infrastructures

MDPI

Article

A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0

Rajesh Natarajan [1], Gururaj Harinahallo Lokesh [2,*], Francesco Flammini [3,*], Anitha Premkumar [4], Vinoth Kumar Venkatesan [5] and Shashi Kant Gupta [6]

[1] Information Technology Department, University of Technology and Applied Sciences-Shinas, Al-Aqr, Shinas 324, Oman
[2] Department of Information Technology, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal 576104, India
[3] IDSIA USI-SUPSI, University of Applied Sciences and Arts of Southern Switzerland, 6928 Manno, Switzerland
[4] Department of Computer Science and Engineering, Presidency University, Bangalore 560064, India
[5] School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, India
[6] CSE Department, Integral University, Lucknow 226026, India
* Correspondence: gururaj.hl@manipal.edu (G.H.L.); francesco.flammini@supsi.ch (F.F.)

Abstract: Background: The Internet of Medical Things, often known as IoMT, is a revolutionary method of connecting medical equipment and the software that operates on it to the computer networks that are used in healthcare 5.0. The rapid development of smart medical devices on IoMT platforms has led to the adoption of major technologies in the modernization of healthcare procedures, the administration of diseases, and the improvement in patient treatment standards. The IoMT offers a variety of cloud-based applications, including data exchange, data screening, patient surveillance, information collection and analysis, and hygienic hospital attention. Wireless sensor networks (WSNs) are responsible for both the gathering and delivery of data. Method: The safety of patients and their right to privacy are the top priorities in the healthcare sector. Anyone may see and modify the patient's health information because the data from these smart gadgets are sent wirelessly through the airways. Hence, we developed a unique elliptic curve cryptography-based energy-efficient routing protocol (ECC-EERP) to provide a high level of security and energy efficient system for healthcare 5.0. Data can be encrypted using the key-based method ECC-EERP. It employs pairs of public and private keys to decrypt and encrypts web traffic and reducse the amount of energy needed by a WSN in aggregate. Result and Discussion: The efficiency of the suggested method was evaluated in comparison with that of a variety of existing methods. The suggested method was evaluated with the use of many parameters such as security, encryption throughput, energy efficiency, network lifetime, communication overload, computation time, and implementation cost. The results showed that the proposed technique provides enhanced security and energy efficiency.

Keywords: Internet of Medical Things; energy optimization; wireless sensor networks; privacy; security

Citation: Natarajan, R.; Lokesh, G.H.; Flammini, F.; Premkumar, A.; Venkatesan, V.K.; Gupta, S.K. A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. *Infrastructures* **2023**, *8*, 22. https://doi.org/10.3390/infrastructures8020022

Academic Editor: GM Shafiullah

Received: 1 January 2023
Revised: 20 January 2023
Accepted: 25 January 2023
Published: 2 February 2023

1. Introduction

Digital technology in modern healthcare is anticipated to dramatically revolutionize healthcare systems around the globe. Smart healthcare uses digital technology to link people, services, and institutions; quickly navigates health data; and immediately addresses medical environment requirements [1]. Patients, physicians, hospitals, and insurance providers are just a few of the groups that benefit from smart healthcare's ability to link the many players in medical systems. New and emerging technologies, including artificial intelligence (AI), the Internet of Things (IoT), fog computing, cloud services, blockchain, monitoring devices, 5G technology, and the IoMT, make this feasible. It is essential that these technologies support the healthcare 5.0 paradigm change. The IoT solutions for the medical industry are shown in Figure 1. The ability to transmit data through a network without

the need for computer-to-computer or human-to-human communication has helped in securing data transmission, managing duties, analyzing opportunities, and connecting gadgets [2,3].

Figure 1. Solutions for the IoT in the medical field.

The IoT will have a huge impact on healthcare 5.0. Medical organizations have made extensive use of IoT-to-network medical equipment to exchange patient records online. There are various new types of sensor-based IoT used in healthcare, each having its own characteristics. For instance, IoT has paved the way for the development of the IoHT, IoMT, IoNT, and IoMT (all acronyms for various Internet-based medical and cognitive wearable things) [4]. The Internet of Nano Things (IoNT) refers to the networking of nanoscale gadgets and communication systems for purposes including detecting, acting with, and transmitting electromagnetic waves. So, modern IoT variants offer interconnected healthcare, which allows for the seamless incorporation of modern medical instruments and the remote, all-encompassing exchange of health information. As an illustration, the idea of conventional healthcare is transformed into "smart healthcare" because advanced devices allow for a monitoring system in medical services [5,6]. As a result, healthcare providers will be able to remotely connect, analyze, and evaluate the health information sensed by biomaterials and interactive wearable technology using variants of the IoT to enhance the quality of the treatment they provide. The Internet of Health Things (IoHT), Internet of Nonmedical Things (IoNT), and Internet of Mobile-Health Things (IoMT) all offer widespread health services meant to aid in patient-specific therapies, compliance, assertive supervising, efficient prognosis, timely and accurate detection of diseases, constant care, and intelligent restoration [7,8]. Portable healthcare is developing as a result of the combination of advancing digital technology and devices, allowing for wireless connectivity and assistance of patients suffering from long-term disorders outside of healthcare institutions. As a result, biosensors hold great promise as tools for disease detection and management [9,10].

1.1. Historical Perspective on Healthcare's Technological Development from Version 1.0 to 5.0

The healthcare sector has seen a significant transformation of technology-driven strategies with a move from healthcare 1.0 to healthcare 5.0. In healthcare 1.0, patient notes were manually maintained and doctor-centric [11,12]. With digitalization, handwritten documentation was transferred to electronic form, commonly known as electronic health records (EHRs), in healthcare 2.0 [13,14]. Healthcare 3.0 witnessed the democratization of EHRs via smartphone apps, creating a patient-centric environment as consolidated storing was replaced. Due to the absence of major decision analysis, these files were vulnerable to assaults from hostile parties. When designing informed decisions based on collected EHRs, healthcare 4.0 combines AI with big data analytics [15,16]. Complications in communication and collaboration across different medical communities resulted from this convergence. As the volume of clinical information grew, so did the difficulty, inefficiency, and slowness of the AI models used to make sense of it. The healthcare 5.0 vision represents a comprehensive plan that unites ultra-responsive business practices centered on patients with lightweight Internet of Things (IoT) technologies, 5G/6G connectivity, and security-based technologies. The development of healthcare provision from healthcare 1.0 to 5.0 is shown in Figure 2. The major goal of healthcare 5.0 is to maintain the patient as the focal point of the healthcare ecosystem. Healthcare stakeholders, including patients, physicians, clinics, and warehouses, assist in medical delivery in order to do this [17]. The motivation of this study was responsiveness and end-to-end service coverage, working with healthcare 5.0, which emphasizes personalization and patient models. The main objectives of healthcare 5.0 are lifetime collaboration, patient well-being, and quality of life. As a result, if a smart healthcare device leaves the healthcare 5.0 system, it is not permitted to read any communications that may be transmitted in the future.

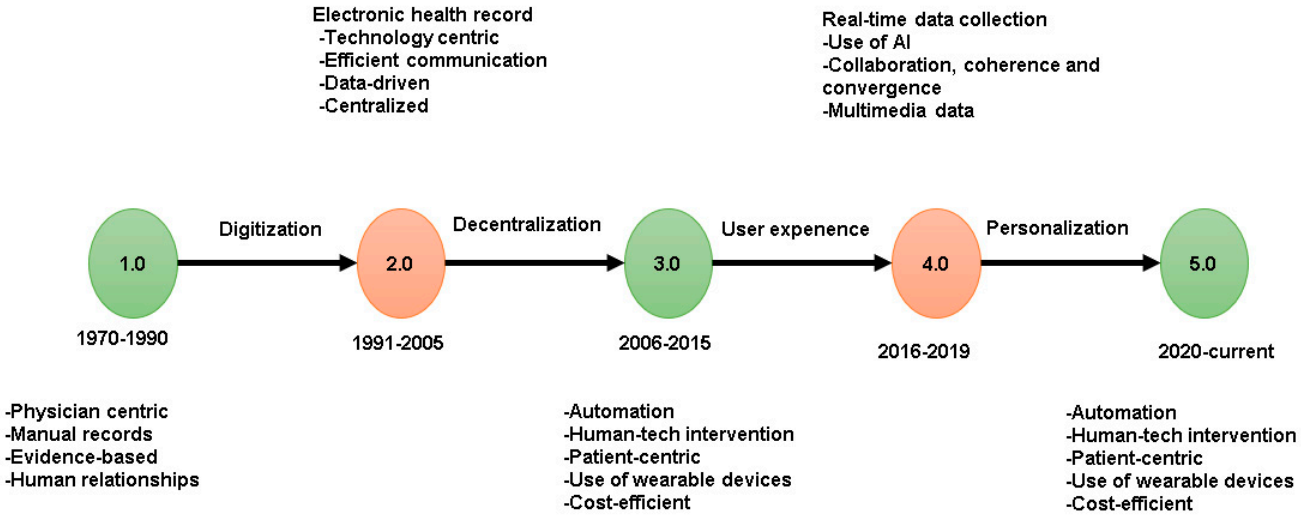

Figure 2. Historical perspective on healthcare 1.0 to 5.0.

1.2. Contributions of the Study

- Initially, the data were collected and stored in a network.
- Next, an elliptic curve cryptography-based energy-efficient routing protocol (ECC-EERP) was developed for the enhancement of security and energy in IoT healthcare 5.0.
- Finally, the performance of the system was analyzed.

The remainder of this paper is structured as follows: Section 2 presents the related studies and problem descriptions. The recommended method is illustrated in Section 3. Section 4 includes the findings and analyses. Section 5 highlights the conclusions.

2. Literature

To deliver more accurate evaluations of heart illness, researchers [18] developed an IoT platform that employs a modified self-adaptive Bayesian algorithm (MSABA). The patient's

wristwatch and heart rate monitor gadget captures and transmits data from the patient's pulse rate, such as their heartbeat and hypertension, to a server. In past decades, heart illness has overtaken many other causes of mortality. It is challenging to predict a person's probability of acquiring heart problems because this requires both specialist knowledge and real-world experience. An adaptive electrocardiogram (ECG) noise reduction method based on empirical mode decomposition was proposed [19]. The advantages of the suggested techniques were used to reduce the distortion-free noise in ECG readings. A common tool for assessing heart problems is ECG. A free-interference ECG is frequently desired for the accurate evaluation of heart diseases.

The ability of robots to discern mental expressions in facial movements should be developed and deployed for the human involvement, information animations, and interaction between individuals and robotics to be effective. As a consequence, in current history, significant efforts have been made to address the issue of facial expression recognition (FER) using convolutional neural networks (CNNs) [20]. The privacy and dependability of drone deliveries across multiple untrusted channels may be managed by the technique known as blockchain. We suggested GaRuDa, a smart contracts drone delivery system for healthcare 5.0 uses, as a result of the preceding circumstances. Yet, owing to restricted zones, rugged terrain, war zones, poor road situations, congestion, and distant areas, the leading healthcare network infrastructure and delivery procedures among different providers struggle [21].

Researchers [22] established the idea of context-aware attributed acquisition with cipher policy-attribute-based encryption (CP-ABE) to safeguard customer data security in an IoT-enabled society in healthcare 5.0. A paradigm change in healthcare 5.0 is anticipated in the medical field, which makes use of patient-centered digital well-being and pushes the operational limits of healthcare 4.0. Through the use of aided techniques, including machine learning, the IoT, big data, and supported communication routes, healthcare 5.0 concentrates on the live monitoring of patients, contextual regulation and wellbeing, and security adherence. Healthcare 5.0 may therefore be hampered by management efficiency in the medical industry, the state testing of estimation techniques, robustness, and an absence of societal and legal structures [23].

According to a study [24], a novel methodology for automating the diagnosis of skin cancer conducts segmentation and categorization of skin lesions. The suggested scheme comprises two phases: the first stage uses a fully convolutional encoder–decoder network (FCN) to acquire the complicated and nonuniform characteristics of skin lesions, with the converter phase learning the lesion's rough esthetic and the decoder phase learning the lesion's boundaries description. By distributing a worldwide learning method via distributed cumulative servers, federated learning (FL) addresses the issues mentioned above. Innovative and proactive universal healthcare represents one of the digital technologies features made possible by the IoMT. Due to the massive size and widespread deployment of IoMT systems, privacy and protection are top issues with the IoMT [25].

Researchers [26] proposed a randomized, proactive, DL-based approach that offers end-to-end protection from network threats in IoMT devices that automatically identifies and rejects harmful data. As more IoMT gadgets and apps are used, smart healthcare faces constantly growing system vulnerabilities. The IoMT is a popular method for developing sustainable urban solutions that support vital facilities over the long term, such as smart healthcare services [27]. Many sectors, which include production, power, banking, academia, travel, home automation, and medicine, employ IoT technology. By effectively managing people and portable resources in clinics, IoT applications can provide significant healthcare services within the field of medicine [28,29].

In a study [30–32], an IoT system for the healthcare industry employing Sigfox, a healthcare system for low-power internal tracking devices, was presented. To assess the efficiency of the medical equipment and patient safety procedures, a proof-of-concept (PoC) was used. Authors [33] examined how patients, digital clinics, and physicians interact using a metaverse tele surgical system. Given the potential advantages, the confidentiality of

patient data was determined and online characters were generated, which communicated with medical partners to provide linked online treatment. Blockchain (BC) is a viable way to provide clarity and data integrity of saved interactions on the metaverse because metaverse elements are distributed [34]. Due to some limitations in the existing literature, we developed an elliptic curve cryptography-based energy-efficient routing protocol (ECC-EERP) for better security and energy in healthcare 5.0.

Problem Statement

The main problem with IoT is security is that all linked devices communicate real-time data. If end-to-end communication is not secured, private information may be compromised. The private details of many people may be used by hackers for their gain. The management of such vast amounts of data in real time may lead to reliability problems. The IoT may decrease the cost of patient care and treatment, but the cost of setting up and maintaining all the equipment is very high. Hence, we developed an elliptic curve cryptography-based energy-efficient routing protocol (ECC-EERP) for the enhancement in security and energy in the healthcare sector. The advantages and drawbacks of the related methods are shown in Table 1.

Table 1. Summary of existing works.

S. No	Reference	Method	Advantage	Disadvantage
1	[35]	Real-time deep extreme learning system (RTS-DELM)	Effectively evaluates federated learning-based healthcare 5.0 network's dependability	Travel time, chance of patient catching an illness, and line-ups
2	[36]	Blockchain-based fog computing model (BFCM)	Interchange of information and data between medical institutions is facilitated by IoMT technology in healthcare industry	IoMT devices are susceptible to variety of attacked due to lack of hardware and software security features
3	[37]	Blockchain-enabled secure communication mechanism for IoT-driven personal health records (BIPHRS)	Dependable security system to protect transfer and storage of healthcare data	Data that have already been recorded cannot be easily changed, all of block codes must be rewritten
4	[38]	Cipher policy-attribute-based encryption (CP-ABE)	In an IoT-enabled world, healthcare 5.0 must protect client data security	Uses patient-centered digital well-being and strains capabilities of healthcare 4.0
5	[39]	Mobile medical service system (MMSS)	Correlation of different medicinal goods is calculated using correlation functions, such as cosine correlation	Large-scale IoT medical systems are challenging to design or administer on single cloud platform

3. Proposed Method

The security and energy efficiency of the Internet of Medical Things (IoMT) technologies have to be improved in healthcare services. We therefore developed the elliptic curve

cryptography (ECC)-based energy-efficient routing protocol (EERP) for reliable transmission and energy efficiency. This section gives a detailed description of the recommended approach. Figure 3 illustrates the proposed method's flow.

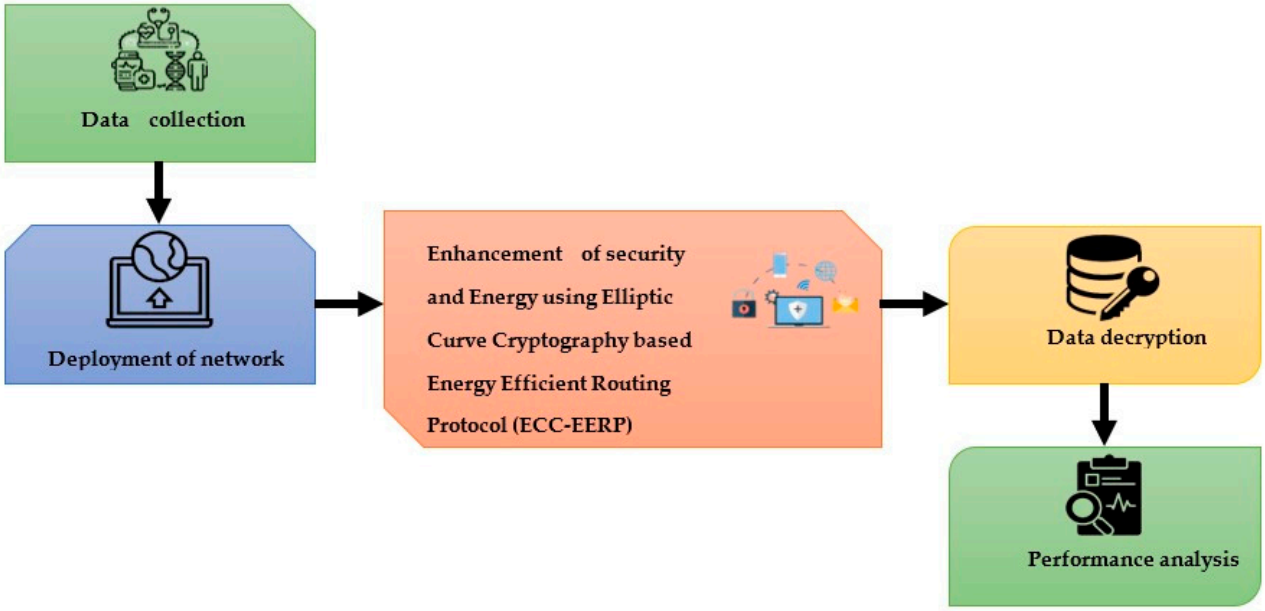

Figure 3. Flow of proposed method.

3.1. Data Collection

Embedded wearable biosensors that can collect biological data from a patient's body. An optical pulse rate sensor measures variations in artery volume produced by pulse waves during the heart's blood-pumping action. Temperature sensors measure body heat from −55 to 150 degrees Celsius. Utilizing electrodes positioned on the body, electrocardiograph sensors analyze the collected of cardiac electronic impulses. Wireless sensor networks include biosensors that increase the patient's level of satisfaction by being simple to wear; achieving the concise and inconspicuous continual assessment of health; and being miniaturized, power effective, and able to recognize biomedical signals such as temperature, heartbeat, high blood pressure, breathing rates, and electrocardiograms [40].

Network technology has the power to fundamentally transform how individuals think about healthcare and lifestyle. The network is capable of providing the assistance needed for revolutionary medical equipment. The cost, flexibility, and capabilities of the IoMT network might all be greatly enhanced by using a network configuration.

3.2. Elliptic Curve Cryptography (ECC)-Based Energy-Efficient Routing Protocol (EERP)

For enhancing the security and optimizing the energy in medical healthcare systems, we developed an elliptic curve cryptography-based energy-efficient routing protocol (ECC-EERP) for secure encryption and transmission. Each sensor node generates a unique encryption code for every communication cycle. The following elements are included in the 186-bit encryption system that was designed to overcome storage limitations. The initial element is composed of 148 bits generated by the ECC, and the devices also include the ECC criteria. The node ID is represented in 15 bits by the second part of the value. However, a WSN typically has 300 or fewer nodes in most real operations; a huge WSN might have numerous nodes. As a result, we allowed 15 bits for the node identity, which may indicate more than 8000 sensors. The next element uses 15 bits to represent the sensor's range from $D_{i,\,CH}$. The sensor node i's random key is defined as $\{K_i, ID_i, D_{i,\,CH}\}$. The authorization method is based on the initial component of the key to reduce networking transmission congestion. A two-party authorization mechanism is used for the key generation between a sink node (SN) and the base station (BS). To start the transfer operations, the cluster heads

(CHs) transfer the hashing ECC code from the individual nodes to the BS. Each node is assumed to be aware of its identity. The computing algorithm is used to create the hashing code for the ECC code. To ensure that ECC encryption speed is acceptable, we tested it. In most cases, an elliptic curve is a cube formula, as shown in Equation (1):

$$b^2 = a^3 + xa + y \tag{1}$$

Each SN in the networking should first be aware of the elliptic curves and a baseline position p that sits on the curves before any information can be transferred across the SNs. Every SN has its storage preconfigured with the baseline position P and the elliptic curve variables. X selects a randomized prime number k_X, and Y selects a randomized prime number k_Y to create a sharing secret key between SN X and SN Y. The secret keys of X and Y are denoted by k_X and k_Y, respectively. Afterward, the common keys $\overline{k}_X$ and $\overline{k}_Y$ for X and Y, respectively, are generated by applying Equations (2) and (3).

$$\overline{k}_X = k_X * P \tag{2}$$

$$\overline{k}_Y = k_Y * P \tag{3}$$

Both A and B's public identities are curved endpoints. The instances for which the baseline position p should be multiplied by itself to create the public keys are specified by the personal keys kA and kB. After exchanging public keys, the public keys are multiplied by their keys, as shown in Equation (4), to create a combined confidential key Q, which we need to be the first part of the suggested encryption key. It is theoretically impossible for an unauthorized person to determine k_X and k_Y, which are the personal keys of A and B, given the known values of $\overline{k}_Y$, $\overline{k}_X$, and P. As a consequence, opponents are unable to determine Q, the combined confidential key.

$$Q = k_X * \overline{k}_Y = K_Y * \overline{k}_X \tag{4}$$

The elliptic curve's primary functions of point adding and point multiplication are used by the SN to produce its public key. The complexity of determining the number of times P is combined with itself to obtain this public key determines the strength of an ECC encryption algorithm. The private key for the SN is represented by this value. The point can be multiplied along the elliptical curves by repeatedly connecting it to its original position. Equations (5) and (6) provide the adding function for any 2 points, (x_1, y_1) and (x_2, y_2), on the elliptical curves under the presumption that a novel position is equivalent to +. (x_3, y_3).

$$x_3 = \lambda^2 - x_1 - x_2 \tag{5}$$

$$y_3 = \lambda * (x_1 - x_3) - y_1 \tag{6}$$

λ is expressed in Equation (7).

$$\lambda = \begin{cases} \frac{b_2 - b_1}{a_2 - a_1}, \ \phi \neq \mu \\ \frac{3a^2 + x}{2b_1}, \ \phi = \mu \end{cases} \tag{7}$$

There are two steps in this approach that handle permutation and concatenation processes, separately. Permutation is a method of modifying the number of one or more bits in a particular bit sequence. In the concatenation operation, two parental bit sequences are combined to create equivalent children's bit sequences by switching out certain bits between the sources. While the concatenation procedure is utilized to modify the sequence of the corrupted text or visual information, the permutation procedure is utilized to provide randomized variety in the cipher text. Utilizing these two techniques has the primary advantage of adding moderate amounts of variation to the cipher text; the encryption procedure is shown in Algorithm 1.

Algorithm 1: Encryption procedure

Divide the text into 93-bit n units $S = \{u_1,\ u_2, \ldots, u_N\ \}$
Generate the 186-bit sequence β
Split β into two equal parts, P_1 and P_2, 88 bits each
Determine the number of 1s in every byte of $[a_1, a_2, \ldots, a_8]$ as well as the number of 1s in every one of the 11 bits of $B\ [b_1,\ b_2, \ldots, b_8]$ in P_2
for $i = 1,\ 2, \ldots, N$ do
$\delta = P_1\ \oplus\ y_i$
$\overline{\delta} = Perm\ \{\ \delta,\ A[i]\ \}$, where Perm is the permutation function
$\alpha = Con\ \{\ \overline{\delta},\ B\ [i]\ \}$, where Con is the concatenation function
$Cipher[i] = \alpha$
end for
Return the ciphertext $Cipher[C_1,\ C_2,\ C_3, \ldots, C_N]$, where C_i is the ciphertext of C_i

The bit series is initially separated into 186-bit units, and then each unit is further split into two 93-bit units. The amount of 1s in every byte and for every row of 12 sequential bits in the 2nd half of the bit string is then determined. Then, we arrange the 88-bit units of 88-bit plaintext into their respective binary format. Because the addition cipher XOR is effective for a similar duration of the keystream, these basic data are XORed with the initial unit of the bit string. Next, every bite of the XORed information is subjected to the permutation procedure. The 7th- and 8th-integer bits in the initial byte of the XORed text are modified, for instance, if the second half of the randomized bit sequence's first byte contains seven 1s. The ciphertext is created by further concatenating the permuted plaintext, as illustrated. To create reasonable variety, this concatenation process is iterated until every one of the 11 bits executes it at least 2 times. Utilizing EERP helps each transmission experience the least amount of congestion while using the least energy possible. It may be used for any scattered or crowded collective topology. EERP makes a choice using energy and sensor factors. Decisions about sorting and forwarding in traditional social routing are dependent on node-specific network factors. To determine a node's social weight, a network graph that describes the social connections between each node is required. Usually, the node's known connections to other nodes in the network are used to build a social graph of this form. Assume WN is a representation of the wireless network's nodes. Each sensor node can transmit and receive information when connected to another node. The data are replicated when another node has a higher weight. If the delay between the two statements' transmission and storage timings is equal, the EERP uses a threshold based on queue order to determine if there is a chance that the two data may be duplicated. The length of each document then determines the power balance between those two data. The EERP uses a threshold based on queue order to determine whether there is a possibility that the two data could be duplicates if the difference between the two data's transmission and storage periods is comparable. There is thus a power equilibrium between these two data that is dependent on their presence. With typical network routing techniques, data are repeated to the linked nodes with a higher data value. This may provide the best delivery rates, but due to the high congestion load, nodes with high data weight may suffer from early elimination. We took into account various elements while designing the recommended EERP in contrast with standard social-based sensing routing in a network. The foundation of the EERP calculation is the energy measurement of the data and node. The transmission times of the data copy are represented by these consumption measurements.

The power ratio, in this case, is $0 < PR\% < 1$. As a consequence, it is more difficult to comprehend the current facts. This is required due to the need of the alternative data to have a lower energy ratio than the data that will be delivered. By using this rule, the amount of duplicated data in the network is decreased. Due to the new propagation choice's steadily decreasing dispersion, we optimize the power strategy based on lifetime (LT). The adaptive behavior of the rule is to decrease power consumption. The data's LT specifies when it needs to be removed and if that time has elapsed. At the data initiator, the LT of the data is first set to TTL 0. Following each transmission or forwarding decision, the value

of LT is moved to the next version. When LT hits zero, the data end and are deleted from the node's buffer. The EERP forwarding option is only used when the power component of the data is less than that of the data that have to be conveyed. The following is the basic tenet of power distribution rate dynamics: Because the EERP prioritizes decreasing the data's power ratio when the data's LT is set to the maximum, the data's power ratio is first lowered from 1. The EERP modifies the power balance by prioritizing the transmission and detecting periods after several transmission and storage durations when the LT decreases to a low value; it becomes clear that the data will be erased shortly. Therefore, we use the following energy ratio, as shown in Equation (8):

$$\boldsymbol{PR_c = np_{(s,T)},\ PR\%} \tag{8}$$

where PR_c is a technique for sending the determination that uses two parts to determine the data repetition threshold. T represents mobility sensing in the first phase of $np_{(s,T,)}$, data sinks and sensors are viewed as portable devices. In the second part of the equation, PR% covers the data's power percentage. Equation (9) illustrates the factors that influence the forwarding decision.

$$PR_c = (1 + T + s),\ \left(1 - \frac{LT_a}{LT_b}\right) \tag{9}$$

The two main sensing functions are considered by the mobility sensing function. These processes include transmission and sensing. LT_a and LT_b, which stand for the data's original and present LT values, respectively, affect the data energy ratio. Remember that EERP was taken into consideration as a mobility-sensing power-aware routing protocol while implementing the forwarding function.

$$WN_c = \sqrt{Radio}range \tag{10}$$

$$(EERP) = \left\{ \begin{pmatrix} EERP & (WN_c)_{data} < (WN_c)_{other} \\ WN_c & WN_c \geq \sqrt{P} \end{pmatrix} \right\} \tag{11}$$

The node degree WN_c, a node indication where it could be preferred to consider both data and node energy, determines how much node power can be saved, as shown in Equations (10) and (11). From a network metric perspective, finding a node whose activities are greater than that of nearby nodes is more efficient. This may have the greatest impact on data transfer. Decryption is the process of restoring encrypted information to its initial state. Typically, encryption is performed backward. It decrypts the data such that only a trusted person with access to the private key or passcode may decrypt the data. Both the encryption and decryption procedures use cryptographic keys. The password that was utilized to encrypt the information should be utilized to decode a specific bit of ciphertext. Each encryption technique aims to make it as challenging as practicable to decipher the ciphertext produced without the key.

4. Performance Analysis

In this study, we introduced a unique elliptic curve cryptography-based energy-efficient routing protocol (ECC-EERP) approach to improve the security and energy efficiency of IoMT healthcare 5.0 systems. The efficacy of the recommended ECC-EERP method in boosting data security and energy savings for healthcare services was assessed. The suggested system offers advantages in terms of security, encryption throughput, energy efficiency, network lifetime, communication overload, and computation time. The existing approaches that we used for comparison included the optimized genetic algorithm (OptiGeA), rank-based energy-efficient key management (RBE-EKM), routing protocol with low-power and random–phase multiple access (RPL-RPMA), and ant colony optimization and integrated glowworm swarm optimization (ACI-GSO).

Simulation Details

The simulated data were taken from Fritzing V0.9.2 b (which simulates the hardware requirements to interface with the sensors) and Arduino IDE (a compiler of instructions for programming IoT sensors). The proposed technique was tested against various benchmark test structures. The IoT security models were then examined. Open-source software underpinned the Arduino controller. This special function helped to identify relevant libraries for each module or sensor. In order to strengthen security, user authentication is based on each biometric characteristic, including audio biometrics. Numerous simulated scenarios pertaining to the security of IoT-based systems were considered in order to investigate and assess the suggested strategy. Table 2 displays the specifics and setup of the hardware.

Table 2. Details and configuration of hardware.

Kubernetes and Devices	Hardware Instruments
Master Node	Laptop dell E6520
	Intel core i7-CPU 2760QM @ 2.40 GHz
	8 GB RAM DDR3
Work Node	Raspberry pi 4
	ARM Cortex-A72
IoT Device	Finger Pulse Oximeter Jumper JPD-450F
	1.6 V
	with Bluetooth v4.2

4.1. Security

Providing effective security standards with limited assets is one of the problems in the IoMT. The suggested solution increases security by effectively encrypting data. The security offered by the suggested and existing methods is shown in Figure 4. The security of both the proposed and existing solutions is shown in Table 3, which demonstrates that the suggested approach offers more security in WSNs than previous methods.

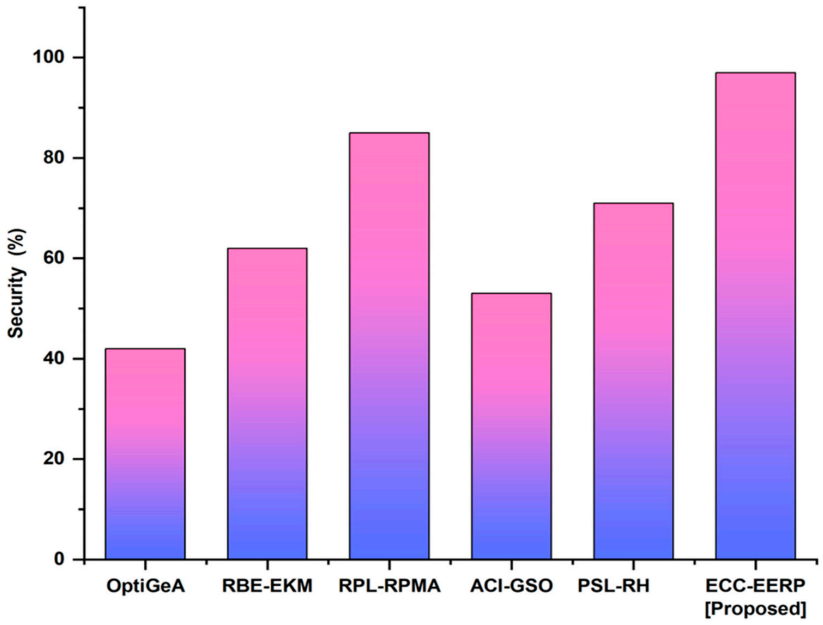

Figure 4. Security of the proposed and existing methods [41–45].

Table 3. Security of the proposed and existing methods.

Method	Security (%)
OptiGeA [41]	42
RBE-EKM [42]	62
RPL-RPMA [43]	85
ACI-GSO [44]	53
PSL-RH [45]	71
ECC-EERP (Proposed)	97

4.2. Encryption Throughput

The entire amount of plaintext data that are properly and quickly encrypted is referred to as the encryption throughput. The throughput for encryption schemes is determined as the average amount of plain text in q bits divided by the average encryption time. The data were effectively and securely encrypted using the suggested approach. Figure 5 and Table 4 show the encryption throughput provided by the proposed and existing methods, demonstrating that the suggested approach offers a reliable and secure encryption throughput.

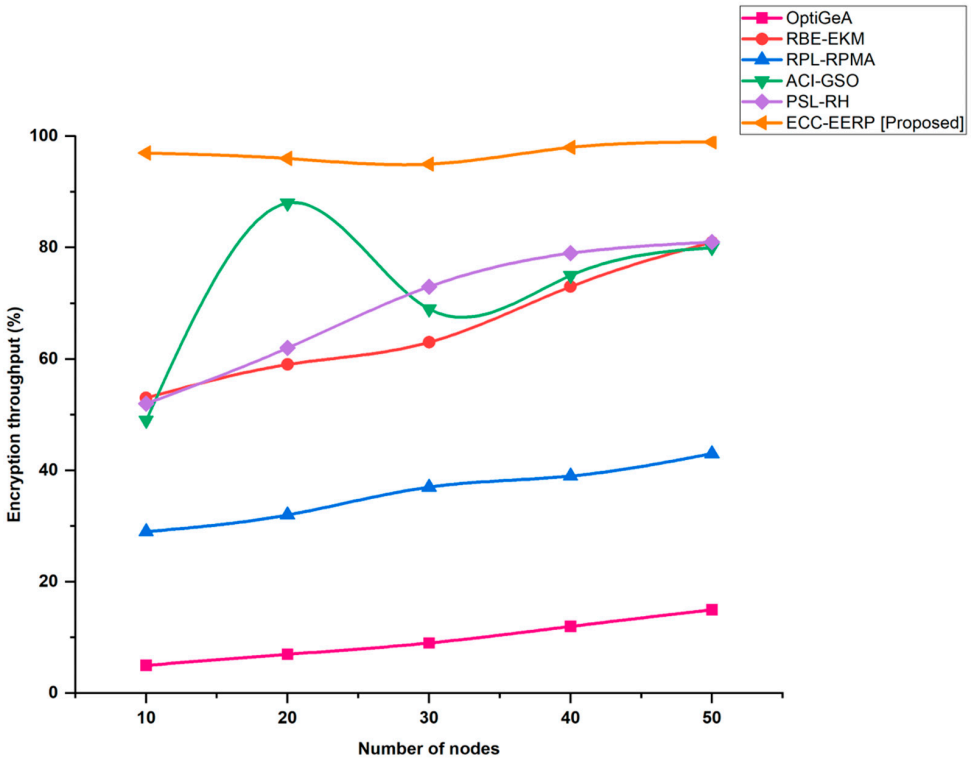

Figure 5. Encryption throughput of the proposed and existing methods [41–45].

Table 4. Encryption throughput of the proposed and existing methods.

Number of Nodes	Encryption Throughput (%)					
	OptiGeA [41]	RBE-EKM [42]	RPL-RPMA [43]	ACI-GSO [44]	PSL-RH [45]	ECC-EERP (Proposed)
10	5	53	29	49	52	97
20	7	59	32	88	62	96
30	9	63	37	69	73	95
40	12	73	39	75	79	98
50	15	81	43	80	81	99

4.3. Energy Efficiency

Energy efficiency is the ratio of the total number of bits that were transmitted to the terminal network (or, in the case of collecting techniques, the core network) to the total amount of energy used by the network to send these messages. The energy efficiency offered by the suggested and existing approaches is shown in Figure 6 and Table 5, demonstrating that the suggested strategy uses less energy for transmission.

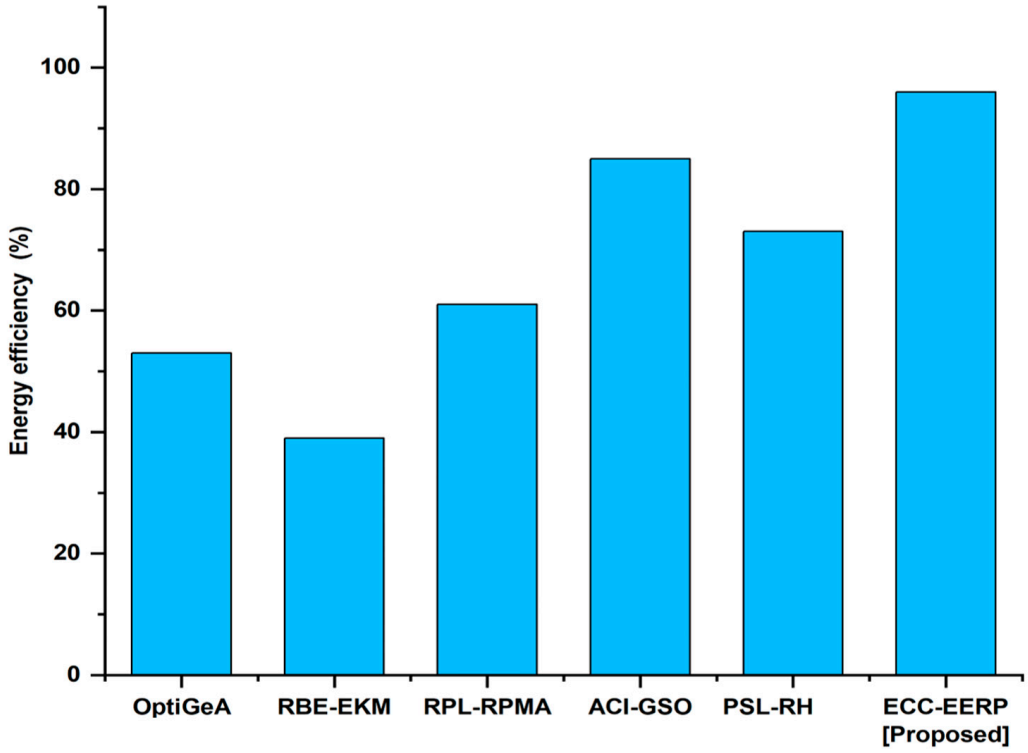

Figure 6. Energy efficiency of the proposed and existing methods [41–45].

Table 5. Energy efficiency of the proposed and existing methods.

Method	Energy Efficiency (%)
OptiGeA [41]	53
RBE-EKM [42]	39
RPL-RPMA [43]	61
ACI-GSO [44]	85
PSL-RH [45]	73
ECC-EERP (Proposed)	96

4.4. Network Lifetime

The main challenge in WSNs continues to be energy saving, which extends the network lifetime. An essential efficiency parameter in WSNs is network lifetime, which is measured as the duration until the power of the initial sensor is exhausted. Managing the communication load across sensor nodes is necessary to increase network longevity. Figure 7 and Table 6 show the network lifetime provided by the proposed and existing techniques. The proposed method offers a longer network lifetime for WSNs.

4.5. Communication Overload

Every node sends two messages throughout the transmitting procedure: one to initiate the interconnection and the other to transmit data, so that the total amount of information transferred in every method is identical. Therefore, if we assume that the amount of data sent to the BS is constant, the communication overload mostly relies on the ciphertext

amount of each scheme. As communication overload rises, transmission quality suffers. The proposed and existing approaches' communication overload is shown in Figure 8 and Table 7. The suggested approach reduces the communication overload for WSNs.

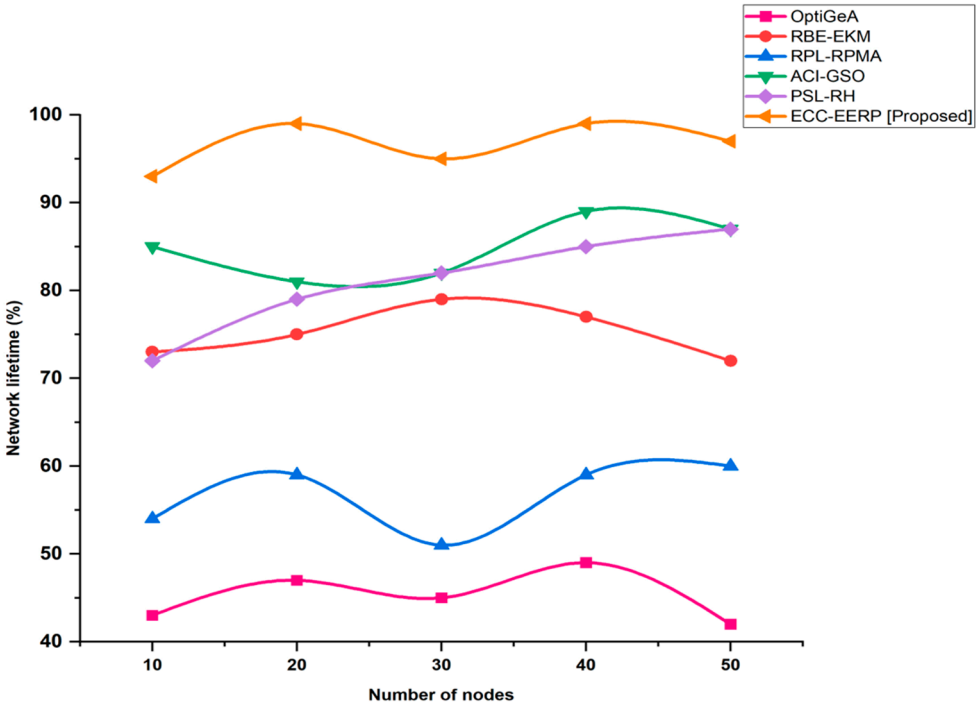

Figure 7. Network lifetime of the proposed and existing techniques [41–45].

Table 6. Network lifetime of the proposed and existing techniques.

Number of Nodes	Network Lifetime (%)					
	OptiGeA [41]	RBE-EKM [42]	RPL-RPMA [43]	ACI-GSO [44]	PSL-RH [45]	ECC-EERP (Proposed)
10	43	73	54	85	72	93
20	47	75	59	81	79	99
30	45	79	51	82	82	95
40	49	77	59	89	85	99
50	42	72	60	87	87	97

4.6. Computation Time

The system's processing time needed during the encryption process is referred to as computation time. IoMT experts and healthcare experts utilize computation time as a crucial performance indicator to assess a method's efficiency in terms of execution time. Figure 9 and Table 8 shos the computation time required by the proposed and existing methods. When compared with the existing method, the suggested method utilizes less time.

4.7. Implementation Cost

Costs associated with developing and implementing an implementation strategy that focuses on one or more particular evidence-based treatments are known as implementation costs. Figure 10 shows the implementation cost provided by the proposed and existing methods. Table 9 shows the implementation cost of the proposed and existing methods. When compared to the existing systems, the proposed method utilizes low cost.

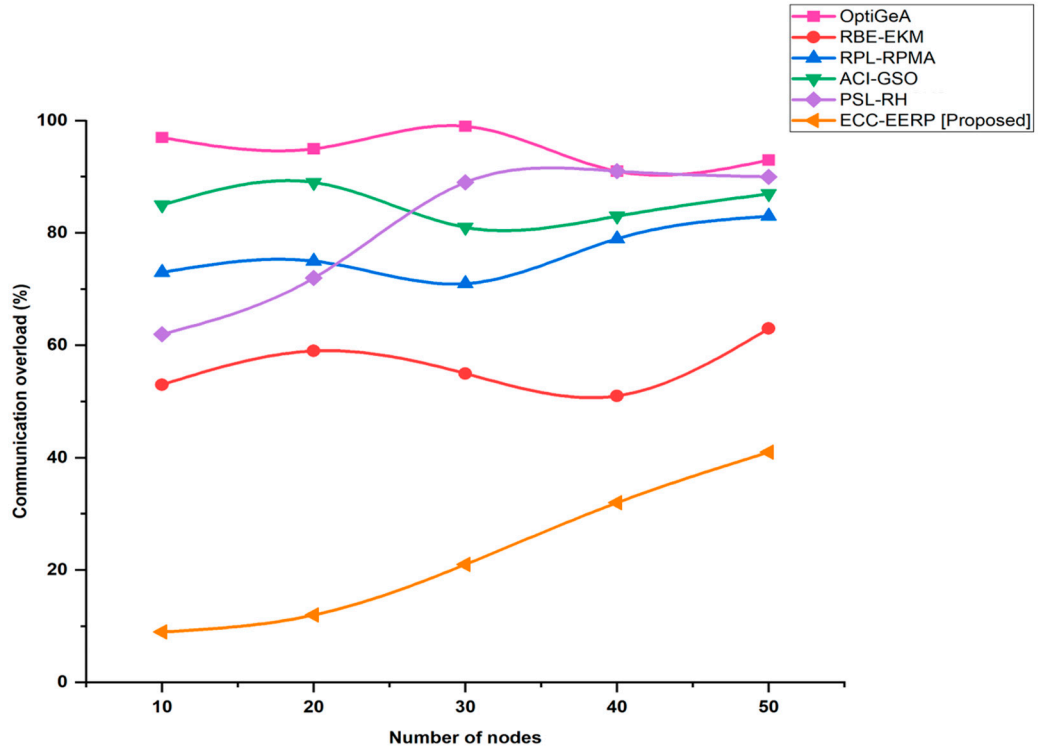

Figure 8. Communication overload of the proposed and existing methods [41–45].

Table 7. Communication overload of the proposed and existing methods.

	Number of Nodes	Communication Overload (%)				
	OptiGeA [41]	RBE-EKM [42]	RPL-RPMA [43]	ACI-GSO [44]	PSL-RH [45]	ECC-EERP (Proposed)
10	97	53	73	85	62	9
20	95	59	75	89	72	12
30	99	55	71	81	89	21
40	91	51	79	83	91	32
50	93	63	83	87	90	41

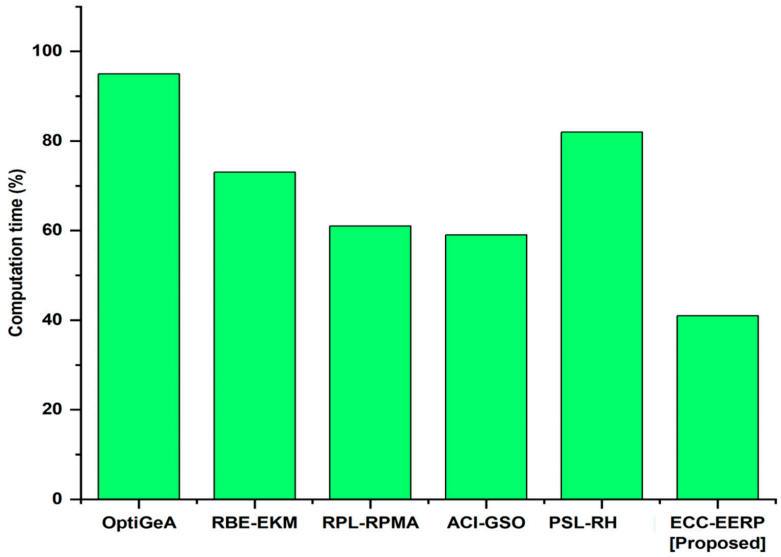

Figure 9. Computation time of the proposed and existing methods [41–45].

Table 8. Computation time of the proposed and existing methods.

Method	Computation Time (%)
OptiGeA [41]	95
RBE-EKM [42]	73
RPL-RPMA [43]	61
ACI-GSO [44]	59
PSL-RH [45]	82
ECC-EERP (Proposed)	41

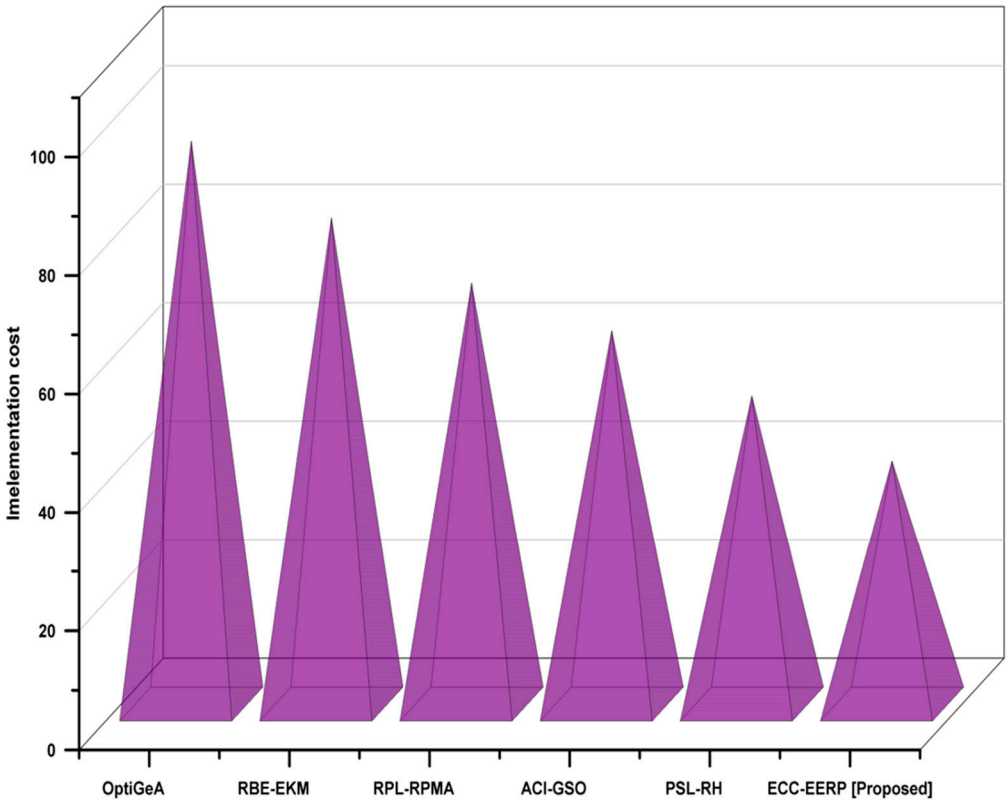

Figure 10. Implementation cost of the proposed and existing methods [41–45].

Table 9. Implementation cost of the proposed and existing methods.

Method	Implementation Cost (%)
OptiGeA [41]	95
RBE-EKM [42]	82
RPL-RPMA [43]	71
ACI-GSO [44]	63
PSL-RH [45]	52
ECC-EERP (Proposed)	41

5. Discussion

For CH selection, researchers [41] developed an optimized genetic algorithm (OptiGeA). The communication distance between the sink and CH during network execution has been shortened using a variety of mobility sink techniques in order to address hotspot challenges and provide a secure and energy-efficient IoMT-equipped WSN. They are complex algorithms that are challenging to effectively construct and may be vulnerable to numerical noise. They have trouble tackling discrete optimization issues. The rank-based energy-efficient key management (RBE-EKM) method aims to find an energy-efficient solution for sending data from the sensor to the base station [42]. To boost the efficacy and longevity

of secured communication, researchers [43] designed a routing protocol with low power and random-phase multiple access (RPL-RPMA). Growing a network inherently causes complexity to increase. Other authors [44] aimed to offer a novel hybrid approach that combines glowworm swarm optimization with ant colony optimization (ACI-GSO). When working with a lot of data, this method has several drawbacks in terms of convergence speed and solution correctness. The CH selection goal is to minimize the distance between the chosen CH nodes. It improves the system's energy efficiency and transmission security. None of the existing methods meet the security and energy efficiency needs of WSN-based IoMT healthcare services. Probabilistic super learning–random hashing (PSL-RH) enhances the security of medical data kept in IoT clouds. Costs for IoT sensors can be reduced by employing the PSL-RH learning strategy. However, the problems faced by PSL-RH include a high mistake rate, ineffective forecast outcomes, and procedure latency, which reduce the effectiveness of the complete security system [45].

6. Conclusions

The Internet of Medical Things (IoMT) and wireless sensor nodes in healthcare offer immense potential for improvements in medical performance and the production of novel clinical findings and innovations. The development of IoMT technologies has been very beneficial to medical infrastructure. However, security and energy-efficiency problems are severely affecting the IoMT. To improve healthcare 5.0, these problems must be addressed. As a result, we developed a novel elliptic curve cryptography-based energy-efficient routing protocol (ECC-EERP) to provide a high degree of security and an energy-efficient system for healthcare 5.0. We compared the effectiveness of the proposed approach with that of many other existing strategies, including the optimized genetic algorithm (OptiGeA), rank-based energy-efficient key management (RBE-EKM), routing protocol with low-power and random phase multiple access (RPL-RPMA), ant colony optimization, integrated glowworm swarm optimization (ACI-GSO), and probabilistic super learning–random hashing (PSL-RH). Numerous factors, including security, encryption throughput, energy efficiency, network lifetime, communication overload, computation time, and implementation cost, were used to assess the proposed system. The suggested method's encryption throughput was 99%. The findings of these measurements demonstrate that the suggested method provides improved security and energy efficiency. In the future, an extensive range of approaches may be used to optimize the effectiveness of communication networks in healthcare 5.0.

Author Contributions: Conceptualization, G.H.L. and S.K.G.; data curation, A.P. and S.K.G.; formal analysis, R.N., V.K.V. and S.K.G.; funding acquisition, G.H.L. and F.F.; investigation, R.N., G.H.L., F.F. and S.K.G.; methodology, R.N., A.P. and V.K.V.; project administration, G.H.L. and F.F.; resources, F.F. and S.K.G.; software, V.K.V. and S.K.G.; supervision, G.H.L. and F.F.; validation, A.P., V.K.V. and S.K.G.; writing—original draft, R.N., G.H.L., F.F., A.P., V.K.V. and S.K.G.; writing—review and editing, R.N., G.H.L., F.F., A.P., V.K.V. and S.K.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest related to this work.

References

1. Reegu, F.A.; Abas, H.; Jabbari, A.; Akmam, R.; Uddin, M.; Wu, C.M.; Chen, C.L.; Khalaf, O.I. Interoperability Requirements for Blockchain-Enabled Electronic Health Records in Healthcare: A Systematic Review and Open Research Challenges. *Secur. Commun. Netw.* **2022**, *2022*, 9227343. [CrossRef]
2. Banumathy, D.; Khalaf, O.I.; Tavera Romero, C.A.; Raja, P.V.; Sharma, D.K. Breast calcifications and histopathological analysis on tumor detection by CNN. *Comput. Syst. Sci. Eng.* **2023**, *44*, 595–612. [CrossRef]

3. Khalaf, O.I.; Natarajan, R.; Mahadev, N.; Christodoss, P.R.; Nainan, T.; Romero, C.A.T.; Abdulsahib, G.M. Blinder Oaxaca and Wilk Neutrosophic Fuzzy Set-based IoT Sensor Communication for Remote Healthcare Analysis. *IEEE Access* **2022**, *21*, 1–13. [CrossRef]
4. Jabbar, M.A.; Shandilya, S.K.; Kumar, A.; Shandilya, S. Applications of cognitive internet of medical things in Modern Healthcare. *Comput. Electr. Eng.* **2022**, *102*, 108276. [CrossRef]
5. Mahesh, T.R.; Kumar, D.; Kumar, V.V.; Asghar, J.; Bazezew, B.M.; Natarajan, R.; Vivek, V. Blended Ensemble Learning Prediction Model for Strengthening Diagnosis and Treatment of Chronic Diabetes Disease. *Comput. Intell. Neurosci.* **2022**, *2022*, 4451792. [CrossRef]
6. Islam, M.M.; Rahaman, A.; Islam, M.R. Development of Smart Healthcare Monitoring System in IOT environment. *SN Comput. Sci.* **2020**, *1*, 185. [CrossRef]
7. Vincent, J.-L.; Einav, S.; Pearse, R.; Jaber, S.; Kranke, P.; Overdyk, F.J.; Whitaker, D.K.; Gordo, F.; Dahan, A.; Hoeft, A. Improving detection of patient deterioration in the General Hospital Ward Environment. *Eur. J. Anaesthesiol.* **2018**, *35*, 325–333. [CrossRef]
8. Wibrandt, I.; Lippert, A. Improving patient safety in handover from Intensive Care Unit to general Ward: A systematic review. *J. Patient Saf.* **2017**, *16*, 199–210. [CrossRef]
9. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Biosensors applications in medical field: A brief review. *Sens. Int.* **2021**, *2*, 100100. [CrossRef]
10. Mahari, S.; Gandhi, S. Recent advances in electrochemical biosensors for the detection of salmonellosis: Current prospective and challenges. *Biosensors* **2022**, *12*, 365. [CrossRef]
11. Gaba, G.S.; Hedabou, M.; Kumar, P.; Braeken, A.; Liyanage, M.; Alazab, M. Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare. *Sustain. Cities Soc.* **2022**, *80*, 103766. [CrossRef]
12. Rajesh, N.; Christodoss, P.R. Analysis of origin, risk factors influencing COVID-19 cases in India and its prediction using ensemble learning. *Int. J. Syst. Assur. Eng. Manag.* **2021**, *75*, 1–8. [CrossRef]
13. Arvisais-Anhalt, S.; Lau, M.; Lehmann, C.U.; Holmgren, A.J.; Medford, R.J.; Ramirez, C.M.; Chen, C.N. The 21st Century Cures Act and Multiuser Electronic Health Record Access: Potential Pitfalls of Information Release. *J. Med. Internet Res.* **2022**, *24*, e34085. [CrossRef] [PubMed]
14. Steinkamp, J.; Kantrowitz, J.J.; Airan-Javia, S. Prevalence and sources of duplicate information in the Electronic Medical Record. *JAMA Netw. Open* **2022**, *5*, e2233348. [CrossRef]
15. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R. Medical 4.0 technologies for healthcare: Features, capabilities, and applications. *Internet Things Cyber-Phys. Syst.* **2022**, *2*, 12–30. [CrossRef]
16. Iyamu, T. The interpretivist and analytics approaches for Healthcare Big Data Analytics. *Adv. Big Data Anal. Healthc. Serv. Deliv.* **2022**, *76*, 74–88. [CrossRef]
17. Mbunge, E.; Muchemwa, B.; Jiyane, S.; Batani, J. Sensors and healthcare 5.0: Transformative SHIFT IN virtual care through Emerging Digital Health Technologies. *Glob. Health J.* **2021**, *5*, 169–177. [CrossRef]
18. Subahi, A.F.; Khalaf, O.I.; Alotaibi, Y.; Natarajan, R.; Mahadev NRamesh, T. Modified Self-Adaptive Bayesian Algorithm for Smart Heart Disease Prediction in IoT System. *Sustainability* **2022**, *14*, 14208. [CrossRef]
19. Hussein, A.; Mohammed, W.R.; Musa Jaber, M.; Ibrahim Khalaf, O. An Adaptive ECG Noise Removal Process Based on Empirical Mode Decomposition (EMD). *Contrast Media Mol. Imaging* **2022**, *2022*, 3346055. [CrossRef]
20. Kandhro, I.A.; Uddin, M.; Hussain, S.; Chaudhery, T.J.; Shorfuzzaman, M.; Meshref, H.; Albalhaq, M.; Alsaqour, R.; Khalaf, O.I. Impact of Activation, Optimization, and Regularization Methods on the Facial Expression Model Using CNN. *Comput. Intell. Neurosci.* **2022**, *2022*, 3098604. [CrossRef]
21. Meenakshi, R.; Ponnusamy, R.; Alghamdi, S.; Khalaf, O.I.; Alotaibi, Y. Development of a Mobile App to Support the Mobility of Visually Impaired People. *CMC-Comput. Mater. Contin.* **2022**, *73*, 3473–3495. [CrossRef]
22. Radhakrishnan, K.; Ramakrishnan, D.; Khalaf, O.I.; Uddin, M.; Chen, C.L.; Wu, C.M. A Novel Deep Learning-Based Cooperative Communication Channel Model for Wireless Underground Sensor Networks. *Sensors* **2022**, *22*, 4475. [CrossRef]
23. Asghar, J.; Tabasam, M.; Althobaiti, M.M.; Adnan Ashour, A.; Aleid, M.A.; Ibrahim Khalaf, O.; Aldhyani, T.H.H. A Randomized Clinical Trial Comparing Two Treatment Strategies, Evaluating the Meaningfulness of HAM-D Rating Scale in Patients with Major Depressive Disorder. *Front. Psychiatry* **2022**, *13*, 873693. [CrossRef]
24. Ogudo, K.A.; Surendran, R.; Khalaf, O.I. Optimal artificial intelligence-based automated skin lesion detection and classification model. *Comput. Syst. Sci. Eng.* **2023**, *44*, 693–707. [CrossRef]
25. Gnanavel, S.; Sreekrishna, M.; Mani, V.; Kumaran, G.; Amshavalli, R.S.; Alharbi, S.; Maashi, M.; Khalaf, O.I.; Abdulsahib, G.M.; Alghamdi, A.D.; et al. Analysis of Fault Classifiers to Detect the Faults and Node Failures in a Wireless Sensor Network. *Electronics* **2022**, *11*, 1609. [CrossRef]
26. Ortiz, J.H.; Romero, C.A.T.; Ahmed, B.T.; Khalaf, O.I. Qos in fanet business and swarm data. *Comput. Mater. Contin.* **2022**, *72*, 1877–1899.
27. Banumathy, D.; Khalaf, O.I.; Romero, C.A.T.; Indra, J.; Sharma, D.K. Cad of BCD from thermal mammogram images using machine learning. *Intell. Autom. Soft Comput.* **2022**, *34*, 667–685. [CrossRef]

28. Sengan, S.; Khalaf, O.I.; Ettiyagounder, P.; Sharma, D.K.; Karrupusamy, R. Novel Approximation Booths Multipliers for Error Recovery of Data-Driven Using Machine Learning. In *Emerging Technology Trends in Internet of Things and Computing, Proceedings of the TIOTC 2021, Erbil, Iraq, 6–8 June 2021*; Communications in Computer and Information Science; Liatsis, P., Hussain, A., Mostafa, S.A., Al-Jumeily, D., Eds.; Springer: Cham, Switzerland, 2022; Volume 1548. [CrossRef]
29. Malik, P.K.; Naim, A.; Singh, R. *Printed Antennas: Design and Challenges*; CRC Press: Boca Raton, FL, USA, 2022.
30. Rajagopal, N.K.; Saini, M.; Huerta-Soto, R.; Vílchez-Vásquez, R.; Kumar, J.N.V.R.; Gupta, S.K.; Perumal, S. Human resource demand prediction and configuration model based on grey wolf optimization and recurrent neural network. *Comput. Intell. Neurosci.* **2022**, *2022*, 5613407. [CrossRef]
31. Refaee, E.; Parveen, S.; Begum, K.M.J.; Parveen, F.; Raja, M.C.; Gupta, S.K.; Krishnan, S. Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5665408. [CrossRef]
32. Kaushal, R.K.; Bhardwaj, R.; Kumar, N.; Aljohani, A.A.; Gupta, S.K.; Singh, P.; Purohit, N. Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 8741357. [CrossRef]
33. Hazela, B.; Gupta, S.K.; Soni, N.; Saranya, C.N. Securing the Confidentiality and Integrity of Cloud Computing Data. *ECS Trans.* **2022**, *107*, 2651. [CrossRef]
34. Gupta, S.K.; Tiwari, S.; Abd Jamil, A.; Singh, P. Faster as well as Early Measurements from Big Data Predictive Analytics Model. *ECS Trans.* **2022**, *107*, 2927. [CrossRef]
35. Rehman, A.; Abbas, S.; Khan, M.A.; Ghazal, T.M.; Adnan, K.M.; Mosavi, A. A Secure Healthcare 5.0 System Based on Blockchain Technology Entangled with Federated Learning Technique. *Comput. Biol. Med.* **2022**, *150*, 106019. [CrossRef]
36. Shadab, A.; Shuaib, M.; Ahmad, S.; Jayakody, D.N.; Muthanna, A.; Bharany, S.; Elgendy, I.A. Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IOMT) Integration. *Sustainability* **2022**, *14*, 15312. [CrossRef]
37. Wazid, M.; Ashok, K.D.; Park, Y. Blockchain-Enabled Secure Communication Mechanism for IOT-Driven Personal Health Records. *Trans. Emerg. Telecommun. Technol.* **2021**, *33*, e4421. [CrossRef]
38. Zaidi, S.Y.; Munam, A.S.; Khattak, H.A.; Maple, C.; Rauf, H.T.; El-Sherbeeny, A.M.; El-Meligy, M.A. An Attribute-Based Access Control for IOT Using Blockchain and Smart Contracts. *Sustainability* **2021**, *13*, 10556. [CrossRef]
39. Liang, X.; Tang, B.; Cai, Z.; Huang, Z.; Luo, B.; Lin, B.; Yang, Y.; Liu, Q.; Zhou, H. Metabolic Feature Profiling and Metabolic Vulnerability Targeting in B-Cell Lymphoblastic Leukemia. *Blood* **2022**, *140* (Suppl. 1), 6361–6362. [CrossRef]
40. Thirukrishna, J.T.; Aishwarya, M.V.; Mansi, S.; Mounisha, B.; Naksha, K. Efficient data Transmission in WSN using wearable sensors for Healthcare Monitoring. *Int. J. Adv. Res. Innov. Ideas Educ.* **2021**, *7*, 446–457.
41. Singh, S.; Nandan, A.S.; Sikka, G.; Malik, A.; Vidyarthi, A. A secure energy-efficient routing protocol for disease data transmission using IoMT. *Comput. Electr. Eng.* **2022**, *101*, 108113. [CrossRef]
42. Anbarasu, S. *Rank-Based Energy Efficient Key Management (RBE-EKM) Scheme Based Routing for Internet of Medical Things (IOMT)*; Bharathiar University: Tamil Nadu, India, 2022.
43. Ambika, K.; Malliga, S. Secure hyper intelligence in routing protocol with low-power (RPL) Networks in IoT. *Adv. Eng. Softw.* **2022**, *173*, 103247. [CrossRef]
44. Reddy, D.L.; Puttamadappa, C.; Suresh, H.N. Merged glowworm swarm with ant colony optimization for energy efficient clustering and routing in the wireless sensor network. *Pervasive Mob. Comput.* **2021**, *71*, 101338. [CrossRef]
45. Khadidos, A.O.; Shitharth, S.; Khadidos, A.O.; Sangeetha, K.; Alyoubi, K.H. Healthcare Data Security Using IoT Sensors Based on Random Hashing Mechanism. *J. Sens.* **2022**, *2022*, 8457116. [CrossRef]