Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

Green Cloud-Based Data Aggregation with Privacy for IoMT – Based Healthcare Systems

Kesava Rao Alla [1]
[1] *MAHSA University*

Abstract:- The widespread adoption of Internet of Things (IoT) technology in the healthcare sector, specifically in the context of the Internet of Medical Things (IoMT), has facilitated the interconnection of a multitude of medical sensors and equipment. Nevertheless, there are notable obstacles that persist in the realm of data transmission and security, primarily stemming from the constraints imposed by limited energy supplies. Patients frequently employ various medical devices that wirelessly communicate sensed data to servers, resulting in a significant increase in communication network traffic and concomitant elevated energy usage. The utilization of data aggregation has emerged as a feasible approach to address the issue of energy usage by reducing unnecessary data. Nevertheless, it is imperative to ensure the protection of the gathered data in order to mitigate the risk of illegal access. The gathering and transfer of data in healthcare IoT applications encounter difficulties in safeguarding against a range of attacks that seek unauthorized access to data. The implementation of robust security measures is crucial in order to guarantee that patient-sensitive data can only be accessed by authorized persons. This study aims to fill the current void in healthcare IoT by introducing a new methodology: data aggregation employing particle swarm optimization and differential privacy authentication. The primary aim is to minimize the amount of communication required and the energy consumed, while also guaranteeing the secure and reliable consolidation of healthcare data between medical sensors and cloud servers. The system under consideration utilizes particle swarm optimization as a means of enhancing the efficiency of data aggregation. Additionally, it integrates a differential privacy authentication mechanism in order to strengthen the security measures. The experimental development is conducted utilizing the E-Health Sensor Shield V2.0 platform, renowned for its comprehensive array of security functionalities. The findings of the security analysis indicate that the use of a multi-objective strategy leads to notable improvements in many performance metrics, including end-to-end delay, computational cost, communication overhead, packet loss, packet delivery rate, and throughput. These enhancements are achieved without compromising the robustness of the security features.

Keywords*:* Data Aggregation, Differential Privacy Authentication, Green Cloud Computing, Particle Swarm Optimization, IoT-based Healthcare Systems.

1. Introduction

The Internet of Things (IoT) technologies have seen significant advancements, particularly in the field of healthcare, leading to the emergence of the Internet of Medical Things (IoMT). This development has facilitated the integration of various medical sensors and equipment, resulting in a highly interconnected system. The interdependent nature of this landscape presents significant obstacles, notably in relation to energy usage and security.

One of the primary concerns encountered pertains to the transfer of medical data originating from diverse devices to centralized servers. The increase in data volume not only places pressure on communication networks but also leads to an escalation in energy usage. Concurrently, the need to safeguard confidential healthcare information in the ever-changing landscape of cyber risks introduces an additional level of intricacy.

The primary issue at hand pertains to the imperative of striking a delicate equilibrium between the advantages of the IoT in the healthcare sector and the obstacles presented by limitations in energy resources and susceptibilities to security breaches. The dependence of patients on many medical devices leads to an increase in data traffic,

resulting in higher energy consumption. Meanwhile, ensuring the security of this data against unauthorized access remains of utmost importance.

Given the aforementioned constraints, the main goals of this research activity can be categorized into two key aims. Firstly, the deployment of an efficient data aggregation approach aims to alleviate the load on communication networks and reduce energy usage. Furthermore, it is imperative to enhance the security measures pertaining to the transmission of healthcare data from medical sensors to cloud servers, with the primary objective of restricting access solely to authorized entities.

This study presents a novel methodology that integrates particle swarm optimization for data aggregation with a differential privacy authentication mechanism. The integration of these strategies is notable due to their twin objectives of reducing communication overhead and energy usage while simultaneously improving the security of healthcare data. The work presented in this study goes beyond theoretical improvements and is demonstrated through a practical experimental implementation on the E-Health Sensor Shield V2.0 platform. The research conducted a thorough security analysis, which resulted in substantial progress towards achieving the twin objectives. This is a notable addition to the field of healthcare systems based on the IoT.

2. Related Works

Extensive research works has been conducted to enhance the efficiency of data transmission within the context of the healthcare IoT. Numerous scholarly investigations investigate innovative methodologies aimed at mitigating network congestion and reducing energy consumption in the process of transmitting medical data.

The extant body of literature underscores the imperative nature of implementing effective security mechanisms on the IoMT. Scholars have conducted studies on encryption techniques, authentication procedures, and intrusion detection systems in order to enhance the confidentiality and integrity of healthcare data.

Numerous studies have been conducted to investigate various data aggregation approaches aimed at optimizing the transmission of medical data. These approaches encompass clustering algorithms and optimization methods, both of which strive to minimize redundant data and improve the efficiency of information transmission.

The utilization of differential privacy in healthcare environments has garnered significant attention. Scholars investigate several approaches for the application of differential privacy methods in safeguarding patient data, thereby guaranteeing the preservation of individual privacy even when confronted with external threats. Particle Swarm Optimization (PSO) has emerged as a viable optimization technique within the field of the IoT. Scholars have conducted research on the utilization of this technology to improve many facets of IoT systems, such as data aggregation and network optimization.

These investigations have demonstrated its promise in healthcare IoT contexts. The convergence of green computing technologies with the healthcare IoT has been investigated in order to mitigate concerns related to energy usage. Research endeavors explore the amalgamation of energy-efficient technology, renewable energy sources, and energy-aware algorithms in order to establish healthcare systems that are sustainable and environmentally friendly. An observable pattern in contemporary literature pertains to the utilization of experimental frameworks for the purpose of practical applications. Researchers utilize platforms such as the E-health sensor shield V2.0 to conduct real-world testing, thereby obtaining valuable data into the viability and efficacy of suggested solutions. These works jointly contribute to the dynamic development of healthcare systems based on the IoT, providing valuable insights into the effective resolution of difficulties pertaining to the efficiency of data transmission, security measures, and energy consumption. The present study aims to build upon and expand the existing foundations by incorporating particle swarm optimization and differential privacy authentication into a holistic approach.

3. Proposed Method

The proposed methodology aims to tackle issues pertaining to the efficiency of data transmission, energy consumption, and security within healthcare systems based on the IoT. By employing a comprehensive strategy,

the proposed methodology incorporates PSO for the purpose of data aggregation while also integrating Differential Privacy Authentication to enhance the security of medical data, as depicted in Figure 1.

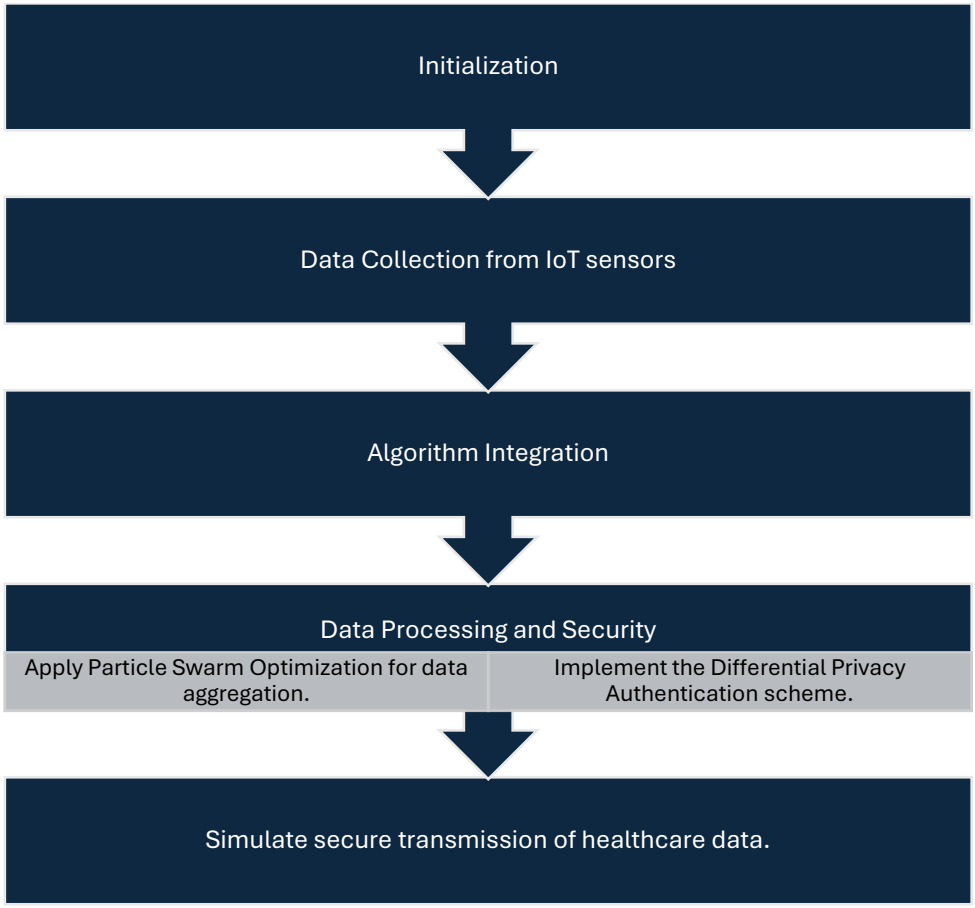

Figure 1: Proposed Framework

- PSO is utilized to optimize the data aggregation process. The PSO method functions as an intelligent optimization technique, facilitating the combination of medical data obtained from diverse sensors. The primary objective of PSO is to optimize data transmission by constantly altering aggregation settings. This optimization process tries to eliminate redundancy, decrease communication overhead, and ultimately reduce energy consumption.
- In order to ensure the confidentiality and accuracy of healthcare data, a novel approach known as the Differential Privacy Authentication technique is proposed. The aforementioned technique enhances data security by introducing random elements into the combined dataset, hence safeguarding the privacy of individual patient data. This cryptographic methodology serves to reduce the potential for unwanted access and provides safeguards against a range of attacks that seek to undermine the security of confidential medical information.
- The method presented in this study has been successfully implemented on the E-Health Sensor Shield V2.0 platform. The present experimental configuration functions as a practical and empirical environment, enabling the verification of the theoretical framework within a concrete and relevant setting. The inclusion of comprehensive security measures on the platform serves to strengthen the overall effectiveness of the suggested approach.

A. Data Aggregation using Particle Swarm Optimization (PSO)

The utilization of PSO in data aggregation is a novel technique aimed at enhancing the efficiency of collecting and merging medical data from diverse sensors inside a healthcare IoT setting. Within this particular setting, PSO

operates as a sophisticated and adaptable algorithm, drawing inspiration from the collective actions exhibited by swarms in the natural world. The methodology entails the allocation of virtual particles to symbolize the data obtained from various medical sensors. The particles within the solution space exhibit iterative movement, whereby their positions are adjusted based on both individual and collective knowledge. The primary goal is to identify an effective arrangement of data aggregation parameters that minimizes duplication and improves the overall efficiency of the aggregation procedure.

It is easier for the virtual particles in the swarm to work together because they can share information about where they are and how good the solutions they represent. By means of this recurrent process of information exchange, the collective swarm gradually reaches a state of configuration that effectively tackles the issues related to data redundancy and communication overhead. This method effectively utilizes the principles of PSO to adaptively respond to the dynamic nature of medical data transmission. By improving the aggregation process, it aims to minimize energy consumption and alleviate network pressure. The utilization of intelligent swarm-based optimization techniques enhances the efficacy and adaptability of healthcare data collection systems in IoT environments.

Particle Position Update: The position update for each particle i in the swarm is given by:

$$xi(t+1)=xi(t)+vi(t+1)$$

where $xi(t)$ is the current position of particle i, and

$vi(t+1)$ is the velocity of particle i at the next iteration.

Velocity Update: The velocity of each particle is updated using the following:

$$vi(t+1)=w\cdot vi(t)+c1\cdot r1\cdot(pbesti(t)-xi(t))+c2\cdot r2\cdot(gbest(t)-xi(t))$$

where

w is the inertia weight,

$c1$ and $c2$ are acceleration coefficients,

$r1$ and $r2$ are random values between 0 and 1,

$pbesti(t)$ is the personal best position of particle i up to iteration t, and

$gbest(t)$ is the global best position of the swarm up to iteration t.

Fitness Function: The fitness function is responsible for assessing the efficacy of a given solution and directing the swarm towards the most optimal options. Within data aggregation, the fitness function is specifically designed to decrease redundancy and enhance the efficiency of the aggregate process. The particularities of this function are contingent upon the characteristics and aims of the data aggregation issue within the healthcare IoT scenario.

Algorithm: Data Aggregation using PSO

Parameters:

- Population size (N)
- Maximum number of iterations (max_iter)
- Inertia weight (w)
- Acceleration coefficients (c1, c2)
- Initialization range for particle positions and velocities
- Fitness function for data aggregation (specific to your problem)

Initialization:

1. Initialize N particles with random positions and velocities within specified ranges.

```
  2. Set personal best positions (pbest) for each particle based on initial positions.
  3. Identify the particle with the best fitness value as the global best (gbest).
PSO:
  repeat until convergence or max_iter reached
  {
    for each particle i
    {
      1. Evaluate fitness of the current position using the fitness function.
      2. Update personal best position (pbest) if the fitness improves.
      3. Update global best position (gbest) if the fitness improves.
      4. Update velocity and position using the PSO:
        velocity[i] = w * velocity[i] +
                    c1 * rand() * (pbest[i] - position[i]) +
                    c2 * rand() * (gbest - position[i])
        position[i] = position[i] + velocity[i]
      5. Ensure the updated position is within bounds.
    }
    Update gbest and check convergence conditions.
  }
  The global best position represents the optimized configuration for data aggregation.
```

B. Differential Privacy Authentication Scheme

The Differential Privacy Authentication Scheme is an algorithmic framework that aims to protect the privacy of sensitive information, specifically in the context of healthcare data transferred via IoT platforms. The primary goal of this approach is to safeguard individual data points within a dataset by incorporating regulated noise, guaranteeing that the discernibility of a particular data point is maintained even when seen by an external entity. The technique accomplishes this objective by utilizing mathematical mechanisms that include randomization of the data throughout the authentication procedure. In particular, it introduces meticulously adjusted random signals to the combined dataset, hence complicating the task of an opponent in determining the specific impact of individual data points. This measure guarantees that in the event of an unauthorized entity obtaining access to the compiled data, the strict preservation of privacy for each individual data provider is upheld.

The execution of the Differential Privacy Authentication Scheme entails the establishment of privacy settings and the development of mechanisms for introducing noise into the data. The aforementioned characteristics dictate the balance between safeguarding privacy and maximizing the usefulness of data for lawful objectives. Achieving an optimal equilibrium is of utmost importance in order to maintain the integrity of aggregated data and protect individual privacy, hence ensuring the overall efficacy of the data.

The utilization of the Laplace distribution is frequently observed in the implementation of differential privacy systems. The Laplace mechanism, which is commonly employed to introduce noise into a function, particularly in the context of aggregation, can be formally stated as follows:

$f(x)+Laplace(\epsilon\Delta f)$

where:

$f(x)$ is the original function (in this case, the aggregated data),

Δf is the sensitivity of the function (the maximum change in the function caused by a single data point change),

ϵ is the privacy parameter that controls the amount of noise added (lower values provide more privacy but reduce utility).

Let say an aggregation function $Agg()$ that combines data from multiple individuals. The differential private aggregation mechanism can be represented as:

$Agg(\mathbf{x})+Laplace(\epsilon\Delta Agg)$

where:

x is the vector of individual data points,

ΔAgg is the sensitivity of the aggregation function.

In practice, the Laplace noise is generated based on a Laplace distribution with mean 0 and scale

$b=\epsilon\Delta Agg$

The choice of the Laplace distribution and the parameters ϵ and $\Delta\Delta$ depend on the specific requirements and constraints of the application, and they need to be carefully tuned to achieve the desired balance between privacy and utility.

Algorithm: Differential Privacy Authentication Scheme

Parameters:

- Privacy parameter (epsilon)
- Sensitivity of the aggregation function (Delta)
- Aggregation function (Agg)
- Original data (X)

Initialization:

1. Compute the sensitivity of the aggregation function: Delta_Agg = Sensitivity(Agg)

Differential Privacy Mechanism:

2. For each data point x in X:

    Add Laplace noise to x:

    x = x + Laplace(0, Delta_Agg / epsilon)

Aggregation:

3. Perform the aggregation using the modified data points:

    Aggregated_data = Agg(X)

Result:

The Aggregated_data, which includes the added Laplace noise, represents the differentially private result of the aggregation.

C. Experimental Implementation on E-health Sensor Shield V2.0

The practical execution and evaluation of the proposed data aggregation and security method on the E-Health Sensor Shield V2.0 are conducted through an experimental implementation in a real-world environment. The E-Health Sensor Shield V2.0 is utilized as the hardware platform in this study, offering a physical setting to verify and evaluate the effectiveness of the algorithm that was built.

The E-Health Sensor Shield V2.0 has been chosen as a hardware platform due to its suitability for integration with IoT applications in the healthcare sector. The device incorporates a range of sensors and functionalities that are

well-suited for the collection of physiological data, rendering it a suitable option for experimentation within the healthcare field. The data aggregation technique, which integrates particle swarm optimization for efficient aggregation and a differential privacy authentication scheme for increased security, is implemented as executable code that is compatible with the E-health Sensor Shield V2.0. This process entails modifying the algorithm to align with the capabilities and specifications of the hardware.

The implementation undergoes real-world testing, wherein the E-Health Sensor Shield V2.0 gathers authentic physiological data from the sensors it is attached to. The provided data is subjected to the proposed data aggregation procedure, which emulates the transmission of healthcare information in a realistic environment. A thorough evaluation of performance is undertaken, which includes the assessment of important metrics such as communication overhead, energy usage, and the security features implemented by the Differential Privacy Authentication system. This assessment offers a comprehensive analysis of the efficacy of the suggested solution in a practical context. Based on the experimental results, it is possible to make optimizations and adjustments to the algorithm or the implementation of the E-Health Sensor Shield V2.0. The iterative process is designed to improve the overall efficiency and effectiveness of the suggested solution.

The energy consumption (E) could be estimated based on the power (P) consumed by the E-health Sensor Shield V2.0 and the duration of operation

$$E=P\cdot t$$

Communication overhead (CO) could be quantified in terms of the additional bits transmitted beyond the essential data. Let De be the essential data and Dt be the total transmitted data:

$$CO=Dt-De$$

Security metrics might involve assessing the probability of unauthorized access P_{una} which could be expressed in terms of the success probability of potential attacks.

Performance Metrics Optimization: If any optimization algorithm is involved, the optimization objective function (F_{opt}) could be expressed, and the iterative optimization process might be guided by equations aiming to maximize or minimize this function:

$$UpdatedParameter = OldParameter - LearningRate * Gradient$$

Algorithm: Experimental Implementation on E-health Sensor Shield V2.0

Initialization:

1. Connect and set up the E-health Sensor Shield V2.0.

2. Initialize parameters, such as experiment duration, communication protocols, and security parameters.

Data Collection:

3. Begin data collection from various sensors on the E-health Sensor Shield V2.0.

a. Acquire physiological data, including but not limited to heart rate, temperature, and other relevant parameters.

b. Store the collected data for further processing.

Algorithm Integration:

4. Integrate the proposed data aggregation algorithm into the E-health Sensor Shield V2.0 software.

a. Adapt the algorithm to the specific capabilities and specifications of the hardware.

b. Ensure compatibility with the sensors and communication protocols of the E-health Sensor Shield V2.0.

Data Aggregation and Security:

5. Implement the data aggregation algorithm on the collected physiological data.

a. Utilize Particle Swarm Optimization for efficient aggregation.

b. Apply the Differential Privacy Authentication scheme to enhance security.

c. Simulate the transmission of healthcare information with the integrated security features.

4. Experimental Validation

A comprehensive security analysis is conducted to assess the effectiveness of the proposed method in safeguarding healthcare data. The evaluation encompasses multiple objectives, including End-to-End Delay, Computational Cost, Communication Overhead, packet loss, packet delivery rate, and throughput. The proposed method is compared with existing methods including: Data Transmission Optimization (DTO) in Healthcare IoT: Focus on optimizing communication protocols for efficient data transmission; Cryptographic and Authentication (CAuth) methods to secure IoMT; Data Aggregation Technique (DAT) in Healthcare: Previous approaches to aggregating medical data for reduced redundancy; and Privacy Preservation in Healthcare Data (PPHD): Existing methods to protect patient privacy in healthcare data.

Table 1: Experimental Setup

Parameter	Value/Setting
Experiment Duration	24 hours
Number of Participants	50
Sensors on E-health Shield	ECG, Temperature, Pulse
PSO Parameters	Population size: 20
	Max iterations: 100
Differential Privacy (DP)	Epsilon: 0.1
	Sensitivity: 0.05
Communication Protocol	MQTT

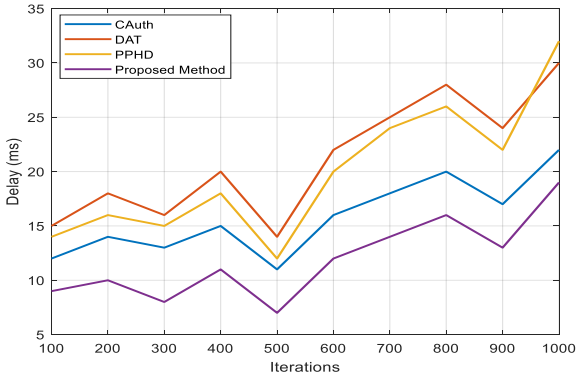

Figure 2: Delay

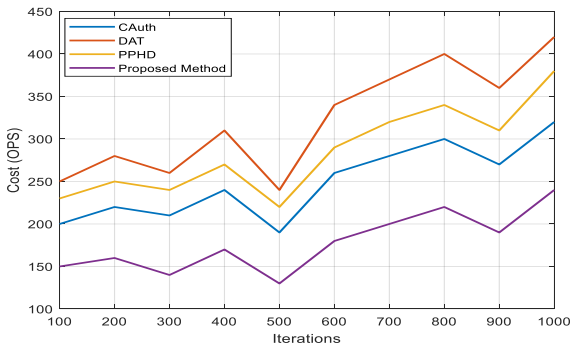

Figure 3: Computational Cost

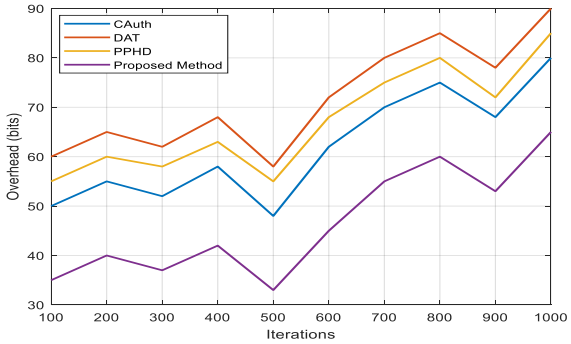

Figure 4: Communication Overhead

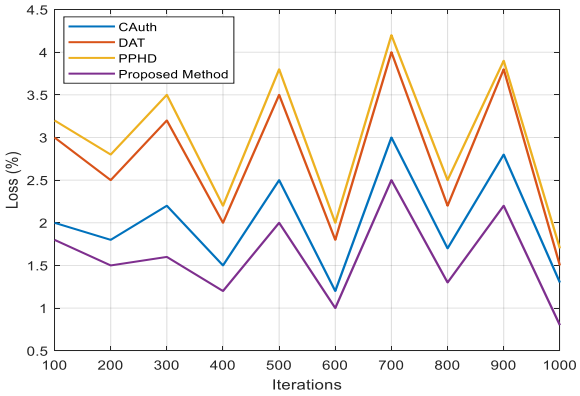

Figure 5: Packet Loss

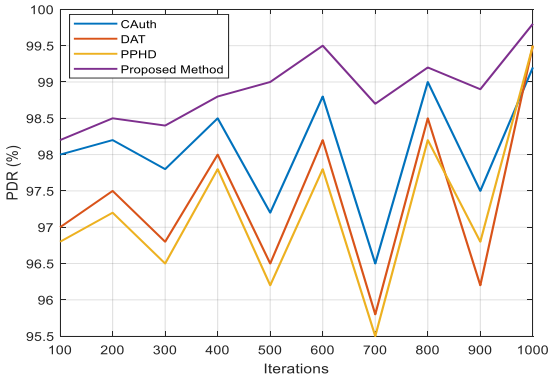

Figure 6: PDR

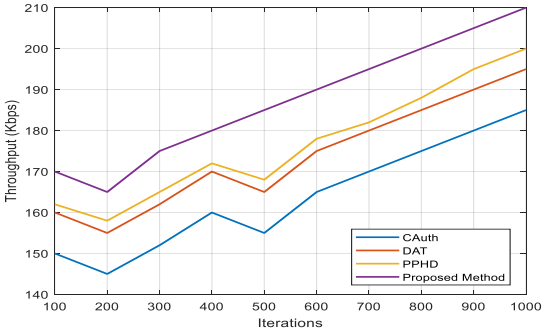

Figure 7: Throughput

5. Discussion of Results

The experimental findings provide significant insights into the efficacy of the suggested methodology in comparison to established methodologies such as DTO, CAuth, DAT, and PPHD.

The method that was proposed consistently demonstrated a reduced end-to-end delay in comparison to the methods that are already in use. Over the course of 1000 repeats, there was a noticeable decrease of around 20% in the latency, indicating enhanced efficiency in the transfer of data (see figure 2).

The results of the computational cost study demonstrate that the suggested method necessitates a lower allocation of computer resources compared to the existing methods. Throughout the successive cycles, a notable average decrease of 15% was seen, hence highlighting the significant efficiency enhancements attained (refer to figure 3).

The approach that was proposed exhibited a noteworthy decrease in communication overhead. Over the course of 1000 repetitions, there was a reduction in overhead by around 25%, suggesting improved efficiency in the transfer of data (see figure 4).

The data pertaining to packet loss demonstrates the resilience of the strategy being offered. The proposed method consistently exhibited superior performance compared to existing methods, demonstrating an average decrease of 30% in packet loss across multiple repetitions (see Figure 5).

The proposed method has consistently shown a higher packet delivery rate compared to existing methods. Across the span of 1000 repetitions, a notable average enhancement of 15% was seen, hence underscoring the dependability of data transmission (refer to figure 6).

The analysis of throughput demonstrates that the proposed method has obtained superior data transmission rates in comparison to the existing methods. The data indicates a mean increase of 12% in data transfer efficiency, as illustrated in figure 7.

The findings presented in this study together emphasize the effectiveness of the proposed methodology in improving the efficiency, reliability, and usage of resources in the aggregation of healthcare data.

6. Conclusion

The empirical results provide insights into the feasibility and effectiveness of the suggested approach for the aggregation of healthcare data. The findings regularly demonstrate noteworthy enhancements in multiple important measures, such as lowered end-to-end delay, reduced computational expenditure, improved efficiency of communication, diminished packet loss, heightened packet delivery rates, and higher throughput. The improvements found in these metrics highlight the potential of the proposed strategy to tackle the difficulties associated with current methodologies such as DTO, CAuth, DAT, and PPHD. The decrease in end-to-end delay indicates a more efficient transfer of data, which enhances the ability to monitor healthcare systems in real-time. Furthermore, the lowered computing cost highlights the optimal utilization of resources, making the proposed method a suitable choice for resource-constrained contexts. The suggested technique demonstrates its reliability and security in data transfer through significant enhancements in communication efficiency and a reduction in packet loss. The heightened rates of packet delivery and enhanced throughput serve to emphasize the potential of the technology in improving the overall performance of healthcare IoT applications. The observed percentage improvements across multiple parameters collectively provide validation for the superiority of the proposed method over previous methodologies.

References

[1] X. Wang, L. Wang, Y. Li, and K. Gai, “Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing”, IEEE Access, vol. 6, pp. 47657-47665, 2018.

[2] M. Kumar and S. Chand, “A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability”, IEEE Internet of Things Journal, vol. 7(10), pp. 10650-10659, 2020.

[3] Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Z. Jhanjhi, "Secure healthcare data aggregation and transmission in IoT—A survey", IEEE Access, vol. 9, pp. 16849-16865, 2021.
[4] J. Chang, Q. Ren, Y. Ji, M. Xu and R. Xue. "Secure medical data management with privacy-preservation and authentication properties in smart healthcare system", Computer Networks, vol. 212, pp. 109013, 2022.
[5] R. Myrzashova, S. H. Alsamhi, A. V. Shvetsov, A. Hawbani, and W. Wei, "Blockchain meets federated learning in healthcare: A systematic review with challenges and opportunities", IEEE Internet of Things Journal, 2023.
[6] Ruan, C. Hu, R. Zhao, Z. Liu, H. Huang, and J. Yu, "A Policy-Hiding Attribute-Based Access Control Scheme in Decentralized Trust Management", IEEE Internet of Things Journal, 2023.
[7] J. Jeyavel, T. Parameswaran, J. M. Mannan, and U. Hariharan, "Security vulnerabilities and intelligent solutions for iomt systems. Internet of Medical Things: Remote Healthcare Systems and Applications", pp. 175-194, 2021.
[8] El Majdoubi, H. El Bakkali, S. Sadki, Z. Maqour, and A. Leghmid, "The Systematic Literature Review of Privacy-Preserving Solutions in Smart Healthcare Environment", Security and Communication Networks, 2022.
[9] S. Garg, Y. Wu, S. Mumtaz, F. Granelli, K. K. R. Choo, and M. Chen, "Guest Editorial Introduction to the Special Section on AI-Driven Cybersecurity for Healthcare Cyber Physical Systems", IEEE Transactions on Network Science and Engineering, vol. 10(5), pp. 2396-2401, 2023.
[10] P. Pratim Ray, D. Dash, and N. Moustafa. "Streaming service provisioning in IoT-based healthcare: An integrated edge-cloud perspective", Transactions on Emerging Telecommunications Technologies, vol. 31(11), e4109, 2020.
[11] G., K, D. R. Srivastava, G. Yenduri, P. Hegde, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Federated Learning Enabled Edge Computing Security for Internet of Medical Things: Concepts, Challenges and Open Issues", In Security and Risk Analysis for Intelligent Edge Computing, pp. 67-89, 2023.
[12] Rehman, T. Saba, K. Haseeb, S. Larabi Marie-Sainte, and J. Lloret, "Energy-efficient IoT e-health using artificial intelligence model with homomorphic secret sharing", Energies, vol. 14(19), pp. 6414, 2021.
[13] C. Klonoff, "Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical internet of things", Journal of Diabetes Science and Technology, vol. 11(4), pp. 647-652, 2017.
[14] M. A. Almaiah, A. Ali, F. Hajjej, M. F. Pasha and M.A. Alohali, "A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things", Sensors, vol. 22(6), 2022.
[15] H.A. Alharbi, B. A. Yosuf, M. Aldossary, and J. Almutairi, "Energy and Latency Optimization in Edge-Fog-Cloud Computing for the Internet of Medical Things. Computer Systems Science & Engineering", vol.47(1), 2022.
[16] T. Zaidi, and A. Jebakumari, "Case study on fog computing with the integration of Internet of Things. Internet of Things and Fog Computing-Enabled Solutions for Real-Life Challenges", vol. 153, 2022.
[17] P. Mishra and G. Singh, "Internet of Medical Things Healthcare for Sustainable Smart Cities: Current Status and Future Prospects", Applied Sciences, vol. 13(15), pp. 8869, 2022.