorities that are often organized into a certification hierarchy, with some root authority located at its highest level. Every certification authority CA(i), located at a lower level i, has a public certificate certCA(i−1)→CA(i) issued by the certification authority CA(i−1) from a higher level i − 1. The root authority CA(0) holds self-certified certificate certCA(0)→CA(0) , i.e. it uses own private key skCA(0) to sign its own identity CA(0) and the public key pkCA(0) . The root CA is trusted by all intermediate CAs and by all users of the PKI. Certification authorities located at the lowest level of the hierarchy are typically responsible for issuing the corresponding certificates to the actual PKI users. We observe that certification authorities need not to be organized into a hierarchy, i.e., it is sufficient to have a single CA for setting up the PKI. This CA would act at the same time as root CA and would also issue PKI certificates to the PKI users. Irrespective of how many CAs are involved into a PKI it is ensured that any PKI user A is in possession of the PKI certificate certCA(i)→A issued by some certification authority CA(i) of that PKI.

1.6.5 Revocation of Certificates

One of central properties of public key infrastructures is the ability of certification authorities to revoke PKI certificates that were issued in the past. There are many reasons, why PKI certificates may need to be revoked, even before the possibly indicated expiration time t. This may happen, for example, once the certified party A can no longer use its secret key skA associated to the PKI-certified public key pkA, because that key was lost, accidentally erased, stolen, or fallen to a cryptanalysis. Also, PKI certificate of some certification authority CA(i) may need to be revoked, either for the same reasons as PKI certificates of the users, or because CA(i) can no longer be trusted to perform certification in a correct way.

In general, each certification authority is responsible for the revocation of certificates that were issued by this authority. For this purpose, each CA(i) maintains a corresponding certificate revocation list crl(i) that it authenticates to prevent manipulations. This list is updated with unique identifiers (serial numbers) of certificates that were issued earlier and have to be revoked. That is, each certificate

issued by CA(i) usually contains some unique identifier and the link to a location, from which crl(i) signed by CA(i) can be obtained. Using the latest version of crl(i) any third party can check, whether some certificate issued by CA(i) has already been revoked, in which case this certificate will be treated as invalid.

1.6.6 Validation of Certificates

Any PKI user A, in possession of a key pair (skA, pkA) and certificate (A, pkA, certCA(i)→A) can use skA to produce a signature σ on some message m, and send (m, σ, (A, pkA, certCA(i)→A)) to the potential verifier V. In order to check whether A is the signer of m verifiers will perform several verification checks:

- ✓ check validity of σ using the public key *pkA*,
- ✓ check validity of the certificate *certCA(i)→A* using the public key of the trusted *CA(i)*, and
- ✓ check validity of certificates *certCA(i−1) →CA(i)* for all intermediate authorities *CA(j)* with $j = i - 1,..., 0$ using their respective public keys *pkCA(j)*

1.7 GROUP SIGNATURES: AUTHENTICATION WITH PRIVACY

Digital signatures stand in conflict with privacy, in particular with regard to anonymity of signers and unlinkability of issued signatures. On the other hand, their unforgeability authenticates the signer as the origin of the signed document. In order to achieve both authenticity and privacy it appears necessary to decouple public verification procedure from the information that would uniquely identify the signer. This can be done, for example, by assuming a group of potential signers and requiring that verification is performed with respect to the whole group.

A vital role in our lives is nowadays played by cryptography, mainly in information technologies, sometimes we even do not realize how relevant. We use it every time we communicate with our bank, we require secrecy during browsing the web, while sending an email to and there are also many other situations where we want to keep our data secret. Sometimes, we just want to hide our and addressee identity. Also, group signatures have inconsiderable importance, as it was mentioned, mainly in information technologies.

A digital signature is a computational technique in cryptography in order to facilitate the authorization of a digital message or document. A valid digital signature proves the receiver that the message was sent in by a valid sender, also the sender cannot lie about not having sent the message and that the information was not tampered in its course. This technique of cryptography is basically applied in software industry, financial transactions, and in cases of legal disputes where there is a necessity to track frauds or counterfeiting of information [51].

Extending the idea of digital signature schemes into groups, a new signature scheme i.e., group signature scheme, first introduced by Chaum and Heyst in 1991, provides authority to any group member to sign messages anonymously on behalf of the group. A client can verify the authenticity of the signature by using only the group's public key parameters. It must be computationally hard to identity of the group member so that he cannot be linked from a signed message or his signature. However, in the case of a legal dispute, the identity of a signer or member can be revealed by a designated entity i.e., the group manager. The major feature of group signature is the security of the information or the data that makes it more important as well as attractive for many real time applications, such as e-commerce, e-auction and e-voting, where the priority is privacy and anonymity of signer which is very much high and important for any organization. As mentioned above, group signature scheme was first introduced by David Chaum and Eugene van Heyst. They presented that time a new type of signature for a group of persons (of course, they do not have to be humans necessarily, but for example computers in the network, smart/sim cards etc.) satisfying the following properties:

1) None but members of the group only can sign messages;
2) The receiver of message can verify that the message received by him is signed by a valid authorized group member, but he cannot discover identity of group member making the signature;
3) If necessary, in case of legal dispute, the anonymity of the group member who signed the message is revealed.

Thus, as seen from the first and second property, one of the major points of the group signature scheme is to provide anonymity to its signers (i.e., group members). Every group member has a private secret key which enables him to sign messages, but

resultant signature maintains the secrecy of the identity of the signer. The third property tells, there is a higher entity (generally called group manager) who has the power and resources to track the signing member, or reveal the signer's identity by using a special algorithm. Revocation of members is supported by some systems as well i.e., where group member can be revoked (or disabled) without putting any affect the ability to sign of unrevoked members.

1.7.1 Motivation of Algorithms

A we know of digital signature and facilities it has provided regarding information security, so extending the idea of digital signature to group where we can parallelly authorize multiple information or documents and save time. Group Signatures have vital role in day-to-day corporate organizations' ecommerce applications. Increase in demand for a more secure and lesser complex Group Signature scheme has always been there. The scheme implemented by us provides these features. The use of elliptic curve cryptography increases the security the scheme by providing desired security level that is achieved by significantly smaller keys in elliptic curve system than in its counterpart- RSA system. Another significant advantage being in general, the algorithms used for encryption and decryption in ECC schemes are faster and can be run on machines that are less efficient.

1.7.2 Group-based Authentication

In the group-based authentication approach users can authenticate themselves on behalf of some group, rather than on the individual basis. That is, the authentication process does not disclose any information that could be used to identify some particular user. Since all disclosed information can only be linked to some group of users, group-based authentication is a suitable approach for achieving user privacy. With this approach users are considered as being authenticated if they can provide a proof of the group membership. Note that group-based authentication is often used for the purpose of access control, where individuals are often assigned to groups and permissions to access and operate on certain resources is granted based on these assignments. In our context we are interested however in group-based authentication techniques applied to digital signatures.

1.8 REQUIREMENTS OF GROUP SIGNATURE

The concept of group signatures, introduced by Chaum and van Heyst, adopts group-based authentication to achieve privacy of signers against potential verifiers. At a high level, group signatures implement the following idea: All potential signers are considered as members of some group. Each signer can issue a signature on behalf of the whole group. Such group signature is publicly verifiable using the public key of the entire group, which provides anonymity of the actual signer. However, there exists a dedicated, possibly trusted party, which can link the group signature to the identity of the signer.

Digital signatures stand in conflict with privacy, in particular with regard to anonymity of signers and unlink ability of issued signatures. On the other hand, their unforgeability authenticates the signer as the origin of the signed document. In order to achieve both authenticity and privacy it appears necessary to decouple public verification procedure from the information that would uniquely identify the signer. This can be done, for example, by assuming a group of potential signers and requiring that verification is performed with respect to the whole group.

A technique of authorizing the documents, messages or relevant information anonymously on behalf of group by any member belonging to it is termed as a group signature scheme, where the group consists of a manager and valid members shown in Figure 1.7. The integrity of sign is verified by a trusted verifier, where he is aware of the sign's correctness but not the identity of the signing member. This concept of group signature put forward by Chaum and Heyst which allows any member of a group to authorize message on behalf of the group. According to their scheme, the following policies must be included in any group signature scheme: Group members are only role persons to authorize the messages by signing them.

- The validation of the signature should be verified without the identity of the signer being revealed
- If a situation of necessity arises, the signature can be opened to reveal the anonymity of signer.

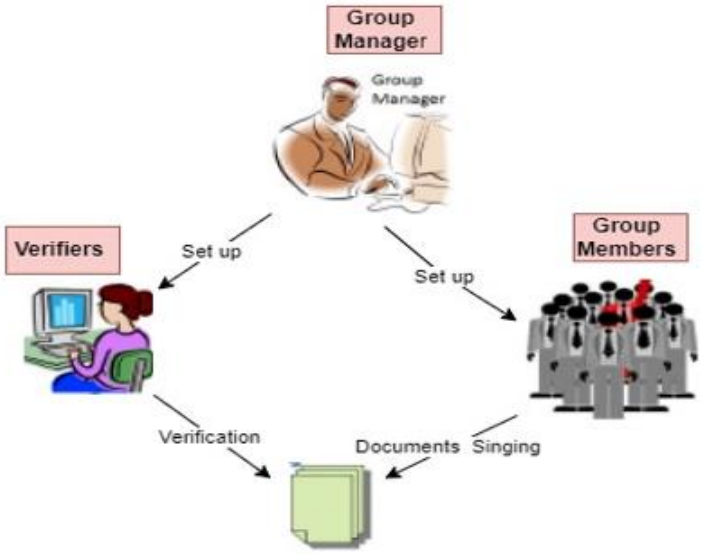

Figure 1.7. Layout of standard group signature system

1.8.1 Group Manager and Group Members

The architecture of a group signature scheme consists of the group manager and multiple group members. The group manager, which can either be a single authority or a coalition of several entities, is responsible for the initialization of the group, for the admission and in some schemes also for the revocation of group members. During the initialization process the group manager chooses own secret key and defines public group parameters containing the group public key. Once the group parameters are established the group manager can use own secret key to issue membership certificates to the prospective group members. In some schemes the group manager can further use own secret key to revoke existing group members from the group.

Each group member is in possession of a membership certificate issued by the group manager. This certificate represents the secret signing key of the respective group member. That is, each group member can use it to produce group signatures on arbitrary messages. Any verifier can publicly check the validity of some issued group signature using the group public key. The group signature thus proves that the signer belongs to the group.

The distinguished property of group signatures is that the group manager can open group signatures and identify their signers using the information collected during the admission process. In comparison to ordinary digital signatures, group signatures have extended security goals. In particular, the unforgeability requirement ensures that

only group members are able to issue valid group signatures. In addition, group signatures provide privacy by requiring that no other party, except for the manager of the group, should be able to identify the actual signer. Furthermore, group signatures should remain unlinkable, meaning that no party, except for the group manager, can link two or more signatures produced by the same signer. Also, the opening procedure performed by the group manager implies security requirements of its own to protect a group member from malicious accusations of having produced some group signature if this was not the case.

1.8.2 Differences to Digital Signatures and PKI-based Authentication

Authentication with group signatures reminds of PKI-based authentication, yet with some significant differences. One can see the role of the group manager as being related to that of a PKI certification authority. Indeed, the group manager issues membership certificates to new users and in some schemes also revokes their membership. The main difference to PKI certification is that membership certificates issued by the group manager are confidential and should never be disclosed by the corresponding group member.

Another difference to traditional digital signatures is that group members do not need to possess any public keys since verification of group signatures is performed with respect to the public key of the entire group, defined by the group manager during the initialization procedure. Observe that group signatures are nonetheless publicly verifiable.

The most important difference between ordinary signatures and group signatures are the additional privacy guarantees offered by the group signature schemes: namely, their (public) verification procedure does not leak any information about the actual signer. The verifier is only convinced that the signer is a valid member of the group. This can be seen as a relaxation of the authentication goals offered by traditional signatures, which allow verifiers to uniquely identify the signer of a given signature. In group signatures this property is replaced with the ability of the group manager to open group signatures. That is, although publicly verifiable group signatures do not disclose their signers, any verifier is assured that signers can be identified by the group manager. Note that by requiring the (trusted) group manager to open all group signatures we would immediately obtain the functionality of traditional signature schemes. This shows intuitively that group signature scheme has richer functionality

and more versatile applicability than traditional signature schemes.

In group signature schemes, the only person capable of addition of new members and revoking of the existing members from the group is the group manager. In case of legal disputes, if any, the responsibility of revealing the identity of the member or signer is of group managers. Also, we have to take care that all channels used during the communication are not synchronous which says the sender after putting a message though the channel does not need to wait for the receiver to receive the message off the channel. The channel communication between the sender and the receiver is assumed to be anonymous. Basic terms used in the group signature schemes are group public key which the verifier uses to check the validation of the signature, group's secret key which is used by a member of group to generate his signature and the group manager's secret key that is used to track the identity of the signing member. A standardized group signature scheme contains the following five phases:

1.Setup Phase: group manager computes the public key and the secret key in this phase by implementing the algorithm for group key generation. He inputs a security parameter to the algorithm and it returns the group public key and also the secret key of group manager. The secret key is kept with him and the group public key is circulated among the members.

2. Join Phase: an interactive protocol is established in this phase between the group manager and the to-be-member after which the user becomes a valid group member. A secret key is chosen by the Group member using which another parameter is generated by the member. This generated parameter is sent to the group manager. Then using his own secret key, the group manager generates the group member's signing key and returns it to newly joined group member.

3. Sign Phase: This is the signing phase in which an protocol is established between the group member and the verifier where he has to verify a group signature whether it is generated by a valid group member or not. Group member uses the signing key pairs to sign the message. The generated group member signature of knowledge is sent by the member to the verifier for verification.

4. Verify Phase: This phase implements a deterministic algorithm using given group public key and the signed message to verify the validity of the group signature. Signer sends his signature to the verifier, i.e. the signature generated

by the signature of knowledge. The message is accepted if true value is returned by the verification phase else the message is rejected if false value is returned by the verification phase.

5. Open Phase: This phase implements a deterministic algorithm to reveal the identity of the signer, by taking input a signed message and the secret key of group manager. The signature is taken as input by the group manager and using the private parameters outputs the identity of the signer as return value. This open algorithm is implemented when a incident of a legal dispute arises.

1.8.3 Properties

- **Anonymity:** Given a sign which is valid must be difficult for anyone to discover the identity of the signer computationally. As the constant differs every time, the same member generates different signature for every new message to be signed. The group manager only can determine the identity of the signing member using his secret key. For a nonmember it is almost not possible to discover the secret parameters of the signing group member as the knowledge of the secret key of the group manager is required and so without the secret key of the group manager it is almost impossible to determine the secret parameters of the signer and hence an outsider cannot determine the identity of the signer. In this property we conclude that if neither group manager's secret key nor group member's secret key is exposed then it is infeasible to reveal the signer of an authorized valid signature.

- **Unforgeability:** Only a valid authorized member belonging to the group can produce a valid signature i.e., a valid member only can produce a signature on behalf of his group.

- **Unlinkability:** This property states that deciding if two valid signatures were generated by the same group member is difficult. According to this property one cannot conclude that both signatures are from the same member or not if he's provided with two signatures.

- **Traceability:** Using only open algorithm and the group manager's secret key, the group manager can track the identity of the signing member if given any valid signature. Like in case of any legal dispute or emergencies, any signer's identity can be traced by the group manager only. It is not possible for an

outsider to track the signer because open algorithm, which used to trace a signing group member, requires the knowledge of the secret key of the group manager.

- **Exculpability:** The group members even along with the group manager are not able to sign a document on behalf of any other group member. The knowledge of the secret parameters of the group member is required to generate a valid signature. And every member has his own unique secret key that are used to generate the signature. Even a group manager cannot sign on behalf of any group member because the group manager does not have the members' secret keys.

1.9 SCOPE AND OBJECTIVE OF THE RESEARCH WORK

WBANs have stringent resource constraints. Additionally, the system is challenged by a hugged and for security and privacy not to mention their practicability and usability [26]. WBAN security schemes are initially set up by symmetric cryptosystems due to shortage of resources. This system has issues with providing weak security comparatively as it is not resilient to physical compromise and delays in revealing the symmetric keys. It also achieves many security needs of BSN (Biosensor Node) based healthcare system. In addition, the sensor's node primary weakness is their limited computation capacity energy, communication rate and memory space [6], [43] s.

In this research, the theory has been applied for WBAN security. The theory is designed to access the patient's information with improved security on WBAN. Much research has been conducted to study the security issues in WBANs. The Proposed encryption scheme using identity-based group signature algorithm (IBGS) based on secure key signature management in healthcare systems. The introduction of IBGS provides data access of the patient through high security. At first, the communication system consists of WBANs that sense information controlled by the IBGS with biosensors. WBAN with biosensors is linked with the network to monitor multiple patients' information. This scheme was divided into three five stages Setup, Join, Sign, Verify and Open. The findings showed that the scheme achieves more reliability and provides better security for the system. This protocol uses an identity-based group signature algorithm between biosensors and Group Manager (GM) with full

anonymity to authenticate the message. Here, the base station or access point is considered the trusted authority and it generates the secret key for the biosensor based on group id and transmits the generated secret key to the biosensor manager. The GM is responsible for generating a signature on the message that has been sent to it by one of its group members and broadcasts the message to the base station whether it is verified. Upon successful verification, the message is accepted. Besides, sound informal security evaluation has been performed to demonstrate that IBGS attains necessary security properties and is safe from sundry attacks. The proposed scheme satisfies all the requirements of unforgeable, anonymity, unlinkable, traceability.

The health-related information between on-body sensors and monitoring devices in WBAN systems subsequently transmitted over the internet to central controllers in hospitals is strictly private and confidential. Health-related information must be encrypted so that the patient's privacy is protected. Healthcare professionals who have access to information must be confident that the patient's vital information is not tampered with or altered and when it is truly originate from the monitored individual. Furthermore, an overly secure system might disallow healthcare professionals from accessing vital health-related information in certain emergency events and thus jeopardize patient's life. Moreover, enriching the current systems with security and privacy mechanisms significantly increases the cost of energy for communication which results in more power drain from small batteries. Based on the importance of security in WBAN, the scope of this proposed work is to enhance the existing WBAN security algorithms and to develop a framework for securing the human health care data along with maintaining the energy efficiency of the system. Hence, in order to enhance the security mechanism in human health care monitoring mechanism, the objective of this work intents to

- To study the various security threats faced by WBAN.
- To enhance the existing WBAN security algorithms to achieve better Human Healthcare Monitoring in a WBAN platform
- To securely generate and distribute the secret keys between the sensor nodes and the base station for secure end-to-end transmission.
- To achieve the proposed work is improved Security and energy efficiency in comparison with existing works.

1.10 THESIS ORGANIZATION

The Thesis is organized as follows:

Chapter 1 gives Introduction about the Human Health Care System, Wireless Body Area Network and Sensors. It also had discussed the security in WBAN, scope and objective of the research.

In Chapter 2, a comprehensive review has been conducted to develop a meaningful classification of state-of-the-art authentication schemes in WBAN and to assess and analyze them at a deeper level. The strengths and limitations of the schemes have been evaluated. This chapter has also provided a classification of security schemes to assess the security level of WBAN.

In Chapter 3, a novel authentication using identity-based group signature (IBGS) protocol has been proposed to provide security to the WBSN. The proposed method employs identity-based group signature algorithm between biosensors and group manager (GM). This scheme involves four parties: a trusted authority, the group manager, the group members, and verifiers. The trusted authority acts as a third helper to setup the system parameters. The GM selects the group public/secret keys; he (jointly with the trusted authority) issues membership certificates to new users (biosensor's) who wish to join the group; and in case of disputes, opens the contentious group signatures to reveal the identity of the actual signer. Finally, group members anonymously sign on group's behalf using their membership certificates and verifiers check the validity of the group signatures using group public key. Finally, a comparative performance analysis reveals that IBGS achieves better performance and shows promising results while providing more robust security and privacy.

In Chapter 4, a novel authentication ID-based Group Signature (IDGS) model along with Secret key induced Elliptic Curve Cryptography (SECC) methodology has been proposed, at first, the Group Manager (GM) is selected from the sensors in the remote body sensor system using Normalized Opposition Based Learning BAT Optimization Algorithm (NOBL-BOA). Afterward, clustering with Information Entropy induced K-Means Algorithm (IEKMA) takes place to improve energy efficiency. Next, to provide security to the WBSN, message authentication is carried out based on novel authentication ID-based group signature protocol. the formal security proof for IDGS has been provided using necessary security properties.

Finally, the SECC is used to encrypt the message for secure data transmission. The simulation results reveal that in comparison with existing works, the proposed work achieves improved security and energy efficiency.

Chapter 5 describes the outcome analysis on IBGS model and IDGS with SECC model with the Measurements consider the common metrices of my proposed systems of the percentage of Packets Transmitted, Average Delay, Energy Consumption and Key Mismatch Rate are used to evaluate the proposed representation.

Finally, Chapter 6, concluded by summarizing the entire research work done, presented the contributions and suggested some future directions for extending the current research work.

1.11 SUMMARY

Chapter one summarizes some of the introductory details needed to do this research along with the scope and objective of this research. The organization of this research work is also given. The next chapter gives a detailed literature review on the existing similar research done.

CHAPTER 2

LITERATURE REVIEW

2.1 RESEARCH GAPS

In healthcare, WBANs have shown a great application and is benefiting us in various ways such as patients with biosensors are allowed to roam here and there which in turn increases patient's mobility and minimizes the load of patients in hospitals. For the WBAN to be a concrete application of the healthcare system, it is paramount to ensure that the data sensed by the WBAN sensors is safe and not exposed to unauthorized entities and security attacks. In light of this, strong security solutions and authentication schemes are needed for the success and large-scale adoption of the WBANs. To this end, a plethora of security solutions and authentication schemes have been suggested by researchers over the last two decades.

In this chapter, an updated comprehensive review has been conducted on state-of-the-art authentication schemes in WBAN. The strengths and limitations of the schemes have been discussed. Besides, the objectives and comments on each scheme have been provided. Moreover, this chapter provided a classification of security schemes to assess the security level of WBAN.

2.1.1 Literature Search and Selection Process

This chapter has provided the current state-of-the-art in the form of a review which will be a stepping stone for researchers working in this direction. A systematic and qualitative review has been employed to study various papers related to security and authentication schemes in WBANs and the findings from this review have been well- discussed to assist researchers in doing further research [52].

2.1.2 Review Plan

The review started with the review plan, research questions (RQ) identification, an effective search process, key factors for inclusion and exclusion, and quality estimation. Various related research articles and reviews have been identified and assessed for quality and then finally, quality material has been selected for the review.

2.1.3 Research Questions

For refining the process of this review, several RQs have been framed about security and authentication in WBAN. Main RQs and their targets relevant for this

review are listed in Table 2.1.

Table 2.1. Research Questions and their Targets

Q. No.	Research Questions	Target
RQ. 1.	What is the security-related aspects of WBAN?	It targets exploring the security essentials, and security attacks in WBAN.
RQ. 2.	What security issues exist in WBAN and how they are dealtwith?	It targets on providing a range of security schemes applied to ensure security in WBAN.
RQ. 3.	What are the existing security schemes for WBAN?	This review aims to provide a view of security schemes to protect the WBAN system from various attacks from an adversary.
RQ. 4.	What are the existing authentication schemes for WBAN?	This review explores various authentication schemes in WBAN- biometric based, blockchain based, cryptography based, fuzzy based, password based, PUF based, machine learning based, and smart card based.
RQ. 5.	How is an authentication scheme built?	The review aims to provide the design and development steps of an authentication scheme in WBAN.

2.1.4 Search Process

The Literature selection process applied by us for choosing the appropriate research papers relevant to the review has been represented in Figure 2.1. The relevant matter related to our research has been dispersed across various Book Chapters, Conferences, and Journals. Primarily popular online repositories have been searched for extracting relevant materials such as IEEE Explore, Science Direct, Springer, Taylor and Francis Online, IGI Global, etc. Secondarily, a manual search in the relevant area has been conducted. The descriptors used for searching these online repositories are ‘WBAN’, ‘WBAN Security’, ‘WBAN’, ‘Security Challenges’, ‘WBAN Security Solutions’, ‘WBAN Security Features and Attacks’, ‘Security Schemes in WBAN’, ‘WBAN Authentication Schemes’, ‘Authentication Design’, etc.

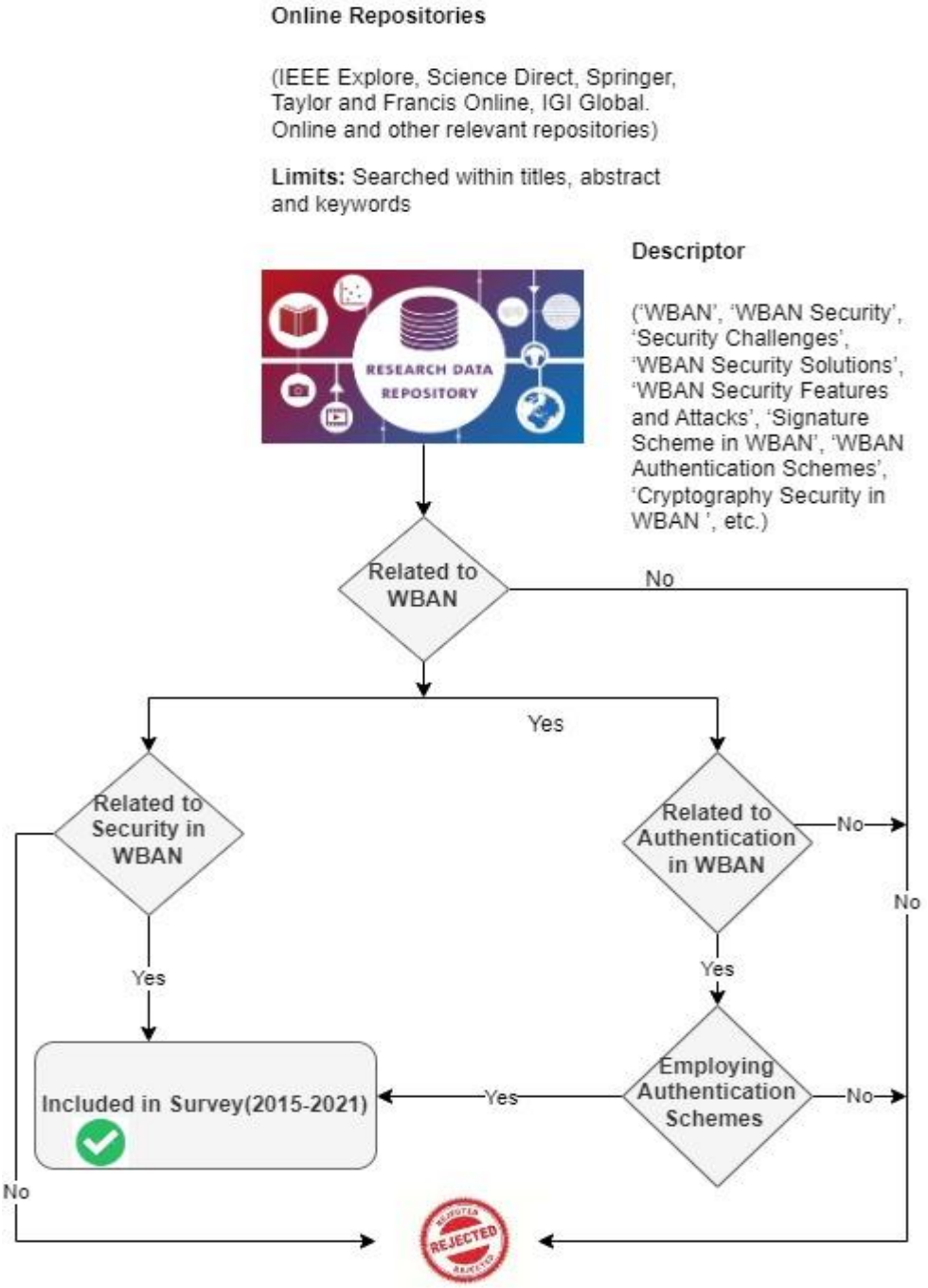

Figure 2.1 Literature Selection Process

2.1.5 Key factors for inclusion and exclusion

The selection of research papers has been based on two categories: One category includes articles similar to security aspects in WBAN and the other on authentication schemes in WBAN. The extracted articles have been examined based on their publication years. Research papers from various Journals, Conferences, and Book Chapters on the categories mentioned above have been included (from 2015 to 2021) in the review, and the rest have been excluded.

2.1.6 Quality Evaluation

This section carried out the quality estimation of the papers included in the review, and the process followed the directions of DARE and CDR [53]. Quality hiding questions have been provided in Table 2.2, and these questions have been kept in mind during the selection of papers.

Table 2.2 Quality hiding questions

Q. No.	Question Description	Answer
Q1	• Does the selected research paper allude to security and authenticationin WBAN? • The selected paper included an overview of security and authenticationin WBAN where the term security in WBAN or authentication in WBAN was not used. Whether such papers were excluded from thereview?	Yes No
Q2	• Does the abstract, title, and full-text of the paper delineates 'security in WBAN' and 'authentication in WBAN'? • Does the abstract, title, and full-text of the paper delineate the security and authentication in TMIS, WMSNs, E-Health, BASNs, IoT, WHSNs?	Yes Yes

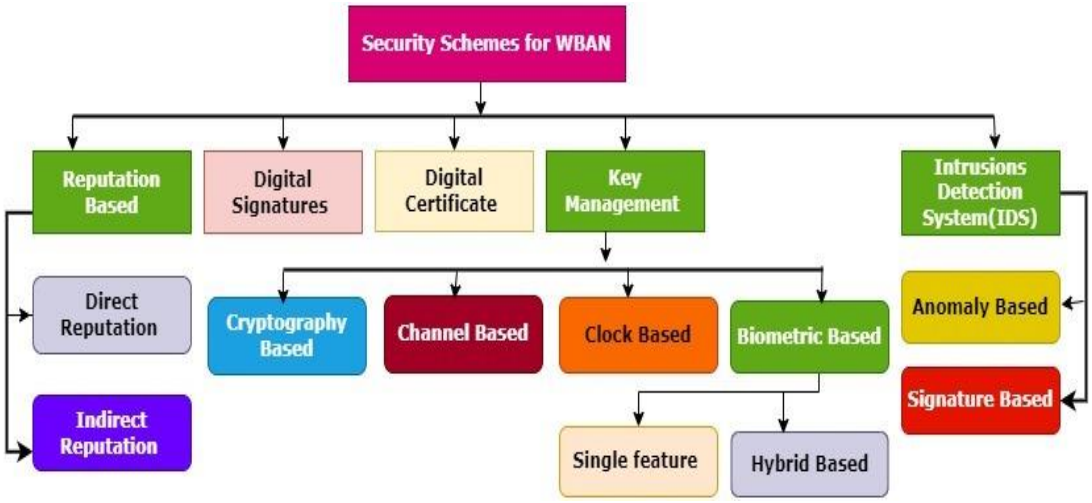

Figure 2.2 Classification of Security Schemes for WBAN

2.2 CLASSIFICATION OF SECURITY SCHEMES IN WBAN

To design a strong security mechanism for WBAN, it is imperative to comprehend the security and privacy needed by these networks. It is noteworthy that the security mechanisms applicable to other networks may not work for WBAN, as firm resource constraints are associated with the sensor nodes. Some of the well-

known security schemes implemented in WBAN (the classification of security schemes has been presented in Figure 2.2) to protect the system from various attacks from adversaries have been discussed as follows [54]:

2.2.1 Reputation Based Schemes

The reputation-based scheme relies on the information or past conduct of the network nodes to evaluate their reliability numerically. The numerical value of reliability assists in assessing the compliance of the behaviour of the node in the future as it will be near past values [55].

2.2.2 Digital Signature schemes

Digital Signature schemes are the mathematical cryptographic primitive used to achieve authentication, integrity, and non-repudiation for the digital messages and documents shared during communication. By employing the hash function over the data, the message digest is generated by the sender node and further signed using its private key then forwarded to the receiver node. The receiver node then verifies the signature by using the public key of the sender node. If the result is valid, then the data is extracted by applying the hash function [56].

2.2.3 Digital Certificate schemes

Digital Certificate scheme [57] uses a digital certificate (sort of electronic file) to bind the owner's entity with its public key cryptographically and acts as identifying information in digital form. For validating the information carried in the certificate a trusted third party, i.e., Certificate Authority (CA) is used. In addition to the public key of the owner, the digital certificate carries the name of the owner, a unique number assigned to the certificate for identification, the expiry date of the certificate, and the digital signature of CA. However, digital certificate schemes are impractical for WBANs as the resource-scanty nodes need to maintain the certificate as well as their public key.

2.2.4 Key Management schemes

Key management schemes are useful in providing security to WBAN by keeping data safe and secure from adversaries. Key management involves the generation of cryptographic keys (used to encrypt/decrypt data), renewal of keys, the key agreement between involved parties, distribution of secret keys among concerned parties, and key revocation [58]. For WBANs, many key management schemes have been proposed by the researchers, and they are discussed as follows:

2.2.5 Cryptography based schemes

Cryptography based schemes can be categorized into the symmetric key, asymmetric key, and hash function-based schemes. In symmetric key based key management schemes, a single key/ symmetric key is utilized to perform encryption and decryption of data such as AES, DES, Blowfish, etc. In asymmetric key based key management schemes, public-private key pair is used for enciphering and deciphering the data such as RSA, DSA, ECC, etc. Hash function based key management schemes uses a hash function for securing the data. Examples are SHA, HMAC, MAC, etc.

2.2.6 Channel based schemes

Channel based schemes classify attackers and genuine nodes by utilizing the RSS variance [59].

2.2.7 Clock based schemes

In these schemes, the clock frequency of the sensor node is utilized as unique as well as dynamic data for the generation of key pairs between the communicating nodes [60].

2.2.8 Biometric based schemes

The biometric based schemes either use behavioral or physiological features for extraction or generation of keys. The phases involved in the biometric based key management schemes are the acquisition of biometric data, biometric feature extraction, and using the extracted feature for key management operations (generation, agreement, etc.) [61].

2.2.9 Single feature-based schemes

Single feature biometric based key management schemes use a single biometric feature such as iris, fingerprint, ECG, HRV, PPG for the key management process.

2.2.10 Hybrid Schemes

Hybrid biometric based key management schemes use multiple biometric features combinations for the key management process. However, a lightweight hybrid scheme is needed to save the energy of the resource starving sensor nodes.

2.2.11 IDS

An IDS is a useful measure in the arsenal of security mechanisms that are widely used in WBANs to track the unauthorized access attempts and manipulation to the system. An IDS performs real-time monitoring of the system to gather and analyses

the collected information which is utilized to locate all the possible inbound and outbound malicious activities [62-63].

2.2.12 Anomaly based IDS

An anomaly-based IDS compares the performance baseline of the normal traffic events with the sample network traffic events and observes for any incorrect or abnormal behaviour, which seems to be an intrusion attempt. If any intrusion is detected, then a flag is raised. However, the chances of false-positive flags are there as it adapts itself to new attacks with time using machine learning techniques [63].

2.2.13 Signature based IDS

A Signature based IDS looks for the known attacks patterns/signature in its database to identify any intrusion attempt. The detection by this sort of IDS is fast, and configuration is easy. The flags raised in case of intrusions are more standardized and easier to comprehend. Compared to Anomaly based IDS the flags raised are smaller in number. However, it is essential to keep the database up to date to counter the recent attacks [63].

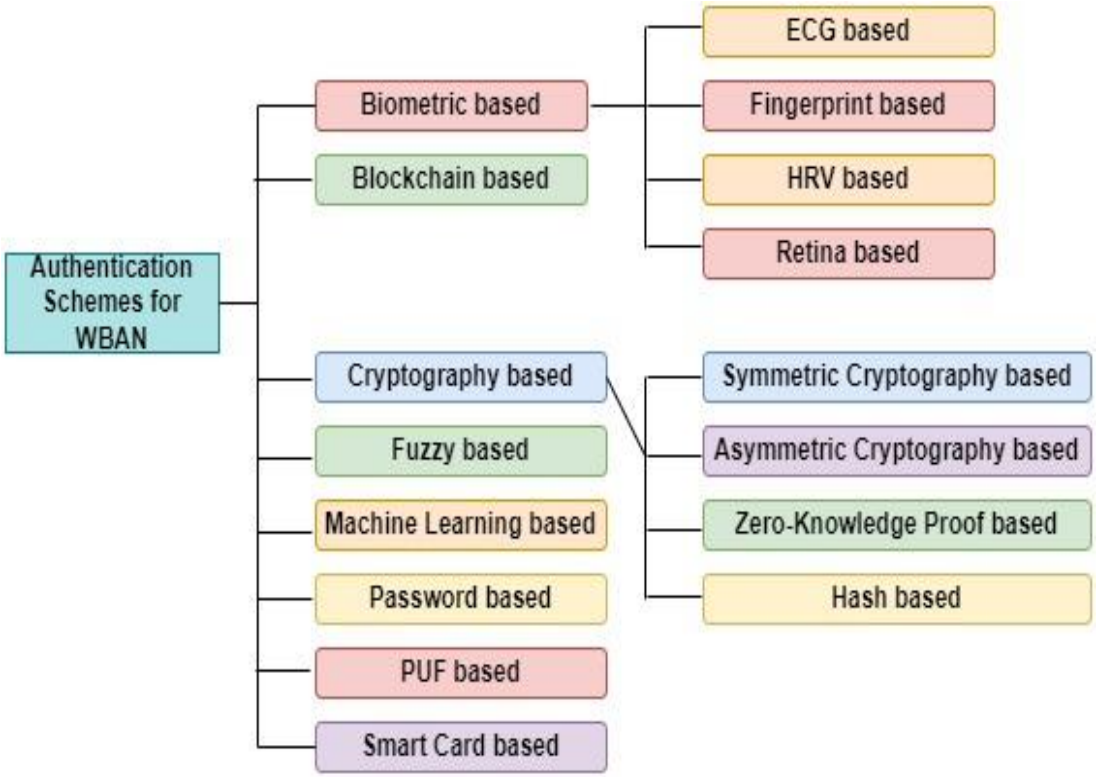

Figure 2.3 Classification of Authentication Schemes for WBAN

2.3 CLASSIFICATION OF AUTHENTICATION SCHEMES FOR WBAN

The Classification of existing authentication schemes has been presented in Figure 2.3.

2.3.1 Cryptography based

The cryptography-based authentication schemes have been described in the following subsections.

2.3.2 Symmetric Cryptography based

Symmetric Cryptography is the simplest kind of conventional technique of encipherment which utilizes one secret key (private) for enciphering and deciphering the electronic information. It is an old and best-known straightforward technique that has some notable advantages such as lightweight, simple, quick, time, and computation- savvy process. These advantages make it suitable for WBAN security. However, the inherent issue of secure key exchange before message exchange is a significant problem. Some of the widely accepted and used symmetric cryptographic algorithms are AES, DES, Triple DES, IDEA, etc. Some of the relevant symmetric cryptography-based authentication schemes have been provided in Table 2.3 and focuses on providing an overview of the objectives along with strengths and limitations of the symmetric cryptography-based authentication schemes. The insights provided in the Table will benefit the researchers in understanding these schemes and will assist in designing an improved or newer authentication scheme.

Table 2.3 Symmetric-key Cryptography based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[72]	Designed an efficient scheme for Ambient Assisted Living system meeting key security requirements and preventing the system from sundry security attacks	+ Robust and efficient as well as capable in providing strong forward secrecy as it withstands famous attacks and is superior compared to other related schemes. + The proposed scheme is efficient compared to [64] and [65] in terms of computation cost. -Scheme lacks key escrow resilience [66] and non-repudiation compared to [64]. -Scheme lacks known key security compared to [65].	The proposed scheme lacks key escrow resilience, non-repudiation and insecurity towards known key attacks. Moreover, the scheme is compared with only two schemes.

[71]	Developed two schemes to provide a secured authenticated key exchange between nodes	+These protocols are computation- savvy and reduce communication costs remarkably. +Successfully minimizes storage cost and complexity in the network. - The scheme did not evaluate privacy, and the well-known attacks were not discussed.	High efficiency with resistance to sundry attacks. However, privacy preservation is not evaluated, and security from various significant security attacks is not presented.
[68]	Proposed a scalable yet energy efficient authentication and key agreement scheme	+The scheme was inexpensive compared to another relevant scheme concerning computations, communication and memory requirements. The scheme successfully achieved many security properties. -The scheme did not withstand many security attacks and did not attain many security features.	The proposed scheme achieves low communication, computation and storage cost in contrast with related schemes. No discussion on resilience from major security attacks is provided.
[69]	Designed an energy efficient authentication scheme based on symmetric cryptography	+ The scheme uses simple hash and XOR operations with fewer steps to provide security + Resources are utilized efficiently to preserve energy -the scheme lacks a discussion on many security features and various adversarial attacks.	Lacks discussion on many security features and various adversarial attacks. Proposed scheme eliminates the use of computationally intensive hash chains and bilinear pairing.
[70]	Developed a lightweight and energy efficient authentication scheme	+The scheme provided an improvement over Li et al.'s scheme [67] by resolving sensor impersonation and server impersonation attacks. + Scheme is suitable for application in mobile phones and wireless sensor nodes as well with the same efficiency -The scheme does not discuss about protection from relevant security attacks such as modification and eavesdrop	Energy-efficient and resource savvy scheme. Hence, suitable for the resource scanty sensor nodes of WBAN.

Among the discussed symmetric-cryptography based authentication schemes for WBANs, the scheme [68] and [69] are computation-savvy. With reference to achieving security features, is efficient, whereas, with reference to resisting security attacks, the scheme is efficient.

2.3.3 Asymmetric Cryptography based schemes

Asymmetric Cryptography is an encipherment technique that utilizes two distinct, yet related keys for achieving two primary purposes: authentication and

confidentiality. The pair of keys: the public key is used for enciphering the message and is known to everyone, and the private key is used for deciphering the enciphered message and is kept secret to the owner. It is noteworthy that although the security level provided by asymmetric cryptography is high but the vulnerability towards MitM and Chosen plain text attacks and large overheads involved in the management of keys makes it unsuitable for the resource-scanty WBAN sensor nodes. Some of the popularly known examples associated with this cryptography technique are RSA, ECC, DSA, ElGamal, etc. Some of the relevant asymmetric cryptography-based authentication schemes have been provided in Table 2.4 and focuses on providing an overview of the objectives along with strengths and limitations of the asymmetric cryptography-based authentication schemes.

Table 2.4 Asymmetric-key Cryptography based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[73]	Developed an anonymity-preserving remote authentication scheme for WBANs	+The scheme is adequate for low-power mobile units in WBANs and has lower communication and computational overhead compared to Liu et al. [64]. +The scheme is a secure and lightweight certificateless scheme with better scalability. -Resilience towards security attacks was not evaluated	Developed an ECC and Bilinear pairing-based authentication scheme which was successful in minimizing run time and computational complexity by 52.6% and 17.6% respectively and guaranteed remote authentication with the support of anonymity.
[65]	Developed an ECC and Bilinear pairing-based scheme that proves secure mutual authentication between the legal client and AP	+The scheme is resilient to unknown key-share and key-compromise, impersonation attacks as well as ensures no key control -The DoS attack was not considered, and it does not provide real anonymity and unlinkability	Compared to Liu et al. [64] improvement of 50.58% at client-side and 3.87% at application provider side was achieved. However, the scheme is unable to provide real anonymity.

[74]	Proposed a novel revocable certificateless encryption and signature scheme and provides remote anonymous authentication	+ The scheme is highly practical and provably secure + The proposed scheme is secure against adaptive chosen-plaintext attack and is scalable and appropriate for large WBANs + It revokes certificate of the misbehaving client and evicts them from the system + Scheme successfully achieves major security features resistance to major security attacks has not been studied	The scheme is scalable and practical for large scale deployment of WBANs. Although the proposed scheme has many merits associated with it, however, the authors did not discuss the security of the scheme from various attacks.
[75]	Proposed a bilinear pairing-based authentication scheme which is practically suitable for WBANs.	+The scheme is efficient compared to Zhao [65] and Liu et al. [64] in terms of providing real anonymity, lower communication and computational overhead. -Lacks real anonymity	The proposed scheme can be applied practically to WBANs. However, the storage cost was not considered by the authors.
[76]	Designed an anonymity-preserving and lightweight authentication scheme for WBANs	+ The proposed scheme achieves mutual authentication, desired security features such as anonymity, unlinkability, forward security and withstands MitM, modification and impersonation attacks. - However, it does not withstand replay and stolen verifier attacks compared to [65].	The proposed scheme is suitable for practical WBAN and imparts provable security and minimizes computations at the client-side. Scheme solved the problem of [65] in terms of client impersonation attack and provided its improved version
[77]	Designed a provably secure anonymity-preserving authentication scheme for WBANs	+The proposed scheme is suitable for practical WBAN and achieves security and minimizes computations at the client-side. -However, it lacks non-repudiation, unlinkability, key escrow resilience and known key security compared to [75].	Designed an authentication scheme to remedy the security flaw in Liu et al. [64] (impersonation attack).
[78]	Designed a computationally efficient and anonymity-preserving authentication scheme for WBANs	+In terms of storage, computation and communication overhead, the proposed scheme outperforms [75]. +The developed scheme is equipped with better security and is practically applicable in WBANs. -However, computation overhead at the application provider side is higher than [75].	Proposed an anonymous authentication scheme to provide an improved version of [75] (better security, reduces computation burden by 31.58% and avoids impersonation attack).

[79]	Developed a secure and anonymous 1-round authentication scheme which achieves desirable security properties and computationally efficient.	+The proposed scheme makes use of many low-cost computational operations (computationally efficient). +It is suitable for WBANs and ensures various security requirements. The scheme utilizes 82 bytes message size (smaller than similar schemes) and is energy-efficient. -The scheme does not discuss many important security attacks needed for the security of the scheme	However, resilience towards security attacks, namely, replay, modification, eavesdropping, man-in- the-middle etc. was not studied.
[80]	Developed an efficient certificateless remote authentication scheme with anonymity	+The proposed scheme is secure from malicious insider attacks, remedies the flaw (client impersonation) in [75]. +The scheme provides immunity from key escrow problems with ease in implementation. -Does not provide security from modification, MitM and replay attack compared to [75].	Minimized run time (WBAN client) by 51% relative to [75].
[81]	Developed a computation savvy and secure authentication scheme consisting of three protocols for mHealth systems	+The scheme achieves session independence and protects the privacy of the session, along with simple key management. - Authentication at Tier 1 was not provided by the scheme.	Protocols 1 and 2 are dedicated for authentication at third-tier while Protocol 3 is for the second tier. However, the scheme does not talk about authentication at tier 1.
[82]	Designed two schemes: Firstly, a computation savvy online/offline signature scheme (OOCLS) was designed. Secondly, a remote authentication scheme with heterogeneity (HRAAP)was proposed based on OOCLS	+ OOCLS scheme is unforgeable -The scheme does not contemplate mobile users - Does not consider sending data to multiple servers	It is possible to apply HRAAP into IoTs, where the client uses CL-PKC and the server uses PKC. Lesser energy usage, time savvy, and computation savvy are some of the notable advantages of HRAAP. A framework for secure data communication between client and application provider is provided utilizing the proposed scheme HRAAP.
[83]	Designed an asymmetric bilinear pairing based Secure authentication scheme for WBANs.	+The scheme achieved mutual authentication, anonymity, forward secrecy security properties and the scheme is	Designed an improved version of Wu et al.'s scheme [78] by eradicating the client impersonation attack

		safe from impersonation, replay and tampering attacks. -The scheme only provides a formal proof to show security and no implementation on any simulation tool has been provided	issue and compared to [75] and [78], reduced computations and achieved reliable security.
[84]	Proposed a conditional privacy-preserving authentication scheme	+Reduces communication and authentication overhead by using batch authentication and is safe from batch authentication attack +Successfully eliminates the possibility of forgery and batch authentication attack possibility -Lacks batch verification function	The proposed scheme resists batch authentication and forgery attack and reduces the computation and communication overhead. The scheme uses certificateless cryptography and employs ECC for signature construction.
[85]	Proposed an anonymity preserving authentication scheme that provides conditional privacy and tracks malicious users	+Ensures genuine patient and doctor communication by using the conditional tracking system. +Tracking is performed to identify the unauthorized doctors if any with minimum computations +The scheme achieved anonymous authentication from doctor to patient and patient to doctor by using minimum computations in signature and certificate authentication. -Lacks a discussion on important security attacks such as MitM, modification, impersonation, eavesdropping, etc.	The scheme efficiently authenticates the doctor before the transmission of health-related information to him/her.

2.3.4 Hash based schemes

The hash function is a cryptography-based authentication mechanism that works on variable input length to generate a fixed-length output and does not require any key to encipher/decipher the data. For a hash function to be useful, it should possess these qualities: (i) collision-resistant, (ii) deterministic, (iii) puzzle-friendly, (iv) computationally-efficient, (v) pre-image resistant and (vi) impossible to reverse engineer. There are many cryptographic hash functions that are used by the researchers to perform hash-based authentication, and they are: SHA family, MD family, MAC, and HMAC, and among these SHA-1, SHA-256 and MD5 are most popularly used by researchers. Some of the relevant symmetric cryptography-based

authentication schemes have been provided in Table 2.5 and focuses on providing an overview of the objectives along with strengths and limitations of the hash-based authentication schemes. The insights provided in the Table will benefit the researchers in understanding these schemes and will assist in designing an improved and better authentication scheme.

Table 2.5: Hash based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[86]	Designed a lightweight authentication scheme for 2-tier WBANs	+The protocol provides full anonymity with the utilization of only XOR and hash function. -The scheme is not suitable for multi-tier WBANs and is limited to 2-tier WBAN topology	Scheme outperforms [65, 63-64] in terms of energy drainage, computation and communication burden.[89] is an improvised version of [86].
[87]	Proposed an anonymous and energy-saving mutual authentication scheme for two-hop WBANs	+The scheme is safe from MitM, replay, sensor node impersonation, and desynchronization attacks. -Does not discuss non-Repudiation	The scheme achieved a significant reduction in energy, processing and communication overhead compared to [65], [63] and [86].
[88]	Proposed a privacy preserving and computationally lighter mutual authentication scheme for WBANs	+ The scheme withstands replay, server impersonation, stolen- verifier, eavesdropping attacks +Schemes is lightweight, energy- efficient and computation- efficient. -The scheme does not cover the modification attack	[88] proved that Li et al.'s scheme [67] is vulnerable to the wrong session key establishment and jamming attack, and provided a new version of privacy- preserving and computationally-lighter mutual authentication scheme for WBANs.
[89]	Designed an efficient authentication scheme	+ Achieves important security parameters + High security	The scheme achieves high security and efficiency in comparison to [67].

2.3.5 ZKP based schemes

In ZKP schemes, one party proves another party by conveying the assurance that they know the secret, without revealing any data linked to them. In ZKP based schemes, digital authentication is performed using ZKP, where no password or sensitive information is required. ZKP can solve the risks involved in password-only authentication schemes, safeguards data from cybercriminals,

preserves the viability of blockchain, bolsters the security of cloud accounts, and secures transactions and payments made online. However, a major disadvantage associated with ZKP is if the user forgets or loses his/her password (only the user knows his copy and no one else) then all the data is lost forever. Some of the relevant symmetric cryptography-based authentication schemes have been provided in Table 2.6 and focuses on providing an overview of the objectives along with strengths and limitations of the Zero Knowledge Proof-based authentication schemes. The insights provided in the Table will benefit the researchers in understanding these schemes and will assist in designing an improved or newer authentication scheme.

Table 2.6: Zero Knowledge Proof based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[90]	Developed an effective, lightweight authentication scheme (TinyZKP) based on ZKP	+Low computation overhead and simpler key management compared to competitive schemes based on ECDSA +Scheme is suitable for highly resource-constrained WBANs -The scheme does not contemplate major security requirements	The proposed scheme is fast, memory-efficient, and energy-efficient in comparison with T-ECDSA and W-ECDSA schemes
[91]	Developed a BANZKP scheme themed on the commitment scheme and ZKP.	+Less key usage, memory efficiency, resilience towards attacks and less energy overhead are some of its features -Non-compliant with postural movements	The protocol is based on the two cryptographic primitives: Commitment scheme and ZKP scheme. The scheme makes use of fewer keys and minimizes energy consumption significantly, which makes the scheme memory and computationally efficient. However, it does not contemplate body moves.
[92]	Developed a three-phase authentication scheme (BANGZKP)	+Provides a fix to the issues present in BANZKP (concerning security and networking) + Efficient in terms of delay, throughput and number of authentication messages transmissions needed +In terms of energy consumption	BANGZKP utilizes hop-by-hop authentication as well as a new random key allocation technique and provides a better solution over BANZKP [91].

2.3.6 Biometric based

The goal of all biometric based WBAN authentication schemes is to provide a

stronger form of authentication using biological traits. Some of the relevant biometric-based authentication schemes have been discussed in Table 2.7 and focuses on providing an overview of the objectives along with the strengths and limitations of the biometric- based authentication schemes. The insights provided in the Table will benefit the researchers in understanding these schemes and will help in designing an improved and better scheme.

Table 2.7: Biometric based Authentication Schemes [3]

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[93]	An energy- efficient key establishment scheme has been proposed. A framework was designed to verify the security level of the proposed scheme	+ Scheme is energy efficient and has lesser computation and storage overhead − It does not consider the optimum value of vault size and difference tolerances − It does not cover essential security attacks such as Wormhole, Sink, and Sybil	Scheme successfully counters the attacks mentioned above in addition to session hijacking, MitM, impersonation and denial of service attacks and achieves a high precision feature extraction. But the scheme is limited to ECG features and does not work for PPG, EMC, ECC or their combination and was not analytically analyzed.
[94]	Designed a Retina-based human authenticatio n whichis incessant towards geometric alteration	+ Efficient storage needs and template matching procedure +Perpetual against any geometric alterations + There is no need to localize Optic Disc and Fovea −Number of registrations are very few (5 per person) − It does not cover any security attacks and any security features	The authors used retina as a biometric feature from which the Voronoi Diagram is generated. This unique diagram helps in retina-based identification. The scheme could be improved if artificial intelligence is employed, which will assist in the training of feature points and further improved database.
[95]	Proposed a novel scheme that provides an improved ECG-IJS system for secure key establishment and authentication.	+ Energy-efficient key allocation and distribution +Minimizes transmission overhead -Sharing of common key among neighbours makes the scheme susceptible to node compromise.	A framework was designed to verify the security level of the proposed energy-efficient hash-based authentication scheme utilizing ECG as a biometric feature

[96]	Proposed a novel authentication scheme utilizing HRV as a biometric feature (used to generate keys).	+ Scheme is efficient in terms of cost, power, energy, and time Utilizes a single key for enciphering the messages and the bit transmission time of the proposed scheme is higher than DES, and RSA − No security attacks have been covered	Compared with PSKA, DES and RSA, the proposed scheme is power and energy-efficient, cost and time savvy. For securing the system, Data Authentication Function (DAF) is used.
[97]	Designed a strong biometric and password-based authentication scheme	+Safe from various security attacks -The scheme is not anonymity preserving. No simulation tool has been used for the implementation of the scheme	The authors proposed a computation-savvy authentication scheme for hierarchical WBANs. The scheme combines benefits of both passwords as well as biometric features.
[98]	Designed and implemented a BAN sensor system for inter- node authentication.	+Allows real-time tracking of ECG data (taken as a physiological characteristic) + Achieves 100% correct authentications, i.e. chances of false-positive authentications are slim + Deals with the real-world inconsistencies in the sensed data and safe from Replay attack Utilizes pre-agreed session keys instead of generating new session keys - It does not consider the case of more than one person with different ECG abnormalities	The developed BAN sensor system involves hardware design, data processing, and feature (ECG) detection. The data obtained from the sensor system is then utilized for inter-node authentication. However, the scheme does not cover many important security attacks, such as modification, impersonation, MiTM, etc.
[99]	Designed a mutual authentication and key establishment scheme between sensor node and cellular phone (sink).	+ Safe from several attacks - The scheme is not suitable for practical WBAN applications even if it counters fake sink attacks -Due to the utilization of Public Key encipherment technique, the scheme is practically not feasible for resource-scanty sensor nodes	Provided an improved version of Salama et al.'s scheme by eradicating various attacks. Fingerprint biometrics has been used for providing mutual authentication between the sink and the sensor.

[100]	Designed a hybrid authentication scheme using cardiac inter-pulse interval (IPI) as Biokey.	- In terms of storage, computation and communication overhead the proposed scheme outperforms existing schemes - Scheme includes the master key update and avoids the occurrence of several attacks The scheme is susceptible to impersonation and DoS attack.	To maintain the secrecy of the communication, the group key distribution technique was used, where the key can be dynamically updated. They are the first to combine certificateless cryptography with biometric features (ECG). The scheme involves five phases: offline registration, ECG feature extraction, authentication, group key distribution, and group key updating.

Koya et al. [100] show better performance in comparison with other ECG based authentication schemes. Among the discussed schemes, Peter et al.'s scheme [97] achieves 100% correct authentications and chances of successful attack by the adversary are lesser than 0.1%. Moreover, Koya et al.'s scheme [100] provides resilience from many more security attacks and achieves more security features compared to other schemes. Schemes discussed in [93], [94], [95] and, [97] does not cover analysis on resilience towards security attacks. Compared to other schemes, [99] achieves conditional privacy and protects the user identity.

2.3.7 Blockchain based

Using the features mentioned above of Blockchain technology, we can ensure secure storage, medical data sharing, patients' history tracking and, privacy in WBAN. The blockchain-based authentication schemes have been discussed in Table 2.8 and focuses on providing an overview of the objectives along with the strengths and limitations of the blockchain-based authentication schemes. The insights presented in Table will benefit the researchers in understanding these schemes in a better way and will help in designing an improved or newer scheme.

Table 2.8: Blockchain based Authentication Schemes

Scheme	Objective	Strengths (+) andLimitations (-)	Comments
[101]	A blockchain-based two-way authentication scheme for Medical Cyber Physical System is proposed	+The scheme provides privacy protection and ensures secure storage of medical records along with the reduction of computation and memory costs. -There is a lack of study on security towards various attacks and communication costs. −Comparison is performed with only two schemes −Communication overhead is not studied	Authors proposed a blockchain-based medical data storage model which ensures mutual authentication between hospital and blockchain node. Secure and reliable sharing of medical data between hospitals is provided. The proposed scheme uses logout operation to solve key expiration problem.
[102]	A novel secured blockchain-based authentication scheme with anonymity for WBANs is proposed	+ ID-based blind signature concept is utilized along with message recovery to achieve authentication and data source-origin authentication +Ensures verifiability, session key secrecy, key control security, unknown key share, immutability and consensus property −Resilience towards critical security attacks is not studied −Computation cost at client-side is high	The scheme achieves low communication and total computation cost compared to counterpart schemes. Meets more security features in contrast to the related centralized architecture based WBAN authentication schemes. Its lightweight design makes its implementation in WBAN easier.
[103]	Proposed a lightweight and anonymity preserving blockchain- based authenticated key agreement scheme for two-hop WBANs.	+Minimizes Communication Cost and Computation cost at the sensor node. +Sensor node capture attack is prevented by the usage of biometric identity −Computation cost at hub node is high	The scheme utilizes simple XOR and hash function to achieve lower communication and computation cost. Authentication and key establishment are performed across regions in the cloud service layer using a consortium blockchain network.

Among all the discussed blockchain based authentication schemes, [102] is efficient in terms of maintaining the secrecy of the established session key. At the

same time, [103] is efficient in terms of minimizing computation and communication overhead.

2.3.8 Fuzzy based

Some of the important fuzzy-based authentication schemes for WBANs have been discussed in Table 2.9 and focuses on providing an overview of the objectives, along with the strengths and limitations of the channel-based authentication schemes. The insights provided in the Table will benefit the researchers in understanding these schemes and will help in designing an improved and better scheme.

Table 2.9 Fuzzy based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[104]	Designed an intra-body device-to-device authentication scheme using fingerprints generated from patient's gAit. (BANDANA)	+Avoids brute-force and impersonation attack + Malicious device attached by the adversary is easily detected. + Extraction of fingerprints through a video recording is difficult. - Not suitable for inter-body device- to-device authentication - Discussion on many important security attacks and security features is not provided.	Binary fingerprints were used as an input to the quantization algorithm, which is further used for calculating the reliability and then on that fuzzy cryptography is applied to derive unique shared secrets. The shared secrets generated from the gait sequences follow good random distribution.
[105]	Designed an optimum key establishment scheme based on IPIs employing fuzzy commitment for intra- WBAN environment.	+Key negotiation is quick and secure. + Feature extraction process is fast, hence achieves low latency. + Energy and computation overhead is low + For extraction of features, 0latency algorithm is used + Success rate of key negotiation is 99.88% -Scheme suffers from IPI synchronization issue -Not suitable for subject doing day- to-day activities -Not an appropriate scheme for more than one subjects	Scheme consists of 4 stages: system initialization, feature collection, generation of witness, key binding and its exchange. The scheme does not consider datasets containing records of commercial wearables. Ensures randomness of IPIs and witness.

[106]	Designed a privacy-preserving mutual authentication and key agreement scheme for TMIS	+ Biometric data noise is removed through error correction techniques + Utilizes simple hash and XOR functions for minimizing the computation cost + Error detection is fast + Resolves man-at-the-end and phishing attacks -Non-Repudiation property is not considered	The scheme has a provision of securely revoking the smart card and biometric template. Scheme outperforms the related schemes in terms of security and cost. The scheme mutually authenticates the user and the server and ensures the security of the scheme from various attacks.
[107]	Designed a secure and stable fuzzy-vault and fuzzy-extractor based authentication scheme Body Sensor networks	+ Effectively counters the forgery attacks + Minimizes loss of data by 40%, energy drainage by 20% and delay compared to counterpart encoding schemes. + Achieves reduction in noise by 4% compared to other schemes by using adaptive filtering mechanism - No discussion on the security analysis of the proposed scheme in terms of resilience towards security attacks is provided except forgery attacks.	The proposed scheme efficiently counters the issues such as loss of data, high energy dissipation and high delay in the network. Utilizes adaptive filtering mechanism for effective noise removal from the signals of the extracted features.
[108]	Designed a Rotation- assisted fuzzy vault (RAFV) based authentication scheme for WBANs	+ Vault rotation by adversary is impossible even if he/she has the knowledge of locking elements. + Vault processing is faster compared to Fuzzy Vault scheme. -Communication cost compared to fuzzy vault scheme is higher. -Number of operations required in the scheme is high which in turn increases the execution time. -Security of the proposed scheme is decided by the key size.	RAFV is an extension of fuzzy vault-based authentication scheme, which makes use of RSSI for obscuring the locked vaults which prevents key from getting disclosed to adversary. RAFV prevents adversary from performing data manipulation and impersonation. No discussion on the security analysis of the proposed scheme in terms of resilience towards important security attacks is provided.

Among the discussed schemes, schemes [104] and [108] effectively counter brute-force attacks, whereas scheme [106] performs well in reducing computation cost as it has not used any encryption/decryption technique and provides a stronger security solution via hash functions and XOR operations. Scheme [107] is efficient among all in terms of minimizing energy overhead, high delay and data loss in the network. Schemes [104] and [105] effectively ensure randomness in the extracted features. Discussion on analysis of the scheme in terms of providing resilience towards important security attacks has been provided in [106] only.

2.3.9 Machine Learning based

Some of the relevant machine learning-based authentication schemes are provided in Table 2.10 and focuses on providing an overview of the objectives along with strengths and limitations of the machine learning-based authentication schemes. The insights provided in the Table will benefit the researchers in understanding these schemes and will assist in designing an improved or newer authentication scheme.

Table 2.10 Machine Learning based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[109]	Proposed an abnormality detection system for detecting any abnormality in the patient's physiological sensed data in real time	+In comparison with counterpart schemes anomaly identification is fast as linear regression is used to determine anomaly in real-time and check whether the patient is critical or not based on the classification technique SVM + Sliding window protocol is not used while training which minimizes complexity [124] -The number of transmissions is very high as normal and abnormal traffic both flow between sink and sensors, which leads to energy drainage	The proposed scheme consists of two phases: Training and Detection. During training, the classification models are built, and deviation from established results leads to abnormality. The scheme achieves High True positive rate and Low False Negative. Achieves reliable results as the framework is applied directly on real patients' data.

[110]	Proposed a risk-based authentication model to detect user activities	+ Scheme verifies and validates the authenticity of the user and device +Delivers offloading feature -No implementation through simulation tool has been shown -Mathematical proof and comparison with relevant schemes are not available	The scheme consists of phases: network bootstrapping, monitor, analyze and adapt. The scheme utilizes Naïve Bayes to assign a risk score to the sensed data (normal/suspicious/abnormal/ critical). This risk helps in determining the level of compromise of the node, and hence the authentication decision is taken.
[111]	Proposed a risk-based authentication model to detect user activities. A scalable Linux kernel meant for IoT device to perform authentication has been developed and implemented module	+ Scheme is capable of notifying and measuring static as well as dynamic activities of different applications simultaneously +Machine learning is used to verify the conduct of applications +Divergence from expected behaviour can be easily detected by the verifier -Comparison with other relevant schemes has not been presented	The proposed authentication scheme assists in legitimizes multiple applications. The proposed module assists in tracking multiple applications in Linux space simultaneously. The proposed architecture is scalable and practically applicable.

From the comparison of the schemes above, it is seen that the scheme Saleem et al. [109] is experimentally analyzed while for the other two schemes, the experimental analysis is missing. In addition to this, a comparison with relevant schemes is provided in [109], while, the other two schemes lack comparative analysis.

2.3.10 Password based

Some of the relevant password-based authentication schemes are discussed in Table 2.11 and focuses on providing an overview of the objectives along with strengths and limitations of the password-based authentication schemes for WBAN. The insights presented in Table will benefit the researchers in understanding these schemes and will assist in designing an improved or newer authentication scheme.

Table 2.11: Password based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[112]	Proposed a novel password-based user access control scheme employing ECC	+ Scheme is capable of performing dynamic node additions, local password updation and does not need medical server assistance + The scheme supports scalability and utilizes less computation -The scheme does not support anonymity -There are mistakes in the formal analysis part	By using password and group theory techniques, legitimate users are authenticated to get access to healthcare applications. The scheme supports scalability and utilizes less computation
[113]	Proposed an efficient and secure password-based authentication scheme	+ The scheme is free from the risks involved due to the loss of the smart card. -No implementation through the simulation tool has been shown -Smart Card needs more storage than earlier schemes -A single shared key is utilized by sensors and gateway	Proposed an efficient and secure password-based authentication scheme by improving Kumar et al.'s scheme.
[114]	Proposed a password based authenticated association scheme	+This practically feasible scheme resists impersonation and MitM attack and provides a stronger and secured authenticated solution -No implementation through the simulation tool has been shown -The scheme utilizes insecure links -Compared to counterpart schemes message size is large as ECC is used	The authors proposed an efficient scheme which first generates a master secret key among nodes and hub, which is further used for generation of pairwise temporal key and this key is then utilized to encipher/decipher the data to provide authentication. However, the sharing of messages among the parties is in plain text, and if any third party gets access to the pre-shared password, then an adversary can make havoc.
[115]	Proposed a three-party password- based secured and privacy-preserving authentication scheme with anonymity	+Computations are less compared to related schemes -Makes use of the public-key algorithm -No implementation through the simulation tool has been shown -Communication cost is higher	This security and privacy-preserving scheme are well- suited for real-time healthcare applications. However, there is an issue with bandwidth as the messages exchanged are lengthy and increases communication costs.
[116]	Proposed a computable password- based robust and secured authentication scheme	+Scheme is efficient in the sense that it works only with HMAC and one-way hash	The authors propounded a three-factor robust authentication scheme that uses a custom password

		functions to provide a greater level of security +In terms of computations and total overhead the scheme outperforms other schemes -The scheme does not consider forward secrecy.	computation algorithm. It is to be noted that dynamic passwords are safer than static passwords. This dynamic password creation in each login round makes the authentication step secure and privacy-preserving. Scheme assists in achieving privacy as personal information leakage are prevented. Smart card revocation, dynamic node addition, password updating are some of the highlights of the scheme.

Among the discussed schemes, [113] is efficient compared to other schemes in terms of computation and communication overhead and provides an important security feature in the form of dynamic passwords, and in turn maintaining the anonymity and security of the user. The schemes in [112], [116] and [105] require a lesser number of computations compared to other schemes. However, the schemes [112] and [116] are inefficient in terms of communication cost. Security verification of the schemes [113-115] through any security verifier is not provided.

2.3.11 PUF based

Some of the relevant PUF-based authentication schemes have been summarized in Table 2.12 and focuses on providing an overview of the objectives along with strengths and limitations of the PUF-based authentication schemes for WBAN. The insights provided in Table will benefit the researchers in understanding these schemes and will assist in designing an improved or newer authentication scheme.

Table 2.12: PUF based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[117]	Proposed an authentication scheme where the sensor nodes before communication exchange share secrets via a control unit which helps in	+ Do not require complex encryption techniques, i.e. public or private key cryptography. Reduces the burden on sensor nodes. + Does not introduce any new entry point for the attacker at the cost of burden reduction. + No pre-establishment of challenge-response is needed. + Applicable for real-life	The scheme is compliant with body movements and maintains integrity. The scheme allows the addition of nodes in the network, change of Node-ID is allowed, nodes can be removed whenever needed, and secret revocation is possible. Further, the scheme is capable of

	authenticating the nodes.	scenarios. - No simulation tool has been used for implementing the scheme.	minimizing the number of transmissions and energy usage in the long run.
[118]	Proposed a computation savvy hierarchical cloud-aided authentication scheme for multi-hop WBAN.	+Outer node is not directly involved in transmitting authentication information, which directly minimizes the overhead on resources. +Once authentication between nodes is established, then it has been observed that conflict rate minimized, accelerated receipt of data packets with time and stable channel utilization. +Uniqueness and reliability is achieved. -No discussion on attacks is provided.	Crossover Ring Oscillator PUFs have been used to authenticate sensor and in-layer nodes and in-layer nodes and sink through the trusted transmission. The scheme is compliant to body movements and maintains integrity.
[119]	Proposed an identity authentication scheme using PUF-embedded sensor devices.	+Saves battery power of sensor nodes hence lifetime. +Thwarts security attacks +Achieves authentication from controller to sensor prior the data transmission from the sensor. -Important security attacks and security features have not been covered.	Proposed an energy-efficient authentication scheme using fewer hash and XOR operations compared to the counterpart scheme [108 and 111]. In case of multiple patients are there, then the self-sensor can be easily located.
[120]	Proposed a PUF-based mutual authentication scheme between sensor pairs and sensor groups, where authentication is carried out via the control unit.	+Do not require complex encryption techniques, i.e. public or private key cryptography. Reduces burden on sensor nodes. +Does not introduce any new entry point for the attacker at the cost of burden reduction. +Effectively counters sender impersonation attack. -The scheme has not been implemented on a real-time practical scenario.	Probability-based schemes developed by authors eliminate chances of sender impersonation attack. The scheme has shown low computations and thwarts multiple attacks.

Among the discussed schemes, in terms of countering security attacks and achieving lower computation cost, the [120] performs best compared to [118] and [119]. The scheme in [117] provides features such as dynamic node addition, node ID change and secret revocation compared to [118, 119 and 120] schemes. Moreover, compared to schemes [119] and [120], the schemes [117] and [118] are compliant with

postural body movements and maintain integrity.

2.3.12 Smart Card based

Some of the relevant smart card-based authentication schemes have been presented in Table 2.13 and focuses on providing an overview of the objectives along with strengths and limitations of the smartcard-based authentication schemes. The insights provided in the Table will benefit the researchers in understanding these schemes and will assist in designing an improved or newer authentication scheme.

Table 2.13: Smart Card based Authentication Schemes

Scheme	Objective	Strengths (+) and Limitations (-)	Comments
[121]	Designed an efficient Proposed a robust authentication scheme which is practically suitable for healthcare applications and secure smart- card based authentication scheme for WMSNs using biometrics features	+Scheme is communication and computation-savvy compared to counterpart schemes +Protects them from MitM, impersonation, stolen-verifier table and online password guessing attacks -The scheme does not detect wrong entered password -Password change phase is faulty, and the scheme is incapable in the protection of a new password	Authors eradicated the security flaws present in a scheme and provided an improved version with lower computation and communication burden and inherited its positive points. It is worthy to note that a single key is used in the entire network, which makes the whole network compromise if any of the nodes in the network gets compromised.
[122]	Proposed an improved version of Liu and Chung's scheme [124] authentication and encryption scheme for IoT based healthcare system	+Secure from various attacks and achieves security features -No implementation through simulation tool has been shown -The secure channel is required while performing registration	Propounded an enhanced version of Liu and Chung's scheme [124] authentication and encryption scheme for IoT based healthcare systems
[123]	Designed an efficient and secure smart-card based authentication scheme for WMSNs using biometrics features	+The highlights of the scheme are dynamic node addition, password change and biometric change phase +Scheme preserves benefits of previous schemes and adds the functionality of dynamic node addition and change of password as well as biometric	Designed an improved and secure smart-card based authentication scheme for WMSNs using biometrics features by overcoming various security flaws in He et al.'s scheme [121] and Li et al.'s scheme [122] and tried to eradicate these flaws.

[124]	Proposed an efficient, secure and privacy-preserving authentication scheme using smart cards and password for both patients and caretakers	+Safe from several attacks -The scheme is insecure from many important security attacks such as replay, offline password guessing, forgery, stolen smart card, etc. and in comparison, with Li et al.'s scheme [125], the computation cost is also high	The scheme is well-suited for hospitals and long-care medical institutions and instantly provides the health status of patients to the caretakers. For logging in to the system password is used, and for data authentication, the smart card is utilized.
[125]	Designed a secure and efficient mutual authentication scheme for TMIS	+Proposed scheme is more efficient and secure than counterpart schemes -High computations in comparison with [118]	The proposed scheme is meant for Telecare Medical Information Systems (TMIS) and provided an improved version of Chaudhary et al.'s scheme [118], and Islam et al.'s scheme [121] by propounding a secure and efficient mutual authentication scheme for TMIS
[126]	Designed a secure and anonymity preserving mutual authentication and key agreement scheme for TMIS	+Number of exchanged messages and the bits involved are very less compared to [122] +Reduces computations in comparison with [122] -No implementation through simulation tool has been shown	The scheme is user friendly, supports local verification of password and secures group key
[127]	Designed an anonymity-preserving ECC-based authentication scheme for WMSNs	+Highly secure and low communication and computation cost compared to related schemes +Time consumption is low compared to related schemes	The proposed secure-anonymous user authentication scheme (S-AUAS) counters susceptibilities present in existing related schemes while keeping the processing and communication cost at a minimum.
[128]	Designed biometrics- based authentication scheme themed on EPR-systems for smart healthcare	+Computation cost at the user side is low compared to related schemes -On-demand, security is not included -Execution time compared to other schemes is remarkably high -Computation cost at the authentication server is high	Identified the vulnerability issues in He et al.'s scheme such as user anonymity attack, late detection of a replay attack, forward/backward secrecy attack, and session-specific information leakage attack and resolved using the proposed scheme

[129]	Developed a smart card-based secure authentication scheme for TMIS	+Requires only single registration +Password change is friendly -No discussion on computation, communication and storage overhead is provided -No formal verification of the scheme is provided for validating the security of the scheme	The proposed scheme identified the vulnerability issues in Quan et al.'s scheme such as the scheme is susceptible to password guessing and MiTM attack. To counter such attacks, the authors proposed a more secure, efficient and reliable authentication scheme. All the phases of were improved.
[130]	Designed a secured three- factor based mutual authentication scheme for TMIS (TFASH)	+The communication cost in login and authentication phase is low compared to other schemes +Includes secure password updation phase -Many important security features such as Non-repudiation, Unlinkability, Untraceability are not discussed	The proposed scheme minimizes storage overhead significantly. The computation cost at the user, server, RC and Total cost is very low compared to counterpart schemes. The scheme achieves a high level of security and utilizes a smaller size key through ECC. The scheme is suitable for practical applications of healthcare systems.

2.4 SUMMARY

In this chapter, we have presented an overview of various security schemes and state-of- the-art related authentication schemes in WBAN to understand their scope, limitations, capabilities, etc. This chapter has explored various authentication schemes in WBAN- biometric based, blockchain based, cryptography based, fuzzy based, machine learning based, password based, PUF based, and smart card based. Moreover, this chapter has provided a view of security schemes to protect the WBAN system from various attacks from an adversary. This literature review has helped us in identifying the merits and demerits of the discussed schemes and motivated us to alleviate the issues in existing schemes and prevent adversaries from intimidating legitimate users or exploiting WBAN services, by designing a secured, identity-based group signature model (IBGS) for WBAN.

CHAPTER – 3

AN EFFICIENT SECURE AUTHENTICATION SCHEME FOR WIRELESS BODY SENSOR NETWORK USING IDENTITY BASED GROUP SIGNATURE (IBGS)

3.1 INTRODUCTION

Wireless Body Sensor Network (WBSN) faces several security problems such as loss of information, access control, and authentication. As WBSN collects vital information and operates in an unfriendly environment, severe security mechanisms are needed to prevent the network from anonymous interactions, authentication is the initial step towards providing security. An enhanced authentication scheme prevents the system from imposters effectively. In this paper, a novel authentication using an identity-based group signature (IBGS) protocol has been proposed to provide security to the WBSN. This protocol uses an identity-based group signature algorithm between biosensors and Group Manager (GM) with full anonymity to authenticate the message. Here, the base station or access point is considered the trusted authority and it generates the secret key for the biosensor based on group id and transmits the generated secret key to the biosensor manager. The GM is responsible for generating a signature on the message that has been sent to it by one of its group members and broadcasts the message to the base station whether it is verified. Upon successful verification, the message is accepted. An extensive set of experiments were carried out and the results were examined in terms of packet ratio, average delay, key mismatching ratio, data privacy rate, information loss rate, computation cost, consumption analysis, system flexibility level and measurement of security on patient health information.

Wireless Sensor Networks (WSNs) are well-known and identify the application in various IoT domains like armed forces, transportation, medicine, and so forth. In addition, Wireless Body Sensor Networks (WBSNs) is the extended version of WSNs that make use of wearable computing tools to process applications. The remote healthcare observation of a patient's health [131] is an instance of WBSN, where doctors often observe a patient's health condition with no requirement of physically

visiting the hospital. With the provided affordability as well as simpler use of sensor nodes and inbuilt tools, WBSNs can be applied with minimum cost. While deploying WBSN, wearable sensors gather and transmit data to distant providers for immediate processing of data. Hence, WBSNs offer additional objects for physicians to start spontaneous responses for deadly health conditions, like sudden infant death syndrome (SIDS). Figure.3.1 depicts the method of cloud-based WBSNs.

Applying wireless protocols like ZigBee [2] for transmitting data in WBSNs domains improves the communication facility for a good experiment. Additionally, in medical sectors, WBSNs are found in video streaming, data transmission, 3-Dimensional video, and entertainment, such as games and social media. Power game-assisted techniques were presented to reduce the interaction disturbance for WBSNs which depends upon the social network. The IEEE 802.15.6 wireless communication standard was created by the Institute of Electrical and Electronics Engineers to improve the measures of WBSNs [132]. The primary purpose of this model is to set a high bar for low-power, short-range, and robust wireless communication around the human body. It can handle a broader range of data values in a variety of applications, including short-range and wireless communications [133].

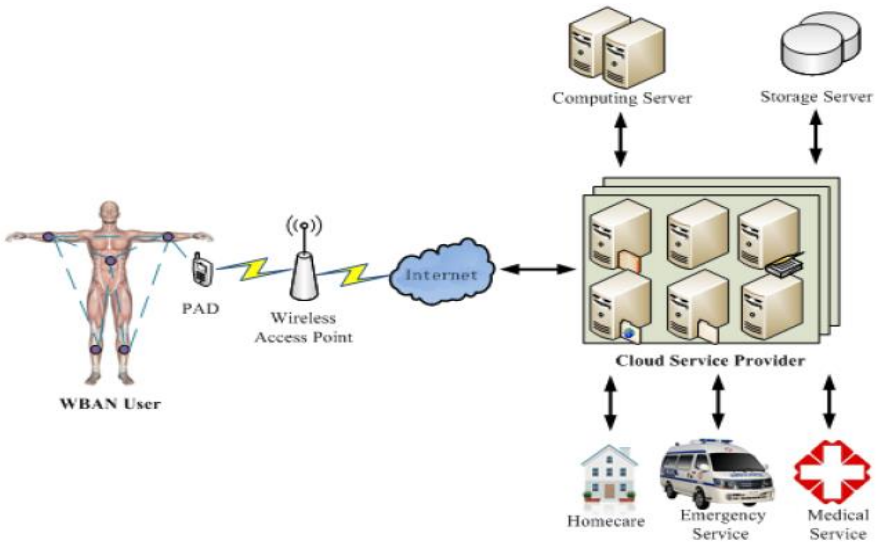

Figure 3.1. Architecture of WBSN

Here, WBSN is constrained with a problem of security level and privacy for given data. This method has the responsibility to offer data integrity as well as privacy, as the data can only be used by authorized users and not by any third parties. But, the resource limitations in WBSNs concern energy, storage, bandwidth potential, processing resources, and so on. The assured stability, as well as data integrity in

WBSN fields, differs every time. IEEE 802.15.6 states 3 levels of security: The initial one is Level 0 which, is unsafe communication; it is considered to be a minimum-security level in 802.15.6 that lacks security measures. Secondly, Level 1 is an authorized approach, which denotes authority as well as concurrent encryption techniques to attain the maximum-security goal in 802.15.6[134]. These standards require all devices that take part in transmitting data should be assured of effective security level. Moreover, a pre-defined Master Key (MK) is enabled in unicast communication; a Pairwise Temporal Key (PTK) has been produced for a single application; a Group Temporal Key (GTK) is provided and distributed with the respective group in case of multicast communication.

Security research in WBSNs: Generally, a communication method of WBSN could be portioned into 2 segments. The primary segment is present within body communication, which implies an interaction among sensor nodes. As the alternate segment presents external to-body communication which denotes that, communication from gateway to another network applicants like a service provider, remote observation as well as cloud servers. To compute the physiological data of clients in WBSNs, diverse inside-body authority approaches are presented [135].

In [136], the inter-pulse duration of the Electrocardiogram (ECG), as well as the Photo platysma gram (PPG), is applied to produce cryptographic keys for encryption and authentication. In [137], it is employed with frequency coefficients of ECG and PPG to generate cryptographic keys [138]. implied a suggestion of a fuzzy vault that has been vastly employed in the application of the field of biometric authorization. Then, a Physiological Signal Key Agreement technique (PSKA) depends upon a fuzzy vault, which is presented in [139]. But, the application of additional chaff points in the PSKA model improves the processing expense. In, extended fuzzy vault models along with ECG signals were projected to enhance the working function. An improved fuzzy vault technique [138] is proposed, which has been utilized for key generation based on the fingerprint.

In [140], Deng et al. developed a method to apply the ECG signal for biometric integrity that requires producing a signal format to validate the similarity by comparison. As the application of these constant templates, this model does not accomplish optimal security performance. In [141], a method assisted by time differentiation ECG feature is presented for authenticity and to filter the authentic key.

But these models depend upon physiological attributes like accuracy, as the gathered signals are from a similar individual which often deals with marginal variations. Additionally, a physiological signal is time-variant, and permanent clock synchronizing is required which is more difficult to attain. Moreover, these methodologies meet compatibility problems while applied with various sensors, which often suffer from real-time shortcomings.

To resolve the certificate handling issue, [142] applied a technique of lightweight cloud-assisted identity-based anonymous authentication and key agreement (IBAAKA) protocol for secure wireless body area network. In IBAAKA, a user's similarities like name, email, and mobile number, are the public keys. Hence, this data does not require maintenance. According to the IBAAKA, massive identity-oriented authentic approaches are presented. But these models are not applicable for WBANs due to the inability to offer client anonymity and are developed for the client-server platform. To convince the security needs of WBANs, [142] deployed ID-based authentication techniques with the application of a certificate-less signature module. Therefore, [144] noticed that Liu et al.'s framework could not support the stolen verifier-table attack. On the other hand, pointed out that the initial procedure is unable to offer anonymity. To enhance security and effectiveness, Zhao projected an anonymous authenticity technique for WBANs. Thus, the method could not provide real-time anonymity due to the customer's pseudo affinities being static measures and affecting the customers. By using the increased security measurements, it is required to develop an anonymous authentication approach to obtain real-time anonymity.

In this chapter, a novel authentication using an identity-based group signature (IBGS) protocol has been proposed to provide security to the WBSN. The proposed method employs an identity-based group signature algorithm between biosensors and group managers (GM). An extensive set of experiments were carried out and the results are examined in terms of Packet Ratio, Average delay, Key Mismatching Ratio, Computation Cost, Consumption Analysis, and Measurement of security on patient health information.

3.2 MOTIVATION BEHIND THE WORK

WBAN is a multifaceted network of hub sensors used to detect and transmit information at various levels in real-time. Sensor units collect critical data and send it

to a medical center for further review. Sensor hubs fully meet the limits of quantity, memory, and power. Information is the most important part of a patient's illness, so security and data protection are paramount. Many killers can undermine critical information about a patient's health. The WBAN Data Security Study is a study conducted around 2019-2022. Many of the articles presented in the course provide a detailed discussion of these articles under consideration. Several studies have been developed to maintain data security in WBAN, and these experiments ensure that remote sensors work effectively on a variety of concepts. Many statistical techniques are considered for success problems such as failure, integration problems, and the use of data modification capabilities. The document is encrypted in various formats such as SHA (Secure Hashing Algorithm), AES (Advanced Encryption Standards), and LEA (Easy Encryption Encryption).

A robust and reliable protocol for WBAN focuses on what can be called sensors that are inserted into patients 'bodies to monitor their health [143]. The human body is connected to the Internet through mobile devices. Healthcare professionals use this data to treat patient diseases such as asthma, diabetes, coronary heart disease, and bleeding. The Security and Energy Protocol is used to use WBAN Advanced Encryption Security (AES) encryption and the SHA-1 hash function to provide BAN security. SHA-I is challenging for WBAN, but the workload is reduced thanks to a chain hash protocol that uses Baker’s Chaos Card for security [145]. Experts are well organized in terms of memory, computing power, and bandwidth. The protocol generates a Baker chaos map for data separation, and this method is used to generate pseudo-random key streams.

Introduction of a lightweight secure communication system for PMS, with a focus on a secure patient monitoring system transportation system. The medical information of the patient is delivered to the gateway via a connected connection from the sensor to the body [146]. This article is dedicated to preventing data theft and ensuring that the key in the data can be identified by the appropriate user. Achievements in the Internet of Things (IoT) by those who bring smart systems, which have a wide range of health services. As a result, these systems put security and privacy at risk. The security system is low-power and resource-intensive. It starts a counter value, called the first value of a vector (IV), multiplied in a pseudo-random manner, using the AES-CTR method. Most counters employ an encryption algorithm like AES-128 bit, which

uses a simple XOR function comparable to the CTR mechanism used in the XOR function.

To transport data over the network, WBAN requires basic and efficient resources. Many technologies have been required for security purposes, and this research paper focuses on integration by generating symmetric keys through a physical layer or a link containing the researched RSSI [147]. This article presents an enterprise solution for improving the diversity and quantity of RSSI data to obtain an accurate image. The employment of different paths between a group of members and a group, or occasionally between two groups, to combine RSSI data with a plethora of overlapping multichannel information, boosting coherence and flexibility, is a critical breakthrough.

The WBAN is linked to the WSN, which is made up of small sensors that collect data from the human body and send it to a biomedical server via a network [148]. The major purpose of the system is to ensure the security and confidentiality of network data. There are a variety of security systems available to ensure data security and avoid a variety of threats. This article goes through cryptography and some of the most essential encryption technologies for data security. Providing strong cryptography and protection of data from large volumes. Use cheating technology to achieve safe time and use accurate memory to think. The critical control protocol is built into the security application.

To make data transfer safer and more dependable, researchers are adopting secure hashing algorithms (SHA) and encryption technologies. It produces digital signatures throughout the hashing process to obtain patient data securely and correctly [149]. This approach has been used to create an asymmetric key with two public keys and two private keys, lengthening and complicating the algorithms. WBAN data transfer with digital signatures, the created program is based on a combination of multiple approaches to prevent data theft on WBAN using hard keys and digital signatures. Because of its public keyless keys [150], such as BNC, and the complete sensor node in encryption and decryption systems, this idea is particularly stable. BNC records each data set using SK and sends it to all sensor nodes in the system using digital signatures.

In this chapter, data was recorded using ECC and Diffie Hallman (DH). The need

of keeping track of essential patient health data is so great that many different systems are utilized to keep track of it. As a result, the asymmetric ECC method is employed in this study [151]. To achieve data security, DH is employed to generate keys in the system. Patients and doctors are two sorts of users, thus this article focuses on user authentication, which involves registering the correct Internet users to keep their personal information in a database, such as their fingers or palms. The ECC and DH algorithms are used to merge this biological data. It is transformed to binary before being assessed for various values such as 128, 192, and 256 bits. Both decryption encryption time and high processing time are taken into account while evaluating masseurs [152].

Data is transmitted via a network using WBAN technology, which is continually evolving. Taking good care of your data might be difficult. For data security, this article employed a three-way authentication mechanism with the ECC Programme [153]. In the study, WBAN was also implemented utilizing star topology. There are two types of keys in asymmetric cryptography: public and private keys, which are mathematically coupled. There are two purposes in cryptography for achieving security: data authentication and patient authentication [154]. To encrypt and decrypt sensitive data, public and private keys are utilized.

3.3 METHODOLOGY

This section defines the models of an identity-based group-signature (IBGS) technique as given in the following. Figure. 3.2 shows the system architecture of the proposed model. The proposed model involves four main components, namely cloud server, Key generation center (KGC), User, and Auditor.

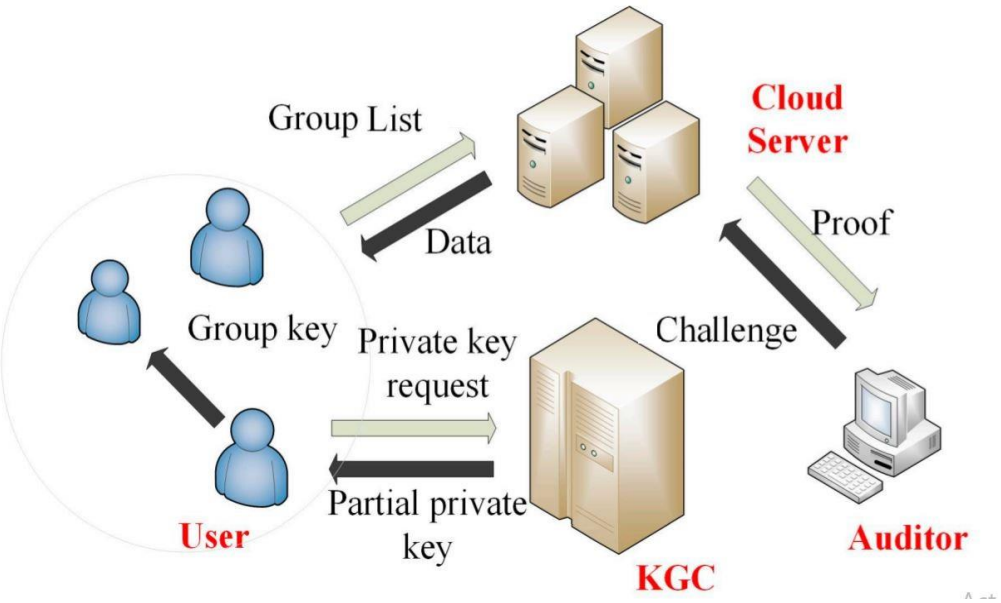

Figure 3.2. System architecture of the proposed model

This model depends upon an identity-based digital signature approach.

Definition 1: (Identity-based Group Signatures) It is an identity-based digital signature method composed of 5 patterns given as follows:

1) **Setup:** A technique, implemented by a Group Manager (GM), consumes an arbitrary security attribute l in the form of input and produces a few system attributes as well as a master key. As a result, the system parameters are known by the primary group public key, while the master key is known by the group manager.
2) **Extract:** The protocol from a GM and member. It has been considered that interaction among a member as well as a GM is private and authorized. Consequently, a member is authorized for this group. The outcome of a membership secret and a membership certificate. The member's secret is divided into two parts: the first is forwarded by a GM, and the second is chosen by the member himself, with two parts validated.
3) **Sign:** A hypothetical model with group public key and membership secret as inputs, where a message m is the outcome of group signature of m.
4) **Verify:** In terms of group public key, a model for introducing the time

of reduced group signature of a message.

5) **Reveal:** The given message is a valuable group signature, and it computes the similarity of the original author using a group public key and a group manager's master key.

A secure ID-based group signature model has to convince every feature provided:

1) Correctness: The VERIFY framework must approve any group signatures generated by a group member using the SIGN paradigm.
2) Unforgeability: The Members of the group can sign communications in the presence of the underlying group.
3) Anonymity: Finding the authentic signer of a letter when given a valuable signature is impossible for everyone but a group manager.
4) Unlinkability: Selecting two different effective signatures is handled by a similar group member who is more sophisticated.
5) Exculpability: A group member or a GM has the authority for signing instead of alternate group members.
6) Traceability: A GM often finds the original signer for a valuable signature for disputes.

3.3.1 Setup

It is assumed to be a system generation method. A GM implements the procedures given as follows:

1) Select p, q, GP_1, GP_2.
2) Select 2 cryptographic hash functions:

$$H: \{0,1\}^* \mapsto GP_1, \quad (1)$$

$$H_1 : \{0,1\}^* \times GP_1 \mapsto GP_1. \quad (2)$$

3) Develop a bilinear function provided:

$$e: GP_1 \times GP_1 \mapsto GP_2. \quad (3)$$

4) Choose a generator unit $P \in GP_1$, hence $e(P,P)$ is a generator unit of GP_2.
5) Choose an integer a from Z_q^* as a secret key of GM; Fix $P_{pub} = aP$ as the PK in this group.
6) Assume the string $f \in \{0,1\}^*$ denotes a separate group member's identifier. The PK of this member is determined by GM as $Q_f = H(f)$. The practical identity of a few group members can be easily predicted by their email or IP address.
7) Suppose $\{0,1\}^*$ A message space is a collection of strings of various lengths. Thus, a PK of this group is: $PK = \{P, P_{pub}, e(\cdot,\cdot), H, H_1\}$ The master key of GM

is $SK = a$.

3.3.2 Extract

Assume a new member U_i requires being an authenticated member of this group. GM would interact with U_i by using the secure channel:

1) U_i transmits its own identifier f_i to GM;
2) GM determines $sk_i = aQ_{f_i}$, and then forwards it to U_i.
3) U_i has a private value b_i and corresponding identifier f_i as its personal secret key as well as personal PK. Let $b_i f_i \equiv 1 \bmod \varphi(n)$, where n is a combination of 2 higher prime numbers.
4) U_i and GM are implements a Schnorr identifying protocol. Thus, GM attains a credential t_i that has been applied to find the membership of U_i.
5) GM is composed with transcription: $trans = \{< f_i, t_i > |$ for all authenticated group member $U_{f_i}\}$. Therefore, the transcriptor is executed by GM.
6) As a result, U_i joins this group as an authenticated member. The credential is t_i, the personal secret key is $\{b_i, sk_i\}$; the personal PK is f_i, and the personal secret key is $\{b_i,\ sk_i\}$; These data are recorded on a smart card that U_i.owns.

3.3.3 Sign

It is named as a generation technique of group signatures. Let U_{f_i} is an actual member of this group. Provided a message $m \in M$, to process the function:

1) Select random and uniform x from Z_q^* and sets $A = xP$.
2) Determine $B = x^{-1} sk_i + H_1(m, A) b_i$, where $x - 1$ implies the contrast of x in Z_q^*.

Thus, the group signature on message m is $\{A, B, and\ f_i\}$.

3.3.4 Veri

It is also a verification module for applied group signatures. Provided a message m as well as alleged group-signature$\{\ A, B, f_i\}$, and different verifier holds a PK that validates the lifetime of group signature by performing the functions given below:

1) Determine $\alpha = e\left(f_i P_{pub}, Q_{f_i}\right)$;
2) Determine $\beta = e(A, f_i B)$;
3) Determine $\gamma = e\left(A, H(m, A)\right)$.

Finally, the verification method validates the equation:

$$\beta =^{?} \alpha\gamma \tag{4}$$

When equality is present, then the verification approves $\{A, B, \text{and } f_i\}$ as a valuable group signature on message m; else, it has been eliminated. Besides, by using a group PK the verifier learns the signature emerging from a group; whereas, by applying personal PK the verifier understands that the signature has been produced by authentic members and not by a GM.

3.3.5 Reveal

This model can only be executed by a GM. As the message m and its valid group signature$\{ A, B, f_i\}$, the GM seeks for transcriptor of respective membership credentials. With the application of the Schnorr identifier and group membership credential, a GM accepts the practical similarity of a group member.

Remark 1: According to the SETUP technique, a model of various trust authorities is used to decide and build many GM to avoid the centralization of group members' identities into a single GM. GM's denial of service is no longer an issue.

Remark 2: The proposed protocol is a signature paradigm that allows each legitimate member to sign papers individually rather than as part of a group. If a protocol for a common signature technique is used, it means that each user can only sign papers.

Remark 3: The presented protocol is present in a setting of super singular elliptic curves whereas the setting of a prime-order multiplicative subgroup is of a definite application. Besides, a predefined curve does not apply the knowledge proof and applied this kind of proof.

3.4 RESULTS AND DISCUSSION

The Network Simulator (NS-2) for the IBGS Model system was used to complete the simulation investigation. It is an evolution of the free and open-source discrete event test system and provides generous support for simulating TCP, routing, and multicasting patterns over wired and remote systems. The size of the network is assumed to be 1000m*850m. With the help of a secure routing mechanism, the sensors in WBANs are positioned to monitor the patient's movements and keep track of their medical records. It maintains density at a very definite level and improves the size of

the network by raising the sensor node's number. Maintaining the network and its density, while improving the number of sensor nodes, improves the network range. For every scenario, five simulations having 100 sensor nodes were performed for lowering energy usage and time of response. The management of medical records has a top security level. The time taken for simulation is 25 milliseconds for one process as given in Table 3.1.

Table 3.1. Simulation Setup

Parameter	Value
Simulator	NS-2.31
Area of Simulation	1000×850 m
Traffic model/Mobility Framework	Random WayPoint Model.
Node movement	50m/s
Number of nodes	100 Nodes
MAC type	802.11
Communication range	250mts
Connection Path Link	Multi-direction
System Interface Type	WirelessPhy
Packet rate	6 Packets/seconds

The Measurements of the percentage of packets transmitted, delay, energy consumption, computational cost, key mismatch rate, data privacy rate, information loss rate, security of patient health data and System Flexibility Level are used to evaluate the proposed representation.

3.4.1 Delivered Packet Ratio

The ratio between the number of transmitted packets by biosensors and the number of received packets by GM is defined as the Packet Delivery Ratio. Various network barriers like data collision, insufficient buffer memory, and channel inaccessibility are causing packet drops. A good quality network architecture has the minimum number of Packet drops whereas middling quality network architectures suffer from a lot of packet drops. The packet Delivery ratio is calculated throughout the simulation period by NS-2. The observed packet delivery ratio values for the proposed scheme IBGS and existing system PSKA and IBAAKA are given in Table 3.2. The comparison graph is plotted and given in Figure 3.DPR is calculated using

Equation 5.

$$\text{DPR} = \frac{Packets\ Rececived\ by\ GM}{Total\ Packets\ sent\ by\ Biosensors} * 100 \quad (5)$$

The delivery rates of the packet for the proposed IBGS method have higher delivery rates than the ratio of the conventional scheme PSKA[139] and IBAAKA[142] and it is exposed in Figure 3.3. The more prominent estimation of the packet delivery ratio implies the better execution of the protocol.

Table 3.2. Tabulation for the Packet delivery ratio values

Number of Patient Data	Delivered Packet Rate (kbps)		
	IBGS	PSKA	IBAAKA
1	1000	750	700
10	1500	1300	1250
20	1800	1500	1400
30	2000	1750	1600
40	2300	2100	2000
50	2500	2340	2150
60	2800	2540	2350
70	3000	2700	2400
80	3500	3050	2800
90	4700	3800	3400
100	5100	4000	3700

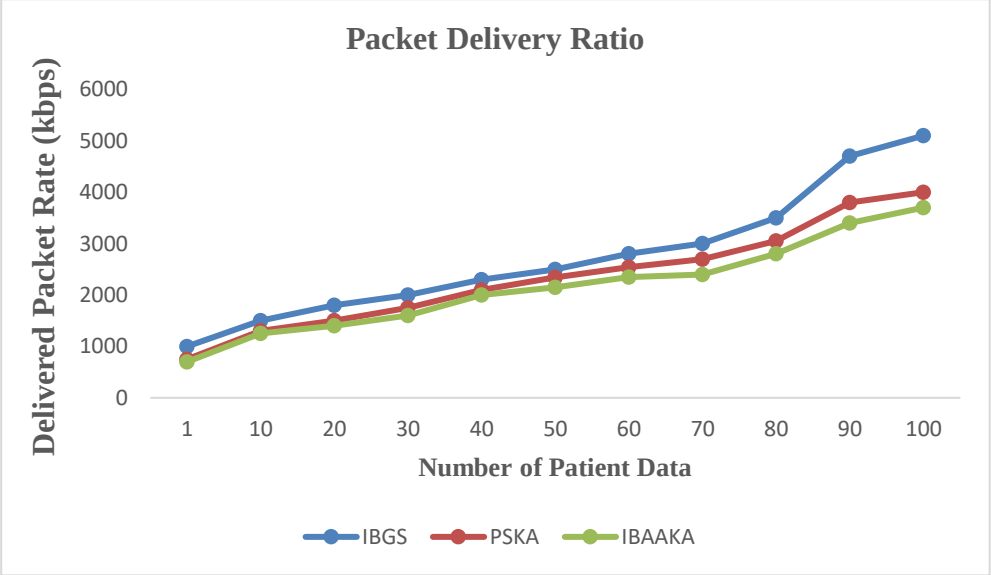

Figure 3.3. The delivery rates of the packet for the proposed IBGS

IBGS achieved 95% of the maximum average packet delivery ratio with the range between 4850 and 5200 kbps. Existing PSKA and IBAAKA are getting 84% and 82% of the packet delivery ratio respectively.

3.4.2 The Average Delay Ratio

Delay is an important parameter describing the overall performance of the network. Therefore, we are interested in finding a biosensor position that minimized the overall network delay. In WBAN, the distance between the biosensor and the Group Manager (GM) is an important factor that determines the delay of the network. The distance between the biosensor and GM changes regularly due to postural mobility. Distance between a biosensor and GM is directly proportional to the delay. Average delay not only depends on the distance of the nodes but also depends on the channel accessibility, i.e., less processing delay. Similarly, WBAN mobility also plays a vital role in network delay. As a sensor node changes position in the network, it also informs the rest of the sensor about its new position. Thus, as mobility increases, these positions notification packets also increase increasing the congestion and average delay of the network. The observed that the average delay ratio values for the proposed scheme IBGS and existing system PSKA and IBAAKA are given in Table 3.3. The comparison graph is plotted and given in Figure 3.4. The average delay ratio is calculated using Equation 6.

$$\text{Delay} = \frac{\sum_{i=0}^{n} PktSend\_Time - PktRecv\_Time}{Time} \quad (6)$$

Table 3.3. The Average Delay Ratio values

Number of Patient Data	IBGS	PSKA	IBAAKA
1	0.5	0.8	0.5
10	0.6	1	0.6
20	0.8	1.2	0.8
30	1	1.4	1
40	1.1	1.6	1.1
50	1.3	1.8	1.3
60	1.4	1.9	1.4
70	1.6	2	1.6
80	1.8	2.2	1.8
90	1.9	2.4	1.9
100	2	2.6	2

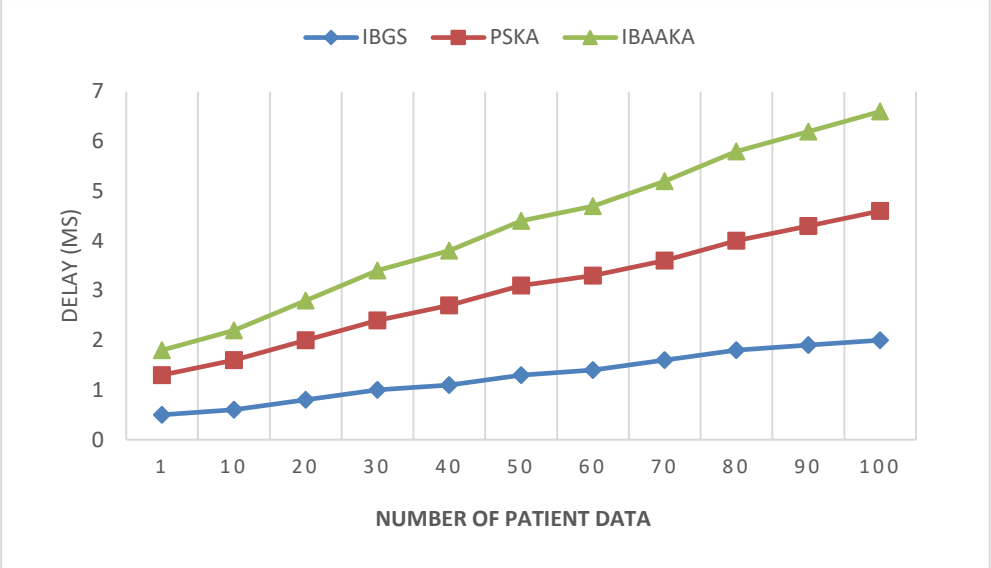

Figure 3.4. The Average Delay analysis

3.4.3 Key Mismatching Ratio

Key Mismatch Ratio (KMR) is defined as the main metric to recognize false private keys generated by malicious nodes which get mismatched when paired with GM. The ratio between various numbers of bits in the secret keys with the total number of key bits created for signature verification is said to be GM. It should be lower for better performance as it recognizes the false private keys generated by the malicious nodes. In this regard, the key mismatch ratio of the proposed method is varied as 0.6 for 20 nodes, 0.8 for 40 nodes, 1.0 for 60 nodes, 1.3 for 80 nodes, and 1.5 for 100 nodes. Compared to the existing methods, the proposed method attains less mismatch ratio as given in Table 3.4. From this analysis, it is cleared the proposed method is more efficient with strong private keys than the existing methods. The key mismatch ratio of the proposed and existing methods is analyzed in Figure 3.5.

Table 3.4. The Key Mismatching Ratio values

Number of Patient Data	IBGS	PSKA	IBAAKA
1	0.2	0.8	0.5
10	0.4	1	0.6
20	0.6	1.2	0.8
30	0.7	1.4	1
40	0.8	1.6	1.1
50	0.98	1.8	1.3
60	1	1.9	1.6
70	1.2	2	1.7
80	1.3	2.4	1.8
90	1.36	2.6	1.9
100	1.5	2.8	2.1

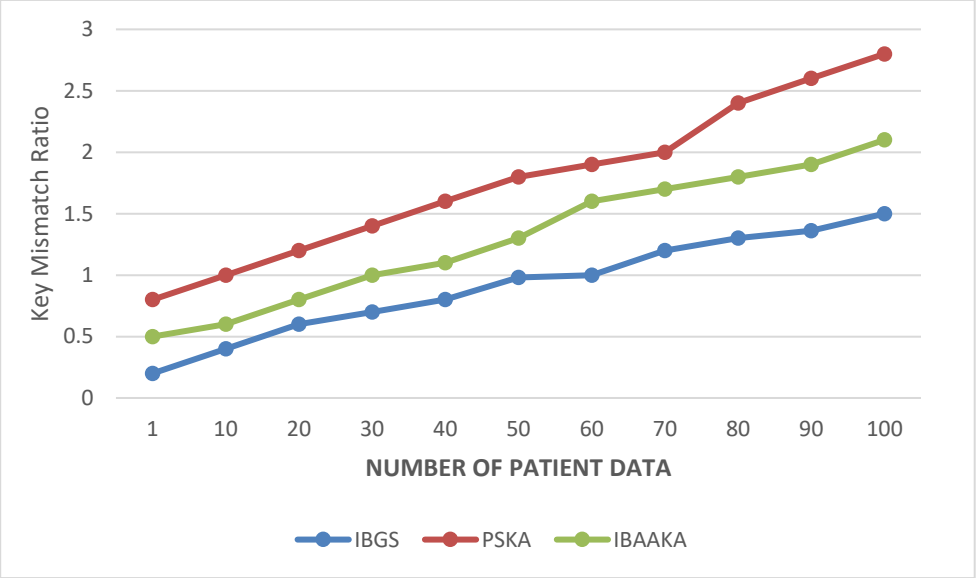

Figure 3.5. Key Mismatching analysis

3.4.4 Data Privacy Rate (DPR)

Data privacy rate is calculated as measure of number of patient data that are correctly accessed only by authorized users with respect to total number of data being broadcasted. It is estimated in terms of percentages (%) and formulated as given below.

$$D_{pr} = \frac{N_{ppa}}{T_{pd}} * 100 \quad (7)$$

In equation (7), N_{ppa} represents number of patient packets accessed only by authorized users and T_{pd} denotes total patient data.

Table 3.5. Tabulation for data privacy rate

Number of Patient Data	Data Privacy Rate (%)		
	IBGS	PSKA	IBAAKA
1	64.13	54.73	47.13
10	66.73	58.12	50.12
20	69.15	60.23	52.76
30	72.45	62.56	54.77
40	74.55	65.67	56.56
50	79.56	67.89	59.34
60	82.68	71.45	61.56
70	85.23	73.67	63.45
80	88.67	76.68	65.22
90	90.77	78.93	68.47
100	92.75	82.12	69.23

Table 3.5 shows the data privacy rate for different patients' information for the proposed IBGS approach in comparison with two other existing methods i.e., PSKA and IBAAKA respectively. The number of patient data in WBAN is varied from 1 to 100 in WBAN. The table shows that the data privacy rate of patient data using IBGS method is higher when compared to other existing methods.

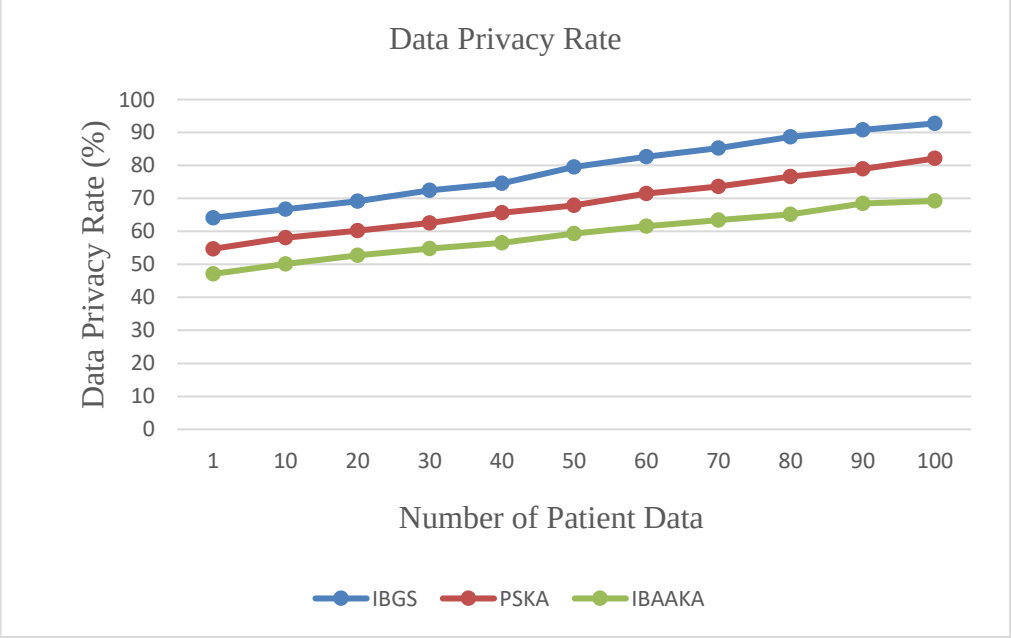

Figure 3.6. Data Privacy Rate

The experimental description of data privacy rate for proposed and existing method is presented in above Figure 3.6. With respect to different number of patient data in the range of 1 to 100 data, data privacy level is obtained. From the result of

experimental analysis, it is observed that the proposed IBGS method results in higher data privacy rate for secured transmission of patient medical data than the existing methods. Data privacy rate with respect to the different number for patients results in the range of 47% to 93%. While the number of patient data is 20, the designed IBGS method results in 69.15 % data privacy rate for monitoring patient activity data in a secure manner. Whereas, existing PSKA and IBAAKA method result in 60.23% and 52.76 % respectively. Therefore, data privacy rate using proposed IBGS method is higher when compared to other existing methods. Graph is drawn with the above table values in below following figure.

With the use of reliable information from IBGS, patient medical data privacy is maintained. According to the utility function of source and intermediate nodes, secure data is maintained for achieving reliable communication. This supports to attain higher data privacy rate in WBAN. The improvement of the proposed IBGS method is calculated as below:

Improvement in percentage = Average of the improvements for 10 results =

$$\frac{Sum\ of\ [(The\ Proposed\ System - Existing\ System) * \frac{100}{Existing\ System}]}{10} \quad (8)$$

Hence data privacy rate is improved by 38% when compared to PSKA and 22% when compared to IBAAKA respectively.

3.4.5 Information Loss Rate (ILR)

Information Loss Rate of designed IBGS method is measured by the ratio of health information loss to the total information for monitoring patient in WBAN. Information Loss Rate is mathematically formulated as follows.

$$Inf_{lr} = \frac{Information\_Lost}{Total\ Information} * 100 \quad (9)$$

As in (9), information loss rate Inf_{lr} can be measured through % or percentage. When the rate of information loss is less, then the method is said to be more efficient.

Table 3.6 Tabulation for Information Loss Rate

Number of Patient Data	Information Loss Rate (%)		
	IBGS	PSKA	IBAAKA
1	50.12	59.45	68.33
10	52.41	62.45	71.23
20	54.26	64.63	73.52
30	56.95	66.36	75.23
40	58.36	68.42	77.63
50	60.28	69.23	78.12
60	61.94	71.36	80.52
70	63.27	73.64	82.26
80	64.12	75.63	84.27
90	66.34	77.74	86.36
100	67.82	79.52	88.21

Table 3.6 shows the information rate for different patients' information for the proposed IBGS approach in comparison with two other existing methods i.e., PSKA and IBAAKA respectively. The number of patient data in WBAN is varied from 10 to 100 in WBAN. The table shows that the information loss rate of patient data using IBGS method is lower when compared to other existing methods. Information loss rate is evaluated for different number of patient data in WBAN. While taking the number of patient data is 100, information loss rate results in 68%. The information loss rate reduces compared to existing methods i.e., PSKA method resulting in information loss rate of 80% and IBAAKA method resulting in information loss rate as 88%. Hence the designed IBGS approach is seen to achieve the lowest information loss rate for diagnosing health information for multiple patients.

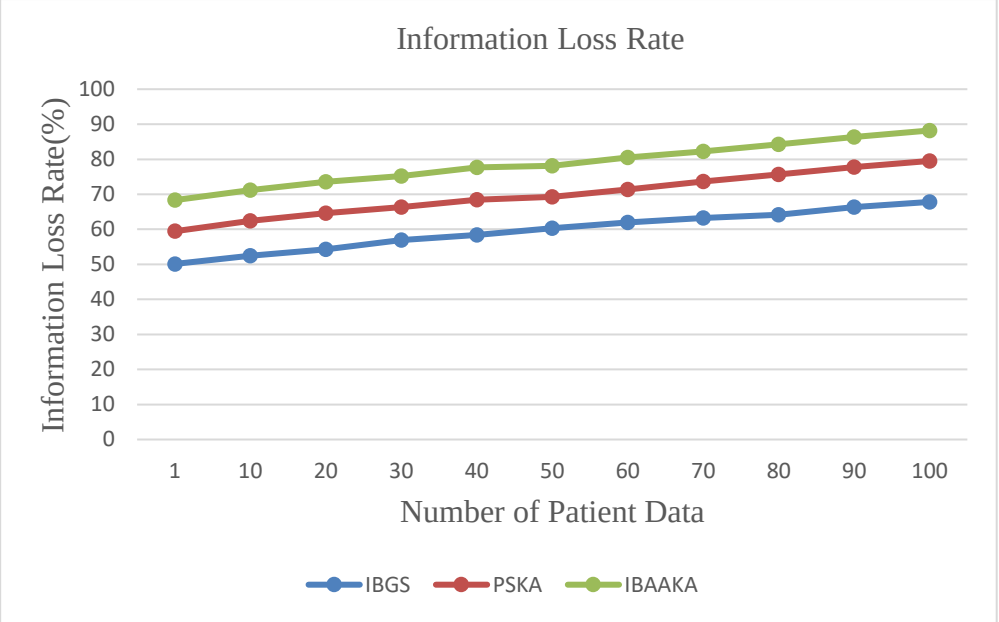

Figure 3.7. Measure of Information Loss Rate

Figure 3.7 shows information loss rate with respect to the number of people (i.e., patients) in WBAN. From Figure 3.7, it is clear that the information loss rate reduces in the proposed IBGS method when compared to the two other methods.

The improvement of the proposed IBGS method is calculated as below: Improvement in percentage

Average of the improvements for 10 results =

$$\frac{Sum\ of\ [(Existing\ System - Proposed\ System) * \frac{100}{Existing\ System}]}{10} \quad (10)$$

Hence information loss rate is improved by 15% when compared to PSKA and 24% when compared to IBAAKA respectively.

3.4.6 Computation Cost

In this section, a detailed computation cost analysis of diverse models takes place under the varying number of messages. A comparative analysis is made with PSKA and IBAAKA in terms of computation cost and energy efficiency cost. Table 3.7 and Figure. 3.8 show the computational cost of our proposed method. Under the message count 1, it is shown that the proposed IBGS requires a minimum computation cost of 1s, whereas the PSKA and IBAAKA models reach a maximum computation time of 2s and 4s respectively. Under the message count 10, it is shown that the proposed IBGS requires a minimum computation cost of 3s, whereas the PSKA and IBAAKA models reach a maximum computation time of 5s and 8s respectively. Under the

message count 20, it is shown that the proposed IBGS requires a minimum computation cost of 5s, whereas the PSKA and IBAAKA models reach a maximum computation time of 8s and 10s respectively.

Table 3.7. Computational Cost (s) of our Proposed IBGS with Existing Methods

Number of Messages	IBGS	PSKA	IBAAKA
1	1	2	4
10	3	5	8
20	5	8	10
30	9	12	16
40	11	15	22
50	14	17	27
60	18	22	29
70	21	24	36
80	25	27	42
90	29	31	47
100	32	34	52

Under the message count 30, it is shown that the proposed IBGS requires a minimum computation cost of 9s, whereas the PSKA and IBAAKA models reach a maximum computation time of 12s and 16s respectively. Under the message count 40, it is shown that the proposed IBGS requires a minimum computation cost of 11s, whereas the PSKA and IBAAKA models reach a maximum computation time of 15s and 22s respectively. Under the message count 50, it is shown that the proposed IBGS requires a minimum computation cost of 14s, whereas the PSKA and IBAAKA models reach a maximum computation time of 17s and 27s respectively. Under the message count 60, it is shown that the proposed IBGS requires a minimum computation cost of 18s, whereas the PSKA and IBAAKA models reach a maximum computation time of 22s and 29s respectively.

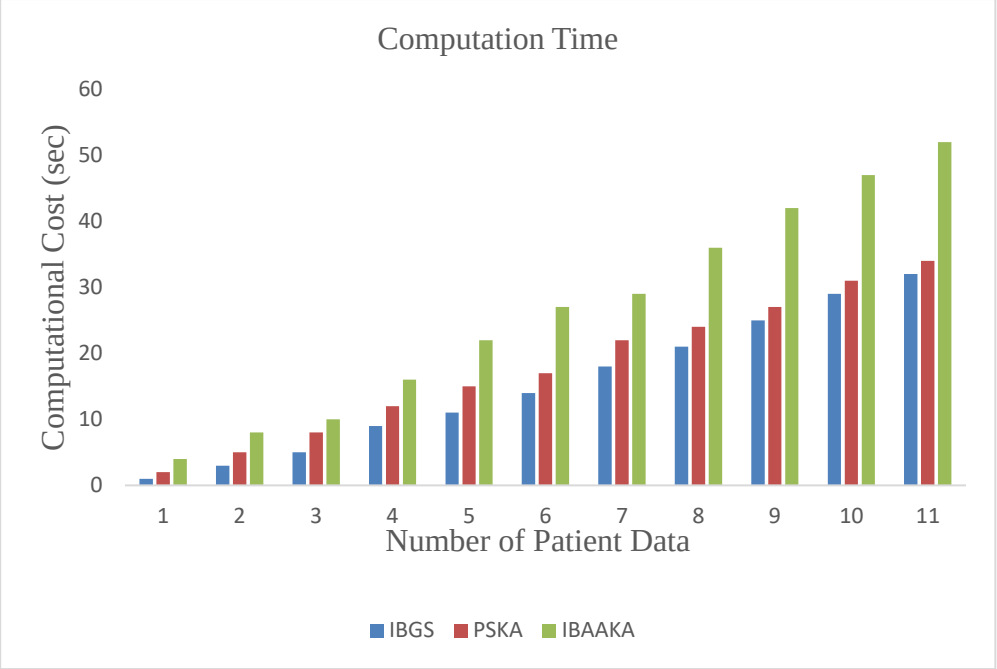

Figure 3.8. Computation cost analysis

Under the message count 70, it is shown that the proposed IBGS requires a minimum computation cost of 21s, whereas the PSKA and IBAAKA models reach a maximum computation time of 24s and 36s respectively. Under the message count 80, it is shown that the proposed IBGS requires a minimum computation cost of 25s, whereas the PSKA and IBAAKA models reach a maximum computation time of 27s and 42s respectively. Under the message count 90, it is shown that the proposed IBGS requires a minimum computation cost of 29s, whereas the PSKA and IBAAKA models reach a maximum computation time of 31s and 47s respectively. Under the message count 100, it is shown that the proposed IBGS requires a minimum computation cost of 32s, whereas the PSKA and IBAAKA models reach a maximum computation time of 34s and 52s respectively.

3.4.7 Consumption Analysis

Table 3.8 and Figure.3.9 show the energy consumption analysis of diverse models under varying message counts. Under the existence of 1 message count, the IBGS model shows a minimum energy consumption of 0.34J whereas the PSKA and IBAAKA models require higher energy consumption of 0.89J and 1.43J respectively. Under the existence of 1 message count, the IBGS model shows a minimum energy consumption of 0.34J whereas the PSKA and IBAAKA models require higher energy consumption of 0.89J and 1.43J respectively. Under the existence of a 10-message

count, the IBGS model shows a minimum energy consumption of 0.76J whereas the PSKA and IBAAKA models require higher energy consumption of 1.23J and 1.8J respectively. Under the existence of 20 message count, the IBGS model shows a minimum energy consumption of 0.91J whereas the PSKA and IBAAKA models require higher energy consumption of 1.54J and 2.45J respectively.

Table 3.8. Energy Consumption of our Proposed IBGS with Existing Methods

Number of Messages	IBGS	PSKA	IBAAKA
1	0.34	0.89	1.43
10	0.76	1.23	1.8
20	0.91	1.54	2.45
30	1.34	1.86	2.91
40	1.76	1.98	3.57
50	2.15	2.47	3.86
60	2.43	2.76	4.92
70	2.8	3.54	5.61
80	3.31	4.9	6.3
90	3.78	5.95	6.9
100	4.39	6.72	7.56

Under the existence of a 30-message count, the IBGS model shows a minimum energy consumption of 1.34J whereas the PSKA and IBAAKA models require higher energy consumption of 1.86J and 2.91J respectively. Under the existence of a 40-message count, the IBGS model shows a minimum energy consumption of 1.76J whereas the PSKA and IBAAKA models require higher energy consumption of 1.98J and 3.57J respectively. Under the existence of 50 message count, the IBGS model shows a minimum energy consumption of 2.15J whereas the PSKA and IBAAKA models require higher energy consumption of 2.47J and 3.86J respectively. Under the existence of 60 message count, the IBGS model shows a minimum energy consumption of 2.43J whereas the PSKA and IBAAKA models require higher energy consumption of 2.76J and 4.96J respectively. Under the existence of 70 message count, the IBGS model shows a minimum energy consumption of 2.8J whereas the PSKA and IBAAKA models require higher energy consumption of 3.54J and 5.61J respectively. Under the existence of 80 message count, the IBGS model shows a minimum energy consumption of 3.31J whereas the PSKA and IBAAKA models require higher energy consumption of 4.9J and 6.3J respectively.

Under the existence of 90 message count, the IBGS model shows a minimum

energy consumption of 3.78J whereas the PSKA and IBAAKA models require higher energy consumption of 5.95J and 6.9J respectively. Under the existence of 100 message count, the IBGS model shows a minimum energy consumption of 4.39J whereas the PSKA and IBAAKA models require higher energy consumption of 6.72J and 7.56J respectively.

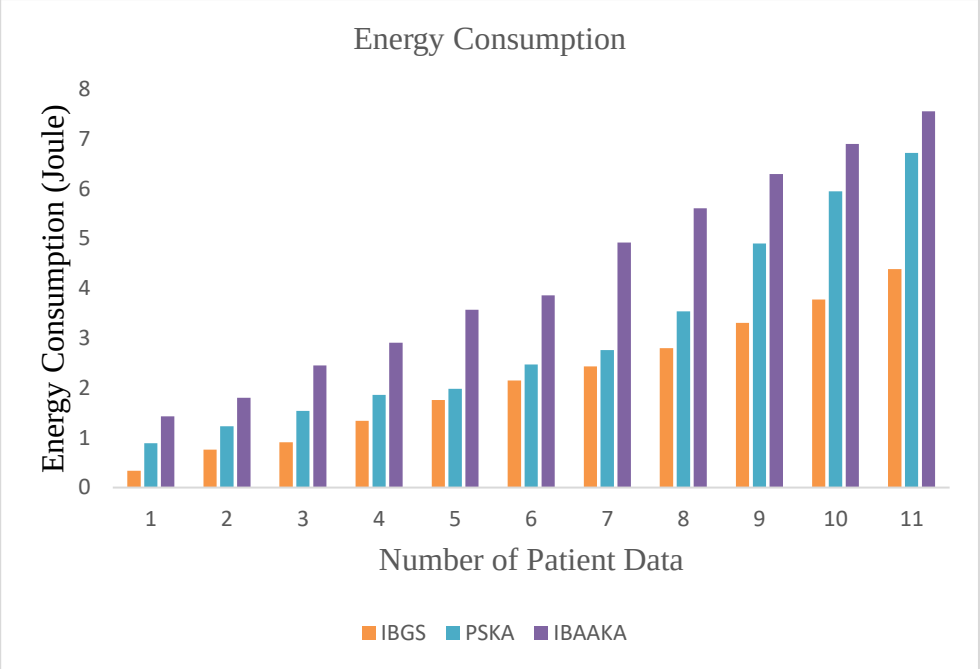

Figure 3.9. Energy consumption analysis

3.4.8 Measurement of Security on Patient's Health Information

The security ratio is defined as the ratio of the number of patient data that are securely transferred to the total number of patient data. The security ratio that is based on the patient's health information is generally measured in terms of percentage (%) and is formulated mathematically as

$$\text{Security Ratio} = \frac{N_{td}}{N_t} \tag{11}$$

Where, Ntd - Number of Patient data that securely transferred to the destination

Nt - Total Number of Patient data

The method is said to be more efficient when the security ratio of patient's health information is higher. In the proposed IBGS method, relay points are used for identifying power position authority and the allocation of resources are considered for measuring security. If high security is to be achieved, a reliable method is essential.

Table 3.9. Tabulation for the security of patient's health information

Number of patient data (Nt)	Security Ratio		
	IBGS	PSKA	IBAAKA
1	72.13	56.73	48.13
10	76.44	58.12	50.12
20	79.13	60.23	52.76
30	82.13	62.56	54.77
40	85.55	65.67	57.56
50	87.56	68.89	59.34
60	88.68	71.45	61.56
70	90.23	74.67	63.45
80	92.34	76.68	65.22
90	94.77	78.93	67.47
100	96.75	82.12	69.23

Table 3.9 shows the security measure for different patients' information for the proposed IBGS approach in comparison with two other existing methods i.e., PSKA and IBAAKA respectively. The number of patient data in WBAN is varied from 1 to 100 in WBAN. The table shows that the security ratio of patient data using the IBGS method is higher when compared to other existing methods. Sensor nodes (i.e., patients) are increased in the range of 10 to 100 in WBAN. For the increase in the number of sensor nodes, the security ratio also increases for all methods. From Table 3.9, the designed IBGS approach is seen to provide more security for patients' health information when compared to other methods. If the system/network includes higher security, then the network optimizes the packet delivery rate, throughput and network lifetime, and so on.

Higher security may lead to more complexity. Therefore, Identity Based Group Signature algorithm is used in the IBGS method for discovering simple and complex information about the patient health's information. As a result, the information loss rate and response time also decrease thereby improving the efficiency of the IBGS approach. Security on patients' health information is evaluated concerning a different number of patients in WBAN. By taking many sensor nodes (i.e., patients) as 100 in WBAN, security on patients' health information improves up to 96.75%. The security of patients' health information is low for existing methods. The results got for the security of patients' health information for the PSKA method is 82.12% and for the IBAAKA method is 69.23%. Hence the designed IBGS approach is seen to provide higher secure patients' health information for achieving security in diagnosing health

information for multiple patients. Table 3.9 compares the security properties offered by the IBGS with existing models. It is shown that the IBGS model has offered maximum security properties over the compared methods except multi-user sharing.

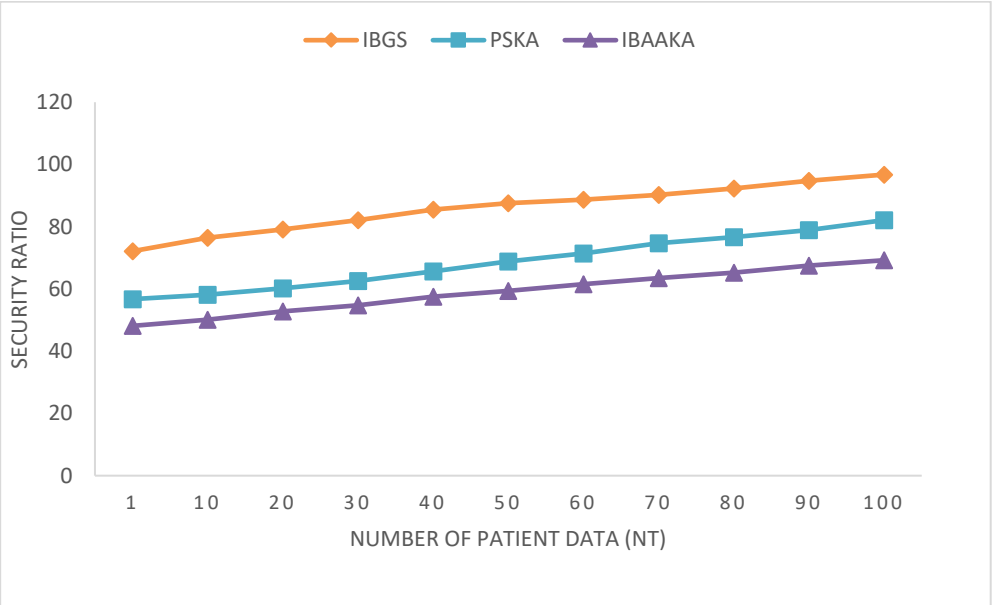

Figure 3.10. Measure of Security on patient's health information

Figure 3.10 shows that the security ratio based on the health information of the patients with the proposed IBGS method is related to 100 nodes like patients. The comparison of the IBGS method with the prevailing PSKA and IBAAKA is given in Figure 3.10. From Figure 3.10, it is evident that security has an improvement compared to the two methods. The enhancement in security is achieved in the designed IBGS mechanism by using Group Signature is implemented according to the utility function of source and upcoming intermediate nodes to achieve reliable communication by using biosensors. In addition, the privacy of the network is also preserved and resources are shared in several body sensors using Group Signature in the proposed IBGS method.

The improvement of the proposed IBGS method is calculated as below:

Improvement in percentage = Average of the improvements for 10 results =

$$\frac{Sum\ of[(Proposed\ Scheme - Existing\ Scheme) * \frac{100}{Existing} Scheme]}{10} \quad (12)$$

Hence security is improved by 25% when compared to PSKA and 48% when compared to IBAAKA respectively as in (12). Table 3.10 compares the security properties offered by the IBGS with existing models. It is shown that the IBGS model has offered maximum security properties over the compared methods except multi-

user sharing.

Table 3.10. Comparison of the security properties of the Proposed IBGS with Existing Methods

Property	IBGS	PSKA	IBAAKA
Public verifiability	1	1	1
Multi-user sharing	1	1	0
Revocability	1	1	N/A
Forward security	1	1	1
Privacy protection	1	1	0
Batch authentication	1	1	1
Proven security	1	1	1
Key replacement resistant	1	1	0
Unforgeability	1	0	0
Unlinkability	1	0	0
Exculpability	1	0	0
Traceability	1	0	0

3.4.9 System Flexibility Level

System flexibility level is measured based on patient's health information in IBGS approach. Relay points are used for identifying power position authority and allocation of resources are considered for measuring security. If the system flexibility level is high, then this method is considered as more efficient.

Table 3.11. Tabulation for System Flexibility Level

Number of Patient Data	System Flexibility Level (%)		
	IBGS	PSKA	IBAAKA
1	75.15	67.22	60.39
10	76.25	68.52	61.63
20	77.39	69.74	62.92
30	78.62	70.86	64.18
40	79.83	72.16	65.36
50	81.34	73.35	66.83
60	82.33	76.58	68.15
70	83.56	77.31	70.36
80	84.71	78.52	71.42
90	86.02	79.82	72.65
100	88.17	80.72	74.12

Table 3.11 shows the system flexibility level for different patients' information for the proposed IBGS approach in comparison with two other existing methods i.e.,

PSKA and IBAAKA respectively. The number of patient data in WBAN is varied from 1 to 100 in WBAN. The table shows that the system flexibility level of patient data using IBGS method is higher when compared to other existing methods.

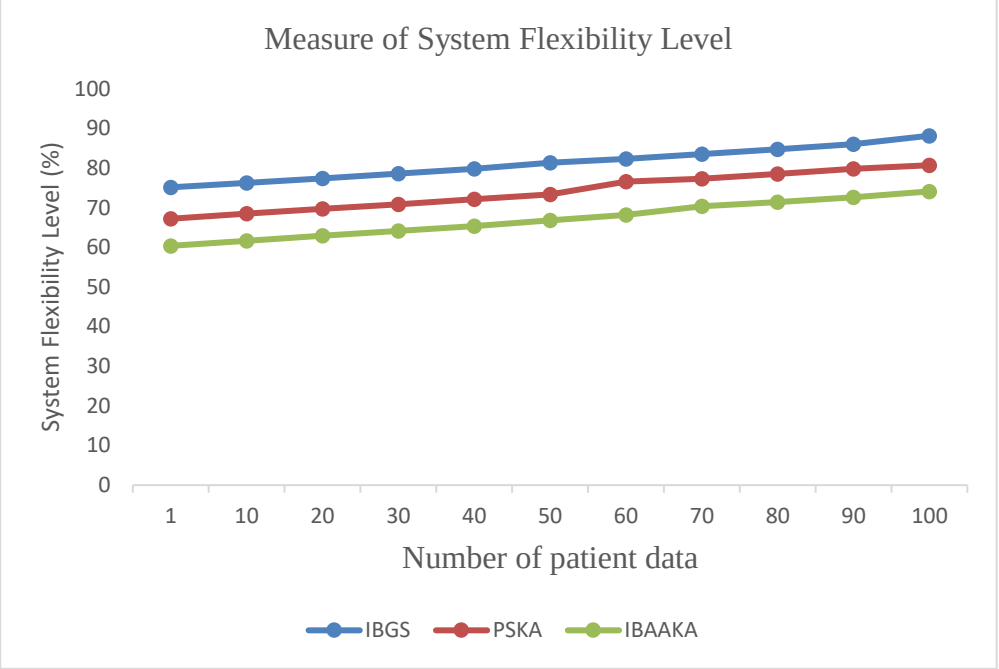

Figure 3.11. Measure of system flexibility level of patient data

System flexibility level is evaluated in terms of a different number of patients in WBAN. By taking the number of patients as 100 in WBAN, system flexibility level results in 86% in the designed IBGS method. The system flexibility level results in lower values for existing methods i.e 80% for PSKA and 73% for IBAAKA. Hence the designed IBGS approach is seen to provide better performance on system flexibility level for diagnosing health information for multiple patients. Figure 3.11 shows system flexibility level based on patient's health data related to 100 nodes with the help of the proposed IBGS method and has its comparison with PSKA and IBAAKA respectively. It is evident from Figure 3.11 that the level of system flexibility is much better than the remaining two methods. Such positive change in the level of system flexibility level is possible through IBGS mechanism with the aim of achieving reliable communication by using biosensors.

The improvement of the proposed IBGS method is calculated as below: Improvement in percentage

Average of the improvements for 10 results =

$$\frac{Sum\ of\ [(Proposed\ System - Existing\ System) * \frac{100}{Existing\ System}]}{10} \quad (13)$$

As in (13), Hence system flexibility level is improved by 10% when compared to PSKA and 21% when compared to IBAAKA respectively.

3.5 SUMMARY

WBSN is constrained by a problem of security level and privacy for given data. In this paper, a new authentication using IBGS protocol has been proposed to provide security to the WBSN. The proposed method employs an identity-based group signature algorithm between biosensors and GM. An extensive set of experiments were carried out and the results are examined in terms of Delivered Packet Ratio, Average delay, Key Mismatching Ratio, Computation Cost, Consumption Analysis, data privacy rate, information loss rate, System Flexibility level and Measurement of security on patient's health information under the varying number of messages. the experimental results show that the designed IBGS approach effectively reduces energy consumption by 19% when compared to existing PSKA and IBAAKA methods. Under the applied set of 100 messages, the proposed IBGS model achieves a minimum computation cost of 32s with the least energy consumption of 4.39J. Then, an identity-based group signature algorithm is implemented in the designed method by using a Utility function to measure the source and forthcoming intermediate node. Hence the strength of the solution is increased with higher security. Therefore, the IBGS approach improves security by 37% when compared to PSKA and IBAAKA methods.

CHAPTER – 4

AN ENERGY EFFICIENCY BASED SECURE DATA TRANSMISSION IN WBSN USING NOVEL ID-BASED GROUP SIGNATURE MODEL AND SECC TECHNIQUE

4.1 INTRODUCTION

Wireless Body Sensor Network (WBSN) is a wireless network of wearable sensing and computing devices connected through a wireless communication channel. It enables continuous monitoring through sensors for medical and nonmedical applications. WBSN faces several security problems such as loss of information, access control, and authentication. As WBSN collects vital information and operates in an unfriendly environment, severe security mechanisms are needed in order to prevent the network from anonymous interactions. The data transmitted through the sensor networks among smart wearable devices help to analyze various security threats. The data transmission using sensor networks may consume more energy, which minimizes the entire network lifetime as well as reduce the data transmission quality. Hence, in this paper, an energy-efficient secure data transmission mechanism is proposed in WBSN using a novel authentication id-based group signature (IDGS) model and SECC technique.

At first, the Group Manager (GM) is selected from the sensors in the remote body sensor system using Normalized Opposition Based Learning BAT Optimization Algorithm (NOBL-BOA). Afterward, clustering with Information Entropy induced K-Means Algorithm (IEKMA) takes place to improve energy efficiency. Next, to provide security to the WBSN, message authentication is carried out based on novel authentication ID-based group signature protocol. Finally, Secret key induced Elliptic Curve Cryptography (SECC) is used to encrypt the message for secure transmission. The simulation results reveal that in comparison with existing works, the proposed work achieves improved security and energy efficiency.

The wireless sensor network provides a significant advantage in health monitoring applications for the next evaluation [155]. Major advancements in wireless sensor network algorithms and applications have stimulated the emergence of specialized biological networks termed Body Sensor Networks (BSNs) or Body Area

Networks (BANs) [156]. This Wireless Body Sensor Network (WBSN) is a type of wireless sensor network (WSN) that is specifically related to healthcare applications [157]. In healthcare monitoring, the sensor nodes are either placed over the surface of the human body or implanted into the human body tissues for monitoring the useful parameters accurately [158]. The sensors in WBANs are said to perform three main tasks, i.e., sensing patients' vital signs, processing and communicating data [159]. The sensor nodes gather all the necessary physiological parameters of the human body such as ECG, pulse, and blood pressure [160]. These biosensors collect physical data via Body Sensor Units (BSUs) and transmit it to its final destination (gateway, base station, personal display assistant) via the Body Control Unit (BCU) for further analysis [161]. As the WBAN reap the benefits of continuous progress, it will not only be employed in medical but will also be integrated into the military applications and sports activities and can save human lives [161, 162]. Although WBANs improve the quality of health care service and bring a lot of convenience to people's lives, security and privacy have always been critical issues in WBANs based health care monitoring services [163].

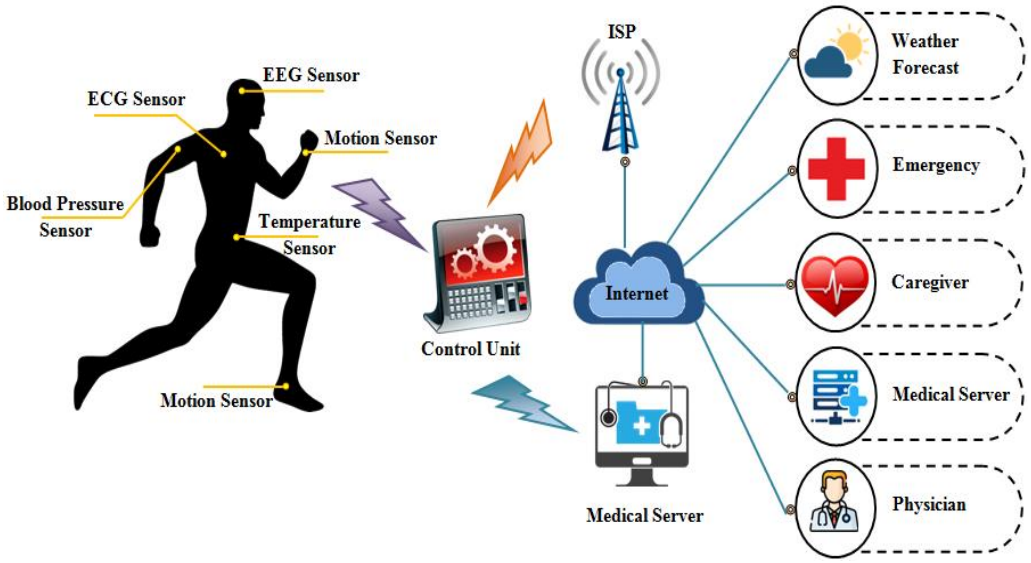

Figure 4.1 General architecture of WBSN

In remote patient monitoring, trusted information has great importance for healthcare providers due to the sensitivity of data [164]. WBANs deal with several critical health-related parameters and the output obtained should be accurate, reliable, trustworthy, and authenticated [165] because it impacts patients' health and life as shown in the Figure 4.1 [166]. Since these sensitive patient data are the basis of clinical

diagnosis, any data leakage or modification may put the patient's life at risk [167]. Now a days, WBANs are not only used in health monitoring, but also sport training, entertainment, military activities, etc. [168]. But security issues including outsider attacks like eavesdropping, malicious attack and insider attacks by compromising sensor nodes can easily affect the data integrity, freshness and confidentiality [169]. Security and privacy of medical data transfer from WBAN to the gateway or towards a remote server are major concerns for the acceptance of Health systems and their adoption [170]. Actually, WBANs technology will not be adopted since there are still security concerns regarding the WBANs [171]. Therefore, with the given resource constraints and issues of security and privacy in WBAN, it is necessary to come up with a stronger solution. Hence in this paper, an energy-efficient secure data transmission mechanism is proposed in WBSN using a novel authentication id-based group signature model and SECC technique.

4.2 MOTIVATION BEHIND THE WORK

Kakali Chatterjee [172] presented a strong mutual authentication protocol based on public-key cryptography for satisfying all security requirements. The data collected by all sensor nodes were sent to the gateway node. The gateway node sent data to the local processing centre (Base Station) through the network coordinator which was called User Device. All the captured data was gathered in the health cloud through that device. The scheme used Pallier cryptosystem which was mainly used for privacy preservation of sensor data. The experiment results showed that the scheme resisted the major vulnerable attacks in wireless body sensor networks with low computational load and communicational load. The drawback of this method was that it was very slow because Pallier cryptosystem uses large keys to obtain the security.

Subramani Jegadeesan et al. [173] explored an Efficient Privacy-Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (EPAW). The method had three phases such as system initialization, registration and EPAW anonymous mutual authentication. The work was different in two aspects; first, the users were authenticated anonymously and preserved the actual identities of the user from other users. Next, the tracking mechanism gave conditional privacy by disclosing the actual identities of misbehaving doctors. The experimental simulation results ensured that the anonymous authentication method outperformed the existing systems in terms of providing data security and privacy with less computational

overhead. However, this system has the limitation that it may be vulnerable to some type of attacks like reverse configuration attack.

Tallat Jabeen et al. [174] developed a data protection genetic-based encryption scheme for higher performance. Nano sensors were involved in the body area networks that generated patient data and transferred it towards Message Queuing Telemetry Transfer (MQTT) broker while MQTT was a public-subscribe messaging protocol. The encrypted data from the MQTT broker was forwarded towards the internet cloud, which was connected to the medical server. The medical server used to store and retain health critical data must be secured unconditionally. In comparison with the LEACH protocol, the proposed MQTT protocol was very secure and lightweight because of its built-in feature of authenticity. On the other hand, the genetic algorithm took 8 bits of plain text as input and converts it into binary number. So, if large bits of plain text were present, then the loss of main data may occur.

Hyunho Ryu and Hyunsung Kim [175] implemented a privacy-preserving authentication protocol for WBANs in healthcare services. The protocol was only based on a one-way hash function and with exclusive-or operation, which was lightweight. The protocol had four phases, first of all, the initialization phase set up a security building block for the overall network. The patient possessed sensor nodes and access points were a target for the registration phase. The authentication phase was for the basic security service to check whether the entity was legal or not and was also to set up a session key for further secure communications. The identity modification phase was used when PT wanted to change SN's identity for privacy reasons. Furthermore, comparison results showed that the protocol achieved more privacy and security features than the other protocols. On contrary, the use of one-way hash function may weaken the security of the system upon repeated use.

Mengxia Shuai et al. [176] presented an efficient and privacy-preserving authentication scheme for WBANs using elliptic curve cryptography (ECC). In the scheme, the method of certificate-less authentication based on identity-based cryptography was adopted, which made it suitable for multi-server architecture without online third-party participation. Security analysis and comparisons with five related authentication schemes demonstrated that the privacy-preserving authentication scheme not only provided the desired security features but also reduced the computation cost effectively. But, in this method patient side operational and

communicational overhead was not considered was the downside of this technique.

Mahender Kumar and Satish Chand [177] projected an identity-based anonymous authentication and key agreement (IBAAKA) protocol for WBAN in the cloud-assisted environment. The presented IBAAKA protocol consisted of three algorithms: setup, registration, and authentication. It ensured that a user's identity remains to hide except the network manager in the registration phase. The security analysis showed that under the random oracle model (ROM) and computational Diffie-hellman (CDH), the assumption developed IBAAKA protocol was provably secured as well as had the potential to achieve required security properties. The result comparison showed that the scheme has the least computation and comparable communication cost than existing techniques. Nevertheless, the encryption operation was highly expensive and not really considered an option for providing message confidentiality in Body Sensor Network environments.

Bhawna Narwal and Amar Kumar Mohapatra [178] propounded a secure and anonymous mutual authentication scheme for WBANs (SAMAKA). In particular, SAMAKA preserved all the desired security features and guards from various security attacks from an adversary. This model presented a secure and anonymity-preserving authentication scheme that mutually authenticated the sensor node (SN) and chief node (CN) via mid node (MN) and agreed on a session key securely by utilizing simple hash and XOR operations. For validating the security of SAMAKA from various adversarial attacks, to attain mutual authentication and ensure secure session key agreement, BAN Logic, AVISPA tool, and RoR Model was used. Moreover, the informal security analysis was presented to highlight that SAMAKA attained the necessary security features and prevented adversarial attacks. Finally, a comparative performance analysis revealed that SAMAKA achieved superior performance and showed promising results. However, the limited memory resources, battery power, and processing capabilities of the body sensor nodes make the implementation of security system very complex and challenging.

Bhawna Narwal and Amar Kumar Mohapatra [179] developed a secured energy-efficient mutual authentication, and key agreement scheme (SEEMAKA) for two-tier WBAN. SEEMAKA achieved desirable security properties and thwarts different security attacks using fewer hash invocations and bitwise XOR operations, nicely meeting the need for limited capable sensor nodes. Security of SEEMAKA was

assessed through sound informal analysis as well as using Automated Validation of Internet Security Protocols and Applications. For verifying the correctness of SEEMAKA, BAN Logic was used. A set of thorough relative analyses between SEEMAKA and other recent authentication schemes was performed and the results manifested that SEEMAKA achieved superior efficiency concerning processing overhead, energy dissipation, and security features. On the other hand, optimization of route selection and the energy conservation goal was not specified in this approach.

M.AYYADURAI et.al [180] presented Data Encryption and Signature-based Authentication protocol (DESA) scheme to provide reciprocated authentication based on signature verification ID for WBSNs. To offer secured communication with low overheads, this mechanism was developed in order to ensure the secrecy of the sensed data within the WBSN entities. The sender sent the encrypted message text labelled with the set of attributes and the signature ID was assigned properly to indicate node authentication. The authorized signature ID was verified and the data encryption was done at the receiver end. Therefore, the presented DESA scheme could tolerate a number of security attacks; provide high security compared to existing security mechanisms. Experimental outcomes revealed superior performance compared to that of baseline techniques. Conversely, energy efficiency was not considered in this model which in turn increased the computational time required for data transmission.

4.3 METHODOLOGY

Advances in wearable devices over the past decade have led to sensors, displays, and smart devices that seamlessly operate on the body. Such advances in wireless low-power sensors and the increasing demand for portable healthcare monitoring systems have inspired the realization of Wireless Body Sensor Networks (WBSNs). WBSN is the collection of sensor nodes placed in, on, or around the human body which monitors the physiological signals. Several sensors and sensor systems such as an electrocardiogram (ECG), electromyogram (EMG), blood pressure (BP) and pulse oxygen saturation (SpO2), etc are collected and the information is then transmitted to a sink node for processing. Although the WBSN technologies bring obvious and attractive benefits to facilitate people's life activity, security and privacy are one of the major problems in WBSN. Due to limited bandwidth resources and computing capabilities, wearable WBSN devices provide less security and authentication system. Also, the energy supply for the sensor nodes is one of the major hurdles in the

development and widespread deployment of WBSNs. To overcome these drawbacks, a novel authentication ID-based group signature model (IDGS) and SECC technique is proposed in this work, to improve the security and energy efficiency of WBSN. The structural design of the proposed system is given below in Figure 4.2.

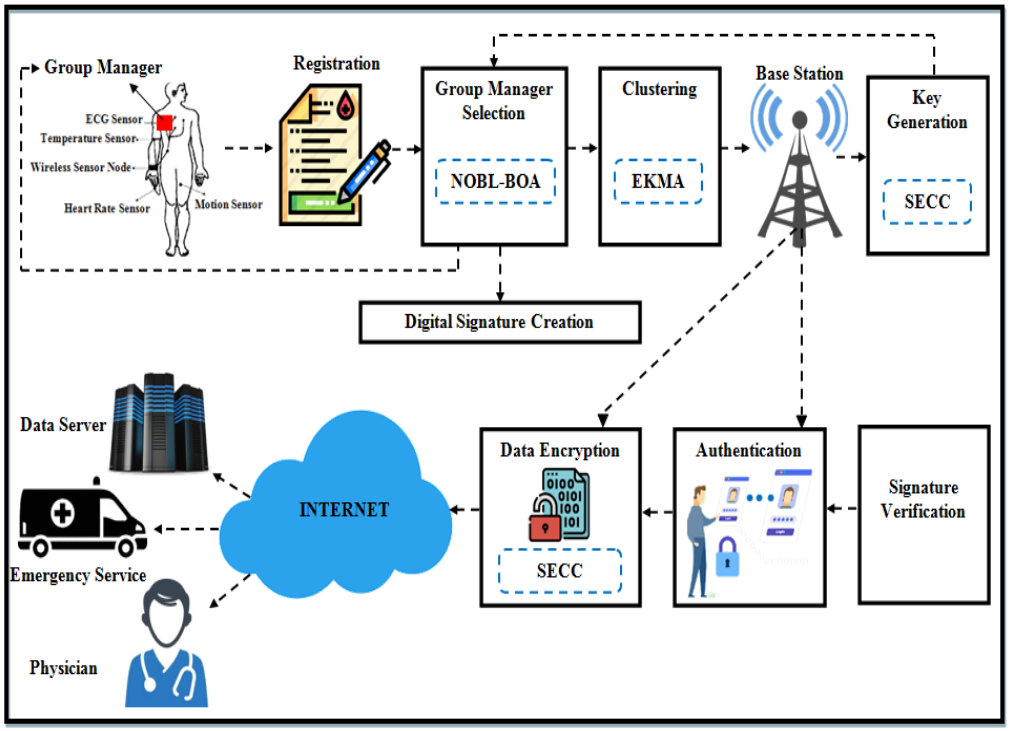

Figure 4.2 Structural design of the proposed system

Figure 2 explains the working flow of the proposed secure data transmission in WBSN system. Initially, the patient who uses the wireless sensors registers their details with the corresponding hospital and obtains a unique registration number. Afterwards, Group Manager is selected from a group of sensor nodes using NOBL-BOA optimization technique. Then, the group managers are clustered together by means of IEKMA clustering method, which improves the energy efficiency of the system. After that, message authentication is carried out between the GM and the Base Station (BS) using the ID-based Group Signature protocol. This verifies that, whether the incoming body sensor data is coming from authorized node or not. On successful authentication, the data is encrypted using SECC encryption technique in order to avoid attacks. Finally, the encrypted data is decrypted and forwarded to the doctor, emergency services and also stored in the data server.

4.3.1 Registration Phase

To begin with, the patient who uses the wireless sensors registers their details

with the corresponding hospital and obtains a unique registration number, and the number is kept confidential. The different number of sensors to sense the information such as temperature, blood pressure, heart rate, etc is attached to the patient's body. These sensors also contain distinctive IDs under the registration number. These sensors form a group and a group manager for this group is selected for efficient transmission of data. The number of sensors implanted on the patient body $\left(s^i\right)$ is represented as,

$$s^i = s^1, s^2, \ldots\ldots, s^n \tag{1}$$

In equation (1), n determines the number of sensor nodes placed on the human body.

4.3.2 GM Selection With NOBL-BOA

The Group Manager (GM) for a group of sensor nodes is selected based on the NOBL-BOA optimization technique. BAT Optimization Algorithm (BOA) is a population-based optimization model inspired by the biological characteristics of food searching and predation behavior of bats. This algorithm consists of four main parameters, frequency, emission, constants, and emission rate. BAT uses echolocation to identify the difference between food and prey. In this technique, the maximum and minimum frequency range of BAT in updating its position is calculated using a random uniform distribution method. Also, the local search of BAT is performed based on random walks. Such random distribution and random walks may tend to local optimum solutions and decrease the convergence rate. To overcome these drawbacks, the Min-Max normalization technique is used to compute the frequency range of bats. And, Opposition Based Learning (OBL) is used for the local search process. OBL is used to enhance diversity and improve the generated solution. These enhancements in conventional BOA are named as Normalized Opposition Based Learning BAT Optimization Algorithm (NOBL-BOA). The optimization procedure of NOBL-BOA is detailed below.

Step 1: Let the initial population of the bat be $s^i = s^1, s^2, \ldots\ldots, s^n$ (number of sensor nodes). Each bat i consists of a definite position x^i with velocity v^i, and frequency f^i. During optimization, each BAT is assigned a uniform frequency

between $\left(f^{\min}, f^{\max}\right)$. The frequency of bat when it searches for prey is given by,

$$f^{i} = f^{\min} + \varepsilon\left(f^{\max} - f^{\min}\right) \tag{2}$$

Where, $f^{\max}, f^{\min}$ indicates the maximum and minimum frequency range and ε is the normalized frequency range computed using min-max normalization,

$$\varepsilon = \frac{f^{i} - f^{\min}}{f^{\max} - f^{\min}} \tag{3}$$

Step 2: The velocity of the bat searching for prey at a time (t) is computed using equation (4),

$$v_{t}^{i} = v_{t-1}^{i} + f^{i}\left(x_{t-1}^{i} - x''\right) \tag{4}$$

Here, v_{t-1}^{i} defines the flight speed of the bat at a time $(t-1)$, x_{t-1}^{i} denotes the position of the bat at a time $(t-1)$ and x'' illustrates the current best bat position.

Step 3: The Bats' position is updated as,

$$x_{t}^{i} = x_{t-1}^{i} + v_{t}^{i} \tag{5}$$

Step 4: The BOA contains both the global and local search capabilities which depend on its parameters. Thus, the balance between the local and global search is achieved by selecting adaptive parameters. The local search strategy is estimated using opposition-based learning, which is computed as follows,

$$\hat{x} = f^{\min} + f^{\max} - x^{old} + \delta L_{t}^{i} \tag{6}$$

In the above-mentioned equation, $f^{\min} = 0$ and $f^{\min} = 1$, δ shows the random number uniformly drawn in the range $(0,1)$, x^{old} signifies the old position and L_{t}^{i} is known as the average loudness of all bats at a time (t). The condition for bat moving towards the prey (χ) is,

$$\chi = \begin{cases} p & \delta < L_{t}^{i} \\ \hat{x} & else \end{cases} \tag{7}$$

In this equation (7), p signifies the movement of the bat towards the prey

(optimal solution). Then, the new solution is obtained and the loudness and emission rates are updated to control the exploration and exploitation.

Step 5: The loudness and emission rate are updated as follows,

$$L_{t+1}^{i} = \eta L_{t}^{i} \tag{8}$$

$$e_{t+1}^{i} = e_{0}^{i} + \left\langle 1 - e^{-\psi t} \right\rangle \tag{9}$$

Where, η and ψ are constants in which $\eta, \psi > 0$, e_{t+1}^{i} specifies the emission rate at the time $t+1$ and e_{0}^{i} is the initial value of emission rate. Finally, the global optimal solution (Group Manager) is obtained which is denoted as S^{k}, k is the $k-th$ sensor node from the set of sensor nodes s^{i}. The Pseudocode of the NOBL-BOA is given in figure 4.3.

Pseudocode for NOBL-BOA

Input: Number of sensor nodes s^{i}

Output: General Manager S^{k}

Begin
Generate the initial bat population s^{i}
Characterize frequency f^{i}, velocity v^{i} at x^{i}
Initialize loudness L^{i} and emission rate e^{i}
While $t <$ max
    For each bat s^{i} **do**
        Fine-tune frequency f^{i}
        Keep posted $v_{t}^{i} = v_{t-1}^{i} + f^{i}\left(x_{t-1}^{i} - x''\right)$
        Update Bats' position x^{i}
        If $\varepsilon > e^{i}$
            Pick the best solution
            Compute local search using OBL
        End if
        If $\delta < L_{t}^{i}$
            Recognize the optimal solution
            Renew loudness using $L_{t+1}^{i} = \eta L_{t}^{i}$
            Revise emission rate e_{t+1}^{i}
        End if
    End for
    Rank the solution and obtain S^{k}
End while
End

Figure 4.3: Pseudocode for NOBL-BOA

4.3.3 Clustering by Means Of IEKMA

After selecting the Group Manager (GM), they are clustered together by calculating the distance between the base station and the group manager. This is done using the IEKMA algorithm. In general, K-Means Algorithm (KMA) is a distance-based clustering algorithm that divides the data into a number of clusters. Then, cluster centers are selected randomly from the range of available base stations and the distance is computed. Based on the distance, the data is mapped into the smallest distance measure. However, K-Means has a difficulty that, it depends on the initial cluster center determination where initial cluster centroids are chosen randomly. This random selection results in the local optimum solution. For that reason, in the proposed work, Information Entropy (IE) is used to select the cluster centers. This initialization increases the clustering accuracy. The adaption of IE in the conventional KMA is known as IEKMA. It is explained further.

Step 1: Consider the set of group managers $\left(G^j = G^1, G^2, \ldots\ldots, G^m\right)$ where, m models the number of group managers in the hospital and the N number of available base stations (cluster centroids) $\left(B^k = B^1, B^2, \ldots\ldots, B^N\right)$. At first, IEKMA determines the number of clusters.

Step 2: Next, to calculate the distance between the GM and Cluster centroids, the cluster centroids are evaluated using the information entropy equation. In IE, the probabilities are computed based on the relative frequencies, which is given as follows,

$$\tau = -\sum_{k \in N} p\left(B^k\right) \log_2 p\left(B^k\right) \tag{10}$$

In (10), τ means the information entropy and $p(\circ)$ mentions the probability value. The optimized centroid calculated from equation (10) is $\left(B^{\hat{k}}\right)$.

Step 3: Then, the Euclidean distance (d) is used to compute the distance between GM and optimized cluster centroids. The Euclidean distance is estimated below,

$$d\left(G^j, B^{\hat{k}}\right) = \left\langle \sum_{j=1}^{m} \left(B^{\hat{k}} - G^j\right)^2 \right\rangle^{1/2} \tag{11}$$

Step 4: Based on the distance, the GM is allocated to the nearest base station (cluster centroids) for efficient transmission of data without any loss and it also improves the lifetime of the WBSN network. This can be mathematically notated as,

$$G^j = \begin{cases} 1 & \min\left\{d\left(G^j, B^{\hat{k}}\right)\right\} \\ 0 & otherwise \end{cases} \tag{12}$$

Where, 1 mention the allocation of the GM to the particular base station and 0 means GM is not assigned to that base station and is used for further process.

Step 5: The process continues by recalculating the cluster centroids and calculating the distance between GM and Cluster centroids and assigning the GM to the minimum distance cluster centroids (base station). The process is repeated until the cluster centers are not changed. In this way, the GMs are allocated to the nearest base station.

4.3.4 Authentication Using ID Based Group Signature Model

In this phase, authentication of messages is carried out between the GM and the Base Station (BS) using the ID-based Group Signature protocol. The ID-based technique allows users' public key to be distinctively derived from their identity and a group signature model allows its group member to sign a message on behalf of the group. The proposed ID-based group signature method comprises Trusted Authority (here, Base Station is considered as the trusted authority) for generating the secret key for the group manager based on the group ID. After generating the Secret key, the Trusted Authority (TA) transmits the generated secret key to the GM. Then, to sign a message, the GM performs signature computation on the message transmitted by one of its member nodes using the generated keys and transmits the message to the BS. BS performs signature verification, and upon successful verification, the BS accepts the message and encrypts it for secure transmission. In the proposed work, the public key and private key of the GM are generated using the Secret key induced Elliptic Curve Cryptography (SECC) algorithm. The working procedure of the ID-based Group Signature technique is detailed as follows.

Step 1: At first, each sensor node should register to the base station and they are assigned a unique ID represented as $\left(x^h\right)$where, $h = 1,2,\ldots,n$ and the ID of the group manager is denoted as γ .

Step 2: Initially, the TA generates its own public key, secret key and public system parameters. For that, TA selects two prime numbers $A1$ and $A2$ where, $\frac{A1-1}{2}$ and $\frac{A2-1}{2}$ are smooth, odd, and co-prime. Consider, $B = A1 \cdot A2$ and select two integers b, c such that,

$$bd \equiv 1 * |\varphi(B)| \tag{13}$$

$$ce \equiv 1 * |\varphi(B)| \tag{14}$$

Where, c is kept as a secret key, b is kept as a public key and d, e are considered as public system parameters of the TA.

Step 3: Next, the secret key and public key for the group manager are computed using the SECC method. The Elliptic Curve equation is cited below,

$$y^2 = x^3 + ax + b(\text{mod } p) \tag{15}$$

Once the integers are mapped into the curve point, the public and private keys are generated. Private Key of GM (g^m) is generated using the secret key c of the TA and the ID of GM γ and is given by,

$$g^m = c * \gamma * |\varphi(B)| \tag{16}$$

Then, the public key (P^{gm}) of GM is calculated as,

$$P^{gm} = g^m \cdot G \tag{17}$$

In equation (17), G indicates the generator point of the elliptic curve.

Step 4: After generating the keys, the TA sends P^{gm}, g^m, d, e to the GM. In the same way, the TA generates the keys for each biosensor using the secret key of TA and the ID of each biosensor.

Step 5: When a new member joins the group, the TA calculates the secret key (s^k) as,

$$s^k = \left(ID^{new}\right)^{P^{gm}} * \bmod(B) + x^h \tag{18}$$

Where, ID^{new} mentions the ID of the new member. Also, the GM evaluates the public key parameter $\left(k^p\right)$ using equation (19),

$$k^p = ID^{new} * \bmod(n) \tag{19}$$

The user membership certificate is the following pair $\left(s^k, k^p\right)$. Afterward, the GM transmits the keys securely to each biosensor. Thus, a biosensor has secret keys $\left(s^k\right)$ and member certificate parameters $\left(k^p\right)$.

Step 6: To sign a message M , the GM performs group signature computation on the message transmitted by one of its member nodes by using γ (GM ID), g^m (secret key of GM), and d, e (public system parameters). The Group signature is estimated as follows,

$$Z = M^{g^m} * \left(P^{gk}\right)^{d+2e-1+1} \bmod(B) \tag{20}$$

$$F = k^p \left(P^{gk}\right)^{s^k+\gamma+r_1} * |B| \tag{21}$$

$$H = k^p \left(P^{gk}\right)^{r_2} \bmod(B) \tag{22}$$

$$T = s^k h(M // Z) + r_1 h(M // Z) \tag{23}$$

In the above equations, $r_1 \& r_2$ signifies the random number and $h(\bullet)$ specifies the publically known hash function.

Step 7: After generating the group signatures, verification is done at the base station (TA). To verify the signatures, Z, F, H, T indicates the valid group signature for the message M . The verification process is mathematically denoted as,

$$H^{eh(M // Z)} * \left(k^p\right)^{eT} \equiv F^{eh(M // Z)} + r_1 h(M // Z) \tag{24}$$

If the verification is successful, the base station accepts the message and encrypts it for secure transmission. If the verification becomes unsuccessful, then the group manager opens the signature to verify the signature issued by the biosensor based on

their unique IDs.

4.3.5 Data Encryption Via SECC

This is the final step of the proposed secure data transmission in the WBSN technique. After signature verification, the data is encrypted in order to avoid attacks. The data encryption is performed with respect to SECC. Elliptic Curve Cryptography (ECC) is an asymmetric cryptographic technique in which each user has its own public and private keys. These keys are further used for data encryption and decryption. To add more security in the proposed work, the conventional ECC algorithm is modified by adding the secret key of the base station while encryption, and in the decryption time, the secret key of the base station is subtracted with the decrypted message. This induction of the secret key of the base station in the general ECC is the so-called Secret key induced ECC (SECC). The steps in SECC are explained further.

Step 1: Let M be the message that is transferred from the base station to the cloud server. At first, the message is encrypted by using the public key $\left(P^{gk}\right)$ of the group manager, which is modeled in equations (25) and (26),

$$\varsigma^1 = \lambda \times P^{gk} \tag{25}$$

$$\varsigma^2 = M + \varsigma^1 + c \tag{26}$$

Here, ς^1, ς^2 shows the cipher text of GM, λ represents the random positive integer selected by the GM and c refers to the secret key of the base station. Now, the cipher texts are forwarded to the receiver gateway.

Step 2: On the receiver side, data is decrypted by using the private key $\left(u^r\right)$ of the receiver node by using the following formula,

$$M = \varsigma^2 - u^r \times \varsigma^1 - c \tag{27}$$

In this way, the sensed patient data is securely sent to the doctor without any loss in information. The ID-based group signature model provides authentication of the message and the SECC encrypts the message which denies the attacks happening during data transmission. Moreover, the efficient use of clustering increases the network lifetime and reduces data loss by assigning the shortest path between the GM and the base station. The experimental outcomes of this proposed system are discussed

in below section 4.4.

4.3.6 Security Analysis

We now examine the proposed scheme's security and show that it satisfies certain security criteria.

Theorem 1: As demonstrated in [181], The proposed scheme can be proved secure in the random oracle model, assuming the CDH problem is hard.

Theorem 1: The suggested technique may be shown secure in the random oracle model, presuming the CDH problem is difficult, as shown in [181].

Proof of Theorem 1: the probability that the challenger solves the CDH problem is

$$ProC \geq \frac{\partial}{9.nQ_1.nQ_2} \quad (28)$$

In [182], ∂ is a non-negligible probability that an adversary can win the game, where nQ_1 and nQ_2 denote the number of Q_2 and Q_2 queries, respectively. As a result, the challenger can solve the CDH problem with a non-zero $ProC$. Due to the difficulty of the CDH problem, the proposed scheme is secure under the random oracle model.

Theorem 2: The Message integrity and source authentication are both possible with the proposed scheme.

Proof of Theorem 2: The identity-based group signature model that was used in this study is existentially unforgeable against attacks using adaptive selective identity and adaptive chosen message [181]. As a result, attackers are unable to access network services by pretending to be a genuine user, and only valid users can be authenticated by sensor nodes. Additionally, hackers are unable to change broadcast messages or inject fake broadcast messages into the network. In order to accomplish message integrity and source authentication, the proposed approach is successful.

4.4 RESULT AND DISCUSSION

Here, the performance of the proposed technique is evaluated by comparing the outcomes with the existing baseline techniques. The analysis is made based on some of the performance metrics. The work is implemented in the working platform of Omnet++. The superiority comparisons are detailed below.

4.4.1 Symbols and descriptions

The detailed description of the symbols used in the proposed techniques is shown in table 4.1.

Table 4.1: Symbols and its description

Symbols	Description
s^i	Group of sensor nodes (SNs)
n	Number of sensor nodes
x^i, v^i, f^i	Position, Velocity and Frequency of bats
$f^{\max}, f^{\min}$	Maximum and Minimum frequency
ε	Normalized frequency
t	Time
v_{t-1}^i	Flight speed of bat at time $(t-1)$
x_{t-1}^i	Position of bat at time $(t-1)$
x'', x^{old}	Best position of bat, old position of bat
δ	Random number $(0,1)$
L_t^i	Average loudness of bat
χ	Condition for bat moving towards prey
p	Movement of bat towards prey
η, ψ	Constants
e_{t+1}^i	Emission rate at time $t+1$
e_0^i	Initial value of emission rate
S^k	Group Manager (GM)
B^k	Base Station (BS)
τ	Information Entropy
d	Euclidean distance
x^h	Unique Id of sensor nodes
c, b, d, e	Secret key, Public key and Public system parameters
g^m	Private Key of group manager
γ	Group manager ID
ID^{new}	ID of new member
k^p	Public key parameter
M	Message
Z, F, H, T	Group signature for message
P^{gk}	Group managers' public key
ς^1, ς^2	Cipher texts
c	Secret key of the base station
u^r	Receiver nodes' private key
λ	Random positive integer selected by GM

4.4.2 Performance assessment of proposed SECC

The results of the proposed SECC technique used for data encryption and decryption are evaluated by means of Encryption Time (ET), Decryption Time (DT), and Security Level (SL). The existing techniques used for the comparison of proposed SECC are Elliptic Curve Cryptography (ECC), Rivest-Shamir-Adleman (RSA), Elgamal, and Diffie-Hellman. The graphical representation of the encryption time taken by the proposed SECC to encrypt the input message is publicized below the Table 4.2.

Table 4.2. Tabulation for ET, DT and SL

Techniques	Encryption Time (ms)	Decryption Time (ms)	Security level (%)
Proposed SECC	2976	3470	96.923
ECC	3807	3896	94.748
RSA	4318	4598	92.125
Elagamal	5193	4588	91.852
Diffie-Hellman	5927	5536	89.794

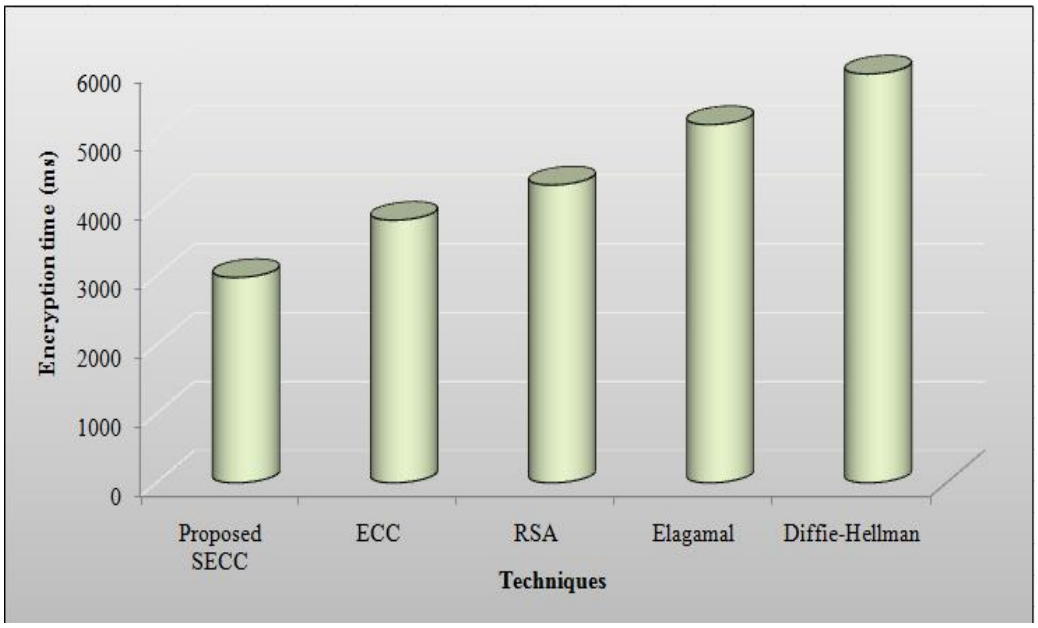

Figure 4.4 Encryption time comparison of proposed SECC

The above figure 4.4 determines the encryption time of the proposed and existing techniques. Encryption time is defined as the time taken by the encryption algorithm to create a cipher text from the plain text. The lower time taken by the system mentions

the better performance achieved. Therefore, from figure 4.4, the encryption time taken by the proposed SECC is 2976ms. On the other hand, the existing techniques have an encryption time of 3807ms (ECC), 4318ms (RSA), 5193ms (Elgamal), and 5927ms (Diffie-Hellman). While comparing the values of both the proposed and existing methods, the proposed SECC has a lower encryption time, which means that the proposed method performs well than the other techniques. The decryption time comparison is estimated in figure 4.5.

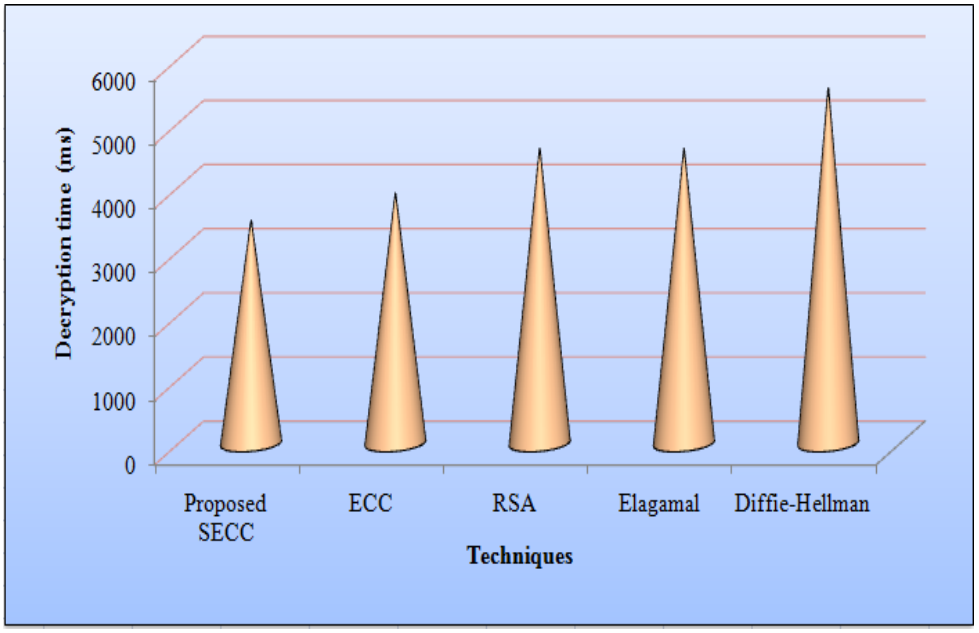

Figure 4.5 Decryption time assessment of proposed SECC with existing ECC, RSA, Elgamal, and Diffie-Hellman

Figure 4.5 depicts the decryption time of the proposed and existing algorithms. The decryption time is the time taken to convert the altered data into its original form. Here, the proposed system requires 3470ms to decrypt the encrypted data. But, the conventional ECC needs 3896ms which is 426ms higher compared to the proposed system. Likewise, other existing methods also take a longer time than the proposed model. So, it is well clear that the proposed system is better than the other state-of-the-art techniques. The security level achieved from the proposed work is graphically represented as follows.

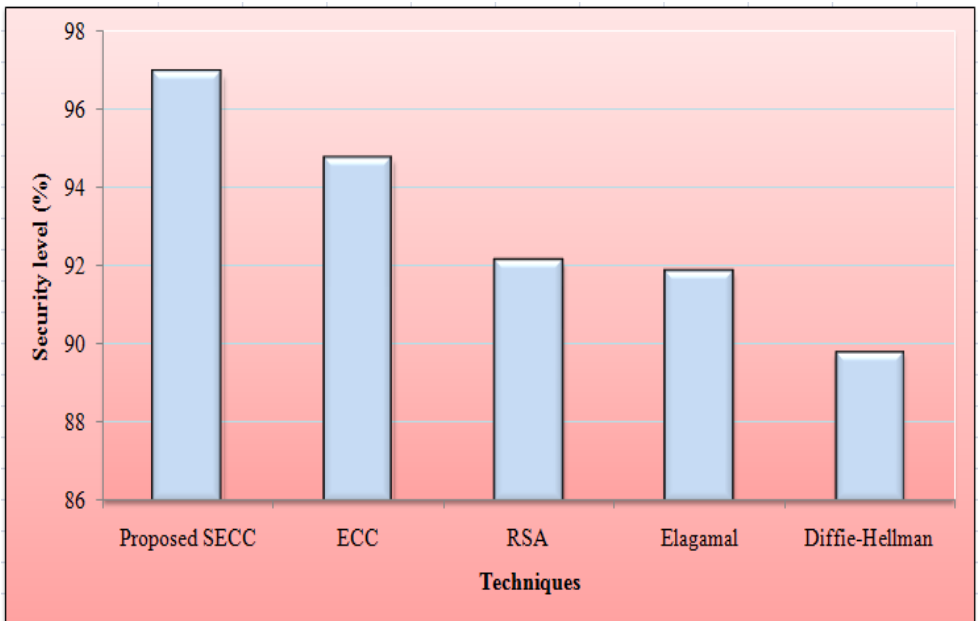

Figure 4.6 Security level analysis of proposed SECC

In the above figure 4.6, the security level attained by the proposed system is compared with some of the existing techniques. From the graph, the security level obtained by the conventional ECC algorithm is 94.748%. However, by including the secret of the base station in the general ECC for enhancing security, the SECC attains 96.923% security which is higher compared to the existing ECC. Also, other existing techniques such as RSA, Elgamal, and Diffie-Hellman have a lower security level of 92.125%, 91.852%, and 89.794% respectively. While comparing the existing and proposed methodologies, the proposed achieves higher results. Therefore, it is evident that the proposed technique is far better than the other state-of-art methodologies.

4.4.3 Superiority Measurement of Proposed Clustering Technique

The performance of the proposed IEKMA clustering technique which is used to cluster the GM based on the nearest base station is analyzed with respect to the clustering time. The results are compared with the existing K-Means Algorithm (KMA), Fuzzy C Means (FCM) technique, and K-Medoid. The outcomes are tabulated further in table 4.3.

Table 4.3. Clustering time of proposed IEKMA and existing KMA, FCM and K-Medoid

Techniques	Clustering time (ms)
Proposed IEKMA	1247
KMA	1595
FCM	1984
K-Medoid	2004

Table 4.4. Tabulation for comparison of Average Delay (AD)

Techniques	Delay in ms				
	Number of Nodes				
	20	40	60	80	100
Proposed IDGS	0.23	0.36	0.59	0.19	1.02
SAMAKA	0.63	0.75	0.88	1.34	1.48
IBAAKA	0.84	0.92	0.94	1.171	1.2
DESA	1.03	1.32	1.76	1.96	2.01
SEEMAKA	1.21	1.68	1.79	1.96	2.14

Table 4.5. Tabulation for Energy Consumption

Techniques	Energy Consumption (joules)				
	Number of Nodes				
	20	40	60	80	100
Proposed IDGS	3322.25	3273.36	4005.36	4333.24	4022.25
SAMAKA	3815.95	4001.29	4152.32	4525.32	5015.95
IBAAKA	3911.26	4143.68	4267.34	5132.85	5411.26
DESA	4216.64	4921.14	5169.25	5672.26	5875.26
SEEMAKA	4819.17	5122.24	5472.63	5651.32	6119.17

Table 4.6. Tabulation for key Mismatch Ratio

Techniques	Key Mismatch Ratio				
	Number of nodes				
	20	40	60	80	100
Proposed IDGS	0.154	0.162	0.232	0.273	0.368
SAMAKA	0.161	0.191	0.241	0.332	0.375
IBAAKA	0.197	0.212	0.265	0.347	0.439
DESA	0.202	0.246	0.307	0.361	0.405
SEEMAKA	0.233	0.251	0.327	0.383	0.469

Table 4.7. Tabulation for Memory Usages (Bits)

Techniques	Memory usage (bits)				
	Number of nodes				
	20	40	60	80	100
Proposed IDGS	177	194	214	273	308
SAMAKA	192	213	261	291	341
IBAAKA	201	233	302	329	362
DESA	234	273	338	382	414
SEEMAKA	263	319	392	401	423

Table 4.8. Tabulation for Packet Delivery Rate (Kbps)

Techniques	Packet Delivery Rate (Kbps)				
	Number of nodes				
	20	**40**	**60**	**80**	**100**
Proposed IDGS	191	289	385	481	578
SAMAKA	187	244	331	377	472
IBAAKA	176	231	328	364	361
DESA	164	189	255	281	359
SEEMAKA	158	164	220	258	281

In table 4.3, the time taken by the proposed IEKMA method to cluster the GM is 1247ms which is very much low. The lower clustering time indicates the enhanced performance of the proposed method. In the meantime, the clustering time of some of the existing clustering techniques is compared with the proposed model in order to verify the performance of the proposed method. When compared to the proposed method, the existing techniques attain higher clustering time than the proposed technique that is KMA (1595ms), FCM (1984ms), and K-Medoid (2004ms) respectively. Hence, it is clear that due to the modifications made in the KMA, the proposed IEKMA achieves improved results.

4.4.4 Performance estimation of proposed IDGS authentication framework

Here, the effectiveness of the proposed IDGS scheme is evaluated by comparing its output such as Average Delay (AD), energy consumption, key mismatch ratio, memory usage, packet delivery rate, computation cost. And computation time with the output of the existing Secure and Anonymous Mutual Authentication and Key

Agreement Scheme (SAMAKA) [178], Identity-based Anonymous Authentication and Key Agreement (IBAAKA) Protocol [177], Data Encryption and Signature-based Authentication protocol (DESA) [180], secured energy-efficient mutual authentication, and key agreement scheme (SEEMAKA) [179] methods.

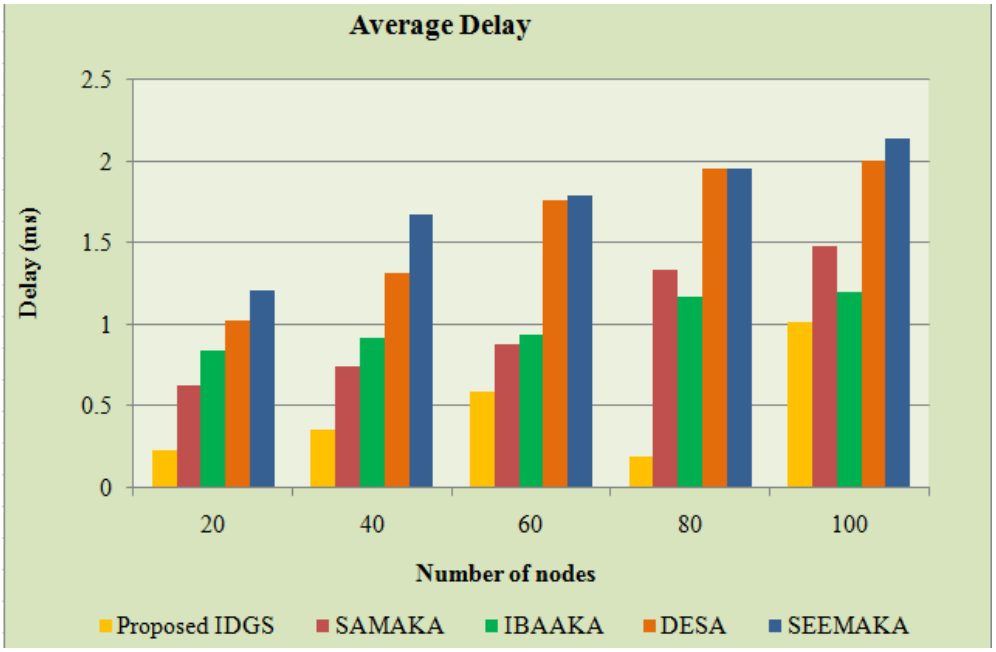

Figure 4.7 AD of the proposed and existing techniques

Figure 4.7 analyzes the average delay of the proposed and existing SAMAKA, IBAAKA, DESA, and SEEMAKA methods. The AD represents the time difference between the packets received currently to packets received previously. The average delay increases as the number of nodes increases as given in the Table 4.4. For the number of 20 to 100 nodes. the time difference taken by the proposed method is increased as 0.23ms to 1.02ms.

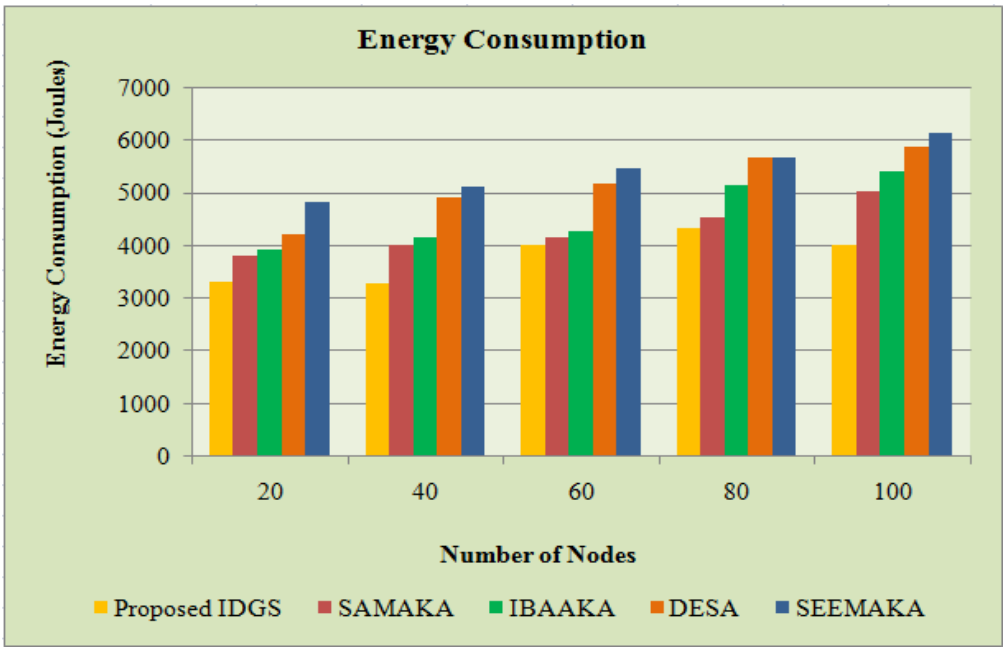

Figure 4.8 Performance evaluation by means of Energy consumption

whereas the time difference taken by the existing methods is increased as, 0.63ms to 1.48ms, 0.84ms to 1.2 ms, 1.03ms to 2.21ms, and 1.21ms to 2.14ms. Hence, the analysis showed that the delay of the proposed method is lower than the existing methods. Figure 4.8 illustrates the amount of energy consumed by the proposed and existing methods. Energy consumption is the important parameter to evaluate the proposed method as it shows the certain level of energy consumed by the nodes during the process of data transmission as given in the Table 4.5. For the maximum of 100 nodes, the energy consumption of the proposed method is 4022.25J. But the existing SAMAKA, IBAAKA, DESA, and SEEMAKA methods consumed 5015.95J, 5411.26J, 5875.26J, and 6119.17 of energy which is higher than the proposed method. For the remaining number of nodes also the proposed method gives a lesser energy consumption value. Therefore, the analysis delivered that the proposed IDGS scheme requires very little energy for an increasing number of nodes.

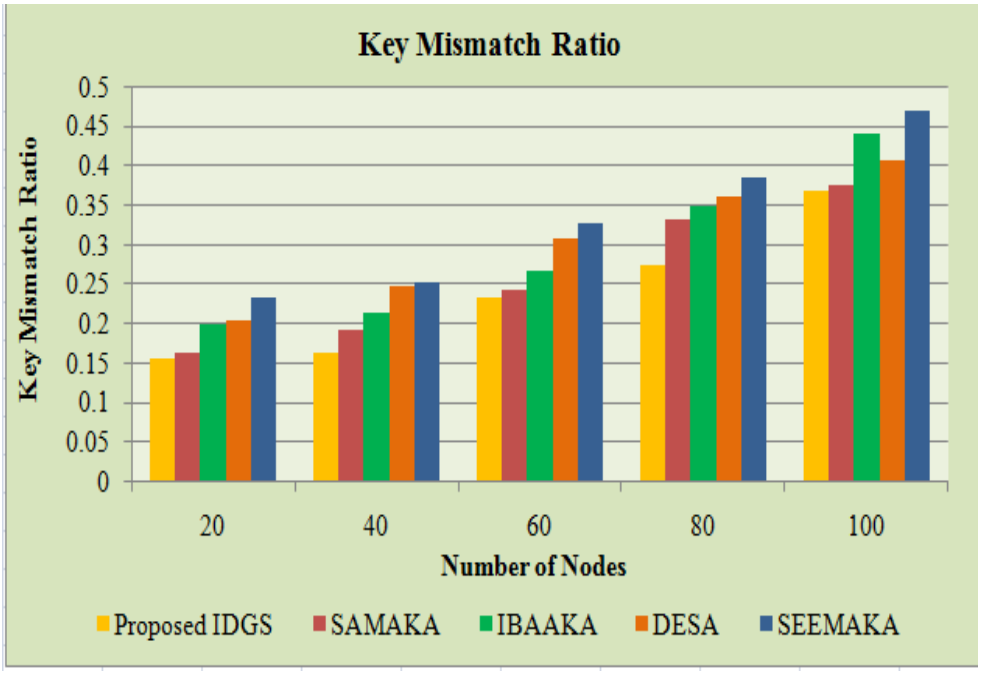

Figure 4.9 Key mismatch ratio analysis of proposed technique

The key mismatch ratio of the proposed and existing methods is analyzed in figure 4.9. Key mismatch ratio is defined as the ratio between various numbers of bits in the secret keys with the total number of key bits created for signature verification. It should be lower for better performance as it recognizes the false private keys generated by the malicious nodes as given in the Table 4.6. In this regard, the key mismatch ratio of the proposed method is varied as 0.154 for 20 nodes, 0.162 for 40 nodes, and 0.232 for 60 nodes, 0.273 for 80 nodes, and 0.398 for 100 nodes. Compared to the existing methods, the proposed method attains less mismatch ratio. From this analysis, it is cleared the proposed method is more efficient with strong private keys than the existing methods.

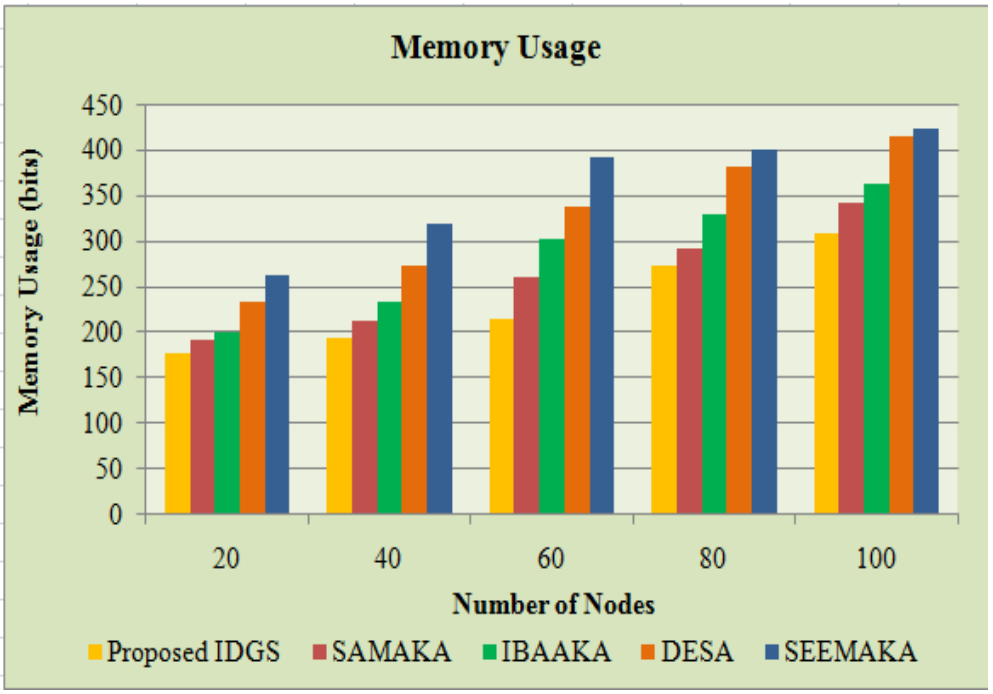

Figure 4.10 Superiority measure based on Memory usage of the proposed and existing techniques

Figure 4.10 evinces the performance of the proposed and existing methods in terms of memory usage. Memory usage is defined as the amount of memory required to store the data as given in the Table 4.7. On analyzing the above figure, memory required by the proposed method is 177bits, 194bits, 214 bits, 273 bits, 308 bits for the number of 20 to 100 nodes.

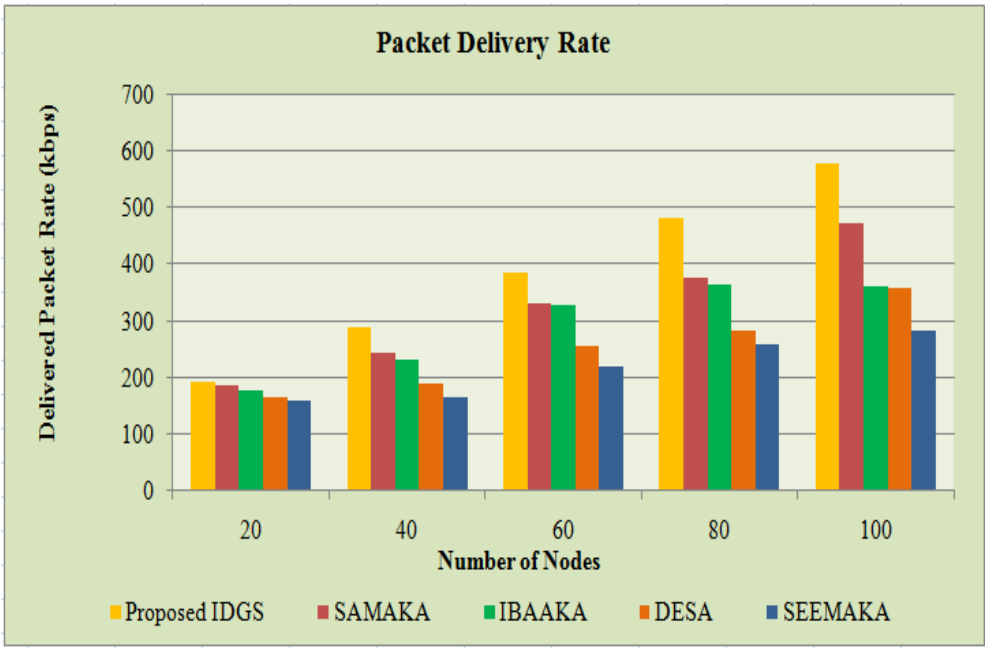

Figure 4.11 Comparison of delivered packet rate of proposed IDGS and existing SAMAKA, IBAAKA, DESA and SEEMAKA

The memory usage of the proposed method is increased with the number of nodes but the increasing level of the proposed method is not exceeded the existing methods. From this analysis, the proposed IDGS's efficiency is proved.

Figure 4.11 evinces the performance of the proposed and existing methods in terms of delivered packet rate. It represents the number of packets that are reached successfully to the receiver node as given in the Table 4.8. For the minimum number of nodes, the packet delivery rate by the proposed method is 191kbps, whereas for a maximum number of nodes the packet delivery rate is 578kbps. But for all nodes, the existing methods have a lower packet delivery rate compared to the proposed method. The analysis concludes that the proposed method is superior to existing methods.

Table 4.9. Tabulation of computation cost of the proposed and existing techniques

Methods	Computation Cost
Proposed IDGS	4.1
IBAAKA	5.13
SEEMAKA	8.23
DESA	12.3
SAMAKA	19.1

Table 4.9 analyzes the computation cost of the proposed and existing methods. The computational cost is defined as the time taken by the system to generate the group signatures as given in the Table 4.9. The computation cost of the proposed method is 4.1 ms, whereas, the existing methods achieve the computation cost of 19.1 ms for SAMAKA, 8.23ms for SEEMAKA, 5.13ms for IBAAKA, and 12.30ms for DESA. From this analysis, the lower computation cost of the proposed method indicates that the proposed IDGS scheme has much better computation efficiency than the existing methods.

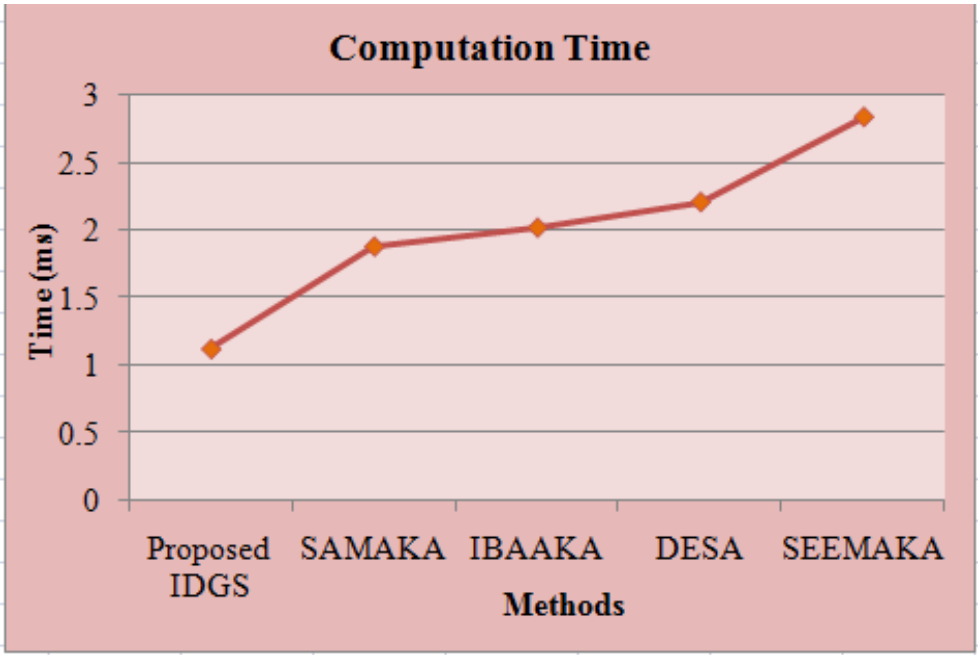

Figure 4.12 Performance evaluation based on computation time

Figure 4.12 compares the computation time of the proposed and existing methods. The computation time of the proposed method is 1.12ms. But the existing methods take the computation time of 1.88ms, 2.02ms, 2.21ms, and 2.84ms which are higher than the proposed method. Thus, the analysis showed that the proposed method has better performance than the existing methods.

4.5 SUMMARY

In this paper, energy-efficient secure data transmission in WBSN is proposed using the novel ID-based Group Signature method and SECC technique. The novel ID-based Group Signature technique is used for message authentication and the SECC technique is used for the secure transmission of patient medical data. In order to improve energy efficiency, this system uses the Clustering technique. Finally, the experimental results are compared with some of the state-of-art authentication and privacy-preserving techniques. Outcomes revealed that the proposed ID-based group signature technique achieves a security level of 96.923%. The computation cost of the proposed IDGS authentication scheme is 4.1ms; also, the system consumes less energy of 4022.25J. The key mismatch ratio of the proposed method is varied as 0.154. The lower value of mismatch ratio shows better performance. Therefore, the proposed scheme is more suitable for securing and authenticating data transmission in the WBSN. In the future, the proposed work will be improved by considering privacy as well as security using improved authentication and authorization techniques.

CHAPTER – 5

RESULTS AND DISCUSSION

5.1 INTRODUCTION

Wireless Body Sensor Network (WBSN) faces several security problems such as loss of information, access control, and authentication. As WBSN collects vital information and operates in an unfriendly environment, severe security mechanisms are needed to prevent the network from anonymous interactions, authentication is the initial step towards providing security. An enhanced authentication scheme prevents the system from imposters effectively. In this paper, a novel authentication using an identity-based group signature (IBGS) protocol has been proposed to provide security to the WBSN. This protocol uses an identity-based group signature algorithm between biosensors and Group Manager (GM) with full anonymity to authenticate the message. Here, the base station or access point is considered the trusted authority and it generates the secret key for the biosensor based on group id and transmits the generated secret key to the biosensor manager. The GM is responsible for generating a signature on the message that has been sent to it by one of its group members and broadcasts the message to the base station whether it is verified. Upon successful verification, the message is accepted.

The Measurements consider the common metrices of my proposed systems of the percentage of Packets Transmitted, Average Delay, Energy Consumption and Key Mismatch Rate are used to evaluate the proposed representation.

5.2 AN EFFICIENT SECURE AUTHENTICATION SCHEME FOR WIRELESS BODY SENSOR NETWORK USING IDENTITY BASED GROUP SIGNATURE (IBGS)

Summary Of Results and Discussion - Chapter 3

The Network Simulator (NS-2) for the IBGS Model system was used to complete the simulation investigation. It is an evolution of the free and open-source discrete event test system and provides generous support for simulating TCP, routing, and multicasting patterns over wired and remote systems. The size of the network is assumed to be 1000m*850m. With the help of a secure routing mechanism, the sensors in WBANs are positioned to monitor the patient's movements and keep track of their

medical records. It maintains density at a very definite level and improves the size of the network by raising the sensor node's number. Maintaining the network and its density, while improving the number of sensor nodes, improves the network range. For every scenario, five simulations having 100 sensor nodes were performed for lowering energy usage and time of response. The management of medical records has a top security level. The time taken for simulation is 25 milliseconds for one process as given in Table 3.1.

Table 3.1. Simulation Setup

Parameter	Value
Simulator	NS-2.31
Area of Simulation	1000×850 m
Traffic model/Mobility Framework	Random WayPoint Model.
Node movement	50m/s
Number of nodes	100 Nodes
MAC type	802.11
Communication range	250mts
Connection Path Link	Multi-direction
System Interface Type	WirelessPhy
Packet rate	6 Packets/seconds

The Measurements of the percentage of packets transmitted, delay, energy consumption, computational cost, key mismatch rate, data privacy rate, information loss rate, security of patient health data and System Flexibility Level are used to evaluate the proposed representation.

The ratio between the number of transmitted packets by biosensors and the number of received packets by GM is defined as the Packet Delivery Ratio. Various network barriers like data collision, insufficient buffer memory, and channel inaccessibility are causing packet drops. A good quality network architecture has the minimum number of Packet drops whereas middling quality network architectures suffer from a lot of packet drops. The packet Delivery ratio is calculated throughout the simulation period by NS-2. The observed packet delivery ratio values for the proposed scheme IBGS and existing system PSKA and IBAAKA are given in Table 3.2. The comparison graph is plotted and given in Figure 3.DPR is calculated using

Equation 5.

$$\text{DPR} = \frac{Packets\ Rececived\ by\ GM}{Total\ Packets\ sent\ by\ Biosensors} * 100 \quad (5)$$

The delivery rates of the packet for the proposed IBGS method have higher delivery rates than the ratio of the conventional scheme PSKA[139] and IBAAKA[142] and it is exposed in Figure 3.3. The more prominent estimation of the packet delivery ratio implies the better execution of the protocol.

Table 3.2. Tabulation for the Packet delivery ratio values

Number of Messages	Delivered Packet Rate (kbps)		
	IBGS	PSKA	IBAAKA
1	1000	750	700
10	1500	1300	1250
20	1800	1500	1400
30	2000	1750	1600
40	2300	2100	2000
50	2500	2340	2150
60	2800	2540	2350
70	3000	2700	2400
80	3500	3050	2800
90	4700	3800	3400
100	5100	4000	3700

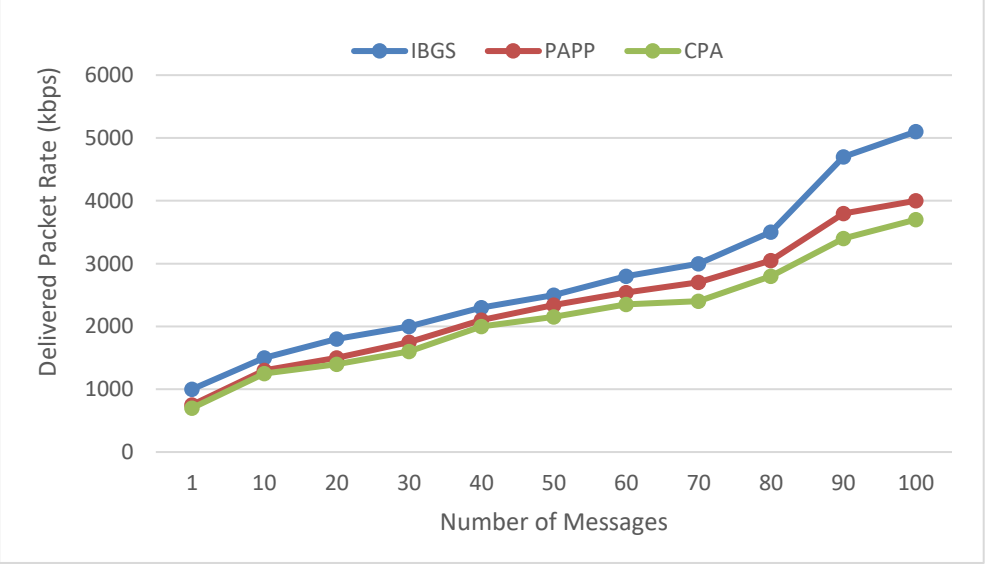

Figure 3.3 The delivery rates of the packet for the proposed IBGS

IBGS achieved 95% of the maximum average packet delivery ratio with the range between 4850 and 5200 kbps. Existing PSKA and IBAAKA are getting 84% and 82% of the packet delivery ratio respectively.

Delay is an important parameter describing the overall performance of the network. Therefore, we are interested in finding a biosensor position that minimized the overall network delay. In WBAN, the distance between the biosensor and the Group Manager (GM) is an important factor that determines the delay of the network. The distance between the biosensor and GM changes regularly due to postural mobility. Distance between a biosensor and GM is directly proportional to the delay. Average delay not only depends on the distance of the nodes but also depends on the channel accessibility, i.e., less processing delay. Similarly, WBAN mobility also plays a vital role in network delay. As a sensor node changes position in the network, it also informs the rest of the sensor about its new position. Thus, as mobility increases, these positions notification packets also increase increasing the congestion and average delay of the network. The observed that the average delay ratio values for the proposed scheme IBGS and existing system PSKA and IBAAKA are given in Table 3.3. The comparison graph is plotted and given in Figure 3.4. The average delay ratio is calculated using Equation 6.

$$\text{Delay} = \frac{\sum_{i=0}^{n} PktSend\_Time - PktRecv\_Time}{Time} \quad (6)$$

Table 3.3. The Average Delay Ratio Values

Number of Messages	IBGS	PSKA	IBAAKA
1	0.5	0.8	0.5
10	0.6	1	0.6
20	0.8	1.2	0.8
30	1	1.4	1
40	1.1	1.6	1.1
50	1.3	1.8	1.3
60	1.4	1.9	1.4
70	1.6	2	1.6
80	1.8	2.2	1.8
90	1.9	2.4	1.9
100	2	2.6	2

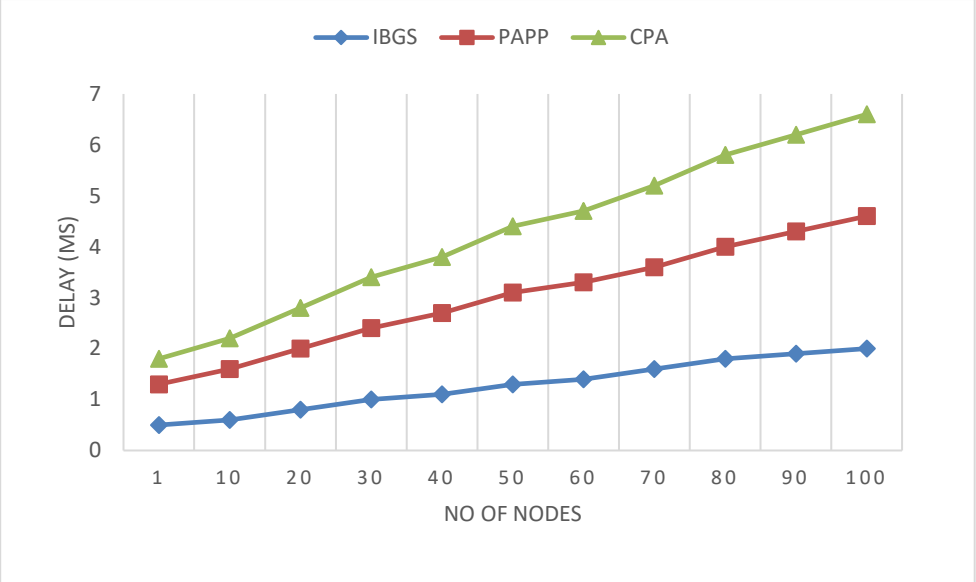

Figure 3.4 The Average Delay analysis

Key Mismatch Ratio (KMR) is defined as the main metric to recognize false private keys generated by malicious nodes which get mismatched when paired with GM. The ratio between various numbers of bits in the secret keys with the total number of key bits created for signature verification is said to be GM. It should be lower for better performance as it recognizes the false private keys generated by the malicious nodes. In this regard, the key mismatch ratio of the proposed method is varied as 0.6 for 20 nodes, 0.8 for 40 nodes, 1.0 for 60 nodes, 1.3 for 80 nodes, and 1.5 for 100 nodes. Compared to the existing methods, the proposed method attains less mismatch ratio as given in Table 3.4. From this analysis, it is cleared the proposed method is more efficient with strong private keys than the existing methods. The key mismatch ratio of the proposed and existing methods is analyzed in Figure 3.5.

Table 3.4. The key mismatching ratio values

Number of Messages	IBGS	PSKA	IBAAKA
1	0.2	0.8	0.5
10	0.4	1	0.6
20	0.6	1.2	0.8
30	0.7	1.4	1
40	0.8	1.6	1.1
50	0.98	1.8	1.3
60	1	1.9	1.6
70	1.2	2	1.7
80	1.3	2.4	1.8
90	1.36	2.6	1.9
100	1.5	2.8	2.1

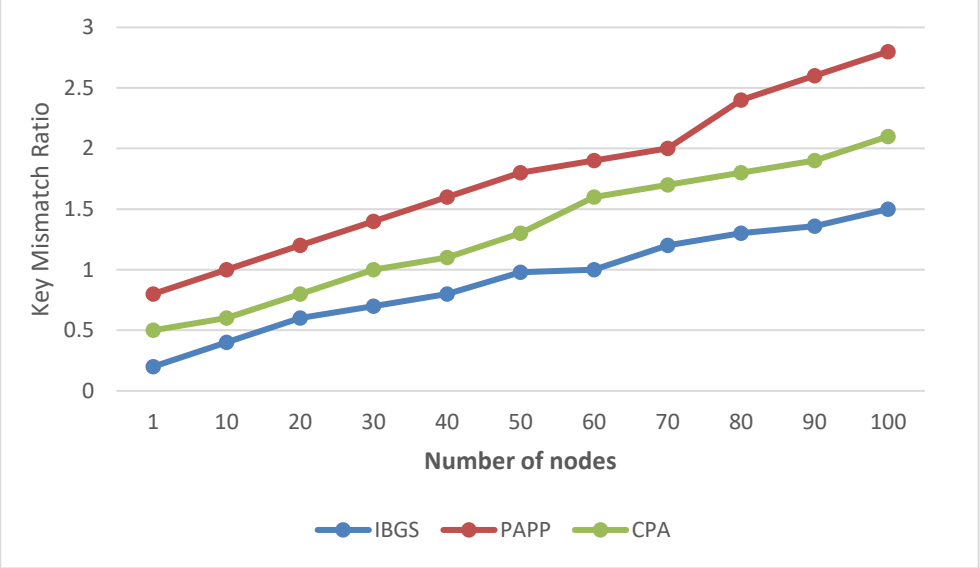

Figure 3.5 Key Mismatching analysis

Table 3.8 and Figure.3.9 show the energy consumption analysis of diverse models under varying message counts. Under the existence of 1 message count, the IBGS model shows a minimum energy consumption of 0.34J whereas the PSKA and IBAAKA models require higher energy consumption of 0.89J and 1.43J respectively. Under the existence of 1 message count, the IBGS model shows a minimum energy consumption of 0.34J whereas the PSKA and IBAAKA models require higher energy consumption of 0.89J and 1.43J respectively. Under the existence of a 10-message count, the IBGS model shows a minimum energy consumption of 0.76J whereas the PSKA and IBAAKA models require higher energy consumption of 1.23J and 1.8J respectively. Under the existence of 20 message count, the IBGS model shows a minimum energy consumption of 0.91J whereas the PSKA and IBAAKA models require higher energy consumption of 1.54J and 2.45J respectively.

Table 3.8. Energy Consumption of our Proposed IBGS with Existing Methods

Number of Messages	IBGS	PSKA	IBAAKA
1	0.34	0.89	1.43
10	0.76	1.23	1.8
20	0.91	1.54	2.45
30	1.34	1.86	2.91
40	1.76	1.98	3.57
50	2.15	2.47	3.86
60	2.43	2.76	4.92
70	2.8	3.54	5.61
80	3.31	4.9	6.3
90	3.78	5.95	6.9
100	4.39	6.72	7.56

Under the existence of a 30-message count, the IBGS model shows a minimum energy consumption of 1.34J whereas the PSKA and IBAAKA models require higher energy consumption of 1.86J and 2.91J respectively. Under the existence of a 40-message count, the IBGS model shows a minimum energy consumption of 1.76J whereas the PSKA and IBAAKA models require higher energy consumption of 1.98J and 3.57J respectively. Under the existence of 50 message count, the IBGS model shows a minimum energy consumption of 2.15J whereas the PSKA and IBAAKA models require higher energy consumption of 2.47J and 3.86J respectively. Under the existence of 60 message count, the IBGS model shows a minimum energy consumption of 2.43J whereas the PSKA and IBAAKA models require higher energy consumption of 2.76J and 4.96J respectively. Under the existence of 70 message count, the IBGS model shows a minimum energy consumption of 2.8J whereas the PSKA and IBAAKA models require higher energy consumption of 3.54J and 5.61J respectively. Under the existence of 80 message count, the IBGS model shows a minimum energy consumption of 3.31J whereas the PSKA and IBAAKA models require higher energy consumption of 4.9J and 6.3J respectively.

Under the existence of 90 message count, the IBGS model shows a minimum energy consumption of 3.78J whereas the PSKA and IBAAKA models require higher energy consumption of 5.95J and 6.9J respectively. Under the existence of 100 message count, the IBGS model shows a minimum energy consumption of 4.39J whereas the PSKA and IBAAKA models require higher energy consumption of 6.72J and 7.56J respectively.

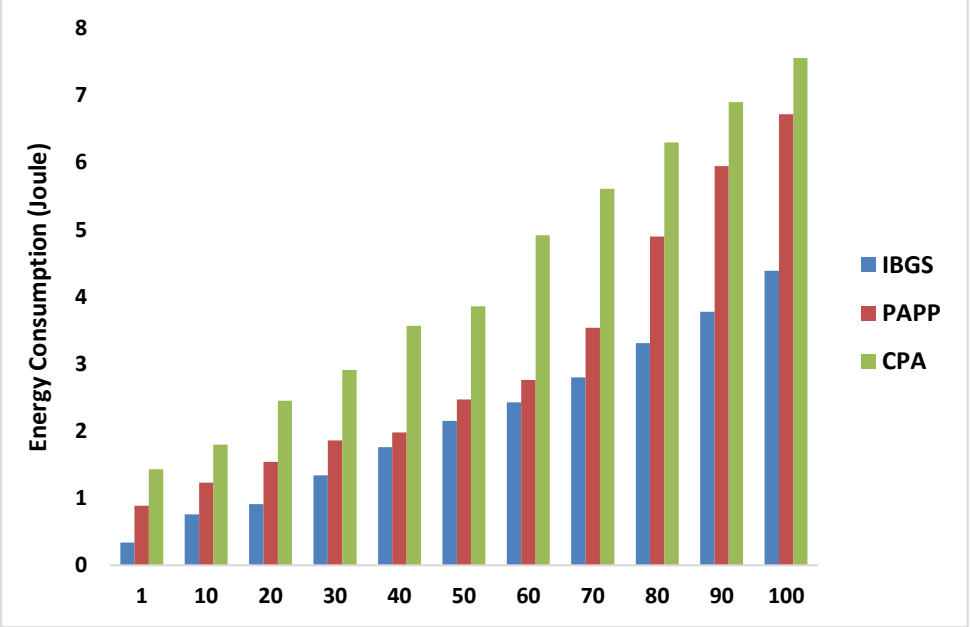

Figure 3.9 Energy consumption analysis

5.3 AN ENERGY EFFICIENCY BASED SECURE DATA TRANSMISSION IN WBSN USING NOVEL ID-BASED GROUP SIGNATURE MODEL AND SECC TECHNIQUE

Summary Of Results and Discussion - Chapter 4:

Here, the performance of the proposed technique is evaluated by comparing the outcomes with the existing baseline techniques. The analysis is made based on some of the performance metrics. The work is implemented in the working platform of Omnet++. The superiority comparisons are detailed below.

The detailed description of the symbols used in the proposed techniques is shown in table 4.1.

Table 4.1: Symbols and its description

Symbols	Description
s^i	Group of sensor nodes (SNs)
n	Number of sensor nodes
x^i, v^i, f^i	Position, Velocity and Frequency of bats
$f^{\max}, f^{\min}$	Maximum and Minimum frequency
ε	Normalized frequency
t	Time
v_{t-1}^i	Flight speed of bat at time $(t-1)$
x_{t-1}^i	Position of bat at time $(t-1)$

x'', x^{old}	Best position of bat, old position of bat
δ	Random number $(0,1)$
L_t^i	Average loudness of bat
χ	Condition for bat moving towards prey
p	Movement of bat towards prey
η, ψ	Constants
e_{t+1}^i	Emission rate at time $t+1$
e_0^i	Initial value of emission rate
S^k	Group Manager (GM)
B^k	Base Station (BS)
τ	Information Entropy
d	Euclidean distance
x^h	Unique Id of sensor nodes
c, b, d, e	Secret key, Public key and Public system parameters
g^m	Private Key of group manager
γ	Group manager ID
ID^{new}	ID of new member
k^p	Public key parameter
M	Message
Z, F, H, T	Group signature for message
P^{gk}	Group managers' public key
ς^1, ς^2	Cipher texts
c	Secret key of the base station
u^r	Receiver nodes' private key
λ	Random positive integer selected by GM

Table 4.4. Tabulation for comparison of Average Delay (AD)

Techniques	Delay in ms				
	Number of Nodes				
	20	40	60	80	100
Proposed IDGS	0.23	0.36	0.59	0.19	1.02
SAMAKA	0.63	0.75	0.88	1.34	1.48
IBAAKA	0.84	0.92	0.94	1.171	1.2
DESA	1.03	1.32	1.76	1.96	2.01
SEEMAKA	1.21	1.68	1.79	1.96	2.14

Table 4.5. Tabulation for Energy Consumption

Techniques	Energy Consumption (joules)				
	Number of nodes				
	20	40	60	80	100
Proposed IDGS	3322.25	3273.36	4005.36	4333.24	4022.25
SAMAKA	3815.95	4001.29	4152.32	4525.32	5015.95
IBAAKA	3911.26	4143.68	4267.34	5132.85	5411.26
DESA	4216.64	4921.14	5169.25	5672.26	5875.26
SEEMAKA	4819.17	5122.24	5472.63	5651.32	6119.17

Table 4.6. Tabulation for key mismatch ratio

Techniques	Key Mismatch Ratio				
	Number of nodes				
	20	40	60	80	100
Proposed IDGS	0.154	0.162	0.232	0.273	0.368
SAMAKA	0.161	0.191	0.241	0.332	0.375
IBAAKA	0.197	0.212	0.265	0.347	0.439
DESA	0.202	0.246	0.307	0.361	0.405
SEEMAKA	0.233	0.251	0.327	0.383	0.469

Table 4.8. Tabulation for packet Delivery Rate (Kbps)

Techniques	Packet Delivery Rate (Kbps)				
	Number of nodes				
	20	**40**	**60**	**80**	**100**
Proposed IDGS	191	289	385	481	578
SAMAKA	187	244	331	377	472
IBAAKA	176	231	328	364	361
DESA	164	189	255	281	359
SEEMAKA	158	164	220	258	281

Here, the effectiveness of the proposed IDGS scheme is evaluated by comparing its output such as Average Delay(AD), energy consumption, key mismatch ratio, memory usage, packet delivery rate, computation cost, and computation time with the output of the existing Secure and Anonymous Mutual Authentication and Key Agreement Scheme (SAMAKA) [178], Identity-based Anonymous Authentication and Key Agreement (IBAAKA) Protocol [177], Data Encryption and Signature-based Authentication protocol (DESA) [180], secured energy-efficient mutual

authentication, and key agreement scheme (SEEMAKA) [179] methods.

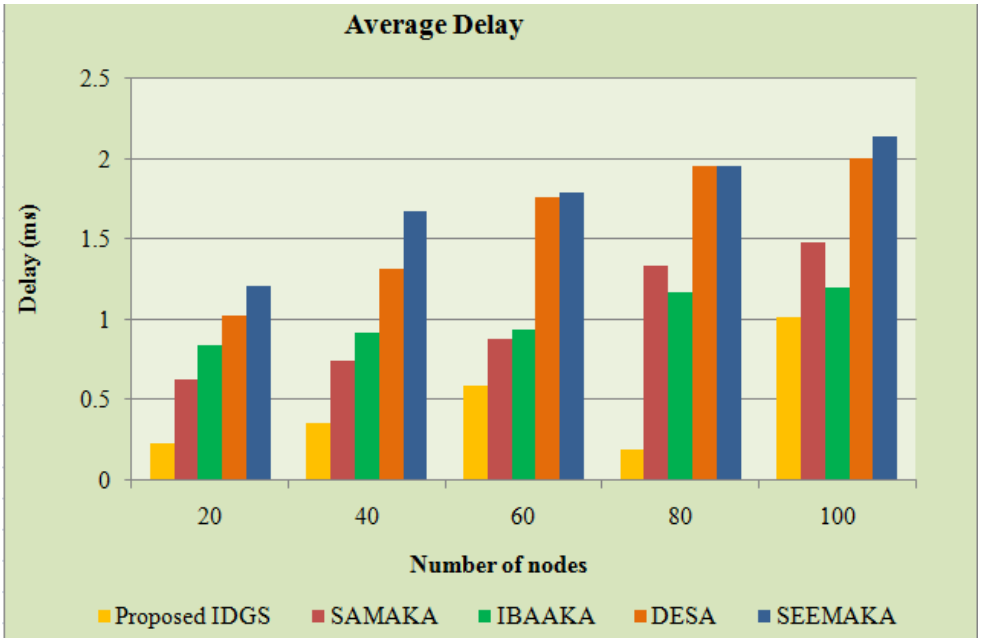

Figure 4.7 AD of the proposed and existing techniques

Figure 4.7 analyzes the average delay of the proposed and existing SAMAKA, IBAAKA, DESA, and SEEMAKA methods. The AD represents the time difference between the packets received currently to packets received previously. The average delay increases as the number of nodes increases as given in the Table 4.4. For the number of 20 to 100 nodes, the time difference taken by the proposed method is increased as 0.23ms to 1.02ms, whereas the time difference taken by the existing methods is increased as, 0.63ms to 1.48ms, 0.84ms to 1.2 ms, 1.03ms to 2.21ms, and 1.21ms to 2.14ms. Hence, the analysis showed that the delay of the proposed method is lower than the existing methods.

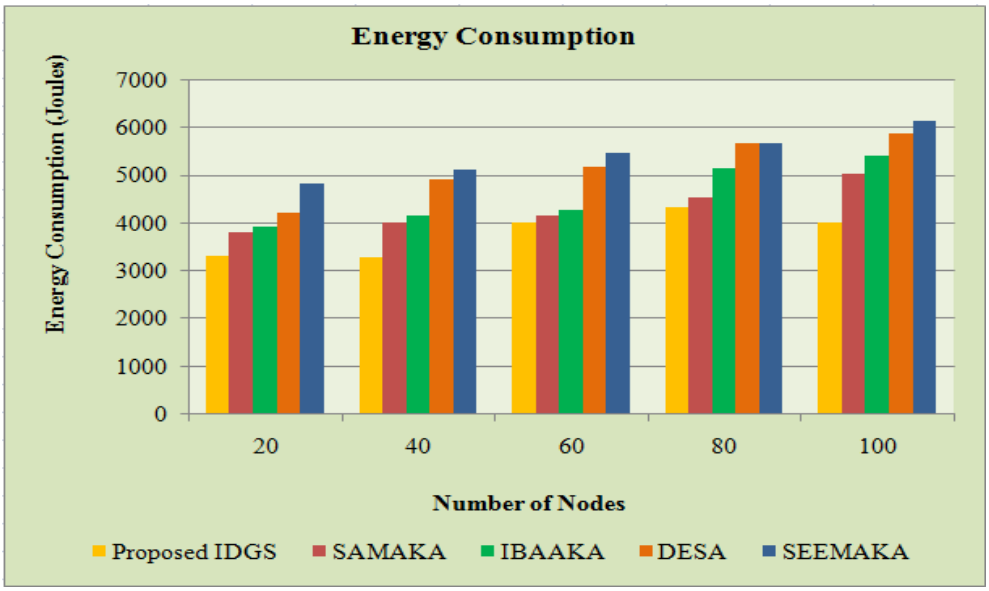

Figure 4.8 Performance evaluation by means of Energy Consumption

Figure 4.8 illustrates the amount of energy consumed by the proposed and existing methods. Energy consumption is the important parameter to evaluate the proposed method as it shows the certain level of energy consumed by the nodes during the process of data transmission as given in the Table 4.5. For the maximum of 100 nodes, the energy consumption of the proposed method is 4022.25J. But the existing SAMAKA, IBAAKA, DESA, and SEEMAKA methods consumed 5015.95J, 5411.26J, 5875.26J, and 6119.17 of energy which is higher than the proposed method. For the remaining number of nodes also the proposed method gives a lesser energy consumption value. Therefore, the analysis delivered that the proposed IDGS scheme requires very little energy for an increasing number of nodes.

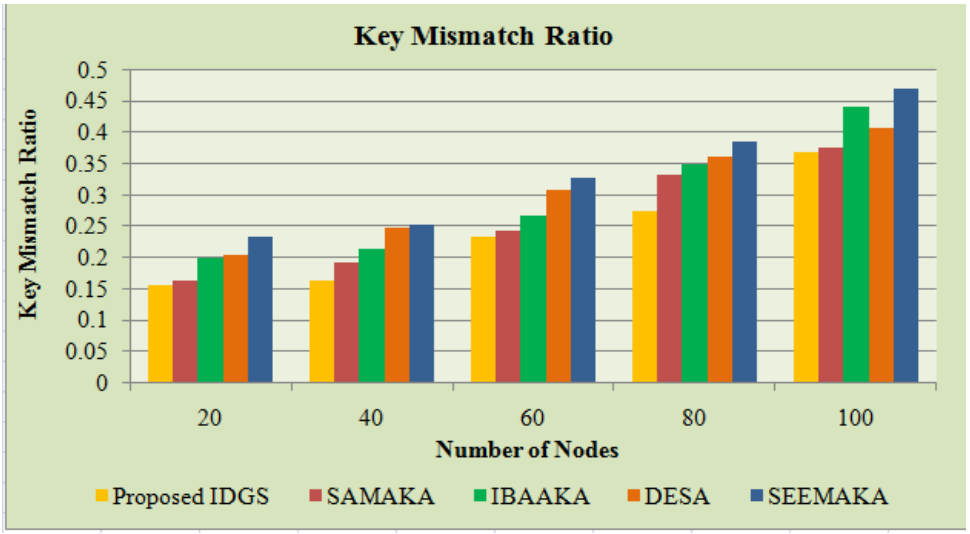

Figure 4.9 Key Mismatch Ratio analysis of proposed technique

The key mismatch ratio of the proposed and existing methods is analyzed in figure 4.9. Key mismatch ratio is defined as the ratio between various numbers of bits in the secret keys with the total number of key bits created for signature verification. It should be lower for better performance as it recognizes the false private keys generated by the malicious nodes as given in the Table 4.6. In this regard, the key mismatch ratio of the proposed method is varied as 0.154 for 20 nodes, 0.162 for 40 nodes, and 0.232 for 60 nodes, 0.273 for 80 nodes, and 0.398 for 100 nodes. Compared to the existing methods, the proposed method attains less mismatch ratio. From this analysis, it is cleared the proposed method is more efficient with strong private keys than the existing methods.

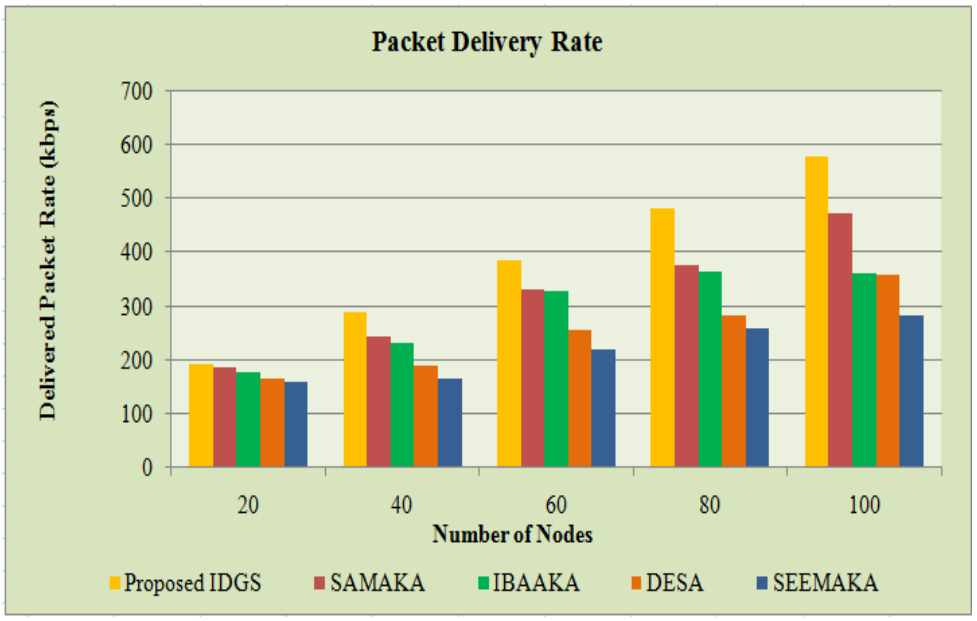

Figure 4.11 Comparison of delivered packet rate of proposed IDGS and existing SAMAKA, IBAAKA, DESA and SEEMAKA

Figure 4.11 evinces the performance of the proposed and existing methods in terms of delivered packet rate. It represents the number of packets that are reached successfully to the receiver node as given in the Table 4.8. For the minimum number of nodes, the packet delivery rate by the proposed method is 191kbps, whereas for a maximum number of nodes the packet delivery rate is 578kbps. But for all nodes, the existing methods have a lower packet delivery rate compared to the proposed method. The analysis concludes that the proposed method is superior to existing methods.

5.4 SUMMARY

WBSN is constrained by a problem of security level and privacy for given data. In this paper, a new authentication using IBGS protocol has been proposed to provide security to the WBSN. The proposed method employs an identity-based group signature algorithm between biosensors and GM. An extensive set of experiments were carried out and the results are examined in terms of Delivered Packet Ratio, Average delay, Key Mismatching Ratio, Computation Cost, Consumption Analysis, data privacy rate, information loss rate, System Flexibility level and Measurement of security on patient's health information under the varying number of messages. the experimental results show that the designed IBGS approach effectively reduces energy consumption by 19% when compared to existing PAPP and CPA methods. Under the applied set of 100 messages, the proposed IBGS model achieves a minimum computation cost of 32s with the least energy consumption of 4.39J. Then, an identity-based group signature algorithm is implemented in the designed method by using a Utility function to measure the source and forthcoming intermediate node. Hence the strength of the solution is increased with higher security. Therefore, the IBGS approach improves security by 37% when compared to PAPP and CPA methods.

Here, by employing a novel IDGS along with SECC methodology, an energy-efficient secure DT is WBSN is proposed. In this, for message authentication, the IDGS model is utilized; likewise, for the secure transmission of patient medical data, the SECC methodology is deployed. The clustering mechanism is utilized here to enhance EE. Lastly, the experiential outcomes are analogized with conventional authentication along with privacy-preserving methodologies. The outcomes displayed that an SL of 96.923% is achieved by the IDGS model. Similarly, the computation cost and energy consumed by the IDGS methodology are 4.1ms and 4022.25J, respectively. The proposed methodology’s key mismatch ratio is 0.154. A better performance was exhibited with the lowest value of mismatch ratio. Hence, it is revealed that the proposed framework is highly effectual in securing along with authenticating DT in the WBSN. This work will be enhanced by pondering privacy along with security utilizing advanced authentication together with authorization methodologies in the upcoming future.

CHAPTER 6

CONCLUSION AND FUTURE DIRECTION

6.1 CONCLUSION

Recently, with the rapid development in wearable medical sensors and wireless communication, Wireless Body Area Networks (WBANs) have emerged as a promising technique that will revolutionize the way of seeking healthcare. Instead of being measured face-to-face, with WBANs patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information is shared among and accessed by various users such as healthcare staff, researchers, government agencies, and insurance companies. In this way healthcare processes, such as clinical diagnosis and emergency medical response, will be facilitated and expedited, thereby greatly increase the efficiency of healthcare. Since the patient-related data stored in the WBAN plays a critical role in medical diagnosis and treatment, it is essential to ensure the security of these data. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments. Patient-related data is often stored in a distributive manner; the open and dynamic nature of the WBAN makes the data prone to being lost. Therefore, it is equally important to protect patient-related data against malicious modification and to ensure its dependability (i.e., having it readily retrievable even under node failure) and its reusability.

In this thesis, an analysis of the existing methodologies for solving the above problems of security has been done and the inadequacy has been realized. Hence a solution has been designed to improve the overall dependability of WBANs. The proposed secure framework comprises six different algorithms in it where each algorithm differs and shows improvement in performance in each and every case. The working of every algorithm is experimented, and results are tabulated by measuring different metrics. Extensive simulations of the proposed algorithms have been done and the results have been compared with existing systems. The proposed algorithm has yielded better results in terms of end-to-end delay, packet delivery ration and throughput.

WBSN is constrained with a problem of security level and privacy for given data. In this paper, a new authentication using IBGS protocol has been proposed to provide security to the WBSN. The proposed method employs an identity-based group signature algorithm between biosensors and GM. An extensive set of experiments were carried out and the results are examined in terms of Delivered Packet Ratio, Average delay, Key Mismatching Ratio, Computation Cost, Consumption Analysis, data privacy rate, information loss rate, System Flexibility level and Measurement of security on patient's health information under the varying number of messages. the experimental results show that the designed IBGS approach effectively reduces energy consumption by 19% when compared to existing PSKA and IBAAKA methods. Under the applied set of 100 messages, the proposed IBGS model achieves a minimum computation cost of 32s with the least energy consumption of 4.39J. Then, an identity-based group signature algorithm is implemented in the designed method by using a Utility function to measure the source and forthcoming intermediate node. Hence the strength of the solution is increased with higher security. Therefore, the IBGS approach improves security by 37% when compared to PSKA and IBAAKA methods.

Here, energy-efficient secure data transmission in WBSN is proposed using the novel ID-based Group Signature method and SECC technique. The novel ID-based Group Signature technique is used for message authentication and the SECC technique is used for the secure transmission of patient medical data. In order to improve energy efficiency, this system uses the Clustering technique. Finally, the experimental results are compared with some of the state-of-art authentication and privacy-preserving techniques. Outcomes revealed that the proposed ID-based group signature technique achieves a security level of 96.923%. The computation cost of the proposed IDGS authentication scheme is 4.1ms; also, the system consumes less energy of 4022.25J. The key mismatch ratio of the proposed method is varied as 0.154. The lower value of mismatch ratio shows better performance. Therefore, the proposed scheme is more suitable for securing and authenticating data transmission in the WBSN. In the future, the proposed work will be improved by considering privacy as well as security using improved authentication and authorization techniques.

6.2 FUTURE DIRECTION

This research work has proposed an ID-based Group Signature algorithms. the proposed work will be improved by considering privacy as well as security using improved authentication and authorization techniques. This was further expanded to use One Time Password and Multifactor Authentication. Finally, a framework combining all the proposed algorithms are given. The framework is yet to be tested in real time and this can be done as a future work.

REFERENCES

[1]. Nagarkar, Shiril, Varsha Nagarkar, Neha Bhatt, Nandkishor Bankar, and Ujwalla Gawande. "Wireless Sensor Networks for Healthcare." NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO (2021): 1204-1208.

[2]. Bhide, Ashlesha, Antra Ganguly, Tejasvi Parupudi, Mohanraj Ramasamy, Sriram Muthukumar, and Shalini Prasad. "Next-Generation Continuous Metabolite Sensing toward Emerging Sensor Needs." ACS omega 6, no. 9 (2021): 6031-6040.

[3]. Carrara, Sandro. "Body dust: Well beyond wearable and implantable sensors." IEEE Sensors Journal 21, no. 11 (2020): 12398-12406.

[4]. Gardašević, Gordana, Konstantinos Katzis, Dragana Bajić, and Lazar Berbakov. "Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare." Sensors 20, no. 13 (2020): 3619.

[5]. Han, Won Bae, Gwan-Jin Ko, Tae-Min Jang, and Suk-Won Hwang. "Materials, devices, and applications for wearable and implantable electronics." ACS Applied Electronic Materials 3, no. 2 (2021): 485-503.

[6]. Cicioğlu, Murtaza, and Ali Çalhan. "Energy efficiency solutions for IEEE 802.15. 6 based wireless body sensor networks." Wireless Personal Communications 119, no. 2 (2021): 1499-1513.

[7]. Waheed, Tabassum, and Faisal Karim Shaikh. "IEEE 802.15. 6 Relaying Protocol for MBANs." In 2021 Mohammad Ali Jinnah University International Conference on Computing (MAJICC), pp. 1-6. IEEE, 2021.

[8]. Hernández, David, Rafael Ors, Juan V. Capella, Alberto Bonastre, and José C. Campelo. "New Contact Sensorization Smart System for IoT e-Health Applications Based on IBC IEEE 802.15. 6 Communications." Sensors 20, no. 24 (2020): 7097.

[9]. Abdulkarem, Mohammed, Khairulmizam Samsudin, Fakhrul Zaman Rokhani, and Mohd Fadlee A Rasid. "Wireless sensor network for structural health monitoring: a contemporary review of technologies, challenges, and future direction." Structural Health Monitoring 19, no. 3 (2020): 693-735.

[10]. Zhou, Jiliang, and Ziqiang Lin. "Lightweight load-balanced and authentication scheme for a cluster-based wireless sensor network." International Journal of Distributed Sensor Networks 17, no. 2 (2021): 1550147720980326.

[11]. Prabu, P., and T. Senthilnathan. "Secured and flexible user authentication protocol for wireless sensor network." International Journal of Intelligent Unmanned Systems (2020).

[12]. Hajar, Muhammad Shadi, M. Omar Al-Kadri, and Harsha Kumara Kalutarage. "A survey on wireless body area networks: architecture, security challenges and research opportunities." Computers & Security 104 (2021): 102211.

[13]. Abidi, Bahae, Abdelillah Jilbab, and El Haziti Mohamed. "Wireless body area networks: a comprehensive survey." Journal of Medical Engineering & Technology 44, no. 3 (2020): 97-107.

[14]. Al Barazanchi, Israa, Haider Rasheed Abdulshaheed, M. Safiah, and B. Sidek. "A Survey: Issues and challenges of communication technologies in WBAN." Sustain. Eng. Innov 1, no. 2 (2020): 84-97.

[15]. Sridhar, M., N. Priya, and A. Muniyappan. "Wireless body area networks: requirements, characteristics, design consideration, and challenges." In Incorporating the Internet of Things in Healthcare Applications and Wearable Devices, pp. 67-85. IGI Global, 2020.

[16]. Tavera, Carlos A., Jesús H. Ortiz, Osamah I. Khalaf, Diego F. Saavedra, and Theyazn HH Aldhyani. "Wearable wireless body area networks for medical applications." Computational and Mathematical Methods in Medicine 2021 (2021).

[17]. Asam, Muhammad, Tauseef Jamal, Muhammad Adeel, Areeb Hassan, Shariq Aziz Butt, Aleena Ajaz, and Maryam Gulzar. "Challenges in wireless body area network." International Journal of Advanced Computer Science and Applications 10, no. 11 (2019).

[18]. Ashraf Darwish1, and Aboul Ella Hassanien, “Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring”, Sensors, 11(6): 5561–5595, 2011

[19]. E. Guenterberg, H. Ghasemzadeh, J. Barnes, K. Gilani, R. Jafari, and V. amachandra,“Locomotion Monitoring using Body Sensor Networks” , Proceedings of the 1st international conference on PErvasive Technologies Related to Assistive Environments, Athens, Greece, July 2008.

[20]. Min Chen, Sergio Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, “Body Area Networks: A Survey,” Mobile Networks and Applications, 16 (2): 171-193, 2011

[21]. J. Ahmad and F. Zafar, “Review of Body Area Network Technology & Wireless Medical Monitoring,” International Journal of Information and Communication Technology Research, 2(2): 186-188, 2012.

[22]. Mehmet R. Yuce, “Implementation of wireless body area networks for healthcare systems”,Sensors and Actuators A: Physical, 162(1): 116–129, 2010.

[23]. Al Barazanchi, Israa, Haider Rasheed Abdulshaheed, M. Safiah, and B. Sidek. "A Survey: Issues and challenges of communication technologies in WBAN." Sustain. Eng. Innov 1, no. 2 (2020): 84-97.

[24]. Tasher Ali Sheikh, Deboraj Muchahary, and Khanjan Changmai Baruah, “A Survey of Reduction the Interference on Cellular Communication System”, International Journal of Computer Applications,95(10):40-43, June 2014

[25]. Zilong Jin, Yoonjeong Han, Jinsung Cho, and Ben Lee, “A Prediction Algorithm for Coexistence Problem in Multiple-WBAN Environment”, International Journal of Distributed Sensor Networks,2015:8 pages, 2015.

[26]. Adam T. Barth, Benton H. Calhoun, Harry C. Powell Jr., James H. Aylor, John Lach, Kyle Ringgenberg and Mark A. Hanson, “Body Area Sensor Networks: Challenges and Opportunities”,Computer, 42(1): 58-65, 2009.

[27]. Zilong Jin, Yoonjeong Han, Jinsung Cho, and Ben Lee, “A Prediction Algorithm for Coexistence Problem in Multiple-WBAN Environment”, International Journal of Distributed Sensor Networks,2015:8 pages, 2015.

[28]. Quentin Lindsey, Daniel Mellinger, and Vijay Kumar, “Construction of cubic structures with quadrotor teams”, In Proceedings of Robotics: Science and Systems, Los Angeles, CA, USA, June 2011

[29]. A. Matlock, R. Holsapple, C. Schumacher, J. Hansen, and A. Girard, “Cooperative defensive surveillance using unmanned aerial vehicles”, In Proceedings of American Control Conference, pages 2612-2617, 2009

[30]. A. C. W. Wong ; M. Dawkins ; G. Devita ; N. Kasparidis, A. Katsiamis ; O. King ; F. Lauria ; J.Schiff, and A. J. Burdett, “A 1 V 5 mA Multimode IEEE 802.15.6/Bluetooth Low-Energy WBAN Transceiver for Biotelemetry Applications”, IEEE Journal of Solid-State Circuits, 48(1): 186 – 198,2012

[31]. Kumar, Ramesh, and Rajeswari Mukesh. "State of the art: Security in wireless body area networks." International Journal of Computer Science & Engineering Technology (IJCSET) 4, no. 05 (2013): 622-630.

[32]. Kargar, Mohammad Javad, Samaneh Ghasemi, and Omolbanin Rahimi. "Wireless body area network: from electronic health security perspective." International Journal of Reliable and Quality E-Healthcare (IJRQEH) 2, no. 4 (2013): 38-47.

[33]. Ferdous, Md Sadek, Farida Chowdhury, and Md Moniruzzaman. "A taxonomy of attack methods on peer-to-peer network." In Proceedings of the 1st Indian Conference on computational intelligence and information security (ICCIIS, 07), pp. 132-138. 2007.

[34]. Han, Nguyen Dinh, Longzhe Han, Dao Minh Tuan, Hoh Peter In, and Minho Jo. "A scheme for data confidentiality in cloud-assisted wireless body area networks." Information sciences 284 (2014): 157-166.

[35]. Tewari, Anurag, and Prabhat Verma. "Security and privacy in e-healthcare monitoring with WBAN: a critical review." International Journal of Computer Applications 136, no. 11 (2016).

[36]. Li, Ming, Wenjing Lou, and Kui Ren. "Data security and privacy in wireless body area networks." IEEE Wireless communications 17, no. 1 (2010): 51-58.

[37]. Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications." Journal of medical systems 36, no. 1 (2012): 93-101.

[38]. Kavitha, T., and D. Sridharan. "Security vulnerabilities in wireless sensor networks: A survey." Journal of information Assurance and Security 5, no. 1 (2010): 31-44.

[39]. Somasundaram, M., and R. Sivakumar. "Security in wireless body area networks: A survey." In International Conference on Advancements in Information Technology. 2011.

[40]. Li, Jin, Kui Ren, Bo Zhu, and Zhiguo Wan. "Privacy-aware attribute-based encryption with user accountability." In International Conference on Information Security, pp. 347-362. Springer, Berlin, Heidelberg, 2009.

[41]. ur Rehman, Obaid, Nadeem Javaid, Ayesha Bibi, and Zahoor Ali Khan. "Performance study of localization techniques in wireless body area sensor

networks." In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1968-1975. IEEE, 2012.

[42]. Sharma, D. "Wireless health care monitoring system with data security and privacy." Int J Res Comput Eng Electron 2, no. 2 (2013): 1-2.

[43]. Javadi, Saeideh Sadat, and Mohammad Abdur Razzaque. "Security and privacy in wireless body area networks for health care applications." In Wireless networks and security, pp. 165-187. Springer, Berlin, Heidelberg, 2013.

[44]. Fatema, Nusrat, and Remus Brad. "Security requirements, counterattacks and projects in healthcare applications using WSNs-a review." arXiv preprint arXiv:1406.1795 (2014).

[45]. Li, Ming, Wenjing Lou, and Kui Ren. "Data security and privacy in wireless body area networks." IEEE Wireless communications 17, no. 1 (2010): 51-58.

[46]. Yazdandoost, Kamya. "Channel model for body area network (BAN)." IEEE 802.15-08-0780-05-0006 (2009).

[47]. Kim, Kyong-Jin, and Seng-Phil Hong. "Privacy care architecture in wireless sensor networks." International Journal of Distributed Sensor Networks 9, no. 5 (2013): 369502.

[48]. Ullah, Sana, Manar Mohaisen, and Mohammed A. Alnuem. "A review of IEEE 802.15. 6 MAC, PHY, and security specifications." International Journal of Distributed Sensor Networks 9, no. 4 (2013): 950704.

[49]. Mišic, Jelena. "Enforcing patient privacy in healthcare WSNs using ECC implemented on 802.15. 4 beacon enabled clusters." In 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 686-691. IEEE, 2008.

[50]. Ahmadi, Ali, Mohammad Shojafar, Seyede Fatemeh Hajeforosh, Mehdi Dehghan, and Mukesh Singhal. "An efficient routing algorithm to preserve $$ k $$ k-coverage in wireless sensor networks." The Journal of Supercomputing 68, no. 2 (2014): 599-623.

[51]. Zhao, Zhenguo. "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem." Journal of medical systems 38, no. 2 (2014): 1-7.

[52]. Rameshkumar, C., and T. Ganeshkumar. "A Novel of Survey: In Healthcare System for Wireless Body-Area Network." In Applications of Computational

Methods in Manufacturing and Product Design, pp. 591-609. Springer, Singapore, 2022.

[53]. B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman. "Systematic literature reviews in software engineering–a systematic literature review", Information and software technology, vol. 51, no. 1, pp. 7-15, 2009.

[54]. M. Hussain, A. Mehmood, S. Khan, M. A. Khan, and Z. Iqbal, "A Survey on Authentication Techniques for Wireless Body Area Networks", Journal of Systems Architecture, pp. 101655, 2019.

[55]. I. Shanmugapriya, and K. Karthikeyan, "Reputation based incentive scheme for secured data privacy in wireless body area network communication", International Journal of Advances in Computer Science and Technology, vol. 10, no. 7, pp. 2095–2117, 2017.

[56]. M. Anwar, A.H. Abdullah, R.A. Butt, M.W. Ashraf, K.N. Qureshi, F. Ullah, "Securing data communication in wireless body area networks using digital signatures", Technical Journal, vol. 23, no. 2, pp. 50–55, 2018.

[57]. M. Toorani, "Cryptanalysis of two PAKE protocols for body area networks and smart environments", International Journal of Network Security, vol. 17, no. 5, pp. 629–636, September 2015.

[58]. M. Masdari, S. Ahmadzadeh, M. Bidaki, "Key management in wireless body area network:challenges and issues", Journal of Network and Computer Applications, vol. 91, no. 1, pp. 36–51. August 2017.

[59]. S. Zou, Y. Xu, H. Wang, Z. Li, S. Chen, and B. Hu, "A survey on secure wireless body area networks", Security and Communication Networks, vol. 2017, 2017.

[60]. T. Jin, W. Yijing, "The research of secure transport protocol based on node's clock characteristics for body area networks", International Journal of Security and its Applications, vol. 8, no. 5, pp. 457–470, 2014.

[61]. S. Peter, B. Pratap Reddy, F. Momtaz, T. Givargis, "Design of secure ECG based biometric authentication in body area sensor networks", Sensors, vol. 16, no. 4, pp. 570, 2016.

[62]. G. Thamilarasu, "iDetect: an intelligent intrusion detection system for wireless body area networks", International Journal of Security andNetworks, vol. 11, no. 1-2, pp. 82–93, 2016.

[63]. K. Rai, M.Shyamala Devi, "Intrusion Detection Systems: a Review", Journal of Network and Information Security, vol. 1, no. 2, December 2013.

[64]. J. Liu, et al., "Certificateless remote anonymous authentication schemes for wireless body area networks", IEEE Transactions of Parallel Distributed Systems, vol. 25, no. 2, pp. 332–342, 2014.

[65]. Z. Zhao, "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem", Journal of Medical Systems, vol. 38, no. 2, pp. 1–7, 2014.

[66]. P. Bharadwaj, H. Pal, B. Narwal, "Proposing a key escrow mechanism for real-time access to end-to-end encryption systems in the interest of law enforcement", In Proceedings of the 3rd International Conference on Contemporary Computing and Informatics (IC3I), Gurgaon, India, pp. 233–237, 2018.

[67]. X. Li, M.H. Ibrahim, S. Kumari, A.K. Sangaiah, V. Gupta, K.K.R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks", Computer Networks, vol. 129, pp. 429–443, 2017.

[68]. J. Iqbal, A.I. Umar, N. ul Amin, N. Din, "Efficient key agreement and nodes authentication scheme for body sensor networks", International Jornal of Advanced Computer Science and Applications, vol. 8, no. 7, pp. 180–187, 2017.

[69]. C.C. Chang, J.S. Lee, J.S. Wu, "An energy conservation authentication scheme in wireless body area network", Communications CCISA, vol. 23, no. 4, pp. 37–54, 2017.

[70]. C.M. Chen, B. Xiang, T.Y. Wu, K.H. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks", Applied Sciences, vol. 8, no. 7, pp. 1074, 2018.

[71]. J. Liu, Q. Li, R. Yan, R. Sun, "Efficient authenticated key exchange protocols for wireless body area networks", EURASIP Journal of Wireless Communication Networks, vol. 2015, no. 1, pp. 1–11, 2015.

[72]. D. He, and S. Zeadally, "Authentication protocol for an ambient assisted living system", IEEE Communications Magazine, vol. 53, no. 1, pp. 71-77, 2015.

[73]. W. Drira, E. Renault, and D. Zeghlache, "A hybrid authentication and key establishment scheme for wban", In 2012 IEEE 11th international conference

on trust, security and privacy in computing and communications, pp. 78-83, 2012.

[74]. H. Xiong, and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks", IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1442–1455, 2015.

[75]. C. Wang, and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing", Journal of Medical Systems, vol. 39, no. 11, pp. 136, 2015.

[76]. Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, and Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth", Journal of Medical Systems, vol. 40, no. 11, pp. 231, 2016.

[77]. D. He, S. Zeadally, N. Kumar, and J.H. Lee, "Anonymous authentication for wireless body area networks with provable security", IEEE Systems Journal, vol. 11, no. 4, pp. 2590–2601, 2016.

[78]. L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks", Journal of Medical Systems, vol. 40, no. 6, pp. 134, 2016.

[79]. J. Liu, L. Zhang, and R. Sun, "1-RAAP: an efficient 1-round anonymous authentication protocol for wireless body area networks", Sensors, vol. 16, no. 5, pp. 728, 2016.

[80]. A.A. Omala, K.P. Kibiwott, and F. Li, 'An efficient remote authentication scheme for wireless body area network", Journal of Medical Systems, vol. 41, no. 2, pp. 25, 2017.

[81]. X. Li, M.H. Ibrahim, S. Kumari, and R. Kumar, "Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors", Telecommunication Systems, vol. 67, no. 2, pp. 323–348, 2018.

[82]. M. E. S. Saeed, Q. Y. Liu, G.Tian, B. Gao, and F. Li. "Remote authentication schemes for wireless body area networks based on the Internet of Things." IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4926-4944, 2018.

[83]. R. Chen, D. Peng, "Analysis and improvement of a mutual authentication scheme for wireless body area networks", Journal of Medical Systems, vol. 43, no. 2, pp. 19, 2019.

[84]. Y. Xie, S. Zhang, X. Li, Y. Li, Y. Chai, "CasCP: efficient and Secure Certificateless Authentication Scheme for Wireless Body Area Networks with Conditional Privacy Preserving", Secure Communication Networks, vol. 2019, 2019.

[85]. S. Jegadeesan, M. Azees, N.R. Babu, S. Umashankar, J.D. Almakhles, "EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)", IEEE Access, 2020.

[86]. M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu. "Secure anonymous mutual authentication for star two-tier wireless body area networks." Computer methods and programs in biomedicine, vol. 135, pp. 37-50, 2016.

[87]. Z. Xu, C. Xu, H. Chen, F. Yang, "A lightweight anonymous mutual authentication and key agreement scheme for wban", Concurrency and Computation: Practise and Experience, vol. 31, no. 14, 2019.

[88]. A. Ostad-Sharif, M. Nikooghadam, D. Abbasinezhad-Mood, "Design of a lightweight and anonymous authenticatedkey agreement protocol for wireless body area networks", International Journal of Communication Systems, vol. 32, no. 12, 2019.

[89]. C. Chunka, and S. Banerjee, "An Efficient Mutual Authentication and Symmetric Key Agreement Scheme for Wireless Body Area Network". Arabian Journal of Science and Engineering, 2021. https://doi.org/10.1007/s13369-021-05532-8.

[90]. L. Ma, Y. Ge, Y. Zhu, "TinyZKP: a lightweight authentication scheme based on zeroknowledge proof for wireless body area networks", Wireless Personal Communications, vol. 77, no. 2, pp. 1077–1090, 2014.

[91]. C. Chaudet, M. Potop-Butucaru, N. Khernane, "Banzkp: a secure authentication scheme using zero knowledge proof for wbans", In: Proceedings of the 13th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, October 2016.

[92]. G. Bu, M. Potop-Butucaru, "Ban-gzkp: optimal zero knowledge proof based scheme for wireless body area networks", Ad Hoc Networks, vol. 77, pp. 28–41, 2018.

[93]. Z. Zhang, H. Wang, A.V. Vasilakos, H. Fang, "ECG-cryptography and authentication in body area networks", IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 6, pp. 1070–1078, 2012.

[94]. M.G. Ullah, B.S. Chowdhary, A.Q. Rajput, A.K. Baloch, A.A. Ursani, S. Latif, "Wireless body area sensor network authentication using voronoi diagram of retinal vascular pattern", Wireless Personal Communications, vol. 76, no. 3, pp. 579–589, 2014.

[95]. S. Pirbhulal, H. Zhang, S.C. Mukhopadhyay, C. Li, Y. Wang, G. Li, ..., Y.T. Zhang, "An efficient biometric based algorithm using heart rate variability for securing body sensor networks", Sensors, vol. 15, no. 7, pp. 15067–15089, 2015.

[96]. A.K. Das, S. Chatterjee, J.K. Sing, "A new biometric based remote user authentication scheme in hierarchical wireless body area sensor networks", Ad Hoc & Sensor Wireless Networks, vol. 28, no.3, pp. 221–256. September 2015.

[97]. S. Peter, B. Pratap Reddy, F. Momtaz, T. Givargis, "Design of secure ECG based biometric authentication in body area sensor networks", Sensors, vol. 16, no. 4, pp. 570, 2016.

[98]. A. Arya, C. Reddy, T. Limbasiya, "An improved remote user verification scheme in wireless body area networks", In Proceedings of the 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017), pp. 113–120, 2017.

[99]. H. Tan, I. Chung, "Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor", IEEE Access, vol. 7, pp. 151459–151474, 2019.

[100]. A.M. Koya, and P.P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network", Computer Networks, vol. 140, pp. 138–151, 2018.

[101]. X. Cheng, F. Chen, D. Xie, H. Sun, C. Huang, and Z. Qi, "Blockchain based secure authentication scheme for medical data sharing", In X. Cheng, W. Jing, X. Song, Z. Lu (Eds.), Data Science. ICPCSEE 2019. Communications in Computer and Information Science, pp. 1058, Springer, Singapore, 2019. 10.1007/978-981-15-011 8-0_31.

[102]. G. Mwitende, Y. Ye, I. Ali, and F. Li, "Certificateless authenticated key agreement for blockchain based WBANs", Journal of Systems Architecture, pp. 101777, 2020.

[103]. J. Xu, X. Meng, W. Liang, L. Peng, Z. Xu, K.C. Li, "A hybrid mutual authentication scheme based on blockchain technology for WBANs", In Z. Zheng, HN. Dai, M. Tang, X. Chen (Eds.), Blockchain and Trustworthy Systems. BlockSys 2019. Communications in Computer and Information Science, pp. 1156, Springer, Singapore, 2020. 10.1007/978-981-15-2777-7_28.

[104]. D. Schürmann, A. Brüsch, S. Sigg, and L. Wolf, "BANDANA—Body area network device-to-device authentication using natural gAit", In Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 190–196. March 2017.

[105]. Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen, and D. Wu, "Optimized fuzzy comMitMent based key agreement protocol for wireless body area network", IEEE Transactions on Emerging Topics in Computing, 2019.

[106]. S. Barman, H.P. Shum, S. Chattopadhyay, and D. Samanta, "A secure authentication protocol for multi-server based e-healthcare using a fuzzy comMitMent scheme", IEEE Access, vol. 7, pp. 12557–12574, 2019.

[107]. R.K. Mahendran, and P. Velusamy, "A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things", Computer Communications, vol. 153, pp. 545–552, 2020.

[108]. J. Hodgkiss, and S. Djahel, "Securing fuzzy vault enabled authentication in body area networks based smart healthcare", IEEE Consumer Electronics Magazine, 2020.

[109]. O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, B. Furht, "Anomaly detection in medical wireless sensor networks using SVM and linear regression models", International Journal of E-Health and Medical Communications (IJEHMC), vol. 5, no. 1, pp. 20–45, 2014.

[110]. M.T. Gebrie, and H. Abie, "Risk based adaptive authentication for internet of things in smart home eHealth", In Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, Canterbury, United Kingdom, pp. 102–108. September 2017.

[111]. T. Ali, M. Nauman, and S. Jan, "Trust in IoT: dynamic remote attestation through efficient behavior capture", Cluster Computing, vol. 21, no. 2, pp. 1–13. April 2017.

[112]. S. Chatterjee, A.K. Das, and J.K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks", Journal of King Saud University-Computer and Information Sciences, vol. 26, no. 2, pp. 181–201, 2013.

[113]. M.K. Khan, and S. Kumari, "An improved user authentication protocol for healthcare services via wireless medical sensor networks", International Journal of Distributed Sensor Networks, vol. 10, no. 4, pp. 1–10. April 2014.

[114]. J. Zhang, X. Huang, P. Craig, A. Marshall, and D. Liu, "An improved protocol for the password authenticated association of IEEE 802.15.6 Standard that alleviates computational burden on the node", Symmetry (Basel), vol. 8, no. 11, 2016.

[115]. S. Shin, S.W. Lee, H. Kim, "Authentication protocol for healthcare services over wireless body area networks", International Journal of Computer and Communication Engineering, vol. 5, no. 1, pp. 50–61, 2016.

[116]. F. Wei, P. Vijayakumar, J. Shen, R. Zhang, L. Li, "A provably secure password- based anonymous authentication scheme for wireless body area networks", Computers and Electrical Engineering, vol. 65, pp. 322–331, 2018.

[117]. L. Xie, W. Wang, X. Shi, T. Qin, "Lightweight mutual authentication among sensors in body area networks through Physical Unclonable Functions", In Proceedings of the IEEE International Conference on Communications (ICC), IEEE, pp. 1–6. May 2017.

[118]. X. Tan, J. Zhang, Y. Zhang, Z. Qin, Y. Ding, X. Wang, "A PUF based and cloudassisted lightweight authentication for multi-hop body area network", Tsinghua Science and Technology, vol. 23, no. 1, 2018.

[119]. W. Zhang, T. Qin, M. Mekonen, W. Wang, "Wireless body area network identity authentication protocol based on physical unclonable function", In Proceedings of the International Conference on Sensor Networks and Signal Processing (SNSP), IEEE, pp. 60–64. October 2018.

[120]. W. Wang, X. Shi, T. Qin, "Encryption-free authentication and integrity protection in body area networks through physical unclonable functions", Smart Health, vol. 12, pp. 66–81, 2019.

[121]. D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks", Journal of Multimedia Systems, vol. 21, no. 1, pp. 49–60. December 2013.

[122]. X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, M.K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity", International Journal of Security and Communication Networks, vol. 9, no. 15, pp. 2643–2655, February 2015.

[123]. A.K. Das, A.K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks", Wireless Personal Communications, vol. 94, no. 3, pp. 1899– 1933, 2017.

[124]. C.-H. Liu, Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks", Journal of Computers and Electrical Engineering, vol. 59, pp. 250– 261, 2016.

[125]. S. Qiu, G. Xu, H. Ahmad, L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems", IEEE Access, vol. 6, pp. 7452–7463, 2017.

[126]. N. Radhakrishnan, and M. Karuppiah, "An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems", Information Medicine Unlocked, pp. 1–11, 2018.

[127]. Y. Kirsal Ever, "Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks", IEEE Systems Journal, vol. 13, no. 1, pp. 456–467, 2019.

[128]. K. Renuka, S. Kumari, and X. Li, "Design of a secure three-factor authentication scheme for smart healthcare", Journal of Medical Systems, vol. 43, no. 5, pp. 133, 2019.

[129]. S. Tritilanunt, "A biometric smart card based remote user authentication for telecare medicine information system", In Proceedings of the 4th International Conference on Cloud Computing and Internet of Things, pp. 59–65, 2019.

[130]. S.S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor-based authentication scheme for health care systems using IoT enabled devices", Journal of Ambient Intelligence and Humanized Computing, pp. 1–16, 2020.

[131]. L. Harn, C. F. Hsu, Z. Xia, and Z. He, “Lightweight aggregated data encryption for wireless sensor networks (WSNs),” IEEE Sensors Lett., vol. 5, no. 4, 2021, doi: 10.1109/LSENS.2021.3063326.

[132]. M. Younan, S. Khattab, and R. Bahgat, “From the Wireless Sensor Networks (WSNs) to the Web of Things (WoT): An Overview,” J. Intell. Syst. Internet Things, pp. 56–68, 2021, doi: 10.54216/jisiot.040201.

[133]. L. K. Ramasamy, F. Khan K. P., A. L. Imoize, J. O. Ogbebor, S. Kadry, and S. Rho, “Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey,” IEEE Access, vol. 9, pp. 128765–128785, 2021, doi: 10.1109/ACCESS.2021.3111923.

[134]. W. Jin, “Design of Intelligent Perception Module Based on Wireless Sensor Network and Basketball Sports Attitude,” Wirel. Commun. Mob. Comput., vol. 2022, 2022, doi: 10.1155/2022/8227604.

[135]. F. Noor, T. A. Kordy, A. B. Alkhodre, O. Benrhouma, A. Nadeem, and A. Alzahrani, “Securing Wireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption,” Wirel. Commun. Mob. Comput., vol. 2021, 2021, doi: 10.1155/2021/5986469.

[136]. J. Iqbal et al., “Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis,” J. Healthc. Eng., vol. 2022, 2022, doi: 10.1155/2022/9210761.

[137]. S. Hussain, S. S. Ullah, M. Uddin, J. Iqbal, and C. L. Chen, “A Comprehensive Survey on Signcryption Security Mechanisms in Wireless Body Area Networks,” Sensors, vol. 22, no. 3. 2022. doi: 10.3390/s22031072.

[138]. J. Hodgkiss, S. Djahel, and Z. Zhang, “A New Attack Method against ECG-Based Key Generation and Agreement Schemes in Body Area Networks,” IEEE Sens. J., vol. 21, no. 15, pp. 17300–17307, 2021, doi: 10.1109/JSEN.2021.3079177.

[139]. Venkatasubramanian, Krishna K., Ayan Banerjee, and Sandeep Kumar S. Gupta. "PSKA: Usable and secure key agreement scheme for body area networks." IEEE Transactions on Information Technology in Biomedicine 14, no. 1 (2020): 60-68.

[140]. Y. Zhang, Z. Zhao, Y. Deng, X. Zhang, and Y. Zhang, “Heart biometrics based on ECG signal by sparse coding and bidirectional long short-term memory,”

Multimed. Tools Appl., vol. 80, no. 20, pp. 30417–30438, 2021, doi: 10.1007/s11042-020-09608-9.

[141]. T. S. Vandana and S. Venkateswarlu, “A biometric-based secure, energy efficient, lightweight authentication protocol for wireless body area networks,” Int. J. Cloud Comput., vol. 10, no. 4, pp. 319–330, 2021, doi: 10.1504/ijcc.2021.119194.

[142]. Kumar, Mahender, and Satish Chand. "A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network." IEEE Systems Journal 15, no. 2 (2020): 2779-2786.

[143]. T.-T. Tsai, H.-Y. Lin, and H.-C. Chang, “An Efficient Revocable Identity-Based Encryption with Equality Test Scheme for the Wireless Body Area Network,” J. Sensors, vol. 2022, 2022.

[144]. M. S. Akhtar and F. Tao, “An Intelligent and Secured Privacy Preserving Framework For Wireless Body Area Networks (WBANs).,” EAI Endorsed Trans. Creat. Technol., vol. 9, no. 30, p. e5, 2022.

[145]. V. A. Devi and others, “A Hybrid Cryptography and End-to-end Security Model for Wireless Sensor Netwoks,” 2022.

[146]. C. M. Kumar, R. Amin, and M. Brindha, “SafeCom: Robust mutual authentication and session key sharing protocol for underwater wireless sensor networks,” J. Syst. Archit., vol. 130, p. 102650, 2022.

[147]. L. Yang, Y. Gao, J. Zhang, S. Camtepe, and D. Jayalath, “A channel perceiving attack and the countermeasure on long-range IoT physical layer key generation,” Comput. Commun., vol. 191, pp. 108–118, 2022.

[148]. Y. Zhou, L. Zhao, Y. Jin, and F. Li, “Backdoor-resistant identity-based proxy re-encryption for cloud-assisted wireless body area networks,” Inf. Sci. (Ny)., vol. 604, pp. 80–96, 2022.

[149]. K. R. Siva Bharathi and R. Venkateswari, “Development of an Integrated Security Model for Wireless Body Area Networks,” in Applied Information Processing Systems, Springer, 2022, pp. 351–359.

[150]. Q. Cheng, Y. Li, W. Shi, and X. Li, “A Certificateless Authentication and Key Agreement Scheme for Secure Cloud-assisted Wireless Body Area Network,” Mob. Networks Appl., vol. 27, no. 1, pp. 346–356, 2022.

[151]. W.-R. Liu, X. He, and Z.-Y. Ji, “Security Analysis and Enhancements of a User Authentication Scheme,” Int. J. Netw. Secur., vol. 23, no. 5, pp. 895–903, 2021.

[152]. L. Prathibha and K. Fatima, “A Novel High-Speed Data Encryption Scheme for Internet of Medical Things Using Modified Elliptic Curve Diffie--Hellman and Advance Encryption Standard,” Int. J. Image Graph., p. 2340004, 2022.

[153]. A. M. Almuhaideb and H. A. Alghamdi, “Secure and Efficient WBAN Authentication Protocols for Intra-BAN Tier,” J. Sens. Actuator Networks, vol. 11, no. 3, p. 44, 2022.

[154]. S. S. Oleiwi, G. N. Mohammed, and I. Al_barazanchi, “Mitigation of packet loss with end-to-end delay in wireless body area network applications,” Int. J. Electr. Comput. Eng., vol. 12, no. 1, p. 460, 2022.

[155]. P. T. Kalaivaani, R. Krishnamoorthi, Design and implementation of low power bio signal sensors for wireless body sensing network applications, Microprocessors and Microsystems, Vol. 79, Article No. 103271, November, 2020.

[156]. R. Bhangwar, A. Ahmed, U. A. Khan, T. Saba, K. Almustafa, K. Haseeb, N. Islam, WETRP weight-based energy & temperature aware routing protocol for wireless body sensor networks, IEEE Access, Vol. 7, pp. 87987-87995, June, 2019.

[157]. K. Pandey, N. Gupta, An energy efficient distributed queuing random access (EE-DQRA) MAC protocol for wireless body sensor networks, Wireless Networks, Vol. 26, No. 4, pp. 2875-2889, May, 2020.

[158]. P. Kasyoka, M. Kimwele, S. M. Angolo, Towards an efficient certificateless access control scheme for wireless body area networks, Wireless Personal Communications, Vol. 115, No. 2, pp. 1257-1275, November, 2020.

[159]. A. Sivasangari, S. Bhowal, R. Subhashini, Secure encryption in wireless body sensor networks, International Conference on Emerging Technologies in Data Mining and Information Security, Vol. 814, Springer, 2019, pp. 679-686.

[160]. F. T. Zuhra, K. B. A. Bakar, A. A. Arain, U. A. Khan, A. R. Bhangwar, MIQOS-RP: multi-constraint intra-ban, qos-aware routing protocol for wireless body sensor networks, IEEE Access, Vol. 8, pp. 99880-99888, May, 2020.

[161]. Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. Islam, D. Giri, A robust authentication and access control protocol for securing wireless healthcare sensor networks, Journal of Information Security and Applications, Vol. 52, pp. 1-14, June, 2020.

[162]. J. D. Rao, K. Sridevi, Novel security system for wireless body area networks based on fuzzy logic and trust factor considering residual energy, Materials Today Proceedings, Vol. 45, No. 2, pp. 1498-1501, 2021.

[163]. M. Shuai, L. Xiong, C. Wang, N. Yu, Lightweight and privacy-preserving authentication scheme with the resilience of desynchronization attacks for WBANs, IET Information Security, Vol. 14, No. 4, pp. 380-390, July, 2020.

[164]. G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, E. M. Mohamed, A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks, IEEE Access, Vol. 8, pp. 131397-131413, July, 2020.

[165]. A.Joshi, A. K. Mohapatra, Authentication protocols for wireless body area network with key management approach, Journal of Discrete Mathematical Sciences and Cryptography, Vol. 22, No. 2, pp. 219-240, March, 2019.

[166]. M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, M. A. Doostari, A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT, Computer Networks, Vol. 177, Article No. 107333, August, 2020.

[167]. J. Zhang, Q. Zhang, Z. Li, X. Lu, Y. Gan, A lightweight and secure anonymous user authentication protocol for wireless body area networks, Security and Communication Networks, Vol. 2021, Article No. 4939589, July, 2021.

[168]. L. Li, L. Liu, H. Peng, Y. Yang, S. Cheng, Flexible and secure data transmission system based on semitensor compressive sensing in wireless body area networks, IEEE Internet of Things Journal, Vol. 6, No. 2, pp. 3212-3227, April, 2019.

[169]. S. R. H. Remu, Md. O. Faruque, R. Ferdous, Md. M. Arifeen, S. Sakib, S. M. S. Reza, Naive bayes based trust management model for wireless body area networks, Proceedings of the 5th international conference on computing advancement, Dhaka, Bangladesh, 2020, pp. 1-4.

[170]. A.Sammoud, M. A. Chalouf, O. Hamdi, N. Montavont, A. Bouallegue, A new biometrics-based key establishment protocol in WBAN: energy efficiency and

security robustness analysis, Computers and Security, Vol. 96, Article No. 101838, September, 2020.

[171]. J. Wang, K. Han, S. Fan, Y. Zhang, H. Tan, G. Jeon, Y. Pang, J. Lin, A logistic mapping-based encryption scheme for wireless body area networks, Future Generation Computer Systems, Vol. 110, pp. 57-67, September, 2020.

[172]. K. Chatterjee, an improved authentication protocol for wireless body sensor networks applied in healthcare applications, Wireless Personal Communications, Vol. 111, No. 4, pp. 2605-2623, April, 2020.

[173]. S. Jegadeesan, M. Azees, R. Babu, U. Subramaniam, J. D. Almakhles, EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs), IEEE Access, Vol. 8, pp. 48576-48586, March, 2020.

[174]. T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band, A. Mosavi, A lightweight genetic based algorithm for data security in wireless body area networks, IEEE Access, Vol. 8, pp. 183460-183469, October, 2020.

[175]. H. Ryu, H. Kim, Privacy-preserving authentication protocol for wireless body area networks in healthcare applications, Healthcare, Vol. 9, Article No. 1114, September, 2021.

[176]. M. Shuai, B. Liu, N. Yu, L. Xiong, C. Wang, Efficient and privacy-preserving authentication scheme for wireless body area networks, Journal of Information Security and Applications, Vol. 52, Article No. 102499, June, 2020.

[177]. M. Kumar, S. Chand, A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network, IEEE Systems Journal, Vol. 15, No. 2, pp. 2779-2786, June, 2021.

[178]. Narwal, A. K. Mohapatra, SAMAKA: secure and anonymous mutual authentication and key agreement scheme for wireless body area networks, Arabian Journal for Science and Engineering, Vol. 46, No. 9, pp. 9197-9219, September, 2021.

[179]. Narwal, A. K. Mohapatra, SEEMAKA: secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks, Wireless Personal Communications, Vol. 113, No. 4, pp. 1985-2008, August, 2020.

[180]. M. Ayyadurai, S. Varalakshmi, K. Chokkanathan, K. S. Kumar, Signature based key authentication protocol for wireless body sensor networks, European

Journal of Molecular & Clinical Medicine, Vol. 7, No. 3, pp. 5563-5572, August, 2020.

[181]. J. Subramani, A. Maria, R. B. Neelakandan, A. S. Rajasekaran, Efficient anonymous authentication scheme for automatic dependent surveillance-broadcast system with batch verification, Communications, Vol. 15, No. 9, pp. 1187-1197, June, 2021.

[182]. J. Katz, J. Loss, M. Rosenberg, Boosting the security of blind signature schemes, International Conference on the Theory and Application of Cryptology and Information Security, Springer, Vol. 13093, 2021, pp. 468-492.