Hindawi
Journal of Healthcare Engineering
Volume 2023, Article ID 9805042, 1 page
https://doi.org/10.1155/2023/9805042

Retraction

Retracted: Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis

Journal of Healthcare Engineering

Received 23 May 2023; Accepted 23 May 2023; Published 24 May 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process. Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Iqbal, M. Adnan, Y. Khan et al., "Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis," *Journal of Healthcare Engineering*, vol. 2022, Article ID 9210761, 19 pages, 2022.

Hindawi
Journal of Healthcare Engineering
Volume 2022, Article ID 9210761, 19 pages
https://doi.org/10.1155/2022/9210761

Research Article

Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis

Jawaid Iqbal,[1] Muhammad Adnan,[2] Younas Khan,[1] Hussain AlSalman,[3] Saddam Hussain,[4] Syed Sajid Ullah,[5] Noor ul Amin,[2] and Abdu Gumaei[6]

[1]*Department of Computer Science Capital University of Science and Technology, Islamabad, Pakistan*
[2]*Department of Information Technology Hazara University, Mansehra, Pakistan*
[3]*Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia*
[4]*School of Digital Science, Universiti Brunei Darussalam, Jalan Tungku Link, Gadong, BE1410, Brunei Darussalam*
[5]*Department of Electrical and Computer Engineering, Villanova University, Villanova, PA 19085, USA*
[6]*Computer Science Department, Faculty of Applied Sciences, Taiz University, Taiz 6803, Yemen*

Correspondence should be addressed to Saddam Hussain; saddamicup1993@gmail.com and Abdu Gumaei; abdugumaei@gmail.com

Received 27 October 2021; Accepted 16 December 2021; Published 4 February 2022

Academic Editor: Deepak Garg

In the struggle against population aging, chronic diseases, and a lack of medical facilities, the emergence of Wireless Body Area Networks (WBANs) technology has ushered in optimism. WBANs use a variety of wearable and implanted biosensor nodes to constantly monitor physiological parameters such as oxygen saturation (SpO_2), electrocardiogram (ECG), electromyography (EMG), electroencephalogram (EEG), blood pressure, respiration rate, body temperature, and pulse rate. Importantly, these vital signs are communicated to a doctor over a public network, who can diagnose ailments remotely and efficiently. Among these communications, the security and privacy of patients are the prime concerns while transferring data over an open wireless channel from biosensor nodes to a Medical Server (MS) through a Base Station (BS) for efficient medical diagnosis. Finding an effective security strategy for patients which rely on WBANs to monitor their health information is a huge challenge due to the confined nature of the WBANs environment. To tackle the above challenges, in this research, a new, efficient, and secure healthcare-enabled software-defined WBANs architecture based on Schnorr signcryption and Hyperelliptic Curve Cryptography (HECC) is suggested in which the SDN technology is integrated into WBANs. By separating the control and data planes in an efferent manner, SDN technology allows you to control and manage the network in a programmable manner. The main features of SDN, such as its programmability, flexibility, and centralized control, make it a simple and scalable network. In this research, first, a Software-Defined Wireless Body Area Networks (SD-WBANs) architecture has been designed, and then a lightweight Schnorr signcryption with Hyperelliptic Curve Cryptography (HECC) has been proposed to preserve sensitive patient data security during transmission on public networks. Moreover, a well-known Multicriteria Decision-Making (MCDM) approach known as Evaluation Based on Distance from Average Solution (EDAS) is also used to demonstrate the success of the suggested system. According to the performance analysis, the suggested approach beats previous state-of-the-art techniques in terms of computation cost, communication overhead, storage cost, and energy usage.

1. Introduction

Recent technological developments in the large-scale integration of physical sensors, microelectronics, and radio transmission on a chip have aided the production of Wireless Sensor Networks (WSNs). WSNs, which are compact and easy to install, can be used in a variety of sectors due to a number of unresolved research challenges. A WSN is made up of spatially dispersed autonomous sensors that monitor environmental or physical elements such as motion, vibration, sound, pressure, temperature, and pollution and transmit their data or and machine learning models to a central location over the network. The more advanced networks are bidirectional, allowing control of sensor activity. WSNs were developed in response to military applications like war zone observation and are currently used in a range of consumer and industrial applications [1].

WBAN is one of the most interesting applications of WSNs in which patients' physiological vital signs such as SpO_2, ECG, EMG, EEG, blood pressure, respiratory rate, body temperature, and pulse rate are monitored using various biosensor nodes deployed inside and/or outside the human body that does not disturb the normal routine activities performed by humans in their daily life. Various resource-constrained biosensor nodes can be utilized in healthcare applications, and they can be linked with various communication devices such as gateways/BS and MS using wireless technologies such as 4G, 5G, LTE, UMTS, Wi-Fi, WiMax, and satellite communication. Moreover, medical experts can securely obtain the patient's real-time medical information from the MS after mutual authentication, and by using a firewall, we can protect the adversaries' attacks along with monitoring incoming and outgoing data traffic in an efficient and reliable way. Medical experts can diagnose the medical information of the concerned patient and provide feedback to the concerned patient attendant in the wards of the hospital to improve the patient's quality of life.

1.1. Software-Defined Network (SDN). With the rapid growth of new technology and the implementation of networking methods in recent years, SDN has attracted the attention of the industry, academia, and government. It is a new technology that allows you to control and manage the network in a programmable manner by separating the control and data planes in an efferent way. There are four parameters through which we define the SDN architecture, as in Ref. [2]:

(i) Separate the control plane from the data plane. The network devices act as a forwarding element (packet forwarding) without any control functionalities.

(ii) The decision for the forwarding element (packet forwarding) is flow-based in which a certain condition is matched in a set of instructions performed by a set of values in the packet field. In SDN, the Open Flow protocol with different APIs is used for the interaction of different planes with each other.

(iii) An SDN controller acts as a logically centralized controller that has an abstract view of the entire network for overall management.

(iv) The applications that are running on top of the SDN controller through programmability works together with the essential data plane devices.

SDN is an emerging technology that can be integrated into many fields, such as WSN, WBAN, VANET, IoT, and cloud. In this context, we mainly focus on the integration of SDN with WBAN. WBANs are one of the most interesting applications of WSNs, and in the following section, the integration of SDN in WSN has been discussed.

1.2. SDN-Based Management in WSN. When integrating SDN in WSN, it manages the following functionalities:

(i) *Management of Network Configuration.* Initially, when the functionalities of SDN are used in WSN, network configuration is required because it was developed for traditional networks. It is very important to develop a protocol that connects the existing SDN functionalities in WSN. The Sensor Open Flow (SOF) protocol is proposed to enable communication between the data and control planes in the WSN environment for this purpose [3]. With the help of this architecture, one can create a central control through which the overall network is to be managed and configured.

(ii) *Provide Scalability and Efficient localization Management.* A typical WSN faces some natural difficulties, and it is very important to remove these difficulties. For this reason, Ref. [4] proposed a smart management scheme for SDWSN in order to improve efficiency and cope with the stated difficulties. This scheme is used for small networks and is limited to a short range. For large-scale networks, Ref. [5] proposed a hierarchical architecture known as SDCSN, in which the clusters are connected to the base station and multiple base stations are connected to the controller. Different architectures are proposed in WSNs in which the SDN functionality can be integrated to provide scalability and efficient localization management for the WSN environment.

(iii) *Mobility Management.* The sensor nodes in an SDN-based WSN can move in order to perform their task and transmit it to the base station. It is very important to check and handle the movement of these nodes in the network. In Ref. [6], the authors have proposed SDN-based WSNs that support IP, and another scheme for WSNs [7] is proposed based on TinyOS that supports IP-based mobility management. Another mechanism is proposed in Ref. [8], in which the IEEE 802.15.4 standard has been investigated for distributed networks in order to manage mobility.

To incorporate the advantages and benefits of SDN-based WSN, examined from the literature review, an SDN-based WBAN solution has been developed. It is taken into account that one of the most crucial challenges in improving the performance of these two networking developments (WSN and SDN) is security. Recent advancements in WBAN offer vulnerabilities beyond those addressed by traditional security services. The public is warned about the serious consequences of both unintentional and malicious misuses.

1.3. Benefits of Software-Defined WBANs Architecture. The unique properties of SDN, such as its flexibility, scalability, programmability, and adaptability, make it feasible for WBANs. The main advantages of using SDN in WBANs [2] are listed as follows:

(i) *Handling of Data*. The WBAN nodes are deployed on a patient body to continuously sense and send his information to the MS in a secure and efficient way for further diagnosis and treatment using machine learning algorithms. All the concerned data like patient records, doctor's profiles, machine learning diagnosis models, and external users such as government agencies, researchers, and financial companies are stored on the medical server. With the help of SDN, this management system makes it possible by logically centralized control.

(ii) *Analysis of Data*. The purpose of collecting data is to perform different operations on it, for instance, diagnosis and analysis, modeling, and medical decision-making, based on requirements.

(iii) *Centralize Management System*. The SDN controller provides logically centralized control that has an abstract view of the entire network. In addition, they provide Quality of Service (QoS) using specific tools.

(iv) *Using Cloud Application*. Collecting, storing, and processing data in WBAN applications is a difficult task and doing so in SDN necessitates a high level of programming ability. Cloud applications such as (SaaS) environments make it easier to store, process, and retrieve data.

1.4. Contributions. The main contributions of this paper are given as follows:

(1) A novel and efficient SD-WBANs architecture has been designed that enables the healthcare system to maintain a better tradeoff between security and cost for efficient disease diagnosis.

(2) An SDN technology has been integrated into WBANs to efficiently manage the data traffic flow in the resource-contained environment of WBANs in a centralized way by separating the data plans and control plans.

(3) A lightweight Schnorr Signcryption with Hyperelliptic Curve Cryptography (HECC) has been proposed to preserve sensitive patient data security during transmission on public networks.

(4) Using the proposed lightweight cryptosystem, better efficiency in terms of security, computation, communication, and storage costs, along with energy consumption, has been achieved.

(5) Medical experts can securely obtain the patient's real-time medical information from the MS after mutual authentication, and by using hardware firewalls, incoming and outgoing data traffic can be efficiently, reliably, and securely routed.

(6) The success of the proposed scheme is demonstrated using a well-known MCDM approach known as EDAS.

1.5. Paper Organization. The article is organized as follows. Section 2 reviews the literature on SDN, SDN-based WSN, and SDN-based WBAN architecture. Preliminaries about HECC are presented in Section 3. The proposed SDN-based WBAN architecture for E-Healthcare System is discussed in Section 4. Our network model is presented in Section 5. The proposed Schnorr Signcryption utilizing Hyperelliptic Curve Cryptosystem is discussed in Section 6. An illustration of performance analysis for the proposed scheme against the state-of-the-arts is given in Section 7. A detailed description of EDAS is also explained in Section 8, and Section 9 gives the conclusion of this research work.

2. Literature Review

The architectural design and its security requirements have been considered in the SDN-based WBAN-enabled healthcare system to design a novel and efficient architecture for SDN-based WBAN. For this purpose, a comprehensive study of the literature is presented, covering the basics of WSN, background of SDN, SDN-based WSN, and SDN-based WBAN architecture review.

2.1. Related Work on WBAN. Wireless technology has caused a boom in the usage of Wireless Body Sensor Networks or WBSN, and its application enables users to evaluate vital signs from around the globe using the Internet. The stated technology is used to reduce cost and has numerous other benefits as well. However, there are certain security issues that WBSN is prone to. The article in Ref. [9] analyzes the WBSN architecture in order to present an overview of security issues particularly concerning authentication, whereas other factors influencing the required communication from WBSN, such as computational and storage cost, have been overlooked. As far as the security of BSN is concerned, the article reports that at least the trio of confidentiality, integrity, and availability must be met [10]. It is obvious that the IoT components operate in a very broad spectrum and thus the security concerns are amplified, and the stated trio is a bare minimum. Open-source wireless channels are used to communicate the collected data in a WBAN; this makes the data susceptible to malicious attacks. Confidentiality and authenticity are required for securing the WBAN from these

attacks. The article in Ref. [11] presents an anonymous technique for ensuring the legitimacy of patients and doctors without letting their infringing on their privacy. Numerous other mechanisms are already present; however, there are many issues as WBAN is a resource-constrained environment, and their usage causes overhead issues. The proposed technique is evaluated and found useful particularly for confidentiality and authenticity-related issues and at the same time it is able to reduce computational complexity. However, the cost in terms of storage, energy, and processing can still be decreased. Other such techniques, for ensuring authentication, have been proposed in Refs. [12, 13]. However, the cost overhead can further be reduced. Chunka and Banerjee [14] have presented a scheme for ensuring security in terms of confidentiality, authentication, and integrity to increase efficiency. However, the communication and computation costs can further be reduced. Saeed Ullah et al. [15] have presented a robust and lightweight scheme for WBAN. However, the achieved balance between security and performance can further be improved. To increase the reliability of WBAN systems, key agreement/management needs to be nominated. For this purpose, the article in Ref. [16] proposes a healthcare monitoring protocol. The proposed scheme has been formally analyzed under the BAN logic. However, the authors did not discuss integrity and confidentiality. In Ref. [17], an ECG-based authentication scheme for the purpose of providing security to sensitive identity, and health information has been presented. However, the scope of the article is limited to authentication only while other key factors such as confidentiality and integrity have been ignored. The authors in Ref. [18] present a framework that robustly preserves privacy by making use of homomorphic encryption. However, the throughput achieved by the framework can be enhanced. In Ref. [19], a systematic approach has been followed to report that the current issues with WBSN include the fact that the data gathered through sensors is poorly managed, and a lack of strategy is observed. For that, the study has suggested the use of homomorphic encryption. Another gap that has been pointed out in this research is that trust management, and the need to properly preserve these sensitive data is reported. Another study [20] performs an insight survey of Wireless Body Area Networks in order to present an overview of its topology, design, and architecture. Secondly, current and future research perspectives concerning privacy and security have also been discussed. Ref. [21] aims to present architecture for WBAN based on an enhanced RSA or ERSA for encryption, and authentication; however, integrity has not been emphasized in the stated research. In Ref. [22], a new cryptosystem has been proposed that covers a few of the stated issues in an extremely efficient manner. The propose framework is based on the concept of lightweight cryptography, and a secure signcryption scheme, which is deployed as an encryption mode. The deployed algorithm is claimed to be using fewer resources, as it uses keys that are short in size. In Ref. [23], the authors review two anonymous schemes of authentication of the WBAN environment. However, the performance of the propose schemes can be improved for a better tradeoff. In Ref. [24], a wavelet transform-based frequency-time domain method has been proposed to separate relevant signals and to compress them without losing any information. The presented framework increases efficiency; however, the achieved performance can be improved further. The authors in Ref. [25] present a heterogeneous framework for BSNs, which uses a Certificateless environment of cryptography for resolving key escrow, and other certificate management-related issues. However, the efficiency in terms of costs can be improved further. In Ref. [26], a Certificateless signature scheme for WBAN maintains the same size of the signature. However, a better balance between performance and security can be achieved. In Ref. [27], a lightweight and secure authentication, and key management protocol have been presented. The proposed mechanism has been evaluated against different security threats and attacks. However, the achieved overhead can be decreased further. Ref. [28] designs an agreement for increasing the security robustness and privacy of WBAN to protect patient data from adversaries' attacks. Nevertheless, the reduction in cost that it has achieved can still be decreased. In this study [17], the authors have designed a novel and efficient ECG-based privacy-preserving WBSN system based on the Manipulatable Haar Transform, a noninvertible transformation algorithm (MHT). Besides using this scheme, the patient data are protected from adversaries' attacks. In this scheme [29], the authors applied a lightweight cryptosystem to ensure data security and privacy with minimal cost. In addition, the wavelet transform frequency-time domain method is applied for separating relevant signals. Furthermore, the lossless compression algorithm is applied to compress these signals in an efficient way and then encrypt them using the SPECG algorithm to enhance the security of data during transmission on public networks. In this scheme [9], the authors have proposed an overview of the Internet of Things, including its architecture, as well as the privacy and security considerations associated with IoT-based healthcare applications.

2.2. Related Work on SDWSN and SD-WBAN. In Ref. [30], the authors present a novel structure for WSN based on SDN technology. In WSN, different protocols have been designed for different purposes, such as routing protocols for load balancing, network topology changes, node energy, etc. It is very difficult to build a single protocol that integrates these kinds of properties. SDN is the best solution for this type of situation. However, some issues need to be solved, such as missing the energy limit for the center, master, and normal nodes, as well as zoning of nodes, etc. In Ref. [31], the author presents a review of the SDWSN literature. The author discusses the problems that are faced by SDWSN and provides the solution and design requirements that are needed to address these problems. In this survey, the author identified the issue in TCP as underling the communication protocol and overhead that occurs in Ref. [32] based on OpenFlow. In Ref. [33], the author reviews the main features of IT-SDN and the present performance evolution of sensing nodes that periodically transmit data. Several experiments are conducted based on the number of nodes to check the maximum capacity of the flow table. Different metrics such as data delay, data delivery, energy consumption, and control overhead are evaluated by comparing the performance of IT-SDN with that of the IETF RPL routing protocol. In Ref. [34], the author proposes WS3N, secure communication for WSN based on SDN technology which

handles node admission as well as symmetric-key distribution. The security algorithm and protocol are combined with the SDN protocol. For improvement purposes, the packet headers are crafted in order to fit the IEEE 802.15.4 frame size and to be compatible with 6LoWPAN networks. In Ref. [35], the authors propose SDN architecture for WSN in order to study the feasibility and utility, such as simplicity in the management of routing policies to be set in the flow table. In Ref. [36], an efficient data delivery system has been proposed, by making use of the Kerberos protocol for authentication of medical data in Software-defined WBAN for a virtual hospital system. In Ref. [37], the authors present a generalized software-defined architecture based on the cloud. The paper provides the unique functionalities, reliability, and knowledge of data mining technology and avoids the complexity of cloud architecture, and its integration with WBAN in SDN.

We analyzed the most recent security and privacy strategies for WBANs in the works referenced above. Based on the literature review, we determined that lightweight and secure healthcare-enabled software-defined WBANs are required for the security and privacy of medical data. Furthermore, different strategies are provided in the literature to increase the security and privacy of BSNs. However, most methods relied on bilinear pairing procedures to secure the transmission of patient-sensitive data from biosensors to MS, which use an inordinate amount of resources. Consequently, these techniques are insecure in the established security model and expensive in terms of processing costs and transmission overhead. Besides, a huge concern is the protection of key exposure, which allows attackers to readily obtain critical patient information for illicit purposes.

3. Preliminaries

3.1. Hyperelliptic Curve Cryptography (HECC). HECC is a public cryptography approach that is similar to Elliptic Curve Cryptography (ECC) in that it is an extension of it. When compared to other encryption techniques, such as ECC, RSA, and the Digital Signature Algorithm (DSA), the HECC gives the same level of security. Because of its modest key size, HECC is ideal for resource-constrained situations. The HECC is divided into species of genus: 2, 3, 4, 5, and 6, with genus 2 being the most secure. The security of HECC is influenced by the hyperelliptic curve discrete logarithm problem, which prohibits an attacker from breaking the keys even if the P and Q are publicly known.

Notation: $x = t\ y = u\ z = v$.

The equation for HECC is as follows:

$$E:\ u^2 + h(t)u = f(t). \tag{1}$$

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

3.2. Genus of Hyperelliptic Curve Cryptography. HECC utilizes key size of a much lesser size as compared to other cryptosystems, such as RSA and end ECC in order to enable better security in a resource constrained environment, for instance, WBAN. Numerous (g) genuine users have been used below for different security scenarios making use of various keys comprising varying key sizes within the prime field (F_p) where the polynomial of the curve determines the value of g in the F_p.

Genus $g = 2$

$u^2 = t^5 + a_3t^3 + at^2 + a_1t + a_0$

Genus $g = 3$

$u^2 = t^7 + a_5t^5 + a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$

Genus $g = 4$

$u^2 = t^9 + a_7t^7 + a_6t^6 + a_5t^5 + a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$

Genus $g = 5$

$u^2 = t^{11} + a_9t^9 + a_8t^8 + a_7t^7 + a_6t^6 + a_5t^5 + a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$

Genus $g = 6$

$u^2 = t^{11} + a_9t^9 + a_8t^8 + a_7t^7 + a_6t^6 + a_5t^5 + a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$

3.3. Jacobian of HECC. A curve's Jacobian is defined on a finite field F, which is represented as $J_E(F)$, and each element of the Jacobian is designated by a divisor D.

$$J_E(F) = \frac{D^{\circ}}{P},$$
$$D = \sum_{P_i \in C} m_i P_i \& m_i \in Z. \tag{2}$$

D is a reduced divisor, and the $m_i \longrightarrow$ *Numbers on the curve*, $P_i \longrightarrow$ *points on the curve*. The m_i cannot be zero because it is a finite number. Each element of the Jacobian is represented by a unique reduce divisor.

Reduce divisor form:

$$D = \sum_{P_i \in C} m_i P_i - \left(\sum_{P_i \in C} m_i \right) \infty. \tag{3}$$

Only opposite points are present in the above equation such as

$$\sum_{P_i \in C} m_i P_i \leq g. \tag{4}$$

The opposite point for $P(t, u) \in C$ *is* $\overline{P}(t, -u, -h(t)) \in C$.

The security of cryptosystems is improved by using the Discrete Log Problem (DLP), and it is difficult to break the scheme/security. In HECC, an effective procedure is computing "D" for bulky whole "C."

$$D = \underbrace{D + D + \cdots + D}_{C_{pa}3}. \tag{5}$$

Scalar multiplication of divisor is a group operation that includes addition and doubling of a divisor. This operation adjusts the divisor of the Jacobian of the HECC by elliptic

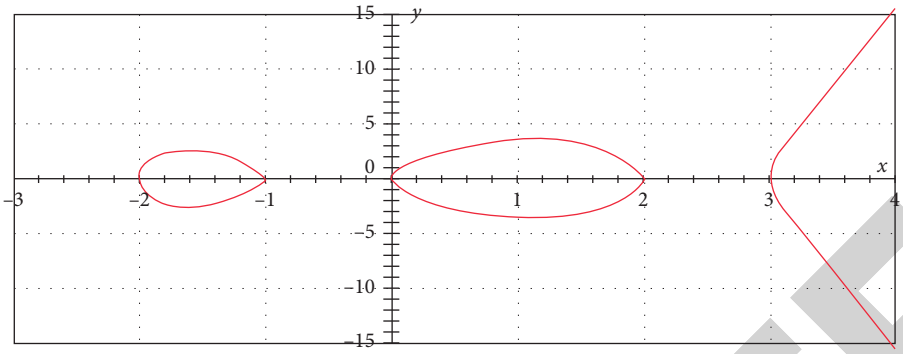

Figure 1: Diagrammatical representation of HECC [22].

curve (ECC) point multiplication. Figure 1 exhibits the diagrammatical representation of HECC.

3.4. Key Generation of HEC. As input HECC uses curve c, large prime numbers, P and D, are divisors for key generation and a couple of keys are generated, private key P_{pub} and public key P_{ri}.

(i) Pick P_{ri} private key randomly from (1, 2, 3, . . ., $n-1$)

(ii) After the selection of private key, use P_{ri} to generate a public key $P_{\text{pub}} = P_{\text{ri}} \cdot D$

(iii) Key pair: $[(P_{\text{pub}}, P_{\text{ri}})]$

3.5. Radio Model. In BSN, we used a first-order radio model to estimate energy consumption. The model's basic parameters are energy transmission, packet length, and distance. This equation is used to transmit data.

$$E_t(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2, & d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4, & d \geq d_0 \end{cases}, \tag{6}$$

$E_t(l,d)$ is the ratio of power consumed by a biosensor in communication. It is proportional to packet length and distance. Long distances require more energy than short distances.

$$E_r(l) = lE_{\text{elec}}. \tag{7}$$

Equation (6) is used to measure the energy consumed during the patient information transmission and receiving. Moreover, E_r (1) shows the total energy required for patient data receiving. In this equation, l is packet length and E_{elec} is energy consumption per bit as follows:

$$E_{\text{elec}} = \frac{50\,\text{nJ}}{\text{bit}}. \tag{8}$$

Our proposed scheme makes use of the concept of the free space model $\varepsilon = \varepsilon_{fs} = 10\,\text{PJ/bit/m}^2$ because of the distance between the two points $d < d_0$. Furthermore, ε_{fs} the power of the amplifier used in this model is a consideration.

4. Proposed Software-Defined Wireless Body Area Networks Architecture for E-Health Care System

The WBANs have been integrated into the SDN framework to enable an efficient and secure healthcare system. WBANs are worn on the patient body to capture data on quantitative real-time patient physiological indications such as heart rate, temperature, and blood pressure, among other things, allowing health treatment to reach beyond geographical boundaries. WBANs allow a large volume of medical data to be transferred to the MS via a BS, a device acting as a gateway. The BSs store and transfer raw data from wearable body area network devices with the SDN-based protocol to the MS for knowledge discovery. MS can be used to examine huge amounts of data created and gathered by body area networks in order to reveal significant knowledge for decision-making. The following components participate in the proposed software-defined wireless body area network architecture, as shown in Figure 2.

4.1. SDN Nodes. In WBANs, the nodes are the biosensors deployed on the body of a patient to sense the details of different vital signs such as blood pressure, pulse rate, heartbeat, EMG, and temperature. After collecting the information, it is sent through the network connector to the base station, which acts as a gateway and uses the IEEE 802.15.6 standard.

4.2. SDN Controller. The SDN controller provides logically centralized control that has an abstract view of the entire network. In our scheme, all the sensitive information about the patients is disseminated towards the SDN controller in encrypted form, from BS and MS, to store and manage the global view of the overall patient medical history.

4.3. Base Station. It is a powerful device that provides an interface between the patient and the medical server. BS collects data from the biosensor node and securely transmits data to the medical server for further analysis and diagnostics. In the meantime, the patient's real-time data are also

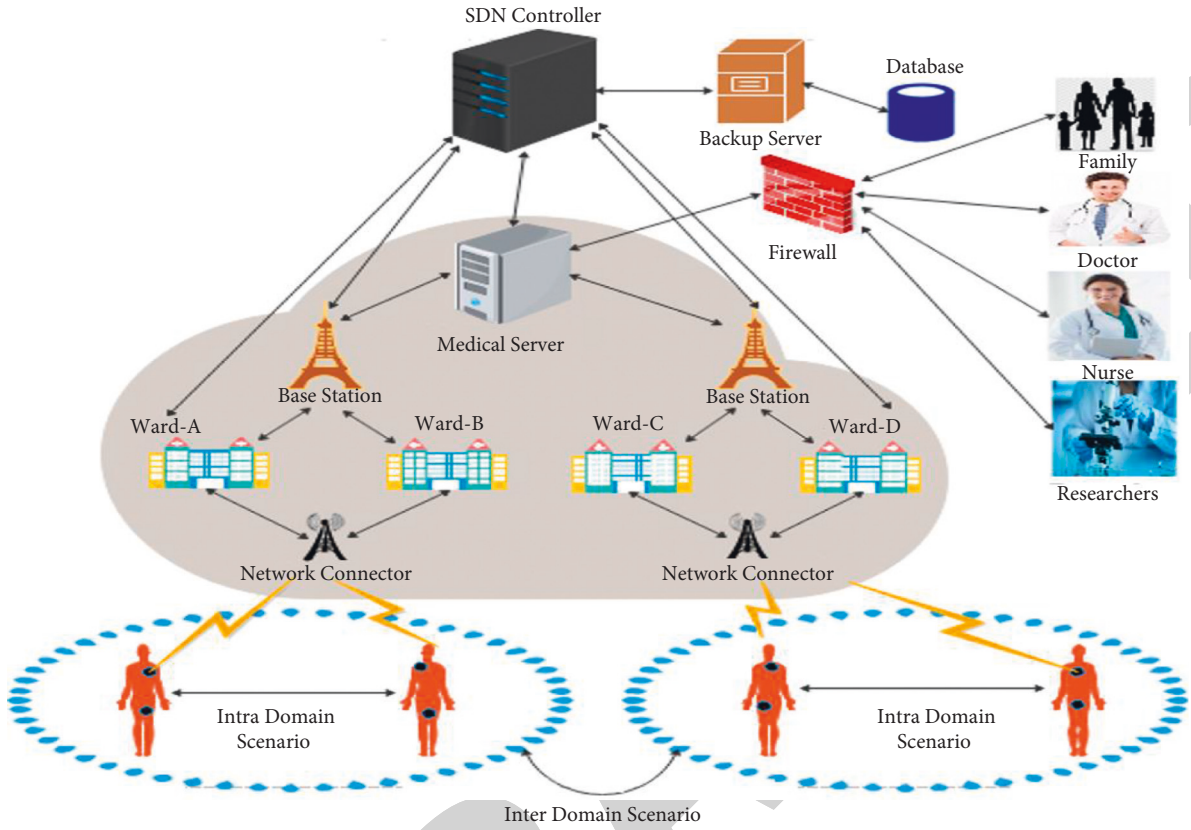

Figure 2: Proposed communication model.

disseminated from BS to the SDN controller to manage the global view of the patient record.

4.4. Medical Server. All the entities registered on the medical server are patients, doctors, researchers, and government agencies. All the patient information that is sensed by sensors can reach the medical server in encoded form through the base station. Different operations are performed on these data, like analysis, modeling, and medical decision-making, based on their requirements in future reference.

4.5. Database. The medical server is connected to the database that stores information about patients, doctors, researchers, and government agencies. The patient history includes patient id, name, age, gender, major disease, and date. The doctor's history includes doctor id, name, specialization, designation, department, ward, and duty timing.

4.6. External Users. The external users consist of doctors, patients, researchers, government agencies, insurance companies, and family members. All users are connected to the medical server to access the patient's record using their attributes defined in the access policy of the medical server.

4.7. Backup Server. In the proposed scheme, all the patient information is also stored in a backup server. In case of any failure, patient information can be recovered from the backup server. In this way, we protect the sensitive information of the patient from any loss and damage.

4.8. Access Control. A fine-grain access control system is constructed in the proposed scheme, through which all external user activities can be managed. External users must be validated; if they are valid users, they are granted authorization; otherwise, they are banned and separated from the WBSN networks.

4.9. Firewall. In the presented scheme for the secure transmission of patient medical information between MS and external users, the concept of a firewall has also been added. The firewall creates a barrier between the MS and external users to manage all the incoming data to the MS from the external users and outcoming patient data from the MS to the external users. In the proposed architecture based on predefined security policies, the firewall either allows or blocks specific users from accessing the patient medical record.

5. Network Model

In the proposed network model, different stretchable biosensor nodes are deployed on a patient's body admitted to a medical ward. These biosensor nodes have limited resources, i.e., memory, processing capability, and power. These biosensor nodes sense patient psychological data, process the

data, and communicate with BS using the IEEE 802.15.6 standard. The BS is a powerful device that collects patient data from the biosensor node and sends it to the MS via a public network for additional monitoring, diagnostics, analysis, and decision-making. MS stores all patient medical history in a logically organized and secure form. The doctor can access the patient's records from the MS using his or her smartphone using the Internet connection. On the basis of this data, the doctor can make a decision and suggest further treatment for the concerned patient. To control the system security of WBANs, we need to maintain data security and privacy. In the proposed WBAN network model, the concept of a firewall is laid between the MS and external users to manage the incoming and outgoing traffic flows and avoid the patient's sensitive medical information from being misused. In this model, a hardware-based firewall on both sides of MS to secure end-to-end communication is proposed. All data packets entering or leaving the network pass through the firewall, and after examining the firewall, it decides whether to allow them or not. All patient traffic must pass through the firewall, which should be strong enough to prevent illegal users from accessing patient data. The proposed generalized firewall-based network model is demonstrated in Figure 3.

5.1. Advantages of Firewall

5.1.1. User Authentication. In the proposed scheme using a firewall, we can authenticate whether the user is valid or not.

5.1.2. Auditing and Logging. We can audit all activities performed in a system, and the patient information may be kept and analyzed at a later date.

5.1.3. Anti-Spoofing. In the presented scheme, we can detect whether the source of the transmitted data is being spoofed.

5.1.4. Network Address Translation (NAT). For secure data transmission, we hide the original address for an intruder.

5.1.5. Virtual Private Network. Using firewall rules, we can establish VPN sessions for the secure transmission of data.

In the proposed scheme, access control can be maintained using a firewall, where two security methods are used, i.e., (a) everything not specifically permitted is denied and (b) everything not specifically denied is permitted. The former is a more popular security design logic method. The first security access control-based firewall network model is given in Figure 4 and described in the following steps:

(1) The biosensor nodes sense patient psychological data, process the data, and communicate with BS using the IEEE 802.15.6 standard.

(2) The BS is a powerful device that collects patient data from the biosensor node and sends it to the MS via a public network. Besides, the patient senses vital signs that are filtered using a firewall before being transmitted towards the MS to protect the WBANs from various virus attacks.

(3) A hardware-based firewall is proposed on both sides of MS to secure end-to-end communication. All data packets entering the network pass through the firewall, and after examining the firewall, it decides whether to allow them or not. Here, in the firewall, the rule and policies are defined, and the data packets are checked for matching the rules to authenticate them. If the data packets match the defined rules and policies, they will be permitted to the MS.

(4) After permission is granted from the firewall, the authenticated patient psychological data/vital signs such as SpO2, ECG, EMG, EEG, blood pressure, respiratory rate, body temperature, and pulse rate are stored inside the MS securely and consistently for further diagnoses and treatment.

(5) If the rules and policies are not matched, then these data packets are discarded, and the user is blacklisted and isolated from the WBANs.

The second security access control-based firewall network model is given in Figure 5 and described in the following steps:

(1) The external users, such as nurses, doctors, researchers, government agencies, insurance companies, and family members, send requests to the firewall in case they want to communicate with MS and want to access patient information for further analysis and decision-making.

(2) In the firewall, the rules and policies are defined, such as the attributes defined in the access policy of the MS.

(3) If the rules and policies are matched, then the users are permitted to access the patient's record stored in the MS.

(4) If the rules and policies are not matched for the users, then the requests of these users are blocked and isolated from the network to protect adversaries' attacks.

(5) addition, we have designed a clear flowchart of firewall-based network communication for user convenience, which is shown in Figure 6.

6. Proposed Schnorr Signcryption Using Hyperelliptic Curve Cryptosystem (HECC)

The proposed Schnorr signcryption using HECC for WBAN contains the following four phases: keys generation phase, Schnorr signcryption phase, Schnorr unsigncryption phase, and secret session key updating phase. The notations used in the proposed method are given in Table 1.

6.1. Key Generation Phase. In this section, we have computed the public and private keys, respectively, for biosensor nodes and MS for the secure transmission of patient physiology

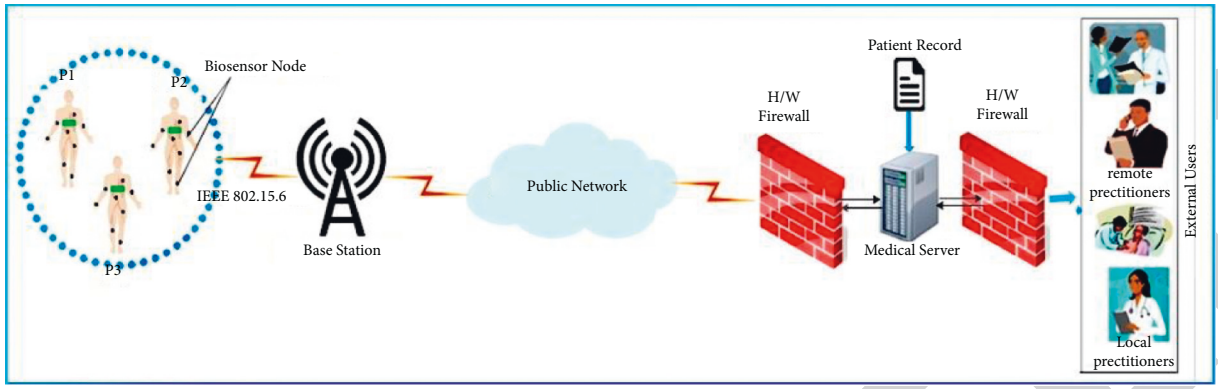

Figure 3: Proposed generalized firewall-based network model.

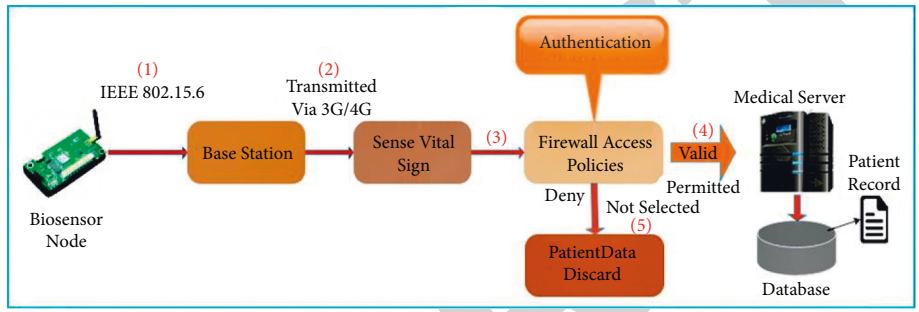

Figure 4: First security access control-based firewall network model.

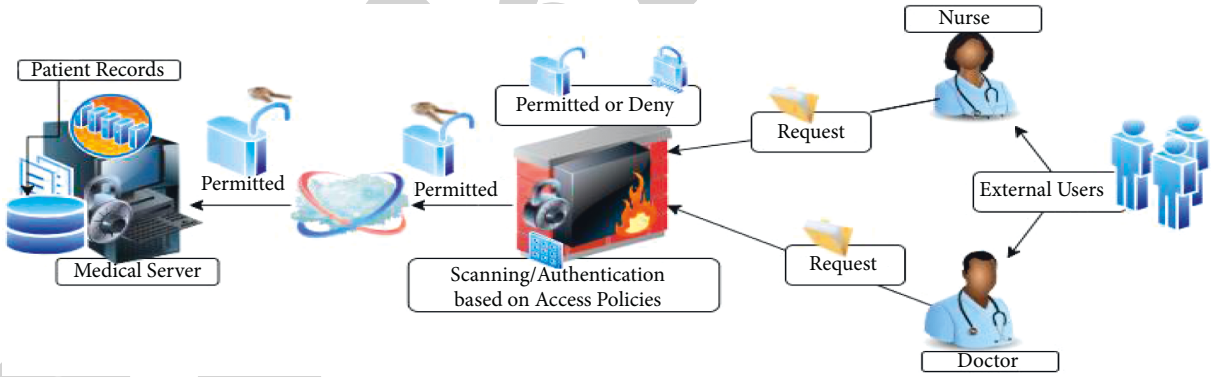

Figure 5: Second security access control-based firewall network model.

data from source to destination nodes in a delay less, consistent, and reliable way to maintain the tradeoff among cost and security. Furthermore, the computed public keys send requests to the centralized Certificate Authority (CA) to get a public key certificate for verification/authentication when patient data are transmitted using public wireless networks. Algorithm 1 is used to generate the keys for deployed biosensor nodes as well as for MS.

6.2. Schnorr Signcryption Phase. A combination of a public key encryption technique and a digital signature scheme makes up the Schnorr signcryption algorithm. In this phase, we have securely disseminated the patients' sensitive data using a secret session key to protect them from adversaries' attacks. Furthermore, for significant messages with dissimilar group participants, the originator (management center) generates the multicast secret session key. To ensure that multicast cluster participants with unique IDs reliably $\{ID_1, ID_2, ID_3, \ldots ID_t\}$ may communicate, the computed session key will be updated after each round to enhance the patient data security along with ensuring forward and backward privacy. Algorithm 2 is used for secure patient information dissemination among biosensor nodes, BS and MS.

6.3. Schnorr Unsigncryption Phase. In this section, MS unsigncrypts the patient signcrypted medical information from received tuples (C, R, S, C_t) using the following algorithm (3). Thus, it computes the one-way message digest

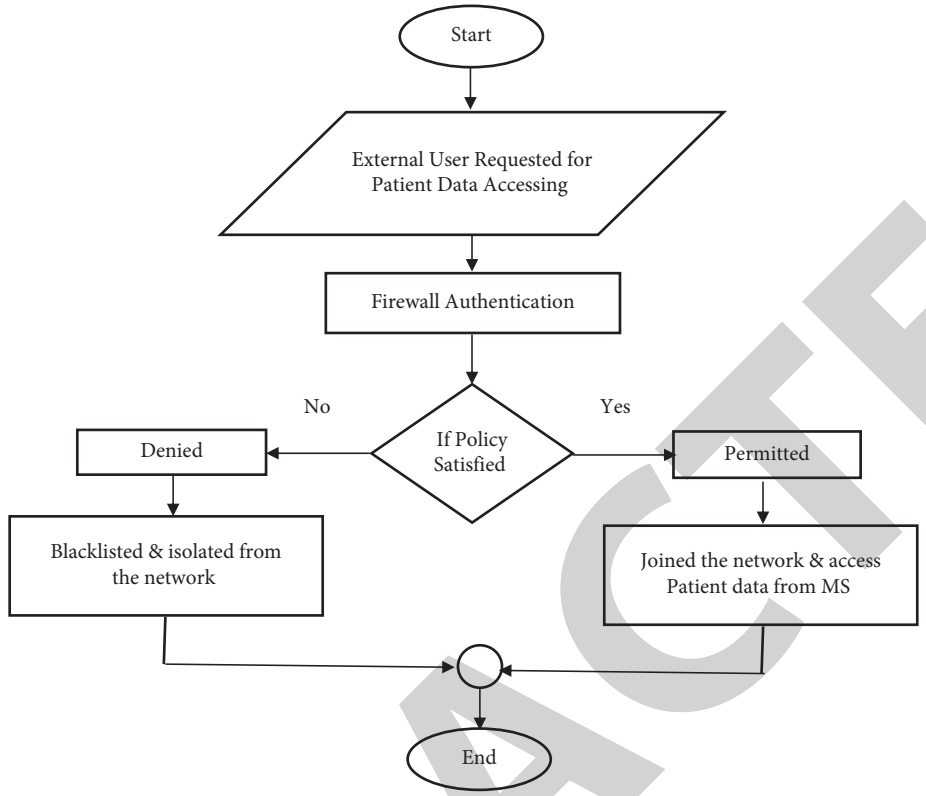

Figure 6: The flowchart of firewall-based network communication.

Table 1: Notations.

Notation	Description
P	Large prime number
Q	Prime number ($P = QR + 1$) R is any number
D	HECC divisor
N	Large prime number of order $n > 2^{80}$
G	Using Schnorr, the set of primitives {g1, g2, ..., gn} generated
a	A small primitive that is randomly created and made publically available
x	For each signcryption process, a private primitive from G is chosen
h/KH	Hash function that only goes one way
$E_k(\cdot)\|D_k(\cdot)$	Key k is used in a symmetric encryption/decryption technique
m/c	Patient data/cipher text
ID	Identification number of biosensor
B_Y	Public key of biosensor node
A_X	Private key of biosensor node
A_{X_i}	Private key of medical server
B_{Y_i}	Public key of medical server
320” > CA	320” > certificate authority
MS	Medical sever
Nonce	Number used once
$\mathscr{M}_{s_k}$	Master secret key
$\perp$	Reject
$\mathscr{WP}_{av}$	Weighted sum of the positive distance
$\mathscr{WN}_{av}$	Weighted sum of the negative distance
$\mathscr{N}_{av}$	Negative distance from average
$\mathscr{P}_{av}$	Positive distance from average
M	Appraisal score
ND	Negative distance
PD	Positive distance

(1) Deployed biosensor nodes on each registered patient admitted to a hospital ward
(2) Biosensor nodes can compute key pairs (A_X, B_Y)

(i) A_X = biosensor node selects private key randomly from $N \in_R \{0, 1, \ldots, n-1\}$
(ii) B_Y = biosensor node public key = A_X . DAlgorithm 1: Biosensor nodes/medical server keys generation phase.

(3) Medical server can compute key pairs (A_{X_i}, B_{Y_i})

(i) A_{X_i} = medical server private key chooses randomly from $N \in_R \{0, 1, \ldots, n-1\}$
(ii) B_{Y_i} = medical server public key = A_{X_i} . D

(4) After computing, the key pairs on both sides both source and destination nodes can get digital certificate of their public keys
(5) Then, the public keys are exchanged along with certificate to each other

(1) Biosensor nodes authenticate medical server public key B_{Y_i} by using their certificates
(2) Choose randomly secret session key x from group G Using Schnorr the set of primitives $\{g_1, g_2, \ldots\ldots, g_n\}$ generated
(3) The value x use for key generation and as a secrete session key
(4) Calculate $K = Hash(B_{Yi}^{x} \bmod P)$
(5) Fragmented K into K_A and K_B
(6) Computes $R = KH_{K_B}(x \| K_B)$
(7) Computes $C_t = E_x(patient\ me\ di\ cal\ in\ f\ ormation || nonce || timestemp)$
(8) Computes $C = C = E_{K_A}(x)$
(9) Computes $S = S = (x - A_X) \bmod P\ \Psi = (C, R, S, C_t)$
(10) Disseminated signcryption text Ψ to medical server
(11) Verification in Firewall if (set rules = = true)
(12) Permitted and biosensor send patient data to medical server
(13) Else
(14) Discard the biosensor data and cannot store in medical server
(15) End

Algorithm 2: Schnorr signcryption (patient data, nonce, timestamp, A_X, B_{Y_i}).

(1) Medical servers can verify the public key of biosensor node B_Y from their certificates
(2) Received tuple (C, R, S, C_t)
(3) Calculate $K = Hash((a^S * B_Y)^{A_{X_i}} \bmod P)$
(4) Split K $into\ k_A\ an\ d\ k_B$ of appropriate length
(5) Calculate x using decryption algorithm $x = D_{K_A}(C)$
(6) Calculate $\Upsilon = H_k(x \| k_B)$
(7) Accept x as valid only if $\Upsilon = R$ then
(8) Calculate ((patient medical information‖nonce‖timestemp) = $D_x(C_t)$
(9) Else
(10) Reject the signcrypted message
(11) Verification in Firewall if (set rules = = true)
(12) Permitted and external user can access patient data from medical server
(13) Else
(14) Deny the request and blacklisted/isolated from the network
(15) End

Algorithm 3: Schnorr unsigncryption (B_Y, A_{X_i}, Ψ).

such as: $K = Hash((a^S * B_Y)^{A_{X_i}} \bmod P)$, then splits the K $into\ k_A\ an\ d\ k_B$ of appropriate length to unsigncrypt the patient signcrypted medical information such as: decryption algorithm $x = D_{K_A}(C)$. Now, it computes $\Upsilon = H_k(x \| k_B)$ and accepts x as valid only if $\Upsilon = R$ then calculates ((patient medical information ‖nonce‖timestemp) = D_x (C_t), otherwise rejects the signcrypted message. Besides, if the firewall rules and policies are matched, then these users are permitted to access the patient's record stored in the MS. Otherwise, the requests of these external users are blocked and isolated from the network to protect adversaries' attacks.

(1) Biosensor nodes can compute key pairs (A'_X, B'_Y)

(i) A'_X = Biosensor node selects private key randomly from $N \in_R \{0, 1, \ldots, n-1\}$
(ii) B'_Y = Biosensor node public key = (A'_X, D)
(iii) Computes $S_{kbio} = [A'_X \oplus (\mathbb{N}once \| \mathscr{M}_{s_k})]$Algorithm 4: Secret session key update phase.

(2) Medical server can compute key pairs (A'_{X_i}, B'_{Y_i})

(i) A'_{X_i} = Medical server private key chooses randomly from $N \in_R \{0, 1, \ldots, n-1\}$
(ii) B'_{Y_i} = Medical server public key = (A'_{X_i}, D)
(iii) Computes $S_{kms} = [A'_{X_i} \oplus (\mathbb{N}once \| \mathscr{M}_{s_k})]$

(3) Send request to CA for digital certificate of their public keys
(4) Now exchanges the public keys along with certificate to each other
(5) Secure communication will be started using session key

6.4. Secret Session Key Updating Phase. The value of x and nonce will be updated for every signcryption process due to which we can achieve the security properties of backward and forward secrecy. If attackers steal the secret value of x, then they can neither calculate the patient information of previous sessions, nor the upcoming session information. Algorithm 4 is used for session key updating.

7. Performance Analysis

In this section, we have evaluated the performance analysis of the proposed architecture in terms of computational cost, communication overhead, energy consumption, and storage cost, and then compared it with the state-of-the-art schemes. Moreover, we have applied fuzzy Evaluation Based on Distance from Average Solution (EDAS) to analyze the efficiency and ranking among the proposed architecture and other states of the art schemes.

7.1. Computational Cost. The computational cost of the suggested approach has been determined in this section based on the experimentation performed in Ref. [39] on a MICA2 sensor with a low-power ATmega128-bit microcontroller running at 7.3728 MHz, 256 KB nonvolatile memory (ROM), and 8 KB volatile memory (RAM). One major process, ECPM, takes 0.81 seconds with 160 bits [40], while M-EXP with 1024 bits takes 22 seconds [9]. The execution time for session key encryption and decryption [41] is 4.543859 seconds. Based on the results of Refs. [41–44], the calculation cost of the proposed method is compared with that of the existing state-of-the-art schemes [41–44]. The 3rd generation MICA2 requires 2.66s for pairing computation, according to the technique [42]. Because a session key is employed for encryption and decryption, and our strategy is more suitable for the resource-constrained environment of WBANs, the processing time of this study is low compared to other previous methods [41–44]. This scheme contains three modular multiplications, six hash, two encryption, and two decryption operations. Besides, it contains one modular multiplications operation on the biosensor side and the other two on the MS side. Figure 7 shows the computational cost comparison of the proposed scheme with other state-of-the-art schemes [41–44]. Moreover, Figure 7 shows that the computational cost of the presented scheme is less as compared to other schemes.

7.2. Communication Overhead. In the proposed scheme, only critical data have been forwarded instead of normal data. This way, our scheme reduces the communication cost as compared to other state-of-the art schemes, as shown in Figure 8. Furthermore, the cost of data transmission is high as compared to data processing in wireless communication.

7.3. Energy Consumption. According to the usual ward size, the proposed scheme's communication distance is less than 100 meters. We utilized the free space model because the distance $d < \mathbf{d}_0$ is large, thus we used: $\varepsilon = \varepsilon_{fs} = 10pJ/bit/m^2$ where ε_{fs} is the free space model's amplifier energy factor. The provided technique outperforms the existing schemes in terms of energy compression [41–44]. One ECPM operation consumes 19.1 mJ of energy, while one pairing computation consumes 62.73 mJ. The next figure, Figure 9, compares the proposed scheme's energy consumption to that of alternative systems [41–44].

In Figure 9, a graph is presented that shows that our scheme consumed less energy and is suitable for the resource-constrained environment of WBSN.

7.4. Storage Cost. In this paper, a novel, efficient, and secure health care–enabled software-defined WBANs architecture has been proposed that uses Schnorr signcryption with HECC for the secure transmission of patient information from biosensor nodes to BS, and further towards the MS for diagnosis and treatment. Due to HECC's shorter key size, storage costs have evidently been reduced as compared to other state-of-the-art schemes. Furthermore, Table 2 shows the key sizes recommended by NIST for various cryptosystems, and Figure 10 visualizes the storage cost comparison regarding the number of nodes.

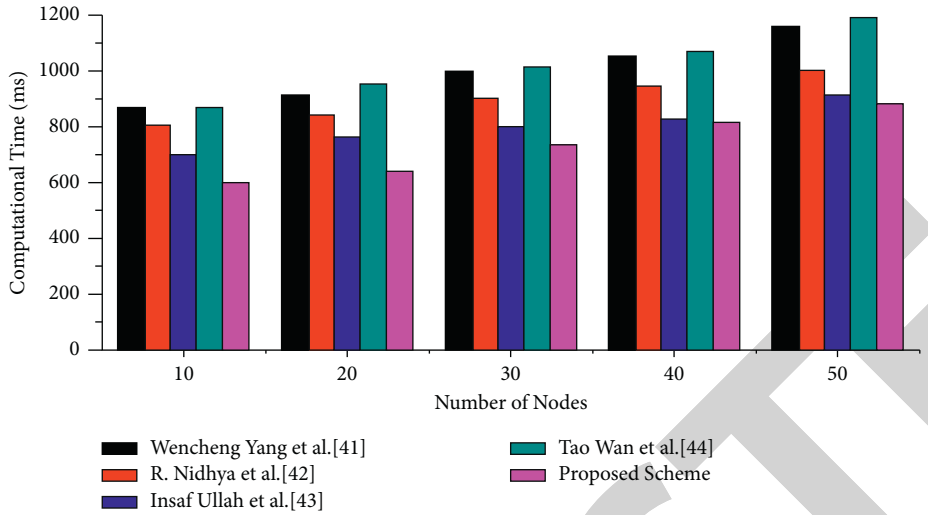

Figure 7: Computational cost comparison.

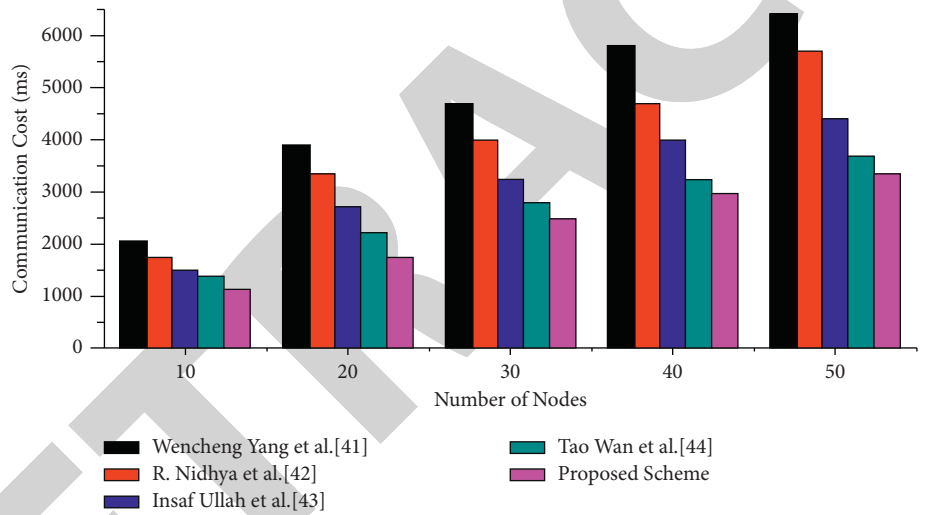

Figure 8: Communication cost comparison.

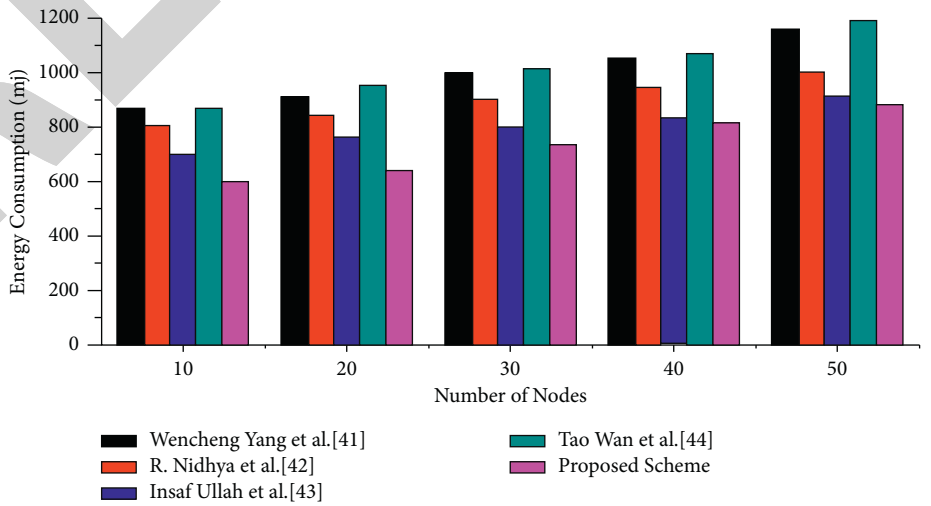

Figure 9: Energy consumption comparison.

Table 2: NIST recommended key size.

Secret key cryptosystem	RSA and Diffie–Hellman	ECC	HECC
80	1024	160	80
112	2048	224	112
128	3072	256	128
192	7680	384	192
256	15360	512	256

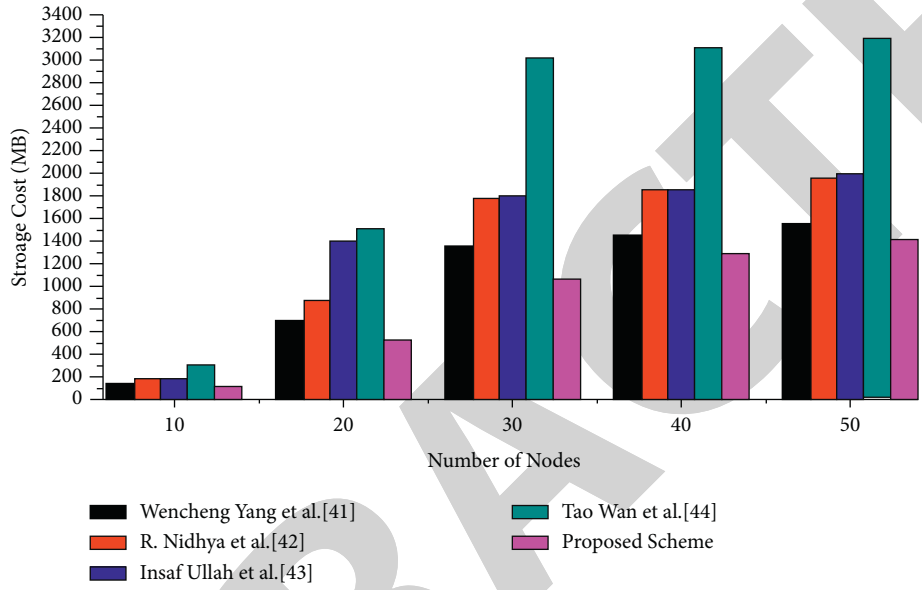

Figure 10: Storage cost comparison.

Table 3: Selected parameters for EDAS.

Criteria⟶	Beneficiary	Nonbeneficiary			
Probability⟶	0.2	0.2	0.2	0.2	0.2
Selected parameters⟶	Security	Communication cost	Computation cost	Storage cost	Energy consumption
Yang and Wang [17]	1	866	38	298.9	1370
Nidhya et al. [21]	0	701	36	177.96	1572
Ullah et al. [38]	0	802	52	176.33	1754
Wan et al. [12]	0	869	47	136.44	2058
Proposed scheme	1	603	59	107.2	1124

8. Fuzzy Evaluation Based on Distance from Average Solution (EDAS) Method

Ghorabaee et al. [43] present the EDAS method, which ranks supplied schemes based on the average solution. The average answer is obtained by calculating the Positive Distance from Average and the Negative Distance from Average. The scheme with the highest values is the best-ranked scheme [44]. The fuzzy-EDAS approach orders alternatives based on the decreasing value of the defuzzified evaluation score [45]. Table 3 displays the chosen criteria that ranks the schemes based on the assessment score. The steps involved in the fuzzy-EDAS technique are outlined in the following discussion.

We outline the following steps to address the decision-making problem that utilizes fuzzy-EDAS methodology. S-1.

The weights of the proposed scheme and previous related schemes are calculated in Table 3 for each of the selected matrices by using the equations in following steps, S-2:

The equations used and the values of Table 3 are utilized to produce a fuzzy averaged decision matrix concerning all of the considered matrices, as presented in Table 4.

$$(\phi) = [\vartheta_b]_{1\times\beta}, \tag{9}$$

while

$$= \frac{\sum_{i=1}^{y} X_{ab}}{y}. \tag{10}$$

S-3: The ideal solution should be maximum in distance from the positive potential solutions and should be minimum in distance from the negative potential solution. The

Table 4: Average of the selected parameters.

Criteria⟶	Beneficiary	Nonbeneficiary			
Probability⟶	0.2	0.2	0.2	0.2	0.2
Selected parameters⟶	Security	Communication cost	Computation cost	Storage cost	Energy consumption
Yang and Wang [17]	1	866	38	298.9	1370
Nidhya et al. [21]	0	701	36	177.96	1572
Ullah et al. [38]	0	802	52	176.33	1754
Wan et al. [12]	0	869	47	136.44	2058
Proposed scheme	1	603	59	107.2	1124
Average	0.4	768.2	46.4	179.366	1575.6

Table 5: Positive distance from average.

Criteria⟶	Beneficiary	Nonbeneficiary			
Probability⟶	0.2	0.2	0.2	0.2	0.2
Selected parameters⟶	Security	Communication Cost	Computation cost	Storage cost	Energy consumption
Yang and Wang [17]	1.5	0	0.181034483	0	0.130489972
Nidhya et al. [21]	0	0.087477219	0.224137931	0.007838721	0.002284844
Ullah et al. [38]	0	0	0	0.016926285	0
Wan et al. [12]	0	0	0	0.239320719	0
Proposed scheme	1.5	0.215048165	0	0.402339351	0.28662097

Table 6: Negative distance from average.

Criteria⟶	Beneficiary	Nonbeneficiary			
Probability⟶	0.2	0.2	0.2	0.2	0.2
Selected parameters⟶	Security	Communication Cost	Computation cost	Storage cost	Energy consumption
Yang and Wang [17]	0	0.127310596	0	0.666425075	0
Nidhya et al. [21]	1	0	0	0	0
Ullah et al. [38]	1	0.043998959	0.120689655	0	0.113226707
Wan et al. [12]	1	0.131215829	0.012931034	0	0.306169078
Proposed scheme	0	0	0.271551724	0	0

following equations are given to compute the matrices for fuzzy Positive Distance from Average (PDA) and fuzzy Negative Distance from Average (NDA) in this step of the fuzzy-EDAS method as existing in Tables 5 and 6.

$$\mathscr{P}_{av} = \left[\left(\mathscr{P}_{av}\right)_{ab}\right]_{\beta\times\beta}. \tag{11}$$

If the state b^{th} is favorable, then

$$\left(\mathscr{P}_{av}\right)_{ab} = \frac{\max\left(0, \left(Ave_b - X_{ab}\right)\right)}{Ave_b}. \tag{12}$$

And for less favorable, it becomes

$$\left(\mathscr{P}_{av}\right)_{ab} = \frac{\max\left(0, \left(X_{ab} - Ave_b\right)\right)}{Ave_b},$$
$$\left(\mathscr{N}_{av}\right) = \left[\left(\mathscr{N}_{av}\right)_{ab}\right]_{\beta\times\beta}. \tag{13}$$

If the b^{th} criterion is more favorable than

$$\left(\mathscr{N}_{av}\right)_{ab} = \frac{\max\left(0, \left(Ave_b - X_{ab}\right)\right)}{Ave_b}, \tag{14}$$

and less desirable, then the given above equations become

$$\left(\mathscr{N}_{av}\right)_{ab} = \frac{\max\left(0, \left(X_{ab} - Ave_b\right)\right)}{Ave_b}. \tag{15}$$

In this step, the matrices of fuzzy weighted negative and fuzzy weighted positive distances are produced as exposed in Tables 7 and 8. For performing this, the equations given below are applied.

$$\mathscr{WP}_{av} = \sum_{b=1}^{y} \lambda_b \left(P\ D\right)_{ab},$$
$$\mathscr{WN}_{av} = \sum_{b=1}^{y} \lambda_b \left(N\ D\right)_{ab}. \tag{16}$$

S-5: By using the following equations, the score of fuzzy appraisal for several alternatives is calculated. After that, in this step, the alternative schemes are sorted based on decreasing the score value of defuzzified appraisal. As shown in Table 9, the best scheme among the selected schemes represents the alternative scheme with the highest value of assessment score.

Table 7: Weighted sum of PDA.

Criteria⟶	Beneficiary	Nonbeneficiary				
Probability⟶	0.2	0.2	0.2	0.2	0.2	$\mathscr{WP}_{av}$
Selected parameters⟶	Security	Communication cost	Computation cost	Storage cost	Energy consumption	
Yang and Wang [17]	0.3	0	0.036206897	0	0.026097994	0.36230489
Nidhya et al. [21]	0	0.017495444	0.044827586	0.001567744	0.000456969	0.06434774
Ullah et al. [38]	0	0	0	0.003385257	0	0.00338526
Wan et al. [12]	0	0	0	0.047864144	0	0.04786414
Proposed scheme	0.3	0.043009633	0	0.08046787	0.057324194	0.4808017

Table 8: Weighted sum of NDA.

Criteria⟶	Beneficiary	Nonbeneficiary				
Probability⟶	0.2	0.2	0.2	0.2	0.2	$\mathscr{WN}_{av}$
Selected parameters⟶	Security	Communication cost	Computation cost	Storage cost	Energy consumption	
Yang et al. [17]	0	0.025462119	0	0.133285015	0	0.15874713
R. Nidhya et al. [21]	0.2	0	0	0	0	0.2
Ullah et al. [38]	0.2	0.008799792	0.024137931	0	0.022645341	0.25558306
Wan et al. [12]	0.2	0.026243166	0.002586207	0	0.061233816	0.29006319
Proposed scheme	0	0	0.054310345	0	0	0.05431034

Table 9: Ranking based on the selected parameters.

Ref. No.	$\mathscr{WP}_{av}$	$\mathscr{WN}_{av}$	$\mathscr{N}(\mathscr{WP}_{av})$	$\mathscr{N}(\mathscr{WN}_{av})$	$\mathfrak{M}$	Rank
Yang and Wang [17]	0.362304891	0.158747134	0.753543287	0.452715337	0.603129312	2
Nidhya et al. [21]	0.064347743	0.2	0.133834268	0.310495064	0.222164666	3
Ullah et al. [38]	0.003385257	0.255583064	0.007040859	0.118871078	0.062955968	4
Wan et al. [12]	0.047864144	0.290063188	0.099550696	-1.47568E-09	0.049775347	5
Proposed scheme	0.480801697	0.054310345	1	0.812763746	0.906381873	1

Table 10: Comparative security analysis.

Security properties	Yang et al. [17]	Nidhya et al. [21]	Ullah et al. [38]	Wan et al. [12]	Proposed scheme
Confidentiality	✓	✓	✓	×	✓
Integrity	✓	×	✓	✓	✓
Nonrepudiation	✓	×	✓	✓	✓
Authentication	✓	×	✓	×	✓
Authorization	×	✓	×	✓	✓
Availability	✓	✓	×	×	✓
Scalability	✓	×	×	✓	✓
Backward secrecy	×	×	×	✓	✓
Forward secrecy	×	✓	×	✓	✓
Unforgeability	✓	✓	×	✓	✓
Transparency	✓	×	✓	×	✓
Verifiability	✓	×	✓	×	✓
Freshness	✓	×	×	✓	✓

$$\mathscr{N}\left(\mathscr{WP}_{av}\right) = \frac{\mathscr{WP}_{av}}{\max_a\left(\mathscr{WP}_{av}\right)},$$

$$N\left(\mathscr{WN}_{av}\right) = 1 - \frac{\mathscr{WN}_{av}}{\max_a\left(\mathscr{WN}_{av}\right)}, \tag{17}$$

$$\mathfrak{M} = \frac{1}{2}\left(\mathscr{NWSPD}_{avg} - \mathscr{NWN}_{av}\right).$$

where $0 \le \mathfrak{M} \ge 1$.

The abovementioned methodology is applied in this section to solve a case study on various efficient scheme selections, such as Yang and Wang [17], R. Nidhya et al. [21], Ullah et al. [38], and Tao Wan et al. [12]. Equations (1) and (2) were then used to generate the objective weights for all of the decision matrices gathered from the three decision-makers. Finally, the aggregate weights were determined by averaging the objective weights for each criterion. Table 3 displays individual objective weights as well as aggregated objective weights. Following that, the average decision

matrix was developed, and the results are displayed in Table 4. The average solution produced was then determined using equations (3)–(8), as shown in Table 5, which also contains the crisp value. Positive distance from average (PDA) and negative distance from average (NDA) values were calculated using equations (9) and (10) and are shown in Tables 7 and 8. In the penultimate stage, equations (9) and (10) are employed to calculate the fuzzy appraisal score for numerous alternatives. Finally, based on the defuzzified evaluation score, equation (10) was utilized to rank the alternatives. Table 9 depicts all of these numbers, and Table 10 depicts the comparative security analysis. Our design plan was discovered to be the finest alternative solution for an electronic voting system.

9. Conclusion

An innovative and efficient SD-WBANs architecture has been presented in this study to deal with the challenges of security and cost consumption, allowing the healthcare system to preserve the tradeoff between security and cost for efficient disease diagnosis. In addition, a lightweight Schnorr signcryption using HECC has been proposed to protect sensitive medical data while being transmitted over public networks. In comparison to the existing state-of-the-art schemes, this cryptosystem has improved efficiency in terms of security, computing, communication, energy usage, and storage cost.

Consequently, the concept of SDN has been integrated with WBANs to efficiently manage the data traffic flow in the resource-constrained environment of WBANs by using data plans and control plans separately in a desirable way. External users can securely obtain the patient's real-time medical information from MS after mutual authentication, and by using hardware firewalls, we can efficiently monitor the incoming and outgoing data traffic in a reliable and secure way. In addition, the success of the proposed scheme is demonstrated using a well-known MCDM approach known as EDAS. An analysis of the performance reveals that the proposed scheme outperforms as compared with other state-of-the-art schemes in terms of computation cost, communication overhead, storage cost, and energy consumption.

In the future, we can develop a smart communication protocol for WBANs to improve the Quality of Service (QoS) by employing various queuing algorithms such as priority queues and weighted fair queues. Likewise, researchers can combine quantum cryptosystems and attribute-based fog-/edge-assisted signcryption with 5G communication technology to improve security and privacy with minimal cost.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest associated with the publishing of this paper.

Acknowledgments

This research was supported by the Researchers Supporting Project number (RSP-2021/244), King Saud University, Riyadh, Saudi Arabia.

References

[1] H. R. Nagesh, M. P. Rajasekaran, and H. M. Ramalingam, "WBAN implementation in a parallel processing environment for E-healthcare applications," *International Journal of Future Generation Communication and Networking*, vol. 13, no. 4, pp. 4963–4969, 2020.

[2] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: a comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2014.

[3] T. Luo, H. P. Tan, and T. Q. Quek, "Sensor OpenFlow: enabling software-defined wireless sensor networks," *IEEE Communications Letters*, vol. 16, no. 11, pp. 1896–1899, 2012.

[4] J. Zhou, H. Jiang, J. Wu, L. Wu, C. Zhu, and W. Li, "SDN-based application framework for wireless sensor and actor networks," *IEEE Access*, vol. 4, pp. 1583–1594, 2016.

[5] F. Olivier, G. Carlos, and N. Florent, "SDN based architecture for clustered WSN," in *Proceedings of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 342–347, IEEE, Santa Catarina, Brazil, July 2015.

[6] M. Ba, O. Flauzac, B. S. Haggar, F. Nolot, and I. Niang, "Self-stabilizing k-hops clustering algorithm for wireless ad hoc networks," in *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication*, pp. 1–10, NewYork, NY, USA, January 2013.

[7] A. Dunkels, "Full TCP/IP for 8-bit architectures," in *Proceedings of the 1st international conference on Mobile systems, applications and services*, pp. 85–98, ACM, Stanford, California, May 2003.

[8] M. A. Shayokh, J. W. Kim, and S. Y. Shin, "Cloud based software defined wireless body area networks architecture for virtual hospital," in *Proceedings of the 10th EAI International Conference on Body Area Networks*, pp. 92–95, NewYork, NY, USA, September 2015.

[9] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, "Privacy and security concerns in IoT-based healthcare systems," *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*, pp. 105–134, 2021.

[10] S. Chaudhary, A. Singh, and K. Chatterjee, "Wireless body sensor network (WBSN) security and privacy issues: a survey," *International Journal of Computational Intelligence & IoT*, vol. 2, no. 2, 2019.

[11] M. Azees, P. Vijayakumar, M. Karuppiah, and A. Nayyar, "An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks," *Wireless Networks*, vol. 27, no. 3, pp. 2119–2130, 2021.

[12] T. Wan, L. Wang, W. Liao, and S. Yue, "A lightweight continuous authentication scheme for medical wireless body area networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 6, pp. 3473–3487, 2021.

[13] A. M. Almuhaideb, "Re-AuTh: lightweight Re-authentication with practical key management for wireless body area

networks," *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8189–8202, 2021.

[14] C. Chunka and S. Banerjee, "An efficient mutual authentication and symmetric key agreement scheme for wireless body area network," *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8457–8473, 2021.

[15] S. U. Jan, S. Ali, I. A. Abbasi, M. A. Mosleh, A. Alsanad, and H. Khattak, "Secure patient authentication framework in the healthcare system using wireless medical sensor networks," *Journal of Healthcare Engineering*, vol. 2021, p. 9954089, 2021.

[16] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," *Wireless Personal Communications*, vol. 117, no. 1, pp. 47–69, 2021.

[17] W. Yang and S. Wang, "A privacy-preserving ECG-based authentication system for securing wireless body sensor networks," *IEEE Internet of Things Journal*, p. 1, 2021.

[18] A. Singh, R. R. K. Chaudhary, and K. Chatterjee, "A novel privacy preservation mechanism for wireless medical sensor networks," *Advances in Electronics, Communication and Computing*, vol. 709, pp. 173–182, 2021.

[19] S. M. Karunarathne, N. Saxena, and M. K. Khan, "Security and privacy in IoT smart healthcare," *IEEE Internet Computing*, vol. 25, no. 4, pp. 37–48, 2021.

[20] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: architecture, security challenges and research opportunities," *Computers & Security*, vol. 104, p. 102211, 2021.

[21] R. Nidhya, S. Shanthi, and M. Kumar, "A novel encryption design for wireless body area network in remote healthcare system using enhanced RSA algorithm," *Intelligent System Design*, vol. 1171, pp. 255–263, 2021.

[22] J. Iqbal, A. Waheed, M. Zareei et al., "A lightweight and secure attribute-based multi receiver generalized signcryption scheme for body sensor networks," *IEEE Access*, vol. 8, pp. 200283–200304, 2020.

[23] S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain, and M. Humayun, "Performance enhancement in wireless body area networks with secure communication," *Wireless Personal Communications*, vol. 116, no. 1, pp. 1–22, 2021.

[24] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 21165–21202, 2021.

[25] J. Iqbal, A. I. Umar, N. Amin, and A. Waheed, "Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, p. 1550147719875654, 2019.

[26] S. U. Jan, "Secure patient authentication framework in the healthcare system using wireless medical sensor networks," *Journal of Healthcare Engineering*, vol. 2021, 2021.

[27] M. Soni and D. K. Singh, "LAKA: lightweight Authentication and key agreement protocol for internet of things based wireless body area network," *Wireless Personal Communications*, pp. 1–18, 2021.

[28] B. Narwal and A. K. Mohapatra, "SAMAKA: secure and anonymous mutual authentication and key agreement scheme for wireless body area networks," *Arabian Journal for Science and Engineering*, pp. 1–23, 2021.

[29] A. Sivasangari, A. Ananthi, D. Deepa, G. Rajesh, and X. M. Raajini, "Security and privacy in wireless body sensor networks using lightweight cryptography scheme," *Security and Privacy Issues in IoT Devices and Sensor Networks*, vol. 3, pp. 43–59, 2021.

[30] Z. J. Han and W. Ren, "A novel wireless sensor networks structure based on the SDN," *International Journal of Distributed Sensor Networks*, vol. 10, no. 3, p. 874047, 2014.

[31] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: challenges and design requirements," *IEEE access*, vol. 5, pp. 1872–1899, 2017.

[32] A. Mahmud and R. Rahmani, "Exploitation of OpenFlow in wireless sensor networks," in *Proceedings of the 2011 International Conference on Computer Science and Network Technology*, pp. 594–600, IEEE, Harbin, China, December 2011.

[33] C. B. Margi, R. C. Alves, G. A. N. Segura, and D. A. Oliveira, "Software-defined wireless sensor networks approach: southbound protocol and its performance evaluation," *Open Journal of Internet Of Things (OJIOT)*, vol. 4, no. 1, pp. 99–108, 2018.

[34] R. C. Alves, D. A. Oliveira, G. C. Pereira, B. C. Albertini, and C. B. Margi, "WS3N: wireless secure SDN-based communication for sensor networks," *Security and Communication Networks*, vol. 2018, p. 8734389, 2018.

[35] R. Friedman and D. Sainz, "An architecture for sdn based sensor networks," in *Proceedings of the 18th International Conference on Distributed Computing and Networking*, pp. 1–10, NewYark, USA, January 2017.

[36] M. Al Shayokh, A. Abeshu, G. B. Satrya, and M. A. Nugroho, "Efficient and secure data delivery in software defined WBAN for virtual hospital," in *Proceedings of the 2016 international conference on control, electronics, renewable energy and communications (ICCEREC)*, pp. 12–16, IEEE, Bandung, Indonesia, September 2016.

[37] V. Moorthy, R. Venkataraman, and T. R. Rao, "Security and privacy attacks during data communication in software defined mobile clouds," *Computer Communications*, vol. 153, pp. 515–526, 2020.

[38] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, and S. Kumari, "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*, vol. 45, no. 1, pp. 1–14, 2021.

[39] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," *Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science)*, vol. 3156, pp. 119–132, 2004.

[40] F. Li and X. Pan, "Practical secure communication for integrating wireless sensor networks into the internet of things," *Sensors Journal*, IEEE, vol. 13, no. 10, , pp. 3677–3684, 2013.

[41] S. Singh, S. K. Maakar, and S. Kumar, "A performance analysis of DES and RSA cryptography," *Int. J. Emerg. Trends Technol. Comput. Sci.*vol. 2, no. 3, pp. 418–423, 2013.

[42] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, "On the application of pairing based cryptography to wireless sensor networks," in *Proceedings of the 2nd ACM Conf. Wireless Netw. Security*, pp. 1–12, ACM, Zurich, Switzerland, March 2012.

[43] M. Keshavarz Ghorabaee, E. K. Zavadskas, L. Olfat, and Z. Turskis, "Multi-criteria inventory classification using a new method of evaluation based on distance from average solution (EDAS)," *Informatica*, vol. 26, no. 3, pp. 435–451, 2015.

[44] M. K. Ghorabaee, E. K. Zavadskas, M. Amiri, and Z. Turskis, "Extended EDAS method for fuzzy multi-criteria decision-

making: an application to supplier selection," *International Journal of Computers Communications & Control*, vol. 11, no. 3, pp. 358–371, 2016.

[45] D. Zindani, S. R. Maity, and S. Bhowmik, "Fuzzy-EDAS (evaluation based on distance from average solution) for material selection problems," *Advances in Computational Methods in Manufacturing*, pp. 755–771, 2019.