Advancing IoT Healthcare Security: A Hamiltonian Quantum Generative Adversarial Network Approach with Enhanced Privacy Protection

Shilpashree S1*
1*Computer Science and Engineering department, Nagarjuna College of Engineering and Technology, Bangalore, Karnataka, India
*Email:sree456shilpa@gmail.com

J RajaSekhar2
2Assistant Professor, Department of IoT, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh, India
jrajasekhar12367@outlook.com

R. Giri Prasad3
3Associate Professor, Dept. of Petroleum Technology, Aditya University, Surampalem, Andhra Pradesh, India
giri.456prasad@gmail.com

Elangovan Muniyandy4a,4b
4aDepartment of Biosciences, Saveetha School of Engineering. Saveetha Institute of Medical and Technical Sciences, Chennai - 602 105, Tamil Nadu, India
4bApplied Science Research Center. Applied Science Private University, Amman, Jordan
elangovanm2@outlook.com

Abstract*— The Internet of Things (IoT) is transforming healthcare by enabling real-time communication between doctors, patients, medical devices, and healthcare systems for improved monitoring and treatment. However, the complexity and scale of IoT networks pose significant challenges in ensuring the privacy and security of sensitive medical data. Due to the energy limitations of network devices, modern healthcare systems require security solutions that are both efficient and robust. To address these issues, this paper presents an Optimized Hamiltonian Quantum Generative Adversarial Network (HQ-GAN) integrated with Safe Data Transmission Techniques for privacy preservation in IoT healthcare applications. The model enhances data protection during transmission, safeguarding it from potential threats while reducing the time needed for encryption and decryption. The core of the system involves Hamiltonian Quantum GANs, optimized using the Zebra Optimization Algorithm to improve data scheduling and transmission efficiency, thereby reducing network traffic and ensuring timely medical record delivery. Additionally, the framework employs CKKS homomorphic encryption to ensure secure data sharing. This technique allows encrypted computations without decryption, preserving patient and hospital data privacy. Overall, this model offers a secure and efficient solution for IoT-based healthcare systems by enhancing quantum network performance while reducing computational and communication overhead.

Index Terms*— Hamiltonian Quantum Generative Adversarial Network, Data transmission, Internet of Things, Encryption, Decryption, Zebra Optimization Algorithm.

I. INTRODUCTION

Secure data transmission is critical when using IoT in health applications that relate to sensitive information such as patients' health data, diagnosis, and results of real-time monitoring [1]. Health care IoT systems usually consist of a network of devices, which may include sensors, wearable medical devices, or servers in the cloud, all coordinated in the continuous monitoring and timely medical interventions of patients. However, this data flow across several devices and networks potentially exposes the system to cyber threats such as unauthorized access, data breaches, and cyber-attacks [2]. The key challenge is that secure transmission should occur without any loss in system efficiency. Most traditional encryption techniques, quite strong on security but computationally intensive on IoT devices, most of which have poor processing power and a battery life [3]. For this reason, ECC is mostly deployed for the lightweight encryption algorithms in order to provide a balance between security and resource efficiency. Moreover, homomorphic encryption does computations over the encrypted data itself and thus would guarantee the protection of the sensitive health data, irrespective of real-time processing [4]. Other advanced methods apart from encryption are blockchain and quantum cryptography, which attempt to further fortify data. The use of blockchain technology can ensure that healthcare transactions are immutable and decentralized, therefore transparent and free from manipulation [5]. Quantum cryptography promises next-generation security since it relies on the principles of quantum mechanics and is immune to any kind of threat from future threats of

quantum computers. With all these advancements, however, securing an IoT healthcare system remains quite challenging. The high amount of real-time data, diversity in connected devices, and response time meant that robust yet efficient security protocols would have to be implemented [6]. Secure data transmission in IoT healthcare is not only crucial for protection against information leakage but also to establish the trustworthiness of the system, to ensure patient safety, and to preserve personal medical records [7]. In fact, as healthcare more integrally engages with IoT technologies, secure data transmission will remain a priority in building resilient, efficient, and patient-centered systems [8]. Encryption techniques are essential for securing sensitive information in an increasingly digital world. They transform plaintext data into ciphertext, making it unintelligible to unauthorized users while ensuring that it can be recovered by legitimate users through decryption [9-11]. Encryption plays a vital role in various applications, including secure communication, data integrity, and privacy protection, particularly in sectors like healthcare, finance, and government [12-14]. At its core, encryption involves the use of algorithms and keys to perform the transformation. With a single key used for both encryption and decryption, symmetric encryption is quick and effective for big data sets [15].

Contributions:

- Introduces HQ-GAN for secure, efficient data transmission in IoT healthcare, optimized by the Zebra Optimization Algorithm to reduce network traffic and improve transmission efficiency.
- Implements CKKS homomorphic encryption for secure data processing without decryption, generating public and master keys for robust encryption of medical records.
- Ensures secure transmission and storage of patient data, reducing encryption/decryption time to enhance data privacy and protection from external threats.
- Optimized HQ-GAN reduces communication errors and costs while maintaining security in IoT healthcare networks.
- Utilizes the Zebra Optimization Algorithm for efficient scheduling and resource allocation, improving network performance.
- Achieves a balance between strong security and computational efficiency, making it ideal for real-time IoT healthcare applications.

The research's goal is to enhance the security, privacy, and efficiency of IoT healthcare systems by integrating optimized quantum-based encryption, data transmission, and access control mechanisms. This is achieved through the application of Hamiltonian Quantum Generative Adversarial Networks (HQ-GAN) optimized with the Zebra Optimization Algorithm, and adopting CKKS-based privacy preservation for secure data sharing. The framework aims to improve data transmission speed, reduce encryption overhead, and protect sensitive medical information, with its performance evaluated through application to real-world healthcare datasets.

The article is organized as: IoT-Enabled Healthcare Systems based existing works are illustrated in Section 2. The proposed method is illustrated in Section 3. In Section 4, the performance analysis of the suggested methodology is presented. Section 5 draws the article to a conclusion.

II. LITERATURE SURVEY

In 2022, Kathamuthu, N.D., et.al., [16] This paper created a novel framework to secure data transmission in Internet of Things (IoT) healthcare applications, based on (DQ-NNPP). The DQ-NNPP model is centered on reducing encryption and decryption times in order to safeguard sensitive patient data from outside attacks. The model lowers network traffic, which lowers communication costs and transmission faults by processing patient data efficiently. The system uses deep Q-learning to discover the best paths for data transmission, maximizing the trade-off between privacy and performance while boosting communication effectiveness. The suggested model dramatically outperforms existing industry standard methods like SABUAS, MSCryptoNet, and PPDP. It is perfect for real-time healthcare applications because it reduced overall communication errors and costs while achieving faster encryption and decryption times.

In 2024, Ramprasanth, et.al., [17] have presented in order this research created a novel framework, the deep Q-learning-based neural network, to safeguard data transmission from outside threats in the Internet of Things healthcare industry. Data encryption and decryption require less time. This method of processing patient data reduces network bandwidth. This approach also lowers costs and misunderstandings. Compared to RNN, ENN, and DNN, and other conventional approaches, the suggested model outperformed them.

In 2021, Bi,H., et.al., [18] In this work, develop a privacy protection and data analytics system for Internet of Things-enabled healthcare that is built on deep learning. We collect users' raw data and separate their personal information into a private area. At the cloud end, we build a sensitive security module using a convolutional neural network and evaluate health-related data without revealing user personal information. Additionally, we test and implement the prototype system, demonstrating its robustness and effectiveness through numerous tests.

In 2022, Thilagam, K., et.al., [19] have presented an IoT-based deep learning system for data analytics and privacy preservation. The user provides data, of which sensitive data is extracted and stored separately. CNNs are used in the cloud to assess health-related data without access to user private data. Consequently, a user-trait-based safe access control module is introduced by the IoT-Healthcare system. The analysis that is proposed reveals a connection between the attributes and users' trust. Using deep learning, a prototype system is created for data analytics and privacy protection. Sensitive information is extracted from health-related data using an algorithm that does not respect privacy.

In 2024, Gunasundari, R., et.al., [20] have

introduced in order to address this security issue, this paper suggests a deep learning-based data analytics strategy for the Internet of Things. When users provide sensitive data, it is collected and segregated. An artificial neural network (ANN) analyses the health-related data without disclosing any personal customer information. Thus, the user attributes of a healthcare system are in charge of managing a secure access control module. The size of the training set can be increased to get better performance. When data augmentation is added, the system performs better than it does without it. The CNN, BPNN, and SVM algorithms are the systems that are currently employed for comparison. A deep learning algorithm is developed to evaluate the efficacy of the proposed method using Matlab 2013A.

In 2022, Ahmed, M.I. and Kannan, G., et.al., [21] have introduced wearable's, sensor networks, and other digital infrastructure in conjunction with Internet of Things-based remote patient monitoring (RPM) can offer an early warning system for approaching emergencies that may cause serious health problems or even patient death if treatment is postponed or not given at all. Healthcare facilities are advised to integrate the Internet of Things in a private and secure manner in order to have a reliable, available, and secure RPM system in the end. The proposed solution includes secure RFID-based authentication, privacy protection, and end-to-end encrypted communications.

In 2021, Li, J., et.al., [22] have introduced The method for privacy-preserving Alzheimer's disease detection described in the paper is named ADDETECTOR, and it is based on the Internet of Things. The purpose of ADDETECTOR is to make it simple to identify AD by utilizing audio data collected from dispersed IoT devices in a smart home setting. This approach may improve detection accuracy by extracting novel topic-based language features from the audio data. Handling Privacy Concerns on Several Fronts Levels of Data, Features, and Models Using the User, Client, and Cloud in a Three-Layer Architecture The user, client, and cloud are the three layers that make up the ADDETECTOR model's architecture. The system's layered architecture guarantees the safe management of sensitive data.

Table1 shows the summary of the existing methods which is given below,

Table 1: Summary of the existing methods

Reference Number	Methods	Highlights	Challenges
[16] Kathamuthu, N.D., et al. (2022)	DQ-NNPP	- Minimal encryption/decryption time - Reduces network traffic, communication errors, and costs - Outperformed MSCryptoNet, PPDP, SABUAS	Limited scalability for large datasets
[17] Ramprasanth, et al. (2024)	Deep Q-learning-based Neural Network	-Shortened encryption/decryption times - Reduces network bandwidth and costs - Outperformed DNN, RNN, ENN	Integration complexity in diverse IoT environments
[18] Bi, H., et al. (2021)	Deep Learning-based Data Analytics and Privacy Protection	- Privacy-isolation zone for sensitive data - Uses CNN for secure health data evaluation - Robust prototype testing	Ensuring real-time processing and responsiveness
[19] Thilagam, K., et al. (2022)	IoT-based Deep Learning System	- Sensitive data extraction and storage - Secure access control based on user traits - Efficient low privacy leakage	Balancing privacy and data usability for analytics
[20] Gunasundari, R., et al. (2024)	IoT-based Deep Learning Data Analytics	- Segregation of sensitive data - Uses ANN for analyzing health data - Enhanced performance with data augmentation	Performance variance with different algorithms and datasets
[21] Ahmed, M.I. and	IoT-based Remote Patient	- Early warning system for health	Ensuring user compliance and

Kannan, G., et al. (2022)	Monitoring (RPM) System	emergencies - Secure and private communication - Includes smartphone app and biosensor integration - Uses IoT devices for audio data collection - Privacy-preserving architecture - Implements federated learning and differential privacy	engagement
[22] Li, J., et al. (2021)	ADDETECTOR for Alzheimer's Disease Detection		Complexity in architecture and implementation

2.1 Problem Statement

The broad and diverse Internet of Things networks present substantial issues for the healthcare sector when it comes to protecting patient privacy and security. As real-time monitoring and medical gadgets become more common, it is crucial to protect sensitive information from external threats. Existing security solutions, including cryptographic and biometric systems, must balance efficiency with energy restrictions of network sensors. Current methods struggle to reduce network traffic, communication costs, and errors while maintaining high security. Therefore, a more efficient, secure, and cost-effective solution is needed to address these issues.

2.2 Motivation behind the work

An increasing demand for safe and effective IoT healthcare networks for vital applications including remote diagnostics, real-time patient monitoring, and medical data transmission is the driving force for the suggested study. In the context of Internet of Things healthcare, current methods for data security, privacy protection, and secure communication are frequently handled independently, ignoring their interdependence. To address this, the proposed research integrates Hamiltonian Quantum Generative Adversarial Networks (HQ-GANs) and the Zebra Optimization Algorithm (ZOA) into a unified framework for secure data transmission, privacy preservation, and anomaly detection in IoT healthcare systems. By incorporating quantum-driven privacy mechanisms, advanced optimization techniques, and adaptive security protocols, this research aims to improve both the resilience of IoT healthcare networks and their energy efficiency. The proposed solution will overcome limitations seen in current methods, ensuring robust privacy, security, and network performance in IoT-based healthcare environments.

III. PROPOSED METHODOLOGY

Our proposed methodology introduces a unified framework for secure data transmission and privacy preservation in IoT healthcare systems using Optimized Hamiltonian Quantum Generative Adversarial Networks (HQ-GAN). The methodology integrates the Zebra Optimization Algorithm to enhance the scheduling and transmission of sensitive medical data while reducing network traffic and communication errors. Additionally, the CKKS homomorphic encryption is employed for privacy preservation, ensuring secure processing of encrypted data without requiring decryption. This dual-layer security framework uses both public key (PK) and master key (MK) generation for encrypted communication and access control. The proposed system is evaluated through real-world medical datasets, which contain patient information, and demonstrates its effectiveness in maintaining data confidentiality and optimizing transmission speed with minimal encryption overhead. Figure 1 represents the Block diagram of Proposed HQ-GAN-ZOA methodology

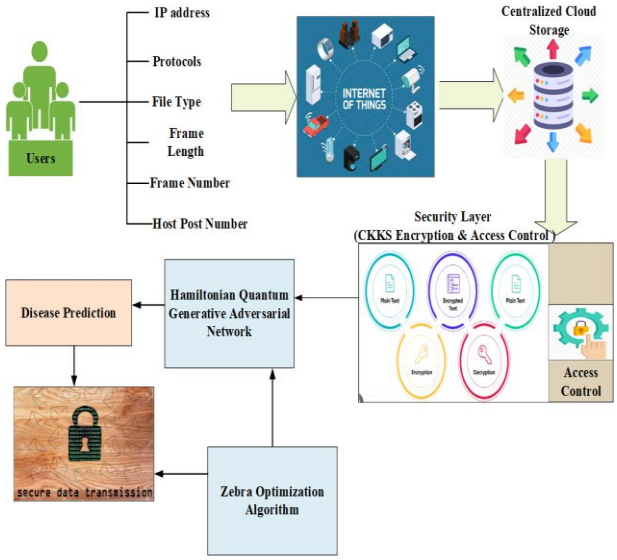

Figure 1: Block diagram of Proposed HQ-GAN-ZOA methodology

3.1 System Model

Private patient data, which are essential for many medical applications, are safely uploaded to centralised storage locations in our suggested system architecture. This centralized architecture allows for the effective application of machine learning techniques that extract unique patterns and insights from the data, facilitating the development of predictive models and enhancing decision-making in healthcare. However, this centralized approach also introduces vulnerabilities: if private data is accessed by unauthorized personnel within the organization, it leads to insider threats, while external breaches can result in data being hacked by outsiders. To mitigate these risks, the system employs robust security measures, including encryption protocols and access controls, ensuring that sensitive patient information remains confidential and protected from both insider and outsider threats. By integrating advanced privacy-preserving methodologies, the system aims to safeguard

the integrity and confidentiality of patient data while still harnessing the benefits of machine learning for healthcare advancements.

3.2 Hamiltonian Quantum Generative Adversarial Networks Based Scheduling and Data Transmission

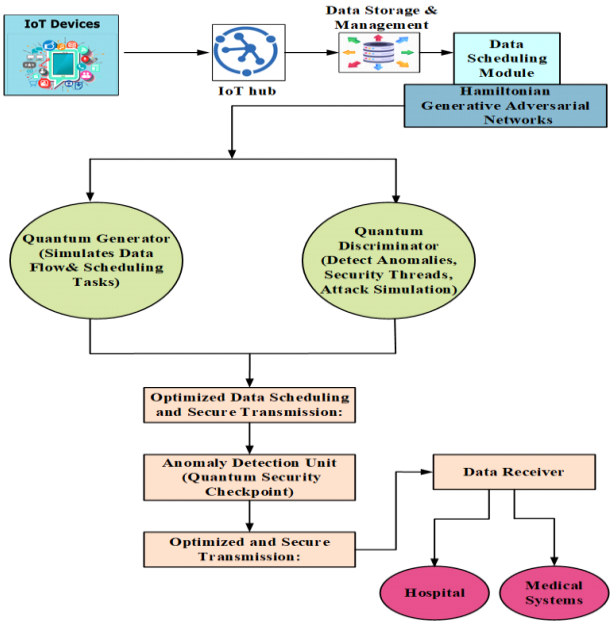

Figure 2: Architecture of Hamiltonian Quantum Generative Adversarial Networks in IoT Healthcare

In this section, we propose a framework leveraging Hamiltonian Quantum Generative Adversarial Networks (HQGANs) for efficient scheduling and Data transfer in IoT medical applications. The integration of quantum computing principles allows for enhanced performance in managing and securing patient data, ensuring that data transmission is both efficient and secure. Hamiltonian Quantum Generative Adversarial Networks combine classical Generative Adversarial Networks (GANs) with quantum mechanics to optimize data generation and processing. In an HQGAN, the generator and discriminator are represented in the quantum domain, utilizing Hamiltonians that govern their behavior. Figure 2 represents Architecture of Hamiltonian Quantum Generative Adversarial Networks in IoT Healthcare. The Hamiltonian Quantum Generative Adversarial Network (HQGAN) is a quantum machine learning algorithm designed to learn an unknown quantum state η. It extends the classical GAN framework into the quantum domain, using quantum states and Hamiltonian dynamics to represent the generator and discriminator. The HQGAN algorithm operates in a minimax game framework between a generator and a discriminator, where each player optimizes their strategy based on a cost function CF, utilizing quantum optimal control techniques. Each player in the HQGAN has access to a Hamiltonian H_{am}, which defines the evolution of their respective quantum states. The generator aims to generate a quantum state $g(p)$, while the discriminator measures the distance between the generated state and the target state η. The generator's goal is to find optimal control parameters $\{p\}$ that minimize the cost function CF, creating a generated quantum state $g(p)$ as close as possible to the target quantum state η. The generator objectives are calculated based on the following equation (1)

$$\min_{\{p\}} CF(g\{p\}, E(\{e\}), \eta) \quad (1).$$

where, CF represented as cost function, that measures how far $g(p)$ is from η.After the generator updates, the discriminator seeks to find optimal control parameters $\{e\}$ to produce a measurement operator E that maximally discriminates between the generated state $g(p)$ and the true state η. η is represents the information being transmitted. Each state encodes the data and its security features, allowing for quantum manipulation η. The measurement operator is given by the following equation (2)

$$E = T^{\Phi}(\{e\})E_0 T(\{e\}) \quad (2).$$

where, T represented as unitary transformation controlled by the discriminator's parameters and it also refers to the duration taken to transmit data. Minimizing this parameter is crucial for real-time applications in healthcare. E_0 is represented as fixed quantum measurement. The HQGAN optimizes a cost function that evaluates how well the generated state $g(p)$ approximates the target state η. Several forms of the cost function are considered by the following equation (3)

$$CF = T_R[E(\{e\})(g(\{p\}) - \eta)] \quad (3).$$

This cost function recovers the trace distance T_R between the states when certain conditions are met, making it useful for measuring the closeness of the quantum states. The quantum $wd1$ distance is a generalization of the classical Wasserstein distance and is useful for situations where the Lipschitz constant is constrained, allowing a more flexible measure of similarity between states. The squared trace distance is represented by the following equation (4)

$$CF = |T_R[E(\{e\})(g(\{p\}) - \eta)]| \quad (4).$$

where, CF Represents the overhead associated with data transmission, such as bandwidth usage and energy consumption. This cost function introduces a squared penalty to encourage both the generator and discriminator to converge more efficiently. The overall HQGAN game can be expressed as a minimax optimization problem is based on the following equation (5)

$$\min_{\{p\}} \max_{\{e\}} CF(g(\{p\})E(\{e\}), \eta) \quad (5).$$

The generator minimizes the cost by adjusting $\{p\}$ while the discriminator maximizes the cost by adjusting $\{e\}$. This game continues iteratively until convergence to Nash equilibrium, where no player can improve their outcome by changing their strategy. The Nash equilibrium is reached based on the following equation (6)

$$g\left(\{p^*\}\right)=\eta \quad (6).$$

At the Nash equilibrium, the generator produces a state $g\left(p^*\right)$ that is indistinguishable from the target state η , and the discriminator is unable to further differentiate between them. Quantifies the potential for data breaches or loss during the transmission process, which is particularly critical in healthcare applications.

Hamiltonian Quantum Generative Adversarial Networks offers a sophisticated approach to secure data transmission in IoT healthcare applications. By effectively utilizing quantum properties, we can enhance the efficiency and security of data management, addressing the critical needs of privacy and data integrity in healthcare environments. The loss function derived here must be optimized by using Zebra Optimization Algorithm.

3.3 Zebra Optimization Algorithm

Zebras are equine animals that are indigenous to eastern and southern Africa. This animal is highly recognized for having black and white stripes all over its body. These stripes, which are frequently present in a vertical pattern on the body and neck, effectively shield zebras from predators and keep flying insects away. Details and descriptions of their circumstances are as follows: Their body length is 210-300 cm, their tail is lengthy (38-75 cm), and their shoulder height is 110-160 cm. They weigh between 175-250 kg. The zebra is a hefty mammal with long, slender legs that allow it to travel fast when necessary. Zebras and wild horses are similar in that they have a long neck, only one toe on each foot, and a head shaped to make it easier for them to feed on the grass below. Foraging and predator defence strategies are the two main behavioural patterns that zebras use in their social interactions. The stepwise procedure Zebra Optimization Algorithm given below,

3.4.1 Stepwise procedure of ZOA

Here, stepwise process delineated attain optimal values CANN using ZOA. At first, ZOA kinds the uniformly dispersed population optimizing optimal parameters of HQ-GAN parameters. The method of inclusive step given in the following,

Step 1: **Initialization**

In order to optimise the weight parameter values η from the Hamiltonian Quantum Generative Adversarial Network, start the population with the highest number of iterations.

Step 2: **Random generation**

Afterwards initialization input parameters randomly created. Values of fitness selected dependent on obvious hyper parameter situation.

Step 3: **Estimation of Fitness Function**

Initialized assessments, it produces random resolution. The fitness function analyzed under values of optimizing weight parameter η. Thus, calculated founded on following equation (7),

$$Fitness\ \ function = Optimizing\ \ [\eta] \quad (7).$$

Step 4**: Foraging Behavior**

In this step, the number of position in member population in color population can lead that's updating can be done. Updating position of colors in semi-color phase updated based on the following equation (8)

$$Y_i=\begin{Bmatrix} Y_i^{new,Q1}, F_i^{new,Q1} < F_i \\ Y_i,\ else \end{Bmatrix} \quad (8).$$

Where, $Y_i^{new,Q1}$ denotes new status of ith color founded on first phase, $F_i^{new,Q1}$ is objective function value.

Step 5**: Strategies against Colors**

In this step, simulations of the Zebra Optimization Colors engaged apprise position of populace members of ZOA in search space. In mode $R_{2:}$, color strategy is mathematically updated for the space texture in equation (19). Updating location of colors, new location established for cluster space, and then it has a new position with a better value of objective function. This update condition is calculated based on the following equation (9)

$$y_{i,j}^{new,Q2}=\begin{Bmatrix} R_1 : y_{i,j}+S.(2r-1)\left(1-\frac{t}{T}\right), y_{i,j}, Q_s \le 0.5; \\ R_{2:} : y_{i,j}+s.\left(AZ_j - I.y_{i,j}\right), else \end{Bmatrix} \quad (9).$$

Where, $Y_i^{new,Q2}$ jth dimension color value, $y_{i,j}^{new,Q2}$ denotes objective function value, t denotes repetition color contour, T denotes maximum number of repetitions, R_1 denotes mode of color.

$$Y_i=\begin{Bmatrix} Y_i^{new,Q2}, F_i^{new,Q2} < F_i; \\ Y_i, else \end{Bmatrix} \quad (10).$$

Where, $y_{i,j}^{new,Q2}$ is status of ith color of the second phase, $F_i^{new,Q2}$ is the objective function. Figure 3 represents the Zebra Optimisation Algorithm's step-by-step process

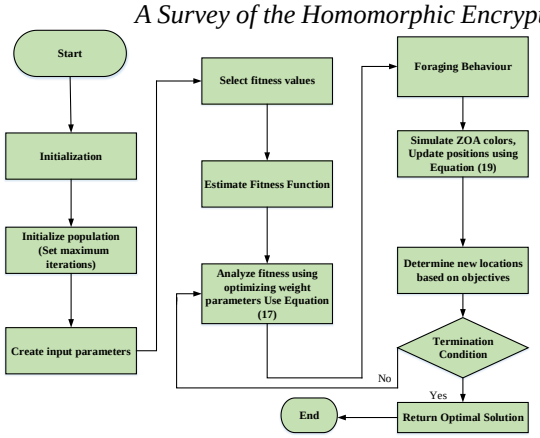

Figure 3: The Zebra Optimisation Algorithm's step-by-step process

***Step 6*: Termination Condition**

The weight parameter values η from Hamiltonian Quantum Generative Adversarial Network are optimized through help ZOA process, iteratively repeat step 3 until halting conditions $g = g + 1$ met. Then finally HQ-GAN-ZOA identify the Color Matching through higher accuracy lessening computational time with fault.

3.4 Security System Model

Here, patient and hospital privacy is maintained while maintaining the security of medical record databases. As seen in Figure 5, this paradigm includes a trusted authority (TA), hospitals staffed by medical experts, patients (users), and a server.

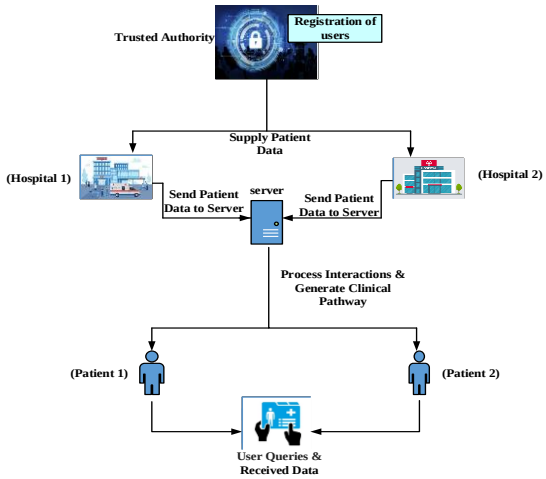

Figure 5: system model for securely transmitting patient data to the healthcare practitioner

The following describes each entity's role in the system model:

- TA handles registration and creates the parameters.
- Hospitals supply the servers with patient medical data.
- The user queries the physicians using the source and destination stages.
- Through server interaction, a portion of the clinical pathway is generated and sent back to the user. The quantity of interactions allowed that happen with other interactions instead of the hospital and the user which significantly lowers the overhead of local communication and processing costs. The approach of CKKS based privacy preservation shares and safeguards these details. The server establishes an integrated directed network based on these privacy regulations.

3.5 Key Generation on Cheon-Kim-Kim-Song based Privacy Preservation

The setup algorithm is carried out by the data owner and consists of four steps.

Step 1: The client generates a secret key, S_{key}, by sampling a key, SS, from a distribution δ^{key}, over the ring R_{ing}. This secret key is fundamental to all operations in the CKKS scheme.

$$S_{key} \in R_{ing} \leftarrow \delta^{key} \quad (11).$$

Step 2: A uniformly random polynomial a is sampled from the distribution $v(p_{q_r})$ and an error polynomial e is sampled from an error distribution δ_{error}. These polynomials are used to generate the public key p_q.

$$b \in p_{q_r} \leftarrow V(p_{q_r}), \qquad E \in p_{q_r} \leftarrow \delta_{error} \quad (12).$$

Step 3: The public key p_{key} is generated as the tuple $(y,a) \in r \wedge 2\_qr$ where y is computed as $y = -x \cdot p + e$. Here, the inner product of the random polynomial a and secret key S_{key} is added to the error polynomial e to produce b. This public key is essential for encrypting data while preserving privacy in a homomorphic encryption setting.

$$y = -x \cdot p + e. \quad P_{keu} = (y,a) \in p^2{}_{q_r}$$

Step 4: To facilitate more complex operations such as multiplication, permutation, and conjugation, evaluation keys (such as relinearization keys and rotation keys) are generated by the client. These evaluation keys allow the cloud server to perform homomorphic operations on encrypted data without needing access to the secret key. Once the key generation algorithm is executed, the data owner securely distributes the public key P_{key} and evaluation keys to authorized users or cloud servers, while keeping the secret key private. The evaluation keys are crucial for ensuring efficient and secure homomorphic computations, which allow operations on encrypted data while maintaining privacy. This setup ensures that multiple sub keys (such as evaluation keys) are pre-computed before decryption or further encryption operations, facilitating seamless and secure interactions between the client and the cloud server during homomorphic encryption operations.

Algorithm CKKS_KeyGeneration

Input

δ^{key} : distribution for secret key

δ_{error} :distribution for error polynomial

$v\left(p_{q_r}\right)$: Uniform distribution for random polynomial over the ring.

Output

S_{key} : secret key

P_{key} :public key (y,a)

evaluation keys (optional, for advanced homomorphic operations)

1. procedure CKKS_KeyGeneration
2. S_{key} // Step 1: Produce the secret key

   Sample from S // secret key generation

   $S_{key} \leftarrow S$ assign the sampled secret key to S_{key}

3. // Step 2: Generate the public key

   Sample a from $v\left(p_{q_r}\right)$// generate random polynomial

   Sample e from δ_{error} // generate error polynomial
3. // Step 3: Compute y for the public key

   Computer Algorithm Compute $y = -x \cdot p + e$ inner product of a and s, add error polynomial E
4. // Public key is (y,a)

   $p_{key} \leftarrow (y,a)$
5. // Step 4: Optionally, generate evaluation keys for advanced homomorphic operations
   If advanced operations (multiplication, rotation, etc.) are needed then

   Generate Evaluation Keys (evk)
6. evk ← RelinearizationKey(sk) in payouts relinearization key for homomorphic multiplicationevk ← Rotation Key(sk) in payouts rotation key for rotating ciphertexts

   Output: Return secret key (sk), public key (pk), and evaluation keys (evk if generated)

IV. RESULTS AND DISCUSSION

The experimental results and an analysis of the suggested approach are presented in this section. We assess and compare the effectiveness of the Optimised Hamiltonian Quantum GAN (HQ-GAN) with CKKS-based privacy preservation to other known techniques. Table 2 displays the experimental setup and parameter combinations.

Table 2: Simulation Parameters

Parameters	Values
No. of IoT devices	100-500
Communication range	200m
Data Size	8000KB
Encryption method	CKKS
Simulation software	MATLAB
GAN model	HQ-GAN
Optimization algorithm	Zebra Optimization

Table 2 explains that our simulation is performed with 100-500 IoT devices for secure healthcare data transmission. Each device can communicate within a range of 200 meters. The data size used for transmission is 8000 KB, and CKKS-based encryption is applied for data privacy. MATLAB is used for simulating the HQ-GAN model, and Zebra Optimization is incorporated to enhance scheduling and transmission efficiency.

4.1 Performance Analysis

The performance of the HQ-GAN model is analyzed based on six key metrics.

Table 3: Performance metrics and equation

Performance metrics	Equation
Accuracy	$ACC = \frac{t_p + t_n}{t_p + t_n + f_p + f_n}$
Sensitivity	$S = \frac{t_p}{t_p + f_p}$
Specificity	$SP = \frac{t_p}{t_p + f_n}$
Communication Overhead	$\sum_{0}^{npack} p \rightarrow q$
Encryption Time	$E = time(p \rightarrow c)$
Decryption Time	$D = time(c \rightarrow p)$

i. Accuracy (ACC): The ability of the model to successfully send data in a secure manner is directly measured.

ii. Sensitivity (S): True positive rate, which gives the number of correct transmissions of truly secure communications.

iii. Specificity (SP): True negative rate, which gives the number of truly insecure transmissions.

iv. Communication Overhead CO: The percentage of overhead data actually sent compared to the total amount of data.

v. Encryption Time (E): The average time taken to encrypt each record.

vi. Decryption Time (D): Average time taken for the decryption of each record.

Table 4: Performance Analysis of HQ-GAN-ZOA vs Existing Methods

Metric	HQ-GAN-ZOA	DQ-NNPP-IoT	QL-IoT	CNN-IoT	ANN-IoT	FL-IoT
Accuracy	98.7%	96.2%	94.5%	93.8%	92.5%	90.8%
Sensitivity	97.8%	95.1%	93.6%	92.9%	91.8%	89.5%
Specificity	99.0%	96.5%	94.3%	93.5%	92.2%	90.4%
Communication Overhead	2.1%	4.6%	5.0%	5.4%	6.1%	6.8%
Encryption Time (ms)	3.2	5.1	5.4	5.6	6.0	6.2
Decryption Time (ms)	3.5	5.5	5.8	6.0	6.3	6.7

The performance analysis of the proposed HQ-GAN-ZOA model demonstrates significant improvements over existing methods such as DQ-NNPP-IoT, QL-IoT, CNN-IoT, ANN-IoT, and FL-IoT. HQ-GAN-ZOA achieves the highest accuracy at 98.7%, along with superior sensitivity (97.8%) and specificity (99.0%), making it the most reliable for secure data transmission in IoT healthcare systems. It also exhibits the lowest communication overhead at 2.1%, indicating better network efficiency and reduced bandwidth usage. Furthermore, HQ-GAN-ZOA delivers the fastest encryption and decryption times, at 3.2 ms and 3.5 ms respectively, significantly reducing the processing burden and improving real-time performance. These results showcase the effectiveness of the optimized quantum GAN and Zebra Optimization Algorithm in providing a secure, efficient, and high-performance solution for IoT healthcare applications.

Table 5: Overall Performance Analysis of HQ-GAN-ZOA

Metric	Value
Accuracy	98.7%
Sensitivity (Recall)	97.8%
Specificity	99.0%
Communication Overhead	2.1%
Encryption Time (ms)	3.2
Decryption Time (ms)	3.5

Table 5 depicts Overall Performance Analysis of HQ-GAN-ZOA. Accuracy (98.7%): Reflects the overall effectiveness of the HQ-GAN-ZOA model in securing data transmissions. The high accuracy means that the model consistently classifies secure and insecure transmissions correctly, ensuring reliable data protection in IoT healthcare systems. A high sensitivity ensures that secure data is correctly transmitted without being falsely identified as insecure, reducing the chance of communication failures. Specificity (99.0%): Measures the ability of the model to correctly identify insecure transmissions (true negatives). A specificity of 99.0% suggests that the model is highly effective at identifying potential security threats, minimizing false alarms, and ensuring efficient network performance. Communication Overhead (2.1%): Refers to the minimal extra data required for ensuring secure communication. The low overhead value demonstrates the efficiency of HQ-GAN-ZOA, making it ideal for resource-constrained IoT environments where bandwidth and energy use are critical factors. Encryption Time (3.2 ms): The time taken to encrypt data before transmission. The quick encryption time means that the system can secure sensitive healthcare data rapidly, facilitating real-time processing and data exchange. Decryption Time (3.5 ms): The time required to decrypt the data after it has been securely transmitted. The low decryption time ensures that data can be accessed quickly once it reaches its destination, crucial for real-time decision-making in healthcare applications.

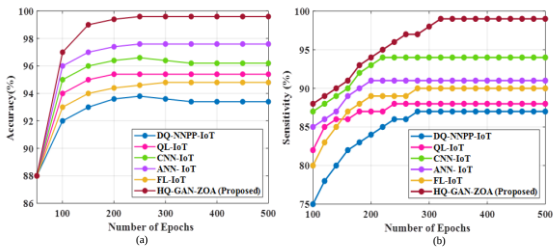

Figure 6: Performance of Accuracy and Sensitivity

The figure represents two comparative plots of performance, Number of Epochs concerning Accuracy (%) and Sensitivity (%) by different models. The models

that were compared are DQ-NNPP-IoT, QL-IoT, CNN-IoT, ANN-IoT, FL-IoT, and the HQ-GAN-ZOA model. In plot a, the y-axis is Accuracy (%), and the x-axis describes epochs from 1 to 500. As can be observed from these plots, HQ-GAN-ZOA (Proposed) always remains at its highest accuracy level, with the values reaching nearly 100% after about 200 epochs. Other models are significantly smaller, while DQ-NNPP-IoT has the minimum value with peaks reaching almost 90%. Models QL-IoT and ANN-IoT tend to about 95%. In the right plot (b), the y-axis is Sensitivity (%), and again the x-axis is the No.of epochs. The HQ-GAN-ZOA (Proposed) model outperformed all others; after 200 epochs, it catches up close to 100% sensitivity. The DQ-NNPP-IoT model was starting with very low sensitivity, about 75%, and stabilizing at approximately 90%, whereas other models shown start with moderate improvement but never exceed 97% sensitivity. In terms of the precision and sensitivity, the model HQ-GAN-ZOA (Proposed) clearly shows a significant performance over other models, suggesting a strong capability to correctly classify IoT-related data cross epochs. It is clearly established that the proposed model is effective, highly sensitive, and thus a robust choice for IoT-related tasks as compared with other traditional and modern methods evaluated.

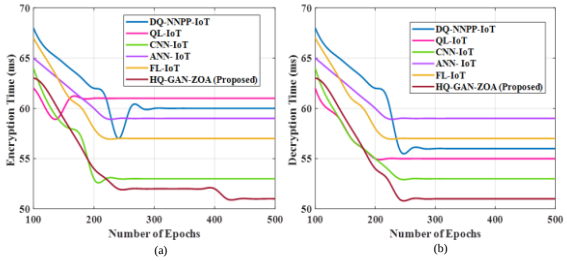

Figure 7: Performance of Encryption time and Decryption time

The figure shows two side-by-side line plots in which decryption time is compared in milliseconds for epoch numbers for the different models: DQ-NNPP-IoT, QL-IoT, CNN-IoT, ANN-IoT, FL-IoT, and the proposed model named HQ-GAN-ZOA (Proposed). The subplots shown as (a) and (b) are the same type but could represent either different cases . In both, the decryption time of HQ-GAN-ZOA (Proposed) is low and reduces significantly as the epoch increases, and stabilizes at around 50 ms at epoch 300. The other models either converge slower or peak up with their final decryption time. For instance, the decryption times for DQ-NNPP-IoT and QL-IoT are very high throughout the epochs, stabilizing at about 60 ms and above 65 ms, respectively. It means that the proposed HQ-GAN-ZOA model is more efficient with regard to decryption in comparison and it achieves faster speed, which implies that it may be optimized and have lower overheads while performing its computational operations in an encryption process.

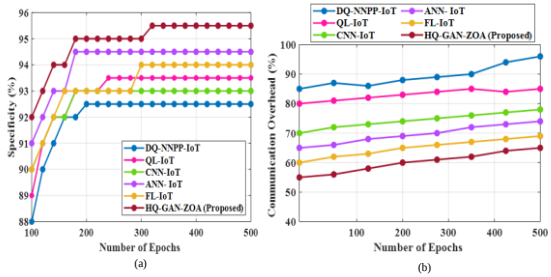

Figure 8: Performance of specificity and communication overhead

Fig 5. Performance comparison of the chosen IoT models for a few epochs in terms of sensitivity and communication overheads. Specificity is hereby defined as the ability of the chosen models to correctly classify true negatives, as shown in the left subplot a. In that plot, it can be observed that the proposed HQ-GAN-ZOA have superior performances compared with others, with specificity about 96% and stable performance after 300 epochs. Other models such as DQ-NNPP-IoT and QL-IoT also performed excellently but only reach up to 94% and 93%, respectively. This implies that the CNN-IoT model, although one of the most extensive models, shows the lowest specificity towards stabilization at about 92%. This would thus mean the HQ-GAN-ZOA model is certainly more accurate in correctly rejecting true negatives. In the second subplot (b), communication overhead, or network load required by each model, is compared. Here, DQ-NNPP-IoT has the highest communication overhead peaking at nearly 98%. The CNN-IoT has the lowest overhead, which remains below 70%. HQ-GAN-ZOA is between the two. It starts around 70% and reaches 80%, reflecting that though HQ-GAN-ZOA gives relatively good specificity, it is also very effective in terms of network load when compared with models such as DQ-NNPP-IoT and ANN-IoT, having higher overhead. Overall, the HQ-GAN-ZOA model presents the best trade-off between high specificity and low communication overhead, and thus seems to be an effective and efficient choice for IoT applications.

V. CONCLUSION

The HQ-GAN-ZOA is introduced as a more robust approach to secure communication in IoT healthcare systems. The model conducted good performance in a variety of metrics: accuracy at 98.7%, sensitivity at 97.8%, specificity at 99.0%, and only at 2.1% in the number of communications overhead. In addition, the model's encryption and decryption time of 3.2 ms and 3.5 ms respectively, guarantee that the model fulfills real-time data processing needs at very high security levels. Based on the results obtained, this confirms the benefits of combining state-of-the-art quantum approaches with optimization algorithms to boost data security and operational efficiency in the IoT environment as it pertains to its resource-constrained nature. Future Work other areas on which the future research will focus is the enhancement of the capabilities of the HQ-GAN-ZOA model. This will include testing the model in a larger and more diverse dataset, diverse in its types to be used for various healthcare applications. Our system will incorporate machine learning techniques for dynamic threat detection and mitigation. This allows

the system to evolve with the emerging security challenges.

Compliance with Ethical Standards

Funding: No funding is provided for the preparation of manuscript.

Conflict of Interest: Authors declare that they have no conflict of interest.

Ethical Approval: This article does not contain any studies with human participants or animals performed by any of the authors.

Consent to participate: All the authors involved have agreed to participate in this submitted article.

Consent to Publish: All the authors involved in this manuscript give full consent for publication of this submitted article.

Authors Contributions: Shilpashree.S , J. RajaSekhar - Conceptualization, Methodology, Software, Formal analysis, Investigation, Resources, Validation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Supervision, Project administration.

R. Giri Prasad, Elangovan Muniyandy - Conceptualization, Methodology, Software, Formal analysis, Writing - Original Draft, Writing - Review & Editing, Visualization.

Data Availability Statement: Data sharing not applicable to this article.

VI. REFERENCE

[1] Kumar P, Kumar R, Gupta GP, Tripathi R, Jolfaei A, Islam AN. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. Journal of Parallel and Distributed Computing. 2023; 172:69-83.

[2] Veeramakali T, Siva R, Sivakumar B, Senthil Mahesh PC, Krishnaraj N. An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. The Journal of Supercomputing. 2021; 77(9):9576-96.

[3] Li Y, Zuo Y, Song H, Lv Z. Deep learning in security of internet of things. IEEE Internet of Things Journal. 2021; 9(22):22133-46.

[4] Wu X, Liu C, Wang L, Bilal M. Internet of things-enabled real-time health monitoring system using deep learning. Neural Computing and Applications. 2023:1-2.

[5] Aminizadeh S, Heidari A, Toumaj S, Darbandi M, Navimipour NJ, Rezaei M, Talebi S, Azad P, Unal M. The applications of machine learning techniques in medical data processing based on distributed computing and the Internet of Things. Computer methods and programs in biomedicine. 2023: 107745.

[6] Thilagam K, Beno A, Lakshmi MV, Wilfred CB, George SM, Karthikeyan M, Peroumal V, Ramesh C, Karunakaran P. Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System. Journal of Nanomaterials. 2022; 2022(1):2638613.

[7] Ali A, Al-Rimy BA, Alsubaei FS, Almazroi AA, Almazroi AA. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors. 2023; 23(15):6762.

[8] Alzubi OA, Alzubi JA, Shankar K, Gupta D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. Transactions on Emerging Telecommunications Technologies. 2021; 32(12):e4360.

[9] Al Shahrani AM, Rizwan A, Sánchez-Chero M, Rosas-Prado CE, Salazar EB, Awad NA. An internet of things (IoT)-based optimization to enhance security in healthcare applications. Mathematical Problems in Engineering. 2022; 2022(1):6802967.

[10] Kanagala P. Effective cyber security system to secure optical data based on deep learning approach for healthcare application. Optik. 2023; 272:170315.

[11] Kute SS, Tyagi AK, Aswathy SU. Security, privacy and trust issues in internet of things and machine learning based e-healthcare. Intelligent Interactive Multimedia Systems for e-Healthcare Applications. 2022: 291-317.

[12] Haseeb K, Saba T, Rehman A, Ahmed I, Lloret J. Efficient data uncertainty management for health industrial internet of things using machine learning. International Journal of Communication Systems. 2021; 34(16):e4948.

[13] Balakrishnan D, Rajkumar TD, Dhanasekaran S, Murugan BS. Secure and energy-efficient data transmission framework for IoT-based healthcare applications using EMCQLR and EKECC. Cluster Computing. 2024; 27(3):2999-3016.

[14] Malarvizhi Kumar P, Hong CS, Chandra Babu G, Selvaraj J, Gandhi UD. RETRACTED ARTICLE: Cloud-and IoT-based deep learning technique-incorporated secured health monitoring system for dead diseases. Soft Computing. 2021; 25(18):12159-74.

[15] Shukla S, Thakur S, Hussain S, Breslin JG, Jameel SM. Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. Internet of Things. 2021; 15:100422.

[16] Kathamuthu ND, Chinnamuthu A, Iruthayanathan N, Ramachandran M, Gandomi AH. Deep Q-learning-based neural network with privacy preservation method for secure data transmission in internet of things (IoT) healthcare application. Electronics. 2022; 11(1):157.

[17] Ramprasanth H, Harish K, Wilfred Blessing NR. Deep Q-Learning-Based Neural Network for Secure Data Transmission in Internet of Things (IoT) Healthcare Application. In Smart Healthcare and Machine Learning 2024 (pp. 41-56). Singapore: Springer Nature Singapore.

[18] Bi H, Liu J, Kato N. Deep learning-based privacy preservation and data analytics for IoT enabled healthcare. IEEE Transactions on Industrial Informatics. 2021; 18(7):4798-807.

[19] Thilagam K, Beno A, Lakshmi MV, Wilfred CB, George SM, Karthikeyan M, Peroumal V, Ramesh C, Karunakaran P. Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System. Journal of Nanomaterials. 2022; 2022(1):2638613.

[20] Gunasundari R, Swathiksha U, Hemalatha S. A Secured IoT Healthcare Architecture-Based Access Control System Using Deep Learning. InSmart Healthcare and Machine Learning 2024 (pp. 175-193). Singapore: Springer Nature Singapore.

[21] Ahmed MI, Kannan G. Secure and lightweight privacy preserving Internet of things integration for remote patient monitoring. Journal of King Saud University-Computer and Information Sciences. 2022; 34(9):6895-908.

[22] Li J, Meng Y, Ma L, Du S, Zhu H, Pei Q, Shen X. A federated learning based privacy-preserving smart healthcare system. IEEE Transactions on Industrial Informatics. 2021; 18(3).

[23] Kim L, Lloyd S, Marvian M. Hamiltonian quantum generative adversarial networks. Physical Review Research. 2024; 6(3):033019.

[24] Trojovská E, Dehghani M, Trojovský P. Zebra optimization algorithm: A new bio-inspired optimization algorithm for solving optimization algorithm. Ieee Access. 2022; 10:49445-73.

[25] Lee J, Duong PN, Lee H. Configurable encryption and decryption architectures for CKKS-based homomorphic encryption. Sensors. 2023; 23(17):7389.