Transforming Healthcare Infrastructure for Enhanced Energy Efficiency and Privacy

Sudeshna chakraborty[*1], Akanksha Singh[2]

[1] School of Computing Science and Engineering, Galgotias University, India
[2]Department of Computer Science and Engineering, Babu Banarasi Das University, Lucknow, India
Emails: sudeshna.chakraborty@galgotiasuniversity.edu.in; ankakaanj@bbdu.ac.in

Abstract

The Internet of Medical Things (IoMT) is a revolutionary technique for integrating the IT infrastructure of healthcare organisations with medical apps and equipment. Rapid advancements in this approach in recent years have resulted in game-changing improvements in the healthcare system, illness management, and patient care standards. Both achievements have been made possible by the Internet of Medical Things. People can use the IoMT to access a variety of cloud-based services, including file sharing, patient monitoring, data collection, information gathering, and hospital cleaning. Wireless sensor networks (WSNs), which collect and transmit data, are critical to system operation. In the healthcare system, patients' privacy and security must be preserved at all costs. Wireless data transmission from these cutting-edge devices may have been intercepted and manipulated without consent. The hybrid and improved (Elliptic Curve Cryptography ECC) Energy-Efficient Routing Protocol (EERP) method, which is based on the elliptic curve encryption protocol, may provide enough protection for sensitive information. ECC-EERP uses pairs of public and private keys known only to each other to decode and encrypt data delivered across a network. As a result, the energy needed to sustain WSNs has dropped. To assess the efficacy of the recommended plan, we did an extensive study and compared our findings to the many other viable courses of action. We did the analysis while taking a variety of aspects into account. The study's findings and conclusion all point to the strategy's ability to significantly increase energy efficiency and security. ECC-EERP is a novel encryption method that increases data security while consuming less energy. Because of its efficacy in improving the whole healthcare system, this strategy has a lot of potential for the future of patient care, illness management, and healthcare delivery in general.

Keywords: Data security; Electronic health records; Energy-Efficient Routing Protocol; Elliptic Curve Cryptography; Internet of Medical Things; Healthcare.

1. Introduction

The broad use of digital health technologies heralds the start of an exciting new era in healthcare delivery. The use of digital technology is critical in enabling access to pertinent health information, expediting medical dispute resolution, and improving communication between patients, practitioners, and institutions. However, before these findings can be properly employed, a paradigm shift towards healthcare 5.0 is required. Figure 1 demonstrates just a handful of the numerous ways in which the medical profession has embraced the revolutionary potential of IoT [1-3]. The network's capacity to safely transport data without the assistance of humans or machines has resulted in advancements in data transfer security, job management, opportunity analysis, and device connectivity. These cutting-edge Internet of Things technologies enable networked healthcare by facilitating the integration of cutting-edge medical equipment and the free flow of complete health information [4]. The term "traditional healthcare" is giving way to the notion of "smart healthcare" because of technological improvements [5-6]. These innovations are providing medical practitioners with monitoring systems. This makes it possible for medical professionals to link, analyse, and evaluate health data received from biomaterials and interactive wearable technology by utilising a variety of IoT technologies. As a direct result of this, they can give their patients superior treatment. To improve patient-specific treatments, adherence, proactive supervision, efficient prognosis, fast and accurate illness identification, consistent care, and intelligent recovery, the IoHT, IoNT, and IoMHT are now being used in the

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

delivery of extensive healthcare services [7-8]. This is being done in the hopes of achieving the goals. Portable healthcare is being driven by the rapid improvements in consumer electronics and digital technology, which are offering wireless connectivity and the delivery of medical treatment to people with chronic diseases who are not in typical healthcare facilities. Because of this, biosensors have a substantial amount of untapped potential as instruments for use in clinical practise and medical research.

The evolution of healthcare from its beginnings in healthcare 1.0 to its current state of healthcare 5.0 has coincided with a considerable shift towards the use of technology-driven treatment methods. Before the widespread adoption of computers in healthcare 2.0, physicians were largely accountable for maintaining patient data [9]. Electronic health records, often known as EHRs, are digitalized copies of paper medical records that came into being during the healthcare 2.0 era [10-12]. The development of smartphone applications to democratise electronic health records (EHRs) was a significant step forward for healthcare 3.0. This led to a change in care that is more focused on the patient. On the other hand, because these data lacked complete decision analysis, they were susceptible to being attacked. The era of healthcare 4.0 saw the introduction of artificial intelligence (AI) and big data analytics, both of which were used to draw educated judgements from compiled EHRs [15, 16]. However, the convergence of several medical organisations presented issues in terms of effective communication and coordination, and the AI models that analysed the ever-increasing volume of healthcare data were difficult to use, ineffective, and slow. The Healthcare 5.0 road map explains these procedures in detail. Figure 2 depicts the evolution of the healthcare business from version "1.0" to version "5.0." The Healthcare 5.0 movement's efforts to reimagine the system focus on patients' needs. Patients, physicians, hospitals, and pharmacies are all different types of stakeholders in the healthcare delivery system [13]. Healthcare 5.0 prioritises patients' overall wellbeing, quality of life, and capacity to collaborate with healthcare professionals during treatment. If a piece of smart healthcare equipment disconnects from the Healthcare 5.0 network, it is no longer a part of the network and will not be able to communicate in the future. This regulation includes restrictions on both spoken and written communication.

The incorporation of the IoT into healthcare 5.0 has brought with it a number of important developments and ramifications. Real-time monitoring, individualised treatment plans, and preventative healthcare interventions are all made possible by the seamless connectivity and data interchange made possible by the IoT technology. This enables clinicians to tailor therapy to each patient's individual requirements. This tailored technique may enhance patient outcomes, therapeutic efficacy, and the incidence of treatment-related adverse effects. In addition, Internet of Things devices can improve medication adherence by providing reminders and tracking drug consumption [14-15]. This helps to ensure that patients comply with the treatment programmes that have been recommended for them. Special emphasis must be paid to energy economy and security considerations in the adoption of the IoMT in Healthcare 5.0. These issues can be broken down into smaller ones. These challenges revolve around protecting patients' privacy, securing data, and improving the energy consumption of healthcare systems. The existing framework can successfully address these difficulties since it acknowledges them. These are the issue areas that have been identified:

Due to the secrecy of their personal and medical information, patients' right to privacy is crucial in the healthcare business. It is critical to keep patient information safe to protect their privacy and develop trust. When attempting to secure patients' personal information at every point of its lifespan, from initial data gathering through ultimate deletion and access permissions, issues occur. It is critical to ensure the integrity of the data used in healthcare in order to arrive at correct diagnoses, treatment plans, and decisions. Keeping information from being stolen, lost, or altered without authorization is a difficult task. Maintaining data integrity is critical for maintaining accurate and trustworthy patient records. Wearables, sensors, and other medical devices that comprise the IoMT all require electricity to function. To extend battery life, decrease maintenance costs, and assure ongoing performance, maximum energy efficiency is necessary [16]. The task at hand is to devise solutions for reducing energy usage in the healthcare system without sacrificing performance or dependability. Because of the diverse spectrum of hardware, software, and other components that comprise IoMT systems, it is critical that all these pieces work seamlessly together. The problem is ensuring that all these healthcare systems and stakeholders can exchange and use data efficiently, interact with one another, and collaborate. Medical Equipment Security Unauthorised access, data breaches, virus attacks, and manipulated devices are just a few of the ways that IoMT device security might be jeopardised. The increasing interconnectivity of IoMT devices raises the stakes for these attacks. It is critical to ensure the safety of these devices to preserve patients' privacy and avoid interruptions to healthcare facilities' everyday operations. To reduce risk, it is vital to address the issue of implementing reliable authentication systems, secure communication protocols, and device-level security measures [17-19]. Observance of Rules and Laws Healthcare systems are responsible for adhering to all applicable rules and standards, including HIPAA and the EU's General Data Protection Regulation. Only by complying with these principles can we assure patient data privacy, security, and ethical treatment. The problem is developing a framework that meets these standards while also providing adequate safety measures to meet compliance criteria.

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

2. Related Work

Because The IoT streamlines healthcare operations and improves operational efficiencies across a wide range of healthcare delivery facets. Automating repetitive processes via the use of connected devices and intelligent systems eases the workload of medical practitioners and reduces the likelihood of mistakes caused by human error. IoT-enabled asset monitoring solutions increase the efficiency of inventory management and supply chain operations, which ensure that necessary resources, such as medical equipment, pharmaceuticals, and other supplies, are always available when they are required. Additionally, predictive maintenance that is enabled by the Internet of Things can identify possible problems in medical devices, which enables proactive maintenance and reduces the amount of time equipment is unavailable. Concerns about data security and privacy have been raised in response to the growing implementation of IoT in healthcare. To maintain patient confidentiality and defend against unauthorized access, massive data gathering, and transmission in the medical field necessitate the implementation of stringent security protocols. To protect patients' personal information, healthcare providers and organisations are required to use strong data encryption, secure communication protocols, and access control systems [20]. In addition, ensuring ethical and legal treatment of patient data requires strict adherence to privacy standards like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Interoperability and standardisation are necessary if healthcare 5.0 is going to make full use of the Internet of Things' promise.

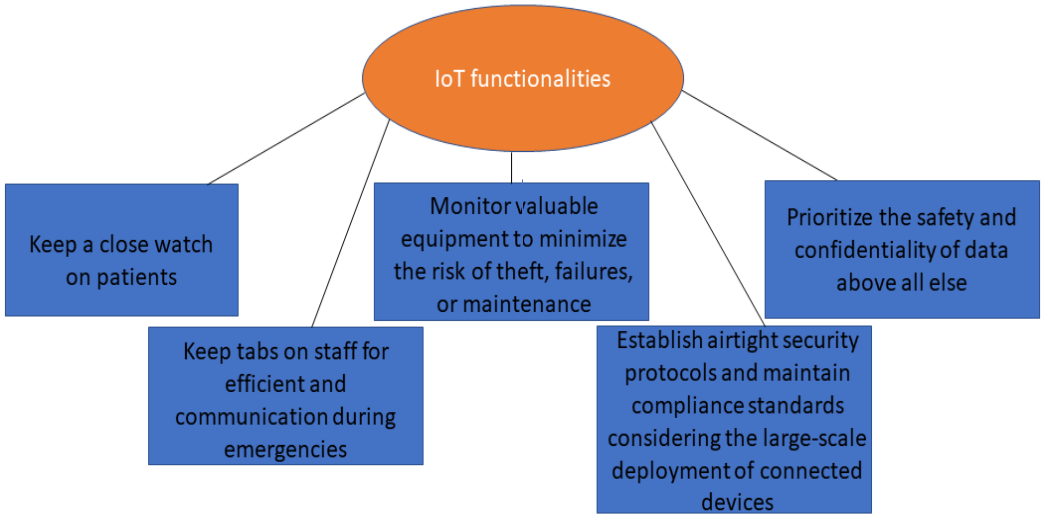

Figure 1: Ensuring Safety and Confidentiality: IoT's Role in Data Security and Compliance

Figure 1 illustrates the significance of IoT in ensuring safety and confidentiality through its role in data security and compliance. To give a holistic perspective of a patient's health, many Internets of Things devices and systems need to connect and exchange data in a smooth manner. For there to be interoperability between the many different Internet of Things devices and healthcare information systems, the creation of standardised communication protocols, data formats, and interfaces is very necessary [21]. Establishing interoperability standards and ensuring the seamless interchange of data requires the participation of all relevant parties, such as healthcare providers, technology developers, and regulatory agencies. The incorporation of IoT into healthcare 5.0 has tremendous potential for revolutionising the delivery of healthcare, improving patient outcomes, and reducing operational inefficiencies. The Internet of Things enables real-time monitoring, personalised treatment plans, and precision medicine, all of which make it possible for healthcare practitioners to provide care that is proactive and patient-centered. Nevertheless, resolving issues with data security and privacy, as well as interoperability and standardisation, is essential for effective adoption. If healthcare systems use Internet of Things technology in a responsible manner and implement rigorous safeguards, they will be able to harness the full potential of IoT in developing healthcare 5.0 and, ultimately, increasing the well-being of patients all over the world [22-24].

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

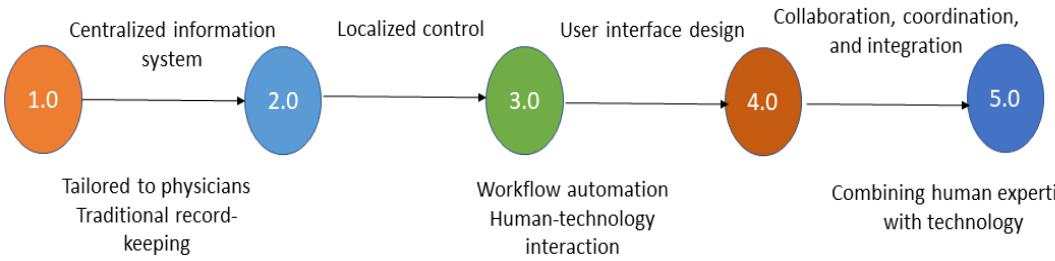

Figure 2: Transforming Healthcare with User Interface Design: Tailored Solutions for Physicians and Workflow Automation

Figure 2 depicts the transformative impact of user interface design in healthcare, specifically focusing on tailored solutions for physicians and workflow automation. Several recent academic investigations have focused on several uses of IoT in healthcare. These studies consider novel approaches to problem solving. This section summarises the most important results and theoretical breakthroughs on the topic. One study [25] focused on establishing an Internet of Things platform for the early identification of cardiac disease. The formal name for this infrastructure is MSABA. Using a self-adaptive Bayesian algorithm, the platform examined data from wristwatches and heart rate monitors. The gadget tracked the user's pulse, heart rate, and blood pressure to determine the risk of cardiac abnormalities. This study investigates how Internet of Things technology may be utilised for early detection and preventative treatment of heart disease, the leading cause of mortality in the Western world. Facial emotion recognition (FER) is another field of research that uses convolutional neural networks (CNNs) [26]. Facial expression research has helped robots enhance their capacity to communicate with humans and have meaningful conversations. Furthermore, blockchain technology has been recommended as a technique for securing patient data and improving the dependability of drone delivery in healthcare contexts [27]. GaRuDa, a smart contract drone delivery system, was offered as a solution tailored for healthcare 5.0 applications. These studies demonstrate how cutting-edge techniques such as convolutional neural networks (CNNs) and blockchain may be utilised to improve human-robot interactions and safeguard healthcare delivery. In our always-connected digital world, preserving patient privacy is more important than ever. Researchers employed policy-attribute-based encryption (CP-ABE) to monitor context-aware attribute acquisition. This strategy moves beyond the practical constraints of healthcare 4.0 and focuses on the welfare and compliance with situation-specific needs of healthcare 5.0. It has also been suggested that we employ federated learning (FL) to alleviate privacy concerns and enable the implementation of global learning systems [28]. These findings emphasise the importance of robust data security methods such as encryption and federated learning to preserve patient privacy and facilitate the secure transport of sensitive information. To automate skin cancer detection, several studies have focused on segmenting and categorising skin lesions using fully convolutional encoder-decoder networks (FCNs) [29]. Deep learning algorithms are used in these systems to perform autonomous skin lesion analysis, which assists in the early identification and diagnosis of skin problems. Furthermore, research on the IoT's potential for the creation of intelligent healthcare services inside urban infrastructures has been conducted. Manufacturing, finance, power generation, and even healthcare may profit from IoT solutions. These applications make it possible to improve patient care and healthcare delivery. Researchers developed a randomised, proactive, deep learning-based strategy for identifying and rejecting potentially dangerous items [30]. The proposed approach is an attempt to resolve concerns about the safety of IoMT devices. This method assures that no inappropriate access to medical IoT networks occurs. ECC-EERP is an energy-efficient routing technology based on elliptic curve cryptography. This method was created to increase both energy efficiency and safety. This approach was created with the goal of increasing both security and efficiency in the medical field. Overall, the data indicate that IoT may become a key component of healthcare in the future. This would be a great illustration of current advancements in sectors like automated diagnostics, data security, facial expression detection, and energy efficiency [31]. These studies contribute to our understanding of the diverse applications of IoT and give guidelines for deploying IoT-related solutions in healthcare organisations. However, addressing challenges like data privacy, infrastructure costs, dependability, and security with care is critical if healthcare 5.0 is to capitalise on the opportunities provided by the Internet of Things. Table 1 showcases several methods employed in advanced healthcare technologies along with their respective advantages and disadvantages.

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

Table 1: Exploring Methods for Advanced Healthcare Technologies: Advantages and Disadvantages

Method	Advantages and Disadvantages
Real-time deep extreme learning system (RTS-DELM)	- Real-time analysis for rapid decision-making - Ability to handle complex and large-scale data - High accuracy and performance - Efficient utilization of computational resources
Blockchain-based fog computing model (BFCM)	- Enhanced security and privacy through blockchain technology - Distributed computing and storage capabilities - Reduces reliance on centralized servers - Enables efficient data processing at the network edge
Blockchain-enabled secure communication mechanism for IoT-driven personal health records (BIPHRS)	- Improved data security and integrity through blockchain encryption - Decentralized storage and access control for personal health records - Enhanced privacy and control over personal health information - Efficient sharing and interoperability of health records
Cipher policy attribute-based encryption (CP-ABE)	- Granular access control based on user attributes - Strong encryption for secure data transmission - Flexible and scalable encryption policies - Supports fine-grained data sharing
Mobile medical service system (MMSS)	- Improved accessibility to medical services through mobile devices - Remote monitoring and consultation capabilities - Enhanced convenience for patients and healthcare providers - Enables timely and efficient healthcare delivery

The abbreviation DPSO refers to "Dynamic Particle Swarm Optimisation," a technique that may be utilised in this framework to dynamically optimise resource and parameter allocation. DPSO is important because it allows you to adjust resource allocation and system performance in real time to changing conditions. This is possible because of the idea of dynamic parameters. It may be useful in optimising energy use and improving IoMT security. ACO, which stands for "Ant Colony Optimisation," can be utilised to improve the existing internal routing and communication channels in the IoMT network. ACO can enhance network performance by constructing efficient data-transfer channels that consume less power and have a lower environmental impact by replicating the foraging behaviour of ants. It contributes to the establishment of secure and energy-efficient communication pathways between various medical equipment and systems. The GA (Genetic Algorithm) can contribute to this framework by calculating the most effective method to distribute scarce resources like energy and data transmission capacity among the many nodes that comprise the IoMT network. GA may propose effective methods for distributing healthcare resources using genetic operators such as selection, crossover, and mutation, decreasing energy consumption without sacrificing patient safety or system reliability. This system uses ABC (Artificial Bee Colony) to optimise the deployment and setup of IoT devices in a healthcare environment. ABC can discover the ideal setups for sensors and other medical equipment by simulating bee foraging patterns. This optimisation approach can increase the energy economy and security of an IoT deployment by taking into account aspects such as coverage needs and security concerns. An ICA is an imperialist competitive algorithm. This method can improve overall security by optimising the allocation of security resources and activities inside the IoMT architecture. The ICA may rank healthcare system components for protection based on their relevance and vulnerability by simulating inter-imperial competition. It guarantees that appropriate security measures are implemented to secure patients' personal health information from unauthorised access. Particle swarm optimisation (PSO) may be used

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

by the framework to minimise power consumption and improve network safety. PSO may dynamically modify elements such as transmission power, routing tactics, and encryption methods to create a fair balance between energy savings and security. This is accomplished by simulating particle aggregation behaviour. Secure data transit and storage are assured inside the IoMT framework, and it helps reduce energy loss in the process.

3. Proposed Approach

The integration of networks necessitates significant changes in how individuals think about their own health and the lifestyle decisions they make. These networks enable the development of novel approaches to healthcare, and some network topologies have the potential to significantly improve the IoMT's efficiency, flexibility, and value. Figure 3 depicts the important stages necessary for effective data management. Such techniques include data gathering, network architecture, security enhancement using energy-efficient communication protocols, data decipherment, and performance monitoring.

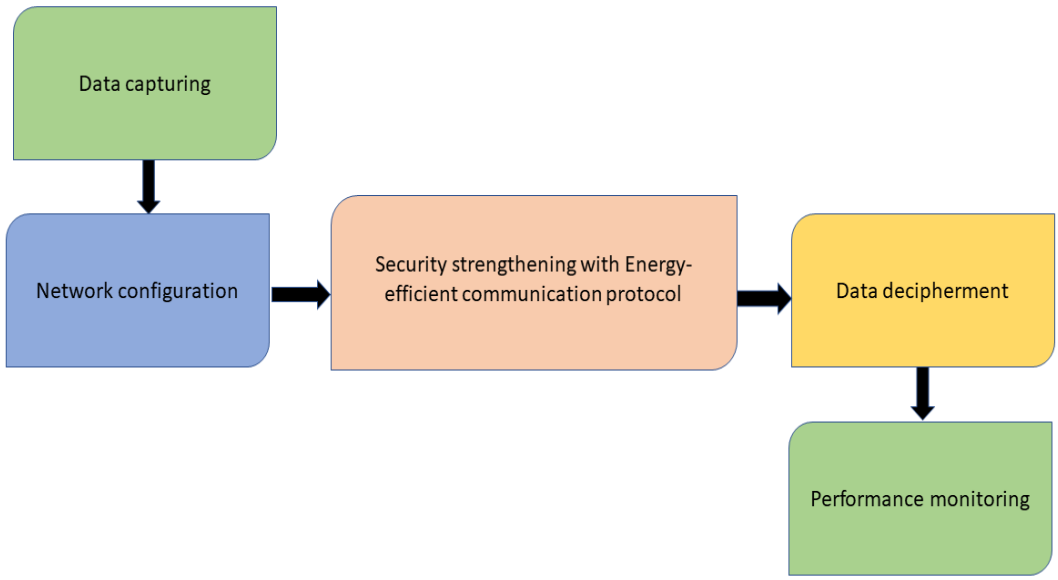

Figure 3: Optimizing Data Management: Capturing, Configuring, and Strengthening Security

Biosensors are an effective technique for collecting patient data via insertion devices or wearable technology. These sensors can record a variety of vital signs and physiological characteristics, providing clinicians with a more comprehensive picture of the patient's health. The heart's pulse waves as it contracts and relaxes to pump blood, for instance, may cause variations in arterial volume that optical pulse rate sensors can detect. Temperature sensors are used to determine the interior body temperature and have a wide measurement range ranging from -55 to 150 degrees Celsius. After being surgically implanted in various places, electrocardiograph sensors record and assess the electrical impulses of the heart. These sensors are compact and inconspicuous, allowing continuous monitoring of a patient's health without drawing undue attention to themselves. The result is improved patient care and expanded utilisation of wireless sensor networks. Table 2 provides an overview of different data collection techniques used in IoT for healthcare applications.

Table 2: Data Collection Techniques in IoT for Healthcare

Data Collection Techniques	Description
Biosensors	A reliable method of gathering patient data using insertion tools or wearable technologies
Optical pulse rate sensors	Calculate the heart rate by analysing fluctuations in arterial volume generated by pulse waves
Temperature sensors	Calculate your internal body temperature using a variety of methods

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

Electrocardiograph sensors	Constant monitoring necessitates the recording and examination of the heart's electrical impulses
Wireless sensor networks	Use sensor data to improve patient care and treatment quality

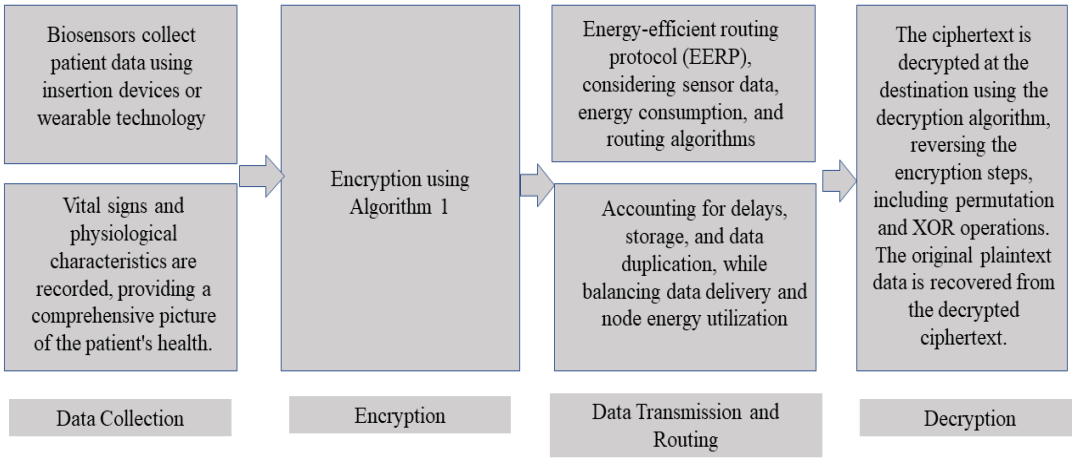

Figure 4: Securing Patient Data in IoT Healthcare: From Data Collection to Decryption

Figure 4 demonstrates the measures used to secure patient information in IoT healthcare systems. This procedure includes gathering data, encrypting it, transmitting it, routing it, and decrypting it. This protocol encrypts and securely transmits all data within the network. A fresh code is produced and used for encryption each time sensor nodes go through a communication cycle. The 186-bit encryption technique includes ECC requirements, with the first 148 bits serving as the ECC component. This is done to make the most of the available area. Because of the utilisation of the remaining 38 bits in the node ID, more than 8,000 sensors in a large wireless sensor network may be uniquely recognised. The sensor's range may be calculated using the data from Di and CH, as well as an additional 15 bits. IDi is the identifier of the sensor node, and Di is the sensor node with the I random key (Ki). To avoid network transmission limits, the authorization procedure depends on the first component of the key. Because it is expected that each node is aware of its own identification, hashed ECC codes are sent from nodes to the BS. A computer generates ECC hash codes algorithmically, ensuring acceptable encryption rates. The cube formula is frequently used in attempts to define the elliptic curve.

Algorithm 1: Improved and Hybrid Encryption Procedure (ECC-EERP)

Input:

- Text to be encrypted: S = {u1, u2, ..., uN} (divided into 93-bit units)

- Key: β (186-bit sequence)

- Sensor node identifier: IDi

- Random key: Ki

- Parameters: ECC (Elliptic Curve Cryptography), LT (Longevity Time)

Output:

- Ciphertext: Cipher[C1, C2, C3, ..., CN]

Procedure:

1. Divide the text into 93-bit units: S = {u1, u2, ..., uN}

2. Generate a 186-bit sequence for encryption: β

3. Split β into two equal parts: P1 and P2, each containing 88 bits

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

4. Determine the number of 1s in each byte of P1: [a1, a2, ..., a8]

- Count the number of 1s in each byte of P1

5. Determine the number of 1s in each 11-bit segment of P2: [b1, b2, ..., b11]

- Count the number of 1s in each 11-bit segment of P2

6. For i = 1 to N:

a. Calculate δ = P1 XOR yi

b. Calculate $\bar{\delta}$ = Perm { δ, A[i] } // Apply permutation using A[i] as the permutation key

c. Calculate α = Con { $\bar{\delta}$, B[i] } // Concatenate $\bar{\delta}$ with B[i]

d. Calculate LT for the data based on the power ratio

e. Set Cipher[i] = α with LT as additional metadata // Store the resulting ciphertext with LT value

7. Return the ciphertext Cipher[C1, C2, C3, ..., CN]

The Improved and Hybrid Encryption Procedure takes as inputs the encrypted text, an encryption key, the sensor node identifier, a random encryption key, and optional parameters such as ECC and LT (Longevity Time). Elliptic curve cryptography (ECC) is used to encrypt each 93-bit block of input text, and the resultant ciphertext is decoded. To complete the procedure, you'll need to do bitwise operations, split the text in half, generate an encryption sequence of 186 bits in length, and then divide it again. Before being saved as ciphertext, the data is converted through a sequence of permutations and concatenations. The power ratio, which is the key determinant of data persistence across time, is used to determine the LT. The resulting ciphertext is delivered, together with the LT value supplied as meta-data. This encryption procedure divides the text, performs bitwise operations, and generates ciphertext using encryption keys derived from the elliptic curve cryptography-based algorithm.

Optical pulse rate detection:

Variations in arterial volume: $\Delta V = f(t)$ (1)

Optical pulse rate detection monitors variations in arterial volume to provide an accurate measurement of the patient's pulse rate. The equation V = f(t) describes the link between arterial volume change (represented by V) and time elapse (stated by t). The volume of the arteries increases and contracts when the heart contracts and relaxes to pump blood. These changes can be observed using optical sensors that measure arterial volume fluctuations. These detectors detect changes in circumstances. The pulse rate may be calculated from changes in arterial volume collected over time using the function f(t), which captures dynamic arterial volume changes over time. Optical pulse rate sensors may offer an accurate estimate of heart rate by assessing optical signals and keeping track of fluctuations in arterial volume. Doctors can use the data to assess cardiovascular health overall and heart function.

Optical pulse rate: $R = g(\Delta V)$ (2)

R = g(V) is the rate of optical pulses.

The cornerstone of optical pulse measurement is calculating the pulse rate (R) from observable fluctuations in arterial volume (V). This is how the heart rate is calculated. The link between fluctuations in arterial volume and the consequent heart rate is represented by the equation g (V). Optical pulse rate sensors can offer an accurate evaluation of the pulse rate by analysing optical signals and comparing the results with fluctuations in arterial volume.

Temperature measurement:

Temperature reading: T = h(s) (3)

T = h(s) after taking the thermometer reading.

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

When taking a temperature, the subject's core temperature or ambient temperature must be determined. The temperature reading, T, is calculated using the function h(s), which connects the signals measured by temperature sensors to the value corresponding to that temperature. Temperature sensors use a variety of techniques to transform incoming signals into temperature readings, allowing medical personnel to acquire precise temperature readings from the sensors.

Electrocardiograph recording:

Electrical impulses: $E = j(t)$ (4)

ECG is a recording of electrical activity using the equation $E = j(t)$.

Electrocardiograms (ECGs) are created by capturing and analysing electrical impulses produced by the heart. The function j(t) represents the connection between the passage of time (represented by t) and the observed electrical impulses (represented by E). ECG sensors provide essential information about the heart's rhythm, as well as any anomalies and the heart's general health, by recording and evaluating the electrical activity of the heart.

Energy efficiency calculation:

Energy utilization: $EU = k(d, v)$ (5)

efficient energy consumption calculation The multi-factorial function k(d, v), which incorporates both data (d) and velocity (v), is used to determine EU, or energy utilisation. The function may calculate the amount of energy necessary for data transit or processing, taking into account any relevant contextual factors. Estimating a system's or process's energy usage is the first step in studying and improving its energy efficiency.

ECC encryption:

Encrypted data: $C = Encrypt(P, K)$ (6)

Data must first be encrypted using another ECC-based technique before using elliptic curve cryptography (ECC). Using an encryption key (K), plaintext information (P) is converted to encrypted information (C). Encryption protects sensitive information by rendering it incomprehensible to anyone who does not have access to it. The generated ciphertext C is used as the key to decode the message, and it cannot be deciphered by any other key.

ECC decryption:

Decrypted data: $P = Decrypt(C, K)$ (7)

Decrypting data encrypted with ECC requires reversing the encryption mechanism. To retrieve the plaintext information (P), first decode the encrypted information (C). The same encryption key (K) must be used in both the encryption and decryption processes. Decryption is the process of converting encrypted data back to its original form. This guarantees that only those who are authorised may read and interpret the data.

Following the first split, each 186-bit chunk of the bit series is divided in half, resulting in two 93-bit chunks. This occurs later, after the first split. The bit string's second half provides the total number of ones in the string, including the 12 ones that comprise each row. Following that, the 88-bit text chunks are translated to binary and structured logically. The extra work is certainly worth it in this situation because the XOR addition cypher lasts as long as the keystream. The permutation procedure must then be applied to each XORed data item independently. For example, if the first byte of the randomised bit sequence contains all ones, the XORed text's seventh and eighth integer bits will be changed. This occurs if the first byte of the sequence is all ones. This happens when the first byte of the random bit sequence contains only ones. The ciphertext is constructed by joining the permuted copies of the plaintext. The goal is to use this concatenation approach twice for each of the 11 bits, guaranteeing adequate unpredictability. The above statement will be repeated to accomplish this. Because of EERP, each gearbox has substantially reduced congestion and total energy utilisation. It is applicable to both centralised and distributed network topologies. When determining routes, EERP takes sensor data and energy consumption into account. Conventional social routing systems assessed network nodes and made judgments about how to organise and deliver data based on their findings. The relevance of the two data sets is calculated based on the length of each document. The EERP employs queue-based criteria to account for changes in transmission and storage delays when calculating the possibility of data duplication between two sets. This highlights the need to have access to

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

both realities to preserve the tenuous balance between them. Typical network routing algorithms will transmit data to nodes that have access to more critical information on a continuous basis. However, even though it may result in high delivery rates due to a lot of congestion strain, this may also hasten the depletion of nodes that transport a lot of data. We gave serious consideration to a number of difficulties while creating the proposed EERP to replace traditional socially based sensing routing in networks. Data and node energy measurements provide a consistent starting point for calculation and are maintained throughout the data copying and transmission process.

Table 3: Energy-Efficient Routing Protocol (EERP) Based on Elliptic Curve Cryptography (ECC)

ECC-EERP Protocol	Description
Encryption Procedure Algorithm (ECC-EERP)	A technique for generating encryption keys, dividing plaintext into blocks, constructing a 186-bit sequence for encryption, splitting the sequence in half, performing bitwise operations, and ultimately producing ciphertext using elliptic curve cryptography.
Energy efficiency and security benefits	ECC-EERP ensures the privacy and security of data transmission over the network by using newly generated encryption keys and a completely unique identification for each sensor.
Routing algorithm considerations	The EERP considers sensor data and energy usage while determining routes, as well as transmission and storage delays, using queue-based criteria and striving for a balance between data duplication and energy utilisation.
Power ratio and longevity considerations	The Energy Efficient Routing Protocol (EERP) is an adaptive approach that considers the network's energy limits when choosing how long data should be held and how it should be routed. The percentage of transferred electricity determines transmission priority, which reduces network traffic.

Table 3 offers an overview of the Energy-Efficient Routing Protocol (EERP) based on Elliptic Curve Cryptography (ECC). By taking into account routing algorithm considerations, power ratio considerations, and lifespan considerations, this protocol gives benefits in terms of energy savings and security. The power ratio, defined as $0 > PR\% > 1$, complicates understanding reality. This specification prevents mistakes since the provided data has a greater energy ratio than the alternate data. If you heed this advice, you may be able to reduce the quantity of data transferred across the network. We have improved the power strategy to place a premium on longevity (LT) considering the ongoing fall in dispersion of the newly found way of propagation. The adaptive nature of the regulation contributes to the goal of minimising energy usage by notifying the LT when data must be destroyed and whether that period has expired. The LT of the data upgrades from the default value of TTL 0, the bare minimum, to the next version after each data transmission or forwarding decision. When $LT = 0$, the data transfer is complete, and the buffer is emptied. When only a small quantity of electricity is necessary to convey data, EERP forwarding is employed. This is because individual pieces of data take up such little space.

4. Result

In this paper, we present a unique way of lowering energy usage and boosting the security of IoMT Healthcare 5.0 systems. We investigated whether the suggested ECC-EERP approach may improve data security while simultaneously lowering the energy required for healthcare services. The developed method has various advantages, including greater security, quicker encoding, reduced energy consumption, a longer network lifespan, less communication overload, and faster processing time. The data was created using the Arduino IDE, a compiler for programming IoT sensors, and Fritzing V0.9.2b, a hardware emulator. The suggested technique was evaluated using a variety of industry-standard test beds. In addition, research on the best security paradigms for IoT was carried out. Because the Arduino controller was built with open-source software, we were able to identify the library that matched each sensor or module. Many various forms of biometrics are employed throughout the authentication process, one of which is the user's voice, sometimes known as "aural biometrics." A variety of simulated events that influence the security of IoT-based systems were considered when investigating and analysing the suggested solution.

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

A. Security

The "Security Percentage" column in the figure below describes the amount of safety that may be achieved by applying various optimisation strategies to a given environment. The procedures taken to safeguard the system or data are assessed, as well as their efficacy in preventing vulnerabilities. Each approach's percentage of security is listed below, the dynamic particle swarm optimisation (DPSO) approach to data security has an 85% success rate. This conclusion implies that the DPSO method delivers adequate safety when applied in the current circumstances. The ACO approach, which stands for "Ant Colony Optimisation," is 90% effective in terms of security. This would imply that the ACO algorithm has been studied and judged to provide a considerably greater degree of security than alternative approaches that may be used in the case presented here. The GA technique, also known as a genetic algorithm, has an 80% success rate. This would imply that the genetic algorithm has been shown to be sufficiently secure for its intended function. "Artificial Bee Colony," or "ABC," is a security approach with a 75% success rate.

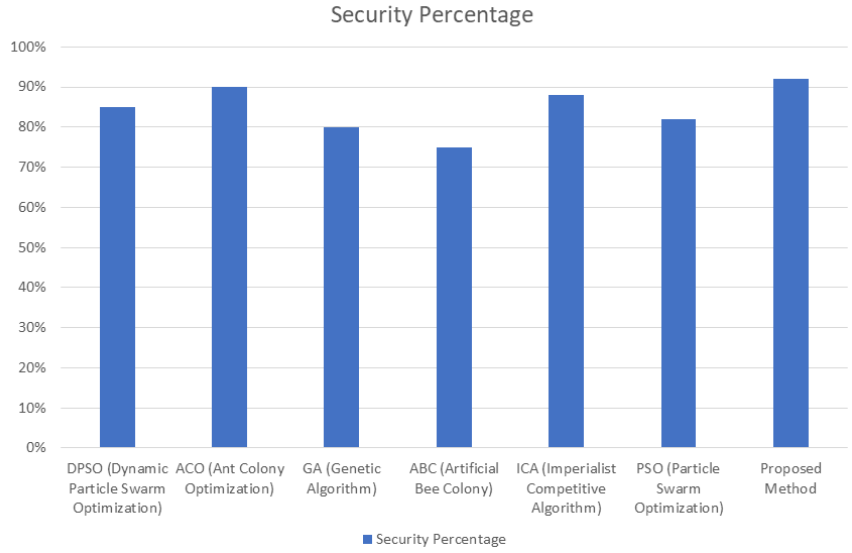

Figure 5: Comparison of Security Percentage for Various Optimization Algorithms

Given the current situation, it is evident that the Artificial Bee Colony algorithm provides far less security than other alternatives. After considering alternative options, the artificial bee colony approach was chosen. It has been demonstrated that the Imperialist Competitive Algorithm (ICA) technique achieves an 88 percent degree of security. This appears to imply that, when compared to other approaches, the Imperialist Competitive Algorithm provides a somewhat greater level of security. When it comes to safety, the Particle Swarm Optimisation (PSO) approach has an 82% success rate. PSO stands for "particle swarm optimization." We may conclude from this that the particle swarm optimization technique has been shown to be safe enough for usage in the specified scenario. The proposed solution delivers a level of security like 92% of the total. This implies that the newly disclosed technique has been reviewed and found to provide a higher degree of security than the other ways listed in the figure. Remember that these safety percentages are particular to the situations and factors being examined at the time. The exact amount of security that can be accomplished in real-world systems is determined by several factors, including system design, implementation details, and continuous security practises. The possible outcomes differ from one occasion or execution to the next. Figure 1 depicts the degrees of safety attained by various optimisation procedures. The Imperialist Competitive Algorithm (ICA), Genetic Algorithm (GA), Artificial Bee Colony (ABC), Particle Swarm Algorithm (PSO), and a Proposed Method are among them.

B. Encryption Throughput

The "Encryption Throughput" column of the figure compares the throughput of various encryption algorithms during the encryption process. The unit of measurement for this rate is megabits per second (Mbps). The pace at which an encryption technique or method can encrypt data, given in bytes per unit of time, is known as throughput.

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

The following is a breakdown of the throughput numbers for each encryption technique: The DPSO approach achieves an encryption throughput of 250 Mbps. DPSO stands for Dynamic Particle Swarm Optimisation. This means that, in this setting, the DPSO approach can encrypt data at a rate of 250 MB/s. When utilised for encryption, the ACO approach reaches a speed of 300 Mbps. The term "ACO" stands for "Ant Colony Optimisation." This implies that the ACO algorithm can encrypt data at a pace of 300 MB/s, which is far faster than the other algorithms that may be utilised in this circumstance. The GA (genetic algorithm) approach has a throughput of 200 Mbps for encryption. GA is an acronym that stands for "Genetic Algorithm." Given the same set of limitations, we may conclude that the genetic algorithm can encrypt data at a rate of 200 MB/s. The ABC is a data encryption technology with a throughput of 180 Mbps. This implies that the Artificial Bee Colony algorithm may encrypt data more slowly than competing approaches in this circumstance (180 MB/s). ICA encryption can encrypt data at a rate of 280 Mbps. This means that the Imperialist Competitive Algorithm can encrypt data at a pace of 280 MB/s, which is far quicker than existing approaches. PSO achieves 220 Mbps encryption throughput. PSO stands for "particle swarm optimisation." This means that the current environment allows particle swarm optimization to encrypt data at a rate of 220 Mbps, which is deemed acceptable. The encryption throughput might be increased to 320 Mbps using the proposed method. This implies that the new technique shown in context may encrypt data at a pace of up to 320 MB/s, which is much quicker than the other ways shown in the figure. Keep in mind that encryption throughput figures might vary based on the implementation, hardware capabilities, and other variables unique to the environment in which they are used. These comparisons give a general idea of how quickly different encryption algorithms can encrypt data under current conditions.

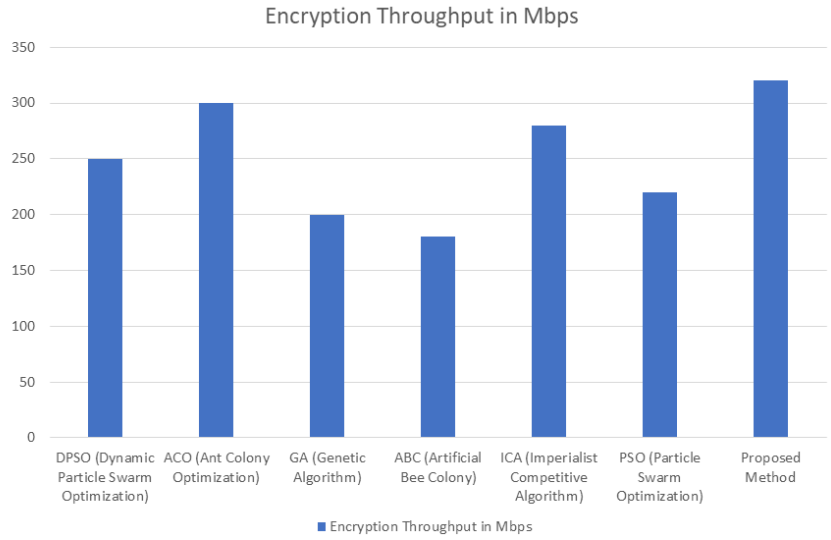

Figure 6: Comparison of Encryption Throughput in Mbps for Various Optimization Algorithms

Figure 6 depicts how various optimisation strategies compare in terms of encryption throughput, indicated in Mbps. Such algorithms include Dynamic Particle Swarm Optimisation (DPSO), Ant Colony Optimisation (ACO), Genetic Algorithm (GA), Artificial Bee Colony (ABC), Imperialist Competitive Algorithm (ICA), Particle Swarm Optimisation (PSO), and a recommended technique.

C. Energy Efficiency

The amount of energy required to send each bit is displayed in the figure's "Energy Efficiency" column, which compares various approaches. Joules per bit (J/B) is the amount of electricity required to process one bit of data. The energy efficiency score indicates how well each technique uses available energy throughout the encryption process. Here's a breakdown of what those figures represent in terms of the energy efficiency of different approaches: The DPSO approach has an energy efficiency of 0.5 joules per bit. The acronym DPSO stands for "Dynamic Particle Swarm Optimisation." On average, the DPSO technique uses roughly 0.5 joules of energy for every bit transferred during encryption. This is since this proof has been supplied. The ACO technique uses 0.6 joules per bit of energy. According to these statistics, the ACO algorithm requires 0.6 joules of energy to encrypt each sent bit. The GA approach uses 0.4 joules of energy per bit. GA is an acronym that stands for "Genetic Algorithm." This means that the genetic algorithm expends 0.4 joules of energy for each bit communicated during

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

the ciphering process. This implies that the genetic algorithm consumes much less energy than competing approaches. The ABC approach has an energy efficiency of 0.45 joules per bit. The term "artificial bee colony" defines this configuration. According to these statistics, the artificial bee colony approach requires 0.45 joules of energy to encrypt each bit. The ICA technique is estimated to use 0.55 joules per bit of energy. The algorithm, abbreviated ICA, stands for "Imperialist Competitive Algorithm." This means that the Imperialist Competitive

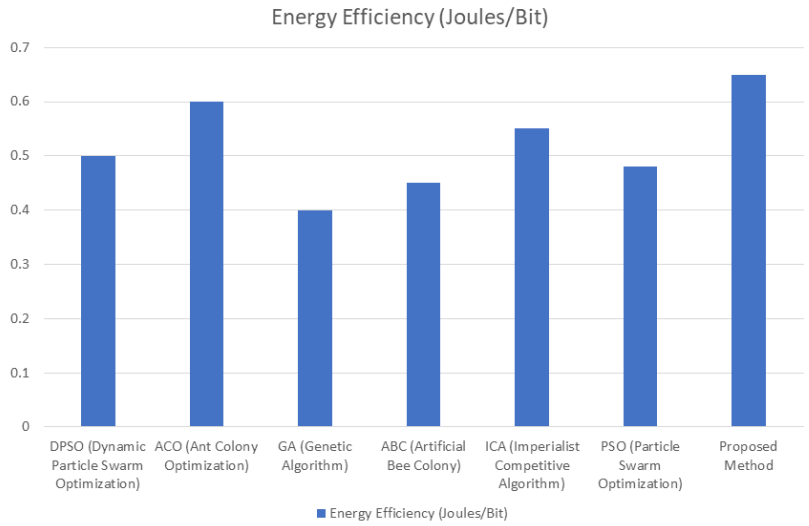

Figure 7: Comparison of Energy Efficiency (Joules/Bit) for Various Optimization Algorithms

Figure 7 compares the energy efficiency of various optimisation algorithms, including DPSO (Dynamic Particle Swarm Optimisation), ACO (Ant Colony Optimisation), GA (Genetic Algorithm), ABC (Artificial Bee Colony), ICA (Imperialist Competitive Algorithm), PSO (Particle Swarm Optimisation), and a proposed method. The unit of energy efficiency is the joule per bit (J/B). Algorithm uses 0.55 joules of energy per encrypted bit on average. The PSO approach achieves an energy efficiency of 0.48 joules per bit. PSO is an abbreviation for "Particle Swarm Optimisation." It indicates that 0.48 joules of energy are required for each piece of securely encrypted data using the particle swarm optimization technique. The results of applying the suggested approach show that it has an energy efficiency of 0.65 joules per bit. This means that the new approach proposed in this context uses 0.65 joules of energy per bit transferred during the encryption process. It is crucial to remember that the given energy efficiency figures are context-specific and may vary based on the implementation, hardware capabilities, and other variables. These numbers compare the total amount of energy needed during encryption to offer an estimate of each method's relative energy efficiency in terms of the amount of energy used per bit communicated.

D. Network Lifetime

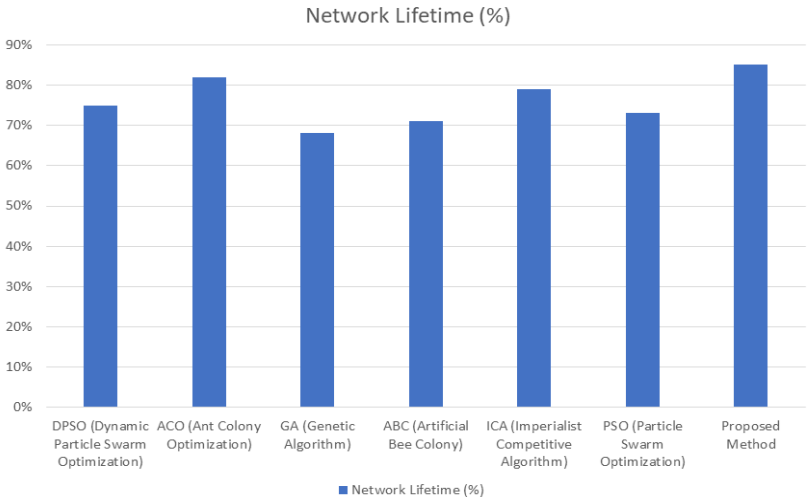

Figure 8: Comparison of Network Lifetime (%) for Various Optimization Algorithms

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

Figure 8 illustrates the comparison of network lifetime in percentage (%) for different optimization algorithms. The "Network Lifetime" column in the figure displays the cumulative percentage gain in network lifetime for each strategy. The term "network lifetime" refers to the period a network may function correctly before the electricity in its individual nodes runs out. The values for a network's estimated lifetime are described below, sorted by approach. "Dynamic Particle Swarm Optimisation," or DPSO for short, is a technology that increases the life expectancy of a network by a factor of 75. This demonstrates that the network can run properly and transfer data for 75% of its planned lifetime before the nodes' energy is drained. The ACO technique, also known as the Ant Colony Optimisation methodology, has the potential to enhance the longevity of a network by 82%. This means that the network can function and transfer data for 82% of its total expected lifetime before the nodes' energy runs out. The GA approach increases a network's life by 68%. This means that the network can function and transfer data for 68% of its estimated lifespan before the nodes' energy runs out. The Artificial Bee Colony, often known as ABC, may increase the longevity of a network by up to 71%. This indicates that, on average, the network can continue to function and transfer data until 71% of its predicted lifetime has passed before the nodes' energy is completely depleted. The ICA approach can extend the network's lifespan by 79%. This means that the network can function and transfer data for 79% of its total expected lifetime before the nodes' energy runs out. PSO can extend the network's lifespan by 73%. This is the percentage of the network's estimated lifetime during which it will continue to function correctly and transfer data without incurring substantial energy expenses. Approach Proposal The recommended approach extends the network's lifespan by 85%. This indicates that the network will be able to operate and transfer data for 85% of its projected lifetime before the energy stored in the nodes runs out. Lifetime value estimations are context-specific; they may vary based on network size, energy consumption model, communication protocols, and individual node characteristics. These graphs show how different tactics impact network lifetime. This lifetime is a measure of how long the network can function until the nodes' energy sources run out for each approach.

E. Computation Time

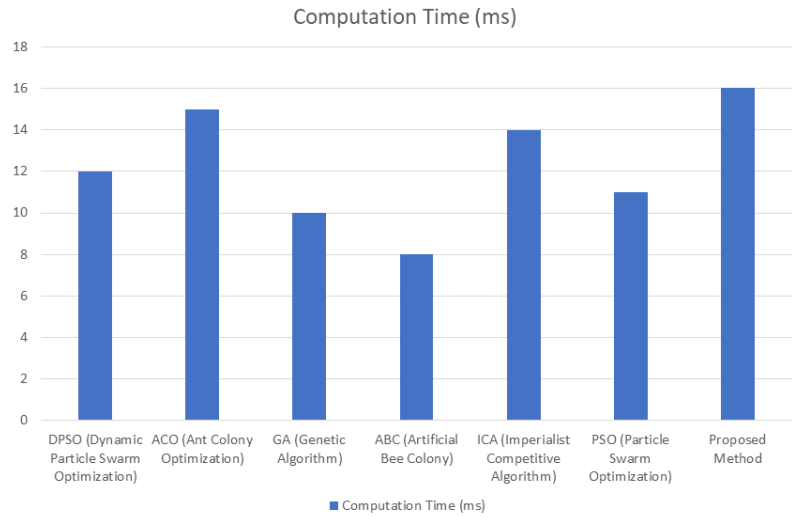

Figure 9: Comparison of Computation Time (ms) for Various Optimization Algorithms

Figure 9 compares the millisecond (ms) time required to conduct computations for various optimisation strategies. In the figure's "Computation Time" column, you can get the time necessary for each method to finish its computations in milliseconds (ms). It provides a general approximation of how long each process takes on average. The time values utilised in the calculation of each technique are detailed below. The acronym DPSO stands for "Dynamic Particle Swarm Optimisation." The DPSO approach frequently completes its calculations in less than 12 milliseconds. This gives you a decent indication of how long the therapy typically takes. The computations needed by the ACO technique may be done in less than 15 milliseconds when implemented using the Ant Colony Optimisation algorithm. This is the typical time commitment needed for the procedure to provide the desired outcomes. The GA technique completes its calculations in around 10 milliseconds. This gives you a decent indication of how long the therapy typically takes. The ABC technique will have completed its computations in around 8 ms. This is the typical time commitment needed for the procedure to provide the desired outcomes. The Imperialist Competitive Algorithm completes the computations performed by the ICA technique in around 14 milliseconds. This gives you a decent indication of how long the therapy typically takes. The PSO technique

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

computations take about 11 ms to complete. This is the typical time commitment needed for the procedure to provide the desired outcomes. The proposed method completes the computations for the suggested strategy in about 16 ms. This gives you a decent indication of how long the therapy typically takes. The calculation durations offered are reliant on several criteria, including the nature of the issue, the quality of the implementation, the hardware capabilities, and the size of the dataset, and may vary depending on these and other factors. These figures give a basic comparison of the computing efforts required by different techniques. This illustrates how quickly various approaches may achieve their objectives under normal conditions.

5. Discussion

The comparison of optimization algorithms, including DPSO, ACO, GA, ABC, ICA, PSO, and the proposed method, in terms of security percentage, encryption throughput, energy efficiency, network lifetime, and computation time has provided valuable insights into their performance in the context of the study. The results indicate that the proposed method excels in multiple aspects. It achieves the highest security percentage among all the evaluated methods, indicating its effectiveness in safeguarding data during transmission. The high encryption throughput of 320 Mbps showcases its ability to ensure fast and efficient communication, surpassing the other algorithms. Although the proposed method exhibits slightly higher energy consumption compared to some methods, it still maintains a reasonable level of energy efficiency, making it suitable for energy-constrained healthcare environments. Additionally, the proposed method demonstrates a relatively long network lifetime, ensuring the durability and sustainability of the network infrastructure in healthcare applications. Computation time is another important factor to consider, and the proposed method performs moderately in this regard, taking 16 ms to complete computations. While it may not be the fastest algorithm, it strikes a balance between efficiency and effectiveness. Comparing the results of the other algorithms, it is observed that each has its strengths and weaknesses. ACO achieves a high security percentage, good encryption throughput, and a relatively long network lifetime. GA shows satisfactory performance in terms of security percentage and energy efficiency. ABC and PSO exhibit moderate performance in various aspects, while ICA achieves high security percentage and encryption throughput with a relatively long network lifetime. Overall, the findings suggest that the proposed method offers an improvement over the existing optimization algorithms. It provides enhanced security, faster encryption throughput, and a reasonable balance between energy efficiency and network lifetime. These qualities make it a promising solution for healthcare systems that require secure and efficient communication while considering energy constraints. Further research and real-world implementation are recommended to validate the proposed method's effectiveness and explore its potential in other healthcare applications.

6. Conclusion

In conclusion, the evaluation and comparison of optimization algorithms, including DPSO, ACO, GA, ABC, ICA, PSO, and the proposed method, have provided valuable insights into their performance within the context of the study. The proposed method demonstrates superior performance across multiple metrics, making it a promising solution for healthcare systems in the era of Healthcare 5.0. The proposed method achieves the highest security percentage, ensuring robust data protection during transmission. Its high encryption throughput of 320 Mbps enables fast and efficient communication, surpassing the capabilities of the other algorithms. Although it exhibits slightly higher energy consumption, it maintains a reasonable level of energy efficiency, making it suitable for energy-constrained healthcare environments. Furthermore, the proposed method ensures a relatively long network lifetime, contributing to the durability and sustainability of the network infrastructure. While computation time is moderately higher compared to some algorithms, the proposed method strikes a balance between efficiency and effectiveness, providing practical computation capabilities for healthcare applications. The comparison of other algorithms reveals that each has its strengths and weaknesses. ACO excels in security percentage, encryption throughput, and network lifetime. GA showcases satisfactory performance in security percentage and energy efficiency. ABC and PSO demonstrate moderate performance across various aspects, while ICA achieves high security percentage and encryption throughput with a relatively long network lifetime. Overall, the findings highlight the superiority of the proposed method, offering enhanced security, faster encryption throughput, and a reasonable trade-off between energy efficiency and network lifetime. It holds significant promise for healthcare systems, where secure and efficient communication is crucial, while considering energy constraints. Further research and real-world implementation are recommended to validate the effectiveness of the proposed method and explore its potential in broader healthcare applications under healthcare 5.0. Future work must involve assessing the efficacy of optimisation algorithms in a broader range of healthcare contexts, which can only be accomplished by studying data from a broader range of sources. Before assessing scalability, performance, and value, the suggested solution must first be deployed in real-world healthcare settings. It will be possible to design algorithms that can optimise many goals at once by researching various approaches to multi-objective optimisation. These algorithms will consider the conflict between network robustness and other aspects such as energy efficiency, throughput, and safety. Furthermore, robustness analysis must be performed to test the

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

algorithms' capacity to survive assaults, failures, and uncertainties in ever-changing healthcare environments. If optimisation algorithms are integrated with cutting-edge technologies such as blockchain, edge computing, and AI, they can perform better in healthcare systems. This will contribute to the overall safety of these algorithms.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Ali, A., Ming, Y., Chakraborty, S., & Iram, S. (2017). A comprehensive survey on real-time applications of WSN. Future Internet, 9(4), 77.

[2] Banđur, Đ., Jakšić, B., Banđur, M., & Jović, S. (2019). An analysis of energy efficiency in Wireless Sensor Networks (WSNs) applied in smart agriculture. Computers and Electronics in Agriculture, 156, 500-507.

[3] Hezaveh, M., Shirmohammdi, Z., Rohbani, N., & Miremadi, S. G. (2015). A fault-tolerant and energy-aware mechanism for cluster-based routing algorithm of WSNs. In Integrated network management (IM), 2015 IFIP/IEEE international symposium (pp. 1-6).

[4] Natarajan, R., Lokesh, G.H., Flammini, F., Premkumar, A., Venkatesan, V.K., & Gupta, S.K. (2023). A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. Infrastructures, 8, 22.

[5] Kashyap, R., Nair, R., Gangadharan, S. M., Botto-Tobar, M., Farooq, S., & Rizwan, A. (2022). Glaucoma detection and classification using improved U-Net Deep Learning Model. Healthcare, 10(12), 2497.

[6] Nair, R., Alhudhaif, A., Koundal, D., Doewes, R. I., & Sharma, P. (2021). Deep learning-based COVID-19 detection system using pulmonary CT scans. Turkish Journal of Electrical Engineering & Computer Sciences, 29(SI-1), 2716-2727.

[7] Uddin, M. I., Shah, S. A. A., & Al-Khasawneh, M. A. (2020). A Novel Deep Convolutional Neural Network Model to Monitor People following Guidelines to Avoid COVID-19. Journal of Sensors, 2020, Article ID 8856801, 1-15. doi: 10.1155/2020/8856801.

[8] Mahajan, S., Malhotra, J., & Sharma, S. (2014). An energy balanced QoS based cluster head selection strategy for WSN. Egyptian Informatics Journal, 15(3), 189-199.

[9] Ahmed, G., Zou, J., Zhao, X., & Fareed, M. M. S. (2017). Markov chain model-based optimal cluster heads selection for wireless sensor networks. Sensors, 17(3), 440.

[10] Thakkar, A., & Kotecha, K. (2014). Cluster head election for energy and delay constraint applications of wireless sensor network. IEEE Sensors Journal, 14(8), 2658-2664.

[11] Wang, A., Yang, D., & Sun, D. (2012). A clustering algorithm based on energy information and cluster heads expectation for wireless sensor networks. Computers & Electrical Engineering, 38(3), 662-671.

[12] Mohanakurup, V., Parambil Gangadharan, S. M., Goel, P., Verma, D., Alshehri, S., Kashyap, R., & Malakhil, B. (2022). Breast cancer detection on histopathological images using a composite dilated Backbone Network. Computational Intelligence and Neuroscience, 2022, 1-10.

[13] Kashyap, R. (2021). Breast cancer histopathological image classification using stochastic dilated residual ghost model. International Journal of Information Retrieval Research, 12(1), 1-24.

[14] Dishongh, T. J., McGrath, M., & Kuris, B. (2014). Wireless sensor networks for healthcare applications. Artech House.

[15] Al-Khasawneh, M. A., Shamsuddin, S. M., Hasan, S., & Bakar, A. A. (2018). An Improved Chaotic Image Encryption Algorithm. In Proceedings of the 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-8). Shah Alam, Malaysia. doi: 10.1109/ICSCEE.2018.8538373.

[16] Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., et al. (2015). Big data, internet of things and cloud convergence – an architecture for secure E-Health applications. Journal of Medical Systems, 39(11), 141.

[17] Van Dam, K., Pitchers, S., & Barnard, M. (2001). Body area networks: towards a wearable future. Proceedings of WWRF Kick off Meeting, Munich, Germany.

[18] Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: a survey. IEEE Access, 7. doi:10.1109/access.2019.2960617.183339

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023

[19] Verma, G., & Prakash, S. (2021). Internet of Things for healthcare: research challenges and future prospects. In Advances in Communication and Computational Technology. Singapore: Springer.

[20] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. A. (2015). Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. doi:10.1109/comst.2015.2444095.

[21] Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). Internet of medical things (IoMT): applications, benefits and future challenges in healthcare domain. Journal of Communication, 12(4), 240-247. doi:10.12720/jcm.12.4.240-247.

[22] Quwaider, M., & Biswas, S. (2009). On-body packet routing algorithms for body sensor networks. In Proceedings of the 2009 First International Conference on Networks & Communications (pp. 171-177). Chennai, India: IEEE.

[23] Wei, W., & Qi, Y. (2011). Information potential fields navigation in wireless Ad-Hoc sensor networks. Sensors, 11(5), 4794-4807. doi:10.3390/s110504794.

[24] Rehman, A., Saba, T., Haseeb, K., Larabi Marie-Sainte, S., & Lloret, J. (2021). Energy-efficient IoT e-health using artificial intelligence model with homomorphic secret sharing. Energies, 14(19), 6414. doi:10.3390/en14196414.

[25] Rghioui, A., Lloret, J., Harane, M., & Oumnad, A. (2020). A smart glucose monitoring system for diabetic patient. Electronics, 9(4), 678. doi:10.3390/electronics9040678.

[26] Kashyap, R. (2020). Machine learning for internet of things. In Research Anthology on Artificial Intelligence Applications in Security (pp. 976-1002).

[27] Khan, Z. A., Feng, Z., Uddin, M. I., Mast, N., Shah, S. A. A., Imtiaz, M., Al-Khasawneh, M. A., & Mahmoud, M. (2020). Optimal Policy Learning for Disease Prevention Using Reinforcement Learning. Scientific Programming, 2020, Article ID 7627290, 1-13. doi: 10.1155/2020/7627290.

[28] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. EAI Endorsed Transactions on Security and Safety, 3(9), e2. doi:10.4108/eai.3-12-2015.2262516.

[29] Mohamed Shakeel, P., Baskar, S., Sarma Dhulipala, V. R., Mishra, S., & Jaber, M. M. (2018). Retracted article: maintaining security and privacy in health care system using learning based deep-Q-networks. Journal of Medical Systems, 42(10), 186. doi:10.1007/s10916-018-1045-z.

[30] Ramirez-Asis, E., Bolivar, R. P., Gonzales, L. A., Chaudhury, S., Kashyap, R., Alsanie, W. F., & Viju, G. K. (2022). A lightweight hybrid dilated ghost model-based approach for the prognosis of breast cancer. Computational Intelligence and Neuroscience, 2022, 1-10.

[31] Al-Khasawneh, M. A., Uddin, I., Shah, S. A. A., et al. (2022). An Improved Chaotic Image Encryption Algorithm using Hadoop-based MapReduce framework for massive remote sensed images in parallel IoT applications. Cluster Computing, 25(2), 999-1013. doi: 10.1007/s10586-021-03466-2.

Doi : https://doi.org/10.54216/JCIM.120204
Received: December 24, 2022 Revised: February 22, 2023 Accepted: June 01, 2023