Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778438

AN EFFICIENT AND SECURE ROUTING SYSTEM FOR WIRELESS BODY SENSOR NETWORKS IN E-HEALTHCARE

Vijay R
Research Scholar, Department of Computer Science and Engineering, Annamalai University
Annamalai Nagar – 608002, Tamil Nadu, India, E-mail: vijayrscs@gmail.com

Dr. R. Saminathan
Associate Professor, Department of Computer Science and Engineering, Annamalai University
Annamalai Nagar – 608002, Tamil Nadu, India, E-mail: samiaucse@yahoo.com

Dr. K.M Baalamurugan
Assistant Professor, School of Computing Science and Engineering, Galgotias University
Greater Noida, Uttar Pradesh, India, E-mail: baalaresearch@outlook.com

ABSTRACT

The development of Wireless-Body-Sensor-Networks (WBSNs) has sparked hope in the fight beside an aging population, persistent infections, and a dearth of medical-facilities. Physiological parameters like Oxygen-saturation (SpO2), Electrocardiogram (ECG), Electromyography (EMG), Electroencephalogram (EEG), Blood-pressure, Respiration-rate, Temperature, and Pulse-rate are constantly monitored by WBSNs using a wide range of implantable and wearable biosensor nodes. A doctor can make a quick and accurate diagnosis from a distance thanks to the transmission of vital signs over a public network. While transmitting data across wireless conduit from biosensor nodes to a Medical-Server (MS) via a Base-Station (BS) for competent medicinal diagnosis, patient confidentiality and privacy are paramount concerns. Due to the restricted nature of WBSNs, it is extremely difficult to find an appropriate security solution for patients who rely on WBSNs to observe their health status. To address these issues, this study proposes a smart, competent, and secures healthcare-enabled Software-Defined-WBSNs design that incorporates SDN technology into WBSNs and is based on Schnorr-Signcryption and Hyper Elliptic-Curve-Cryptography (SSHECC). In order to administer the network in a programmable fashion, SDN technology employs an efferent separation of the control and data planes. SDN's fundamental features—its programmability, adaptability, and centralized management—make it easy-to-expand network architecture. Before proposing a lightweight SSHECC to protect perceptive patient data during broadcast on open systems, this study first designs a Software-Defined-WBSNs architecture. The proposed approach outperforms prior traditional approaches in the performance metrics studied, including compute-cost, communication-overhead, storage-cost, and energy-usage.

Key Terms - Sensor network, E-Health, WBSN, secure routing, privacy, access control.

1. INTRODUCTION

Rapid advances in sensor technology have led to widespread adoption of wireless sensor networks in many diverse settings, including the military, industry, and healthcare [1]. The human body is the focal point of a wireless communication network called WBSN, which links medical sensor nodes worn by patients to monitor and record vital signs in real time. The sensor nodes in this health care system can be worn by the patient or implanted in various parts of the body; either way, they collect data on the patient's health and send it to a central controller or coordinator [2]. These sensor nodes can detect changes in the human body's temperature, blood pressure, heart rate, and mobility. To ensure that medical professionals have access to the data in the future, the Base Station (BS) will transmit the collected patient health data to a medical database server. Data consumers who have successfully authenticated themselves can then retrieve the data [3]. In addition, the automation of WBSN technology allows for better access, faster medical care for those in outlying locations, and better system assistance for the aged and the disabled. WBSN nodes can either be coordinators, terminals, or relays. A coordinator's job is to facilitate communication with the outside world. Data collected by many WBANs about a patient's health may be transferred to a single server housing a healthcare database [4]. The WBSN coordinator is the hub of all the sensor nodes' communications. The WBSN terminal nodes can only run the program that was programmed into them. They are able to detect event data but lack the communication capacity to relay that data to other nodes. Nodes in the middle, called relays, can transmit data gathered at the ends to the coordinator. Figure 1 depicts a conceptual diagram of E-healthcare WBSNs. The following figure summarizes the many methods of sharing patient health data that occur both inside and outside of WBAN. It is shown how a health monitoring system's communication architecture looks like. There are three main types of health monitoring system communication strategies: within the WBAN, outside the WBAN, and between WBANs [5].

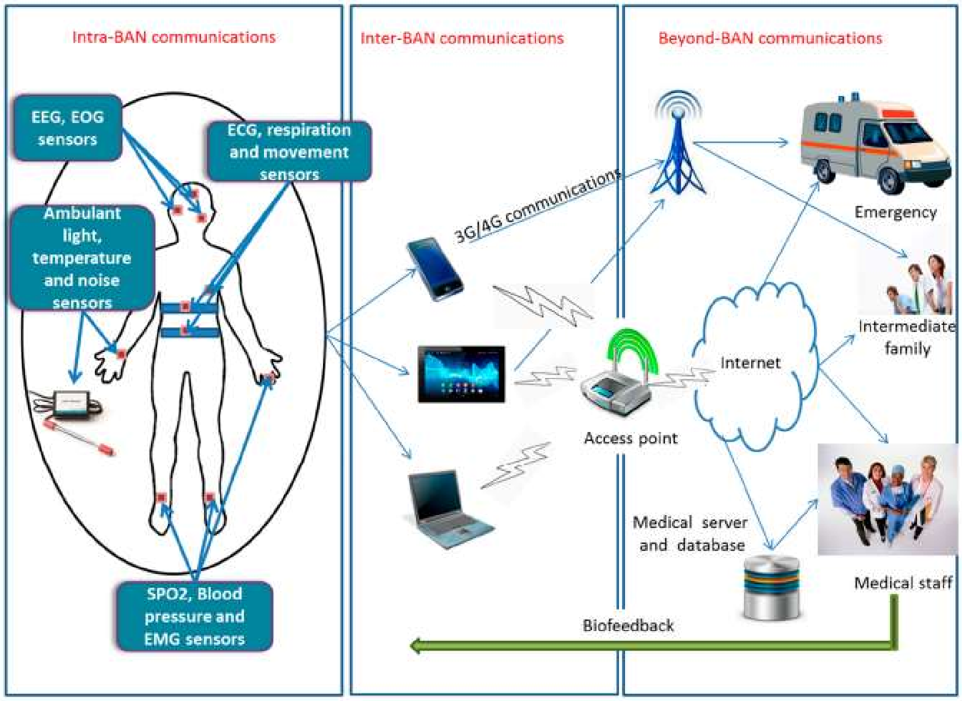
Intra-BAN communications
Inter-BAN communications
Beyond-BAN communications
EEG, EOG sensors
ECG, respiration and movement sensors
Ambulant light, temperature and noise sensors
SPO2, Blood pressure and EMG sensors
3G/4G communications
Emergency
Intermediate family
Internet
Access point
Medical server and database
Medical staff
Biofeedback

Figure 1 General architecture of the WBSNs in E-Healthcare

Smart sensors, for example, may now be made that are compact, low-consumption, and inexpensive thanks to recent advancements in constructing low-consumption electrical circuits for wireless communication. Installed on a wide variety of things, these smart sensors collect data on a wide range of factors [6]. There are numerous varieties of sensors, including those that detect temperature, magnetism, light, mechanical work, and chemicals. They have a tiny battery built in. Since sensors are typically dispersed in unsafe and inaccessible locations, it is quite challenging to recharge this battery. As a result, the energy available to these sensors is limited. A WBSN is the result of multiple Sensor-Nodes (SNs) monitoring and controlling body behavior to gather health data [7].

Today, this highly developed and effective technology has opened up exciting prospects for other intelligent systems like IoT. Each item in the IoT is assigned a unique digital-identifier and is capable of exchanging data with other devices to either offer or request the services needed. The IoT is a network of interconnected computing devices and physical devices, including but not limited to light switches, meters, cars, and the human-body [8]. Specifically, they showcase a variety of services, including remote monitoring of physiological data from the human body, monitoring healthcare providers and patients, hospital medication management, monitoring the environment, irrigation, smart-agriculture, homes, and traffic control [9]. The IoT and WBSNs have been combined to form a new network called the Healthcare-Internet-of-Things (HIoT). With the use of sensor nodes that measure various factors, HIoT keeps tabs on patients or elderly family members. Sensor nodes can monitor vitals and other data for respiratory patients, as those with COVID-19, improving treatment and control for these patients [10]. By analyzing this information, doctors and nurses can better assess the patient's condition.

To monitor its user in real time using remote advanced diagnostic and imaging devices. The recent global outbreak of the Covid-19 sickness has shown the inadequacy of the current healthcare system to deal with a crisis in which people are discouraged from visiting their doctors or hospitals. In the event of a disaster, WBANs can be deployed temporarily in the absence of regular medical personnel. The remote monitoring of patients by medical experts has the potential to save lives [11]. The healthcare industry recognizes that the current healthcare system's service delivery model requires significant reform and that an alternative system, such as WBAN, is essentially required to substantially replace the current healthcare settings. WBAN would mostly replace services provided by Out Patient Departments (OPDs) because of conditions that do not necessitate ongoing hospitalization. When a patient is not bedridden, medical professionals can watch and treat them remotely. The number of people needing hospital care and the likelihood of an outbreak will both decrease. The market for healthcare-related IoT devices is expected to top $300 billion by 2022 [12].

The human body is equipped with sensors. The medical data is gathered by the coordinator via wireless connection and transmitted to a remote server over preexisting internet infrastructure. A remote server can function as an EHR, or Electronic Health Record, to securely store and analyze patients' medical records for use by healthcare providers. Advanced diagnostics are being performed using cloud-based Machine Learning (ML) techniques [13]. Users of WBAN frequently fret over the safety of their private information due to the network's lack of encryption and privacy protections. Since the introduction of electronic devices into the healthcare sector, security and privacy have emerged as two of the most pressing issues [14].

There is no way to leave ultra-sensitive medical records in the hands of enemies. Due to a lack of trust among its users, widespread adoption of WBSN will be hampered by concerns over data security and privacy. The adversaries are drawn to the WBSN system because of its lack of uniformity, openness, and mobility. Because of severe limitations in compute power, storage space, and battery life, traditional cryptographic approaches are inapplicable in IoT-based WBSN [15]. Lightweight cryptographic algorithms are well-suited for WBSN because they reduce the drain on sensor nodes' power supplies. Researchers choose mutual authentication systems using pre-deployed keys because they reduce the amount of mathematical computation needed in a WBSN setting without sacrificing security.

Resource limitations, unpredictable communication, uncontrolled operations, and a lack of centralized management all make routing in WBSNs particularly difficult. In addition, the sensitive nature of health data has made encryption of communications a need in WBSNs. If attackers alter the data even slightly, doctors will incorrectly evaluate it and prescribe the wrong medication [16]. Patients, on the other hand, are very careful to protect the privacy of their medical records because of the potentially devastating effects that could result from an unauthorized third party gaining access to such information. When there are malicious nodes in the system, a safe routing mechanism must protect the privacy, authenticity, and accessibility of all transmitted data. A secure routing method must safeguard the network from routing attacks [17], but it cannot promise to meet all security needs.

This paper proposes a secure routing protocol for WBSNs; we call it SSHECC. The goal of this routing technique is to reduce the amount of energy used in the routing process while keeping communication lines secure. The energy problem plays a critical role in a secure routing strategy since it has a direct impact on the longevity of the network. In order to create an efficient and secure routing mechanism, it is crucial to lessen the load on sensor nodes' power supplies. Because the capture of sensor nodes by attackers has a negative effect on network performance in WBSNs, security is therefore of particular concern in a safe routing strategy. When it comes to keeping sensitive information secret, cryptography is by far the most often used method.

Low-energy consumption makes symmetric-key cryptography a plus, but it's also less secure. In contrast, asymmetric key cryptography systems ensure a higher level of network security at the expense of substantial energy consumption. In order to take advantage of both cryptographic methods while mitigating their respective weaknesses, SSHECC employs a revolutionary key cryptography process, as detailed above.

The key contributions of this research are specified as pursues:

- A smart and effective SD-WBSNs design has been developed, which allows the E-Healthcare to strike a superior balance amid security and cost in order to diagnose diseases quickly and accurately.
- WBSNs have adopted SDN technology to centrally manage data traffic-flow in resource-contained surroundings by decoupling data & control plans.
- Sensitive patient data must be encrypted before being sent over public networks, but a lightweight SSHECC has been developed to do just that.

- The suggested lightweight cryptosystem has improved efficiency across the board, including security, computing, communication, storage, and energy usage.
- Hardware firewalls allow for the efficient, reliable, and secure routing of incoming and outgoing data traffic, allowing medical professionals to access the individual's real-time medicinal data from the MS in a secure manner following mutual authentication.

This article's structure looks like this. Section 2 provides a literature review on existing models related to WBSNs in healthcare. The section discusses the architecture of the suggested model and its implementation. Section 4 discusses the findings of the experiments, and then Section 5 draws the necessary conclusions.

2. LITERATURE REVIEW

This section provides a brief overview of the literature on the topic of keeping data communications private and secure in WBANs. To protect information exchanged between the data sink and external access mechanisms are presented a completely homomorphic encryption scheme. It supplies methods for authenticating messages and protecting them from collisions. Energy usage and computational expense are also assessed [17]. This system controls who has access to BAN devices and ensures that sensitive data stored in the data sink will not be compromised if a data controller device is lost, stolen, or otherwise compromised. The encryption and signature approach is at the heart of role-based encrypted access control. The sensor is capable of managing allowed access permissions and establishing a data access structure [18]. The suggested methodology provides an efficient encryption method that uses less compute and storage space, making it potentially more applicable to real-world scenarios in a BAN. Communication problems between implantable medical nodes and Wireless Access Points (WAPNs) are addressed in a Health Care System (HES) paradigm suggested [19]. Expert system components of HES are geared toward enabling automatic analysis of encrypted medical data with little input from trained medical professionals. A Homomorphic Encryption based on the Matrix (HEBM) privacy-preserving technique is proposed to distort the original medical data before releasing it onto WPANs, and a group key distribution scheme is proposed for secure data transfer in wireless sensor networks [20]. The suggested approach makes use of the benefits of a scalable, easily installed, and low-cost wireless sensor network, as demonstrated by theoretical analysis and simulated tests. However, HES cannot instantly monitor and analyze unexpected disorders, and the diagnostic reliability of the expert system is far from flawless [21].

For mobile networks, authors [22] introduced Ad hoc On-Demand Distance Vectors (AODVs). Each node in an AODV network keeps a steering table with the location of the node that must be traversed in order to reach the final destination. If there is no known path from the sending to the receiving node, the sending node will trigger route discovery. AODV employs a sequence number to guarantee that all of the paths it finds are non-looping and that the most recent data is included in control packets. As a result, flooded control packets can be identified by the nodes. In addition, AODV has a technique for keeping routes updated. When the network size is high, nodes may experience a delay in AODV's path discovery process. Additionally, route finding delays and bandwidth usage are greatly increased when links are lost.

Authors [23], presented centralized LEACH (LEACH-C), an enhanced variant of the Low-Energy Adaptive-Clustering-Hierarchy (LEACH). A federal clustering technique is employed. Each LEACH-C node reports its position and power level to the network's hub. The BS must allocate nodes to the correct clusters and maintain an even distribution of power across the network. BS determines the average energy of the nodes as a means to this end. In this iteration, the Cluster-Head (CH) node cannot be a node with energy lower than the mean. BS uses a process called "simulated annealing" to decide on CHs. This technique is an effort to lessen the load on non-CH nodes' power supplies when transmitting data to CH. To achieve this goal, it seeks to reduce the total of squared-distances amid any node that is not a CH and the closest CH. Distributed algorithms are more appropriate for WSNs than centralized ones since the latter avoid the pitfalls of a central point of failure and are less vulnerable to assaults [24].

To prevent unauthorized use of medical records and to keep patients' identities private, presented an anonymous authentication mechanism for WBANs [25]. Many attacks can be launched against the authentication system used by WBANs. The authentication system used in WBANs must be resilient against both internal and external threats if secure communication is to be maintained at all times. To protect the client's anonymity, the application provider and the network administrator must be unable to determine who sent the message through an interception. The proposed method shields the client's identity and geographical details from prying eyes. The research demonstrates that the suggested system improves upon previous schemes by fixing their security flaws [26].

Secure Multitier Energy-Efficient Routing (SMEER) was introduced for WSNs with varying degrees of homogeneity. SMEER's primary objective is to lessen the network's energy footprint while simultaneously increasing security. The K-means method is utilized to group together similar sensor nodes [27]. Energy-productivity is increased through clustering, which in turn extends the lifespan of the network. It helps SMEER scale better, too. The data- packts delivered to the BS in SMEER are encrypted using elliptic curve cryptography (ECC). ECC raises the network's energy needs, but also provides increased safety. High computational and communication overheads are incurred by the network due to the ALO algorithm [28].

Sensor network routing protocols, according to the authors of [29], are not developed with security in mind. They demonstrated the impact of crippling attacks on popular routing protocols for sensor networks, drawing the conclusion that the adoption of such protocols in WSN may undermine the networks because security was not a primary consideration during their development. They also assured us that we can add security measures to them after the design is finished. To address the vulnerabilities in the WSN routing protocol, in [30] suggested a low-power, high-security routing method for WSNs. In [31], a strategy was presented to encrypt and decrypt cardiograms utilizing the measurement matrix as a symmetric key in a lightweight encryption framework to improve compression at sampling time. Linear Feedback Shift Register (LFSR) output m-sequences seeded by Received Signal Strength Indicator (RSSI) values, which served as the symmetric key [32]. The receiver and transmitter would rearrange this information to create the CS sensing matrix. This approach relies on sensors, however analog sensors must have their output transformed to binary data before transmission. In addition, a novel approach to user access management for a WBAN was proposed by the authors of paper [33]. Their suggested system involved a password, an access privilege mask, and a user ID that was assigned to a certain group. To restrict access to only what is appropriate for a given genuine user, a public key cryptosystem based on elliptic curve cryptography was employed.

The authors of [34] provided a comprehensive overview of privacy-preserving WSN topologies, data-sharing techniques, cryptography, and attributes-based encryption. Several cryptographic concerns were addressed in their work, including storage or computational overhead, the balance between security and flexibility, and trust assurance against assaults. They made it apparent that the most pressing problem in defending against network adversaries is ensuring a safe handoff of data between the client and the server. Storage and computational overheads, as well as delegation problems, were identified as primary causes of cryptographic activities such as key creation, encryption, and decryption. WBAN data storage security vulnerabilities were also noted by authors in [35], in addition to data transmission security issues. To investigate the potential benefits and drawbacks of WSN, researchers suggested a SDN structure; a method for efficient data transmission has been presented. The authors [36] present a cloud-based, generic architecture. It presents the unique features, dependability, and expertise of data mining technologies.

We studied the latest proposed privacy and security measures for WBANs. We concluded from our research that healthcare-enabled Software-Defined WBANs that are both lightweight and secure are necessary to protect the confidentiality of patient information. In addition, various methods are presented in the writing to bolster the confidentiality and safety of BSNs. Still, many approaches rely on resource-intensive bilinear coupling algorithms to encrypt patient- perceptive data during transmission from biosensors to MS. Consequently, these methods are costly in terms of dealing out expenses and broadcast overhead, and they are not secure according to the current security model. Moreover, the security of key exposure is a major worry because it makes it easy for attackers to get sensitive patient information for malicious purposes.

3. PROPOSED METHODOLOGY

Architecture for keeping E-healthcare communications private and secure is presented here. Through measures including encrypted group communication, asymmetric key encryption, and secret sharing, this technique safeguards sensitive patient information gathered by healthcare apps.

The SSHECC is an open-source cryptographic method that builds on the concepts introduced by Elliptic Curve Cryptography (ECC). The SSHECC is just as secure as the Electronic Codebook (ECC), the Public-Key-Infrastructure (PKI), and the Digital-Signature-Algorithm (DSA). SSHECC is great when resources are limited because of its small key size. The SSHECC can be broken down into six different species, or genera, with genus 2 being the safest. The hyperelliptic curve discrete logarithm problem contributes to the safety of SSHECC by making it impossible for an attacker to decrypt the keys even if they are in the public domain. Better security in a low-resource setting, like WBAN, is made possible by SSHECC's use of substantially smaller key sizes contrasted to other approaches like RSA &ECC.

The formula (1) of the SSHECC is as pursues

$$E: r2 + h\,(t)r \;= f(t) \qquad \text{Eq. (1)}$$

h(t) is a polynomial of degree besides h(t) ∈ f(t), and the f(t) is a monic polynomial of degree 2g+ 1 and h(t) ∈ f(t).

Curve's Jacobian is defined on a finite field F, which is represented as JE(F), and each element of the Jacobian is designated by a divisor D.

$$J_e(F) = \frac{D^{\circ}}{P'} \qquad \text{Eq. (2)}$$

D is a reduced-divisor, and the mi ⟶ Numbers on the curve, Pi ⟶points on the curve. The mi cannot be zero because it is a finite-number.

3.1 WBSN Architecture for E-Healthcare System

For a more streamlined and protected healthcare system, the SDN framework has been connected with the WBANs. WBANs are worn by patients to record quantitative, real-time physiologic indicators including heart rate, temperature, and blood pressure, extending the reach of medical care to those in remote locations. With the help of a BS, a gateway device, WBANs make it possible to send voluminous amounts of medical information to the MS. The SDN-based protocol is used by the BSs to store and send raw data from BSNs to the MS, where it can be used for knowledge discovery. To provide useful facts for decision making, MS can be utilized to analyze the vast volumes of data generated and accumulated by BSNs. Figure 2 depicts the proposed architecture for a SD-WBSN, which includes the following subsystems [42].

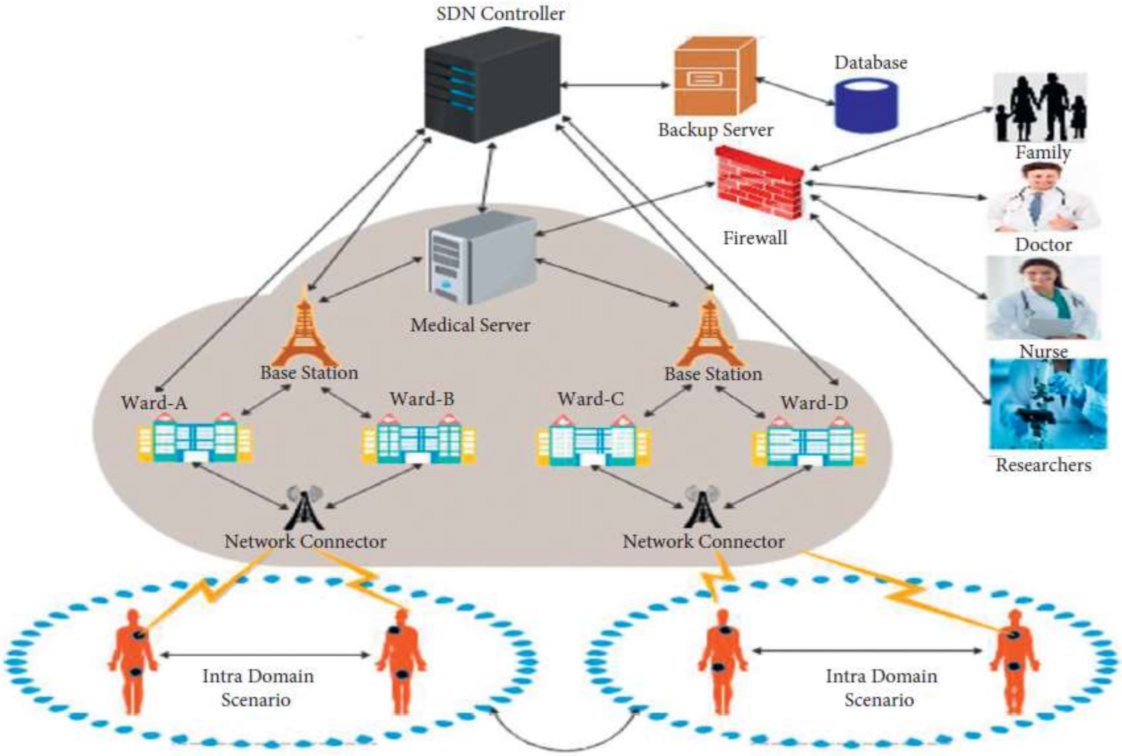

Figure 2 Proposed Model Communication System

SDN Nodes: Nodes in WSANs are the biosensors implanted in a patient to measure factors including blood-pressure, pulse rate, heart rate, Electromyography (EMG), and temperature. Once the data has been collected, it is transmitted via network-connector to the BS, which serves as an entrance.

SDN Controller: The SDN controller offers a high-level, abstract perspective on the entire network and enables centralized, logical control. In our plan, the SDN-controller receives encrypted transmissions from the BS &MS containing all sensitive patient data in order to maintain and manage a comprehensive records healthcare.

Base-Station: It's a high-powered gadget that connects the patient to the healthcare provider's server. Data is gathered from the bio-SN and transmitted to the medicinal attendant in a secure manner by BS. While this is happening, the SDN controller receives real-time data from the BS to maintain a unified patient record.

Medical Server: Users of the medical server include individuals, clinics, universities, and government institutions. Through the Base Station, encoded data gathered by sensors about a patient reaches the medical server. Based on their intended use in the future, these data undergo a variety of processes, including analysis, modeling, and medical decision-making.

Database: There is a link between the database of patient, doctor, researcher, and government agency data and the medical server. It is connected by all users so that they can view the patient's record according to the permissions they have been granted.

Backup Server: The suggested system stores duplicate copies of all patient data on a separate server. The backup server stores patient data in case the primary server goes down. This prevents the loss or theft of the patient's private information.

Access Control: In the proposed method, a fine-grained access control system is built to handle all external user actions. All incoming connections from the outside world must be verified as legitimate users before being allowed access to the WBSN.

Firewall: The concept of a firewall has been incorporated into the presented method for the secure communication of healthcare data amid MS &external clients. It separates the MS from the outside world, managing all information sent to and from the MS, including sensitive patient data. The firewall in the proposed architecture either enables or bans certain individuals from accessing the patient medical record based on established security settings.

3.2 Network Model

Several stretchable bio-SNs are placed on an inpatient's body in the suggested network paradigm. These biosensor nodes are constrained in their ability to store data, analyze information, and generate energy. The IEEE 802.15.6 standard is used for communication between the biosensor nodes and the BS, where the data is processed. The underlying infrastructure of SSHECC is a distributed network of wireless body sensors. Assuming the network has been clustered by the LEACH algorithm [37], we employ this technique. A strong, stable, and energetic Base Station (BS) is a standard component of this network's infrastructure. In addition, it is made up of a small amount of CHs that have greater energy, memory, and computing power than the rest of the SNs, and a far larger amount of "Cluster Member nodes" (CMs) that are standard sensor nodes with more modest resources. Environment data is gathered by CMs and transmitted to the CH node. When a CH receives information from a CM, it relays that information to the home base [38]. In addition, BS is in charge of data processing and network administration. The precise location of BS in the network is known to every node. All of the network's sensor nodes, whether they be Central Hubs (CHs) or mobile hubs (CMs), are stationary and GPS-enabled. Model of the network is shown in Figure 3.

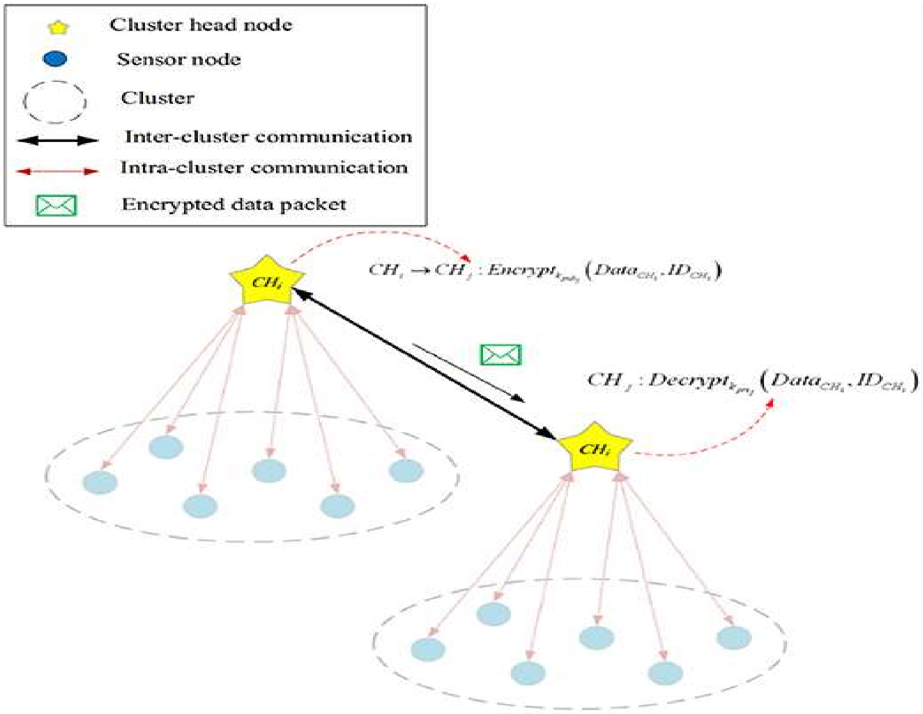
Cluster head node
Sensor node
Cluster
Inter-cluster communication
Intra-cluster communication
Encrypted data packet
CH_i
$CH_i \rightarrow CH_j : Encrypt_{k_{pub_j}}(Data_{CH_i}, ID_{CH_i})$
$CH_j : Decrypt_{k_{pri_j}}(Data_{CH_i}, ID_{CH_i})$
CH_i

Figure 3 Concept Diagram of the Network Model in SSHECC

a. SSHECC

Key creation, signcryption, unsigncryption, and secret session key modernizing are the four stages of SSHECC for WBAN, as shown in Figure 4.

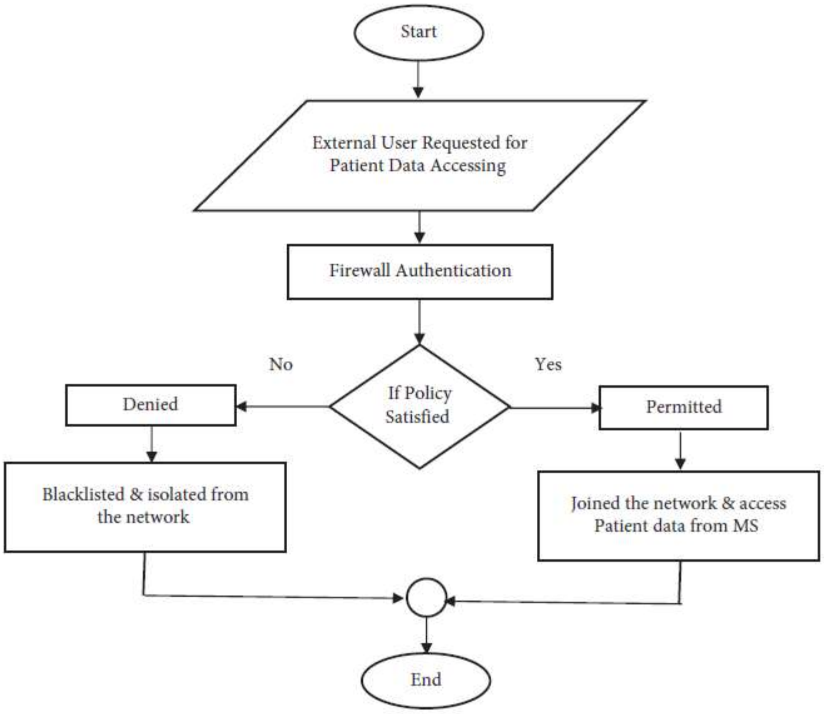
Start
External User Requested for Patient Data Accessing
Firewall Authentication
No
Yes
If Policy Satisfied
Denied
Permitted
Blacklisted & isolated from the network
Joined the network & access Patient data from MS
End

Figure 4 Workflow Diagram of the Proposed Model

Key Generation Phase: To preserve the balance between cost and security, we have estimated open and secret keys for bio-SNs and MS, respectively, to enable the safe broadcast of patient data from source to target nodes in a delay-free, reliable, and steadfast manner. When patients' records are sent over open wireless networks, the determined open keys contact the federal Certificate-Authority (CA) to seek an open key credential for validation [39].

Schnorr Signcryption Phase: The Schnorr signcryption algorithm is a hybrid of open key encryption and digital signature schemes. At this point, we have safely transmitted the patients' private information by using a session key to prevent unauthorized access. Additionally, the instigator creates the multicast-secret session-key for critical messages with diverse group participants. The estimated session-key will be refreshed each round to improve data protection and ensure forward &backward solitude, allowing participants with unique IDs ID1, ID2, ID3,...., IDt to reliably communicate.

Schnorr Unsigncryption Phase: Here, MS deciphers tuples (C, R, S, Ct) containing the patient's signcrypted medical data. In addition, these users have access to the records in the MS if the firewall protocols and guidelines are a good fit. If they try to access the network anyhow, their requests are denied and they are placed in a separate area to prevent attacks from outsiders.

Secret Session-Key Updating: With a new value for x and a new nonce for each signcryption procedure, we can ensure both backward &forward secrecy. If an adversary obtains the furtive value of x, they will be unable to reconstruct past or future patient sessions [40].

4. RESULTS AND DISCUSSIONS

Here, we compare the suggested design to more traditional systems and evaluate its performance with respect to Computing-Cost (CC), Communication-overhead, Energy-utilization, & Storage-cost.

a. Computational Cost:

The total time it takes to encrypt and decrypt a session key is 4.543859 seconds. We evaluate the suggested method by contrasting its computational overhead with that of state-of-the-art schemes currently in use. According to the method, the pairing computation time for the third-generation MICA2 is 2.66s. Our solution is better suited to the resource-constrained atmosphere of WBSNs, and the use of a session key for encryption and decryption reduces the dispensation time of this work when contrasted to existing works. This system uses two encrypting and two decrypting operations, as well as three modular multiplications. The biosensor side has one modular multiplication operation, while the MS side has two. Figure 5 contrasted the designed systems computational Time to that of comparable state-of-the-art techniques [41]. The presented approach also has a lower computational cost than competing schemes.

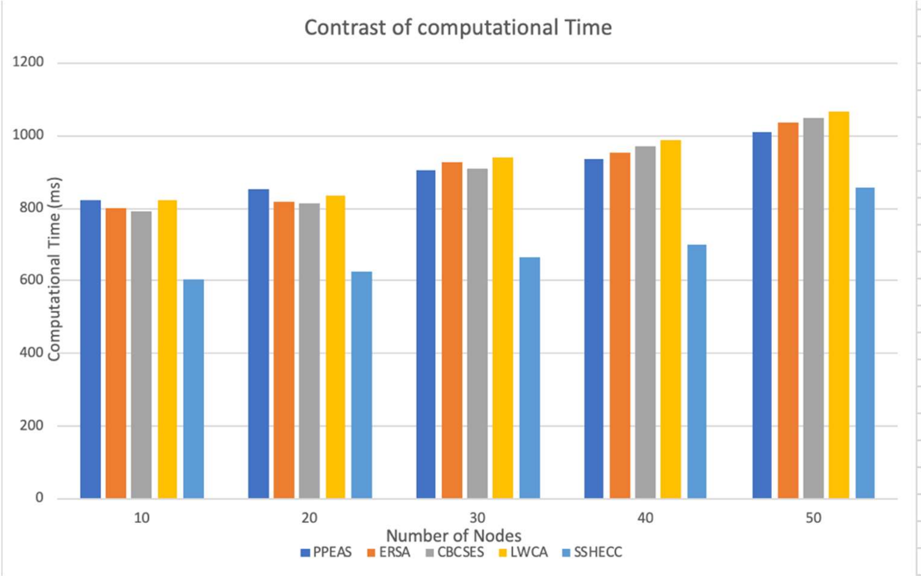

Figure 5 Contrast of Computational Time

b. Communication Overhead:

As can be seen in Figure 6, [42], the suggested strategy minimizes the CC compared to other traditional models since it only forwards vital data instead of regular data. Furthermore, with wireless communication, data transmission costs are disproportionately high relative to data processing costs.

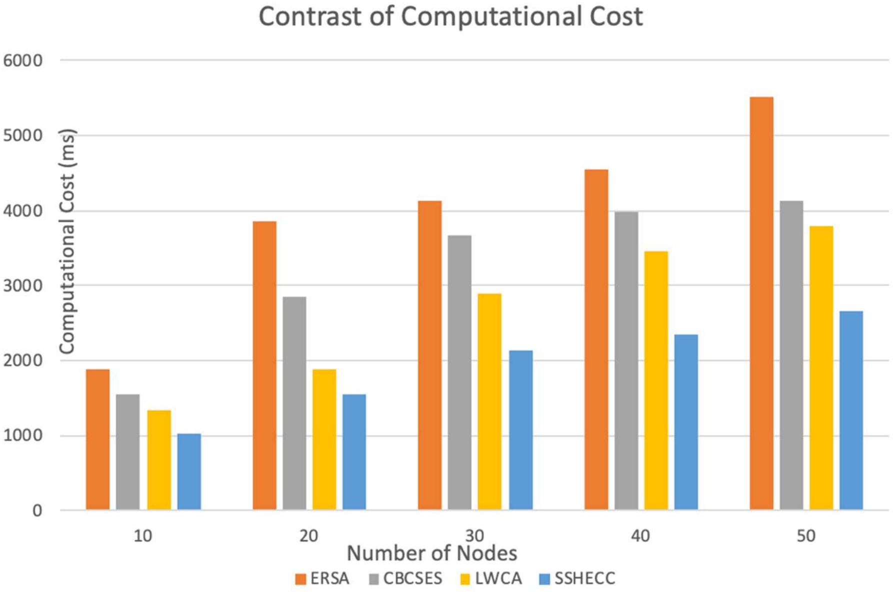

Figure 6 Contrast of Computational Cost

c. Energy Consumption:

The suggested concept has a communication distance of less than 100 meters, based on the average size of a hospital ward. Due to the size of the gap between d < d_0, we choose to work inside a free space paradigm, employing the following: ε= fs = 10pJ/bit/m2 as our amplifier energy factor. In terms of energy compression, the presented method excels over previous techniques. The energy needed to do an ECPM operation is 19.1 mJ, while the energy needed to perform a pairing computation is 62.73 mJ. Figure 7 below contrasts the energy requirements of the proposed method with those of several other systems [43]. In addition, evidence is provided that demonstrates our design is more energy-efficient and better suited to the limited resources of WBSN.

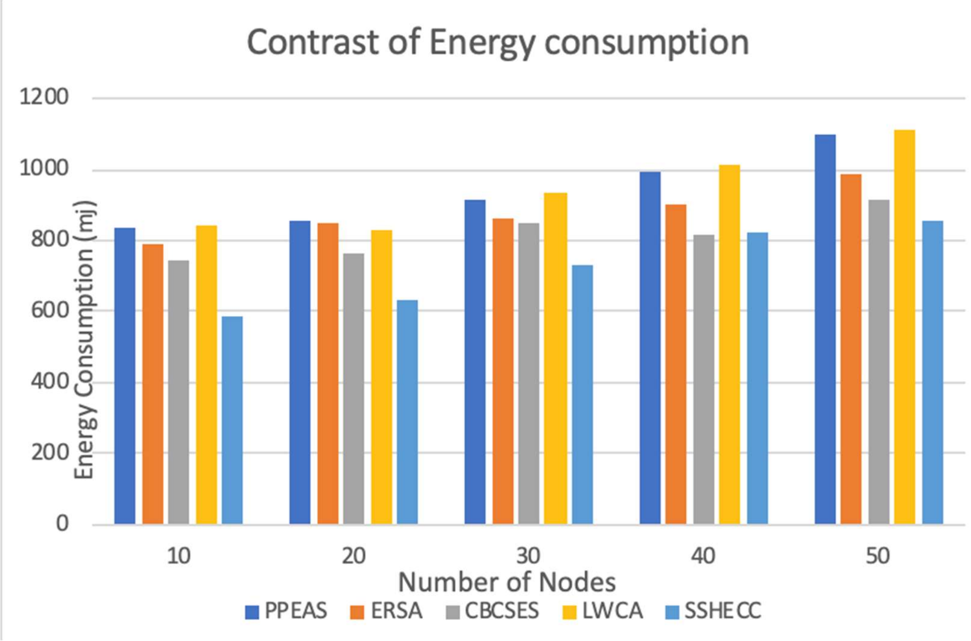

Figure 7 Contrast of Energy Consumption

d. **Storage-Cost:**

It is clear that SSHECC's storage costs are lower than those of other state-of-the-art techniques because of the smaller key size [44]. The relative storage costs as a function of node count are graphically represented in Figure 8.

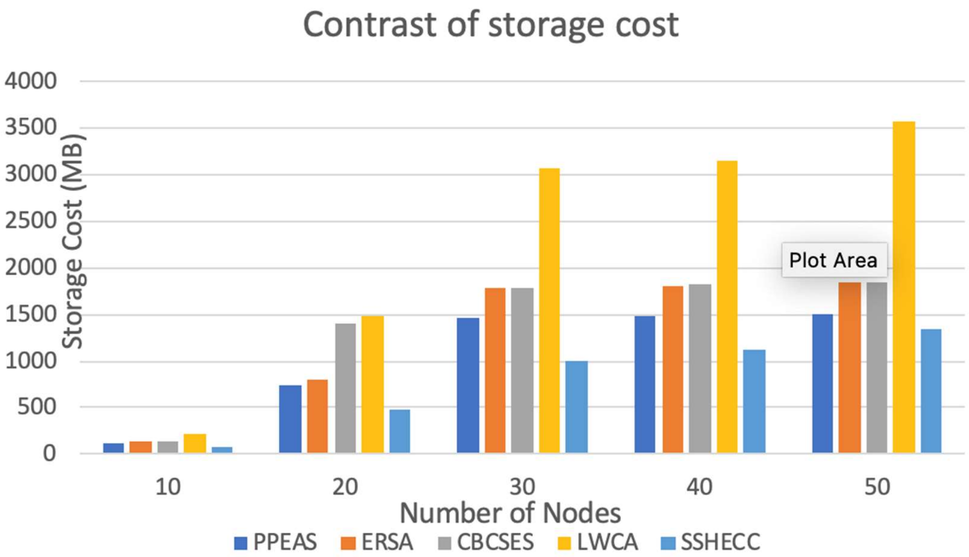

Figure 8 Contrast of Storage Cost

5. CONCLUSION AND FUTURE WORKS

This paper proposes a novel and effective SSHECC architecture to address the security and CC concerns, enabling the healthcare scheme to maintain the tradeoff amid security and cost for effective disease investigation. A lightweight is also in order to safeguard private medical information during its transfer across open networks, this solution has been presented. The security, computational, communication, energy, and storage costs of this cryptosystem are all superior to those of the current state-of-the-art systems. Since WBANs operate in a resource-constrained environment, the idea of Software-Defined Networking (SDN) has been incorporated to better manage data traffic flow via the strategic use of data plans and control plans independently. After mutual authentication, external users can safely access medicinal records from MS, and hardware-firewalls allow us to competently observe received &sending data-traffic without compromising its security.

A future intelligent communication protocol for WBANs can use many queuing strategies, such as precedence queues and slanted fair queues, to enhance the Quality of Service (QoS). Researchers can similarly improve security and privacy at low cost by integrating 5G/6G communication technologies with quantum cryptosystems and attribute-based fog-edge-assisted signcryption.

REFERENCES

1. Sama, N.U., Zen, K., Humayun, M., Jhanjhi, N.Z. and Rahman, A.U., 2022. Security in wireless body sensor network: A multivocal literature study. Applied System Innovation, 5(4), p.79.
2. Iqbal, J., Adnan, M., Khan, Y., AlSalman, H., Hussain, S., Ullah, S.S., Amin, N.U. and Gumaei, A., 2022. Designing a healthcare-enabled Software-Defined wireless body area network architecture for secure medical data and efficient diagnosis. Journal of Healthcare Engineering, 2022, pp.1-19.
3. Hussain, S., Ullah, S.S., Uddin, M., Iqbal, J. and Chen, C.L., 2022. A comprehensive survey on signcryption security mechanisms in wireless body area networks. Sensors, 22(3), p.1072.
4. Nandikanti, A., Sahu, K.N. and Panigrahi, S., 2022. Security issues and solutions for reliable wban-based e-healthcare systems: A systematic review. Ambient Intelligence in Health Care: Proceedings of ICAIHC 2022, pp.21-32.
5. Sengan, S., Khalaf, O.I., Sharma, D.K. and Hamad, A.A., 2022. Secured and privacy-based IDS for healthcare systems on E-medical data using machine learning approach. International Journal of Reliable and Quality E-Healthcare (IJRQEH), 11(3), pp.1-11.
6. Yaghoubi, M., Ahmed, K. and Miao, Y., 2022, November. TIDS: Trust Value-Based IDS Framework for Wireless Body Area Network. In 2022 32nd International Telecommunication Networks and Applications Conference (ITNAC) (pp. 142-148). IEEE.
7. Singla, R., Kaur, N., Koundal, D. and Bharadwaj, A., 2022. Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. Wireless Personal Communications, pp.1-40.

8. Menaga, S., Vanithamani, R. and Hema, P., 2022, August. A Comprehensive Review on Wireless Body Area Network-Technologies, Challenges, Application and Energy Saving Techniques. In 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 541-548). IEEE.
9. Rameshkumar, C. and Ganeshkumar, T., 2022. A Novel of Survey: In Healthcare System for Wireless Body-Area Network. In Applications of Computational Methods in Manufacturing and Product Design: Select Proceedings of IPDIMS 2020 (pp. 591-609). Singapore: Springer Nature Singapore.
10. Gaikwad, V.D. and Ananthakumaran, S., 2023. A Review: Security and Privacy for Health Care Application in Wireless Body Area Networks. Wireless Personal Communications, 130(1), pp.673-691.
11. Iqbal, J., Adnan, M., Khan, Y., AlSalman, H., Hussain, S., Ullah, S.S., ul Amin, N. and Gumaei, A., 2022. Research Article Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis.
12. Reddy, P.C., Nachiyappan, S., Ramakrishna, V., Senthil, R. and Sajid Anwer, M.D., 2021. Hybrid model using scrum methodology for softwar development system. J Nucl Ene Sci Power Generat Techno, 10(9), p.2.
13. Saba, T., Rehman, A., Haseeb, K., Bahaj, S.A. and Lloret, J., 2022. Optimized Embedded Healthcare Industry Model with Lightweight Computing Using Wireless Body Area Network. Wireless Communications and Mobile Computing, 2022.
14. Pawar, R.S. and Kalbande, D.R., 2023. Optimization of quality of service using ECEBA protocol in wireless body area network. International Journal of Information Technology, 15(2), pp.595-610.
15. Ashok, K., Boddu, R., Syed, S.A., Sonawane, V.R., Dabhade, R.G. and Reddy, P.C.S., 2023. GAN Base feedback analysis system for industrial IOT networks. Automatika, 64(2), pp.259-267.
16. Bangotra, D.K., Singh, Y., Kumar, N., Kumar Singh, P. and Ojeniyi, A., 2022. Energy-efficient and secure opportunistic routing protocol for wsn: Performance analysis with nature-inspired algorithms and its application in biomedical applications. BioMed Research International, 2022.
17. Mondal, S., Ghosh, I. and Das, A., 2023. Energy efficient and secure healthcare data transmission in the internet of medical things network. Microsystem Technologies, 29(4), pp.539-551.
18. Reddy, P.C.S., Pradeepa, M., Venkatakiran, S., Walia, R. and Saravanan, M., 2021. Image and signal processing in the underwater environment. J Nucl Ene Sci Power Generat Techno, 10(9), p.2.
19. Singhal, A., Varshney, S., Mohanaprakash, T.A., Jayavadivel, R., Deepti, K., Reddy, P.C.S. and Mulat, M.B., 2022. Minimization of latency using multitask scheduling in industrial autonomous systems. Wireless Communications and Mobile Computing, 2022, pp.1-10.
20. Srivastava, J., Routray, S., Ahmad, S. and Waris, M.M., 2022. Internet of Medical Things (IoMT)-based smart healthcare system: Trends and progress. Computational Intelligence and Neuroscience, 2022.

21. Shaker Reddy, P.C. and Sucharitha, Y., 2022. IoT-Enabled Energy-efficient Multipath Power Control for Underwater Sensor Networks. International Journal of Sensors Wireless Communications and Control, 12(6), pp.478-494.
22. Kumar, K., Kumar, A., Kumar, N., Mohammed, M.A., Al-Waisy, A.S., Jaber, M.M., Shah, R. and Al-Andoli, M.N., 2022. Dimensions of internet of things: Technological taxonomy architecture applications and open challenges—A systematic review. Wireless Communications and Mobile Computing, 2022.
23. Li, X.R. and Jiang, H., 2022. Energy-aware healthcare system for wireless body region networks in IoT environment using the whale optimization algorithm. Wireless Personal Communications, 126(3), pp.2101-2117.
24. Sabitha, R., Shukla, A.P., Mehbodniya, A., Shakkeera, L. and Reddy, P.C.S., 2022. A Fuzzy Trust Evaluation of Cloud Collaboration Outlier Detection in Wireless Sensor Networks. Adhoc & Sensor Wireless Networks, 53.
25. Anbarasan, H.S. and Natarajan, J., 2022. Blockchain Based Delay and Energy Harvest Aware Healthcare Monitoring System in WBAN Environment. Sensors, 22(15), p.5763.
26. Bangotra, D.K., Singh, Y., Selwal, A., Kumar, N., Singh, P.K. and Hong, W.C., 2020. An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare. Sensors, 20(14), p.3887.
27. Chillakuru, P., Madiajagan, M., Prashanth, K.V., Ambala, S., Shaker Reddy, P.C. and Pavan, J., 2023. Enhancing wind power monitoring through motion deblurring with modified GoogleNet algorithm. Soft Computing, pp.1-11.
28. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M. and Shamshirband, S., 2017. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian informatics journal, 18(2), pp.113-122.
29. Muthappa, K.A., Nisha, A.S.A., Shastri, R., Avasthi, V. and Reddy, P.C.S., 2023. Design of high-speed, low-power non-volatile master slave flip flop (NVMSFF) for memory registers designs. Applied Nanoscience, pp.1-10.
30. Bangotra, D.K., Singh, Y., Selwal, A., Kumar, N. and Singh, P.K., 2022. A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. Wireless Personal Communications, 127(2), pp.1045-1066.
31. Shanmugaraja, P., Bhardwaj, M., Mehbodniya, A., VALI, S. and Reddy, P.C.S., 2023. An Efficient Clustered M-path Sinkhole Attack Detection (MSAD) Algorithm for Wireless Sensor Networks. Adhoc & Sensor Wireless Networks, 55.
32. Sucharitha, Y., Reddy, P.C.S. and Suryanarayana, G., 2023. Network Intrusion Detection of Drones Using Recurrent Neural Networks. Drone Technology: Future Trends and Practical Applications, pp.375-392.
33. Liu, L., Shafiq, M., Sonawane, V.R., Murthy, M.Y.B., Reddy, P.C.S. and kumar Reddy, K.C., 2022. Spectrum trading and sharing in unmanned aerial vehicles based on distributed blockchain consortium system. Computers and Electrical Engineering, 103, p.108255.
34. Alahakoon, S. and Logeswaran, R., 2023, May. Review on Workload and Resource Allocation in Edge-Based Wireless Body Area Networks. In 2023 IEEE 13th

Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 304-308). IEEE.

35. Preethichandra, D.M.G., Piyathilaka, L., Izhar, U., Samarasinghe, R. and De Silva, L.C., 2023. Wireless Body Area Networks and Their Applications–A Review. IEEE Access.
36. Islam, F., Akand, T. and Kabir, S., 2022. Energy Efficient Real-Time E-Healthcare System Based on Fog Computing. Journal of Computational and Cognitive Engineering.
37. Adarsh, A. and Kumar, B., 2020. Wireless medical sensor networks for smart e-healthcare. In Intelligent Data Security Solutions for e-Health Applications (pp. 275-292). Academic Press.
38. Upadhyay, S., Kumar, M., Upadhyay, A., Verma, S., Kavita, Kaur, M., Khurma, R.A. and Castillo, P.A., 2023. Challenges and Limitation Analysis of an IoT-Dependent System for Deployment in Smart Healthcare Using Communication Standards Features. Sensors, 23(11), p.5155.
39. Ahmed, S., Naga Srinivasu, P. and Alhumam, A., 2023. A Software Framework for Intelligent Security Measures Regarding Sensor Data in the Context of Ambient Assisted Technology. Sensors, 23(14), p.6564.
40. Chakraborty, C., Othman, S.B., Almalki, F.A. and Sakli, H., 2023. FC-SEEDA: fog computing-based secure and energy efficient data aggregation scheme for Internet of healthcare Things. Neural Computing and Applications, pp.1-17.
41. Yang, W. and Wang, S., 2021. A privacy-preserving ECG-based authentication system for securing wireless body sensor networks. IEEE Internet of Things Journal, 9(8), pp.6148-6158.
42. Nidhya, R., Shanthi, S. and Kumar, M., 2021. A novel encryption design for wireless body area network in remote healthcare system using enhanced RSA algorithm. In Intelligent System Design: Proceedings of Intelligent System Design: INDIA 2019 (pp. 255-263). Springer Singapore.
43. Ullah, I., Amin, N.U., Khan, M.A., Khattak, H. and Kumari, S., 2021. An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for internet of things (IoT) in mobile health (M-health) system. Journal of Medical Systems, 45, pp.1-14.
44. Wan, T., Wang, L., Liao, W. and Yue, S., 2021. A lightweight continuous authentication scheme for medical wireless body area networks. Peer-to-Peer Networking and Applications, 14(6), pp.3473-3487.