*I. J. Computer Network and Information Security,* **2026, 4, 210-232**
Published Online on August 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2026.04.11

# ElGamal Based Homomorphic Encryption Using AT-BiGRU for Efficient Privacy Preserving Disease Prediction Scheme in Healthcare Data

**Bhawana S. Dakhare***
Terna Engineering College, Navi Mumbai, India
Plot No. 12, Sector-22, Opp. Nerul Railway Station, Phase-II, Nerul(W), Navi Mumbai, 400706, India
E-mail: bhawanadakhare@gmail.com
ORCID iD: https://orcid.org/0000-0002-3560-2402
*Corresponding author

**Lata L. Ragha**
Xavier Institute of Engineering, Mumbai, India
Opposite S.L.Raheja Hospital, Mahim Causeway, Mahim (West), Mumbai - 400016, Maharashtra, India
E-mail: lata.ragha@gmail.com
ORCID iD: https://orcid.org/0000-0002-6055-6671

Received: December 23, 2024; Revised: June 2, 2025; Accepted: August 19, 2025; Published: August 8, 2026

**Abstract:** Internet of Things (IoT) has revolutionized mobile healthcare applications, increasing diagnosis speed and accuracy. Disease prediction systems (DPS) improve healthcare quality, but they raise privacy concerns due to sensitive data. These concerns include illegal sharing, misuse, and exposure of sensitive information. However, developing new techniques does not provide improved protection from attackers and fraudsters. This paper suggests an effective privacy-preserving strategy for patient healthcare data from IoT devices in order to anticipate diseases in the contemporary medical field. Heart failure prediction health data is utilized as an input in this proposed approach. Initially, elastic net (EN) is used to reduce the dimensionality of the input raw dataset. Hyper parameter in EN is optimally selected using the Zebra Optimization Algorithm (ZOA). After dimensionality reduction, data is encrypted using the ElGamal technique. During the encryption procedure, the True Random Number Generator-Pseudo Random Number Generator (TRNG-PRNG) encryption method is used to generate the secret key. These encrypted data are securely stored in the cloud. Finally, attention-mechanism-based Bi-directional Gated Recurrent Unit (AT-BiGRU) technique is employed to predict heart disease. The ElGamal-TRNG-PRNG method strengthens privacy and security by achieving encryption and decryption times of 0.30 sec and 0.12 sec, respectively. The suggested model is evaluated and contrasted with current methods using encryption data performance measures. The model achieved 93.47% accuracy, 6.53% error, and 93.45% precision in encrypted data performance metrics. Therefore, this suggested method is the most effective way to safeguard healthcare records.

**Index Terms:** Disease Prediction System; Elastic Net; Zebra Optimization Algorithm; ElGamal; Healthcare data; TRNG-PRNG; AT-BiGRU.

## 1. Introduction

The medical industry's rapid embrace of the IoT has led to the creation of new security vulnerabilities as well as an intensified threat landscape for existing ones. [1]. The data gathered from IoT devices raises privacy concerns because it may be used to identify people and determine their location, as well as to obtain other critical information. Since IoT gadgets run equipment or store sensitive data in their memory, data access is crucial to a safe system [2]. The biggest problem in IoT security is striking a balance between security solutions and IoT device performance. Safety, security, and integrity are regulated by IoT security throughout deployment [3]. Numerous situations, such as the exchange of personal information, communications, and the recording of sensitive data, might give rise to privacy issues. In the IoT environment, the most important elements are personal information confidentiality, behavior, and communication security. These measures safeguard privacy, allow IoT device management, and prevent superfluous access controls [4]. All data should be checked to avoid vulnerabilities from being exploited as a result of strategies for detecting

misbehavior based on assumptions about component interactions [5].

Misbehavior identification in the Internet of Medical Things (IoMT) is difficult because of its limited computation, connectivity, power, and other resources [6]. Insider attacks could jeopardize the security of data transmission among IoMT devices and monitoring agents. To improve misbehavior detection, changes in data lead to higher false-positive rates and decreased detection method efficiency. Hence, IoMT devices need to be more effective and secured [7]. Despite several communication protocols addressing trust and security, there is still a shortage of privacy-preserving measures. Privacy issues may also arise when health monitoring services are outsourced to a semi-trusted cloud [8]. Hospitals must protect the clinical decision model's content, as it is important intellectual property with financial value. Additionally, clients need to safeguard their physiological characteristics and clinical judgments because unintentional disclosure might reveal their health status and cause major problems. As a result of technological developments, novel methods and algorithms have been created, potentially allowing attackers to obtain data with less processing power [9].

Machine learning with a focus on cryptography for privacy protection is being developed to address the challenges of hacking and cybercrime. Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), SHA-512, and Elliptic Curve Cryptography (ECC) are popular cryptography algorithms used to provide security [10]. These techniques, however, may result in slower key generation, lengthy verification processes, increased computational difficulty, and processing delays. Prediction models are valuable resources that require their security and privacy to be maintained by disease prediction systems (DPS). DPSs need to learn predictive algorithms from a large amount of clinical input. This approach is crucial for preventing incorrect decisions and ensuring patient safety. Furthermore, classification techniques such as Random Forest (RF), K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Artificial Neural Network (ANN), Decision Tree (DT), and Deep Belief Network (DBN) reduce the problems of inaccurate predictions, high error rates, and process delays, which affect the overall efficacy of the safety protocol. To address these issues, the study focuses on privacy-preserving disease prediction utilizing modified ElGamal encryption and AT-BiGRU techniques.

The following lists the primary goals of this suggested strategy:

- To reduce the dimensions of the input healthcare data, Zebra Optimization Algorithm (ZOA)-based Elastic Net is used.
- To select the hyperparameters of Elastic Net optimally, ZOA is employed in this approach.
- For encrypting and reducing the noise in the homomorphic encryption, ElGamal based homomorphic encryption algorithm is employed.
- To generate the key in the encryption algorithm, the TRNG-PRNG key generation algorithm is utilized.
- To reduce memory overhead and detect heart disease from encrypted data, an attention-mechanism-based Bi-directional Gated Recurrent Unit (AT-BiGRU) is used.

The rest of the article is organized as follows: Technical limitations and a review of the state of the art are discussed in Section 2. Section 3 provides a thorough explanation of the introduced framework. The performance of the suggested system is examined and assessed in Section 4. The conclusion and future scope are examined in Section 5.

## 2. Literature Review

The healthcare industry has benefited from advancements like IoTs, sensors, and electronic applications, but security, privacy, and assurance remain concerns. To evaluate the security and privacy issues that are now present in health care facilities, numerous studies have been carried out in recent years. In this section, several of the prior pieces are reviewed.

Ma et al., [11] developed a random forest (RF) method, called PHPR. PHPR was capable of making precise predictions and safely training on medical data from various data owners. The system performs real-time handling of outsourced processes and guarantees calculation correctness. Without compromising privacy, the original data and computed results may be processed and kept safely on the cloud. Experiments utilizing real-world datasets demonstrate that PHPR retains the same prediction accuracy as the original classifier even over ciphertexts. However, there was an excessive communication overhead.

Padinjappurathu Gopalan et al., [12] provided a method for gathering patient health data from Internet of Things devices in a way that protects privacy in order to anticipate sickness in a contemporary healthcare system. Through the use of LR-ECC communication, qualified healthcare personnel can safely extract patient information from the system. An EHGA-DLNN based on the Herding Genetic Algorithm was used to evaluate the data for sickness prediction. In comparison to previous approaches, the experimental findings reveal better prediction accuracy, privacy, and security. Security rating was 98.87%. However, these classifiers lack security, posing a substantial risk of exposing the prediction model to outsiders.

Zhu et al., [13] created CREDO which was an extensive medical pre-diagnosis technique that protects privacy and is based on multi-label KNN. It guarantees the security of sensitive health information belonging to medical users while enabling service providers to offer high-efficiency services without disclosing pre-diagnosis model data. ML-KNN

classification was used by the service provider to determine medical occurrences and deliver services. The customer is the only person who can obtain the pre-diagnosis result since the request vector was encrypted before sending. CREDO has less computational complexity. However, medical users can simultaneously be affected by multiple diseases.

Alabdulkarim et al., [14] established a clinical decision-support system that protects patient privacy by utilizing an innovative single decision tree algorithm. To safeguard user data, the system employs nonces to thwart unauthorized parties' decoding and a homomorphic encryption cipher. The approach performs 46.46% better than the Naïve Bayes algorithm, according to simulation findings, even after controlling for key value and size. The frequency of attribute values, identified symptoms, and the model's compliance with hospital dataset privacy regulations serve as validation points. Sharing data privacy raises serious concerns as it may compromise patients' privacy.

Jayaram and Prabakaran [15] suggested a cloud-based, edge-centric healthcare system design with security features. Edge-level progressive homomorphic security that preserves privacy is recommended for secure processing of data and non-sensitive information filtering. Through the filtering and offloading algorithms, the system reduces response time and network capacity use. An adaptable stacked probabilistic classification model was suggested for remote rehabilitation of patients and onboard disease prediction in contrast with present techniques, which boost prediction accuracy and speed. The dataset on Parkinson's disease was empirically evaluated to illustrate the SECHS. However, cloud database's medical data was not adequately protected.

Based on the research mentioned above, several security and privacy concerns to healthcare systems techniques that are currently in use have various drawbacks as, there was too much overhead in communicating [11], classifiers are not secure, which poses a serious danger [12], multiple diseases can be concurrently contracted by medicinal users [13], sharing data privacy exposes patients' privacy at risk [14] and inadequate security for health information kept in cloud databases [15]. All of these approaches have lower levels of data security and confidentiality. Furthermore, predicting reliability and efficacy are typically poor. Thus, this paper resolves the aforementioned issues by using AT-BiGRU techniques and modified ElGamal encryption for privacy-preserving disease prediction.

## 3. Proposed Methodology

Internet of Things (IoT) technologies in healthcare make life easier for patients and medical professionals by proactively analyzing health data to prevent sickness. However, privacy problems occur as an outcome of the usage of patient information and medical data, which can cause treatment delays and perhaps endanger a patient's life. Disease prediction systems are critical in forecasting disease risks, and the expansion of data mining techniques has led to the development of such systems using machine learning algorithms. Despite their potential, these systems have challenges such as information security and prediction efficiency, which restrict their practical application. As a result, attaining reliable disease prediction without sacrificing precision is a difficult undertaking. In this paper, ElGamal with TRNG-PRNG based encryption and modified BiGRU is developed for privacy preserving disease prediction. The overall workflow of this approach is shown in Figure 1.

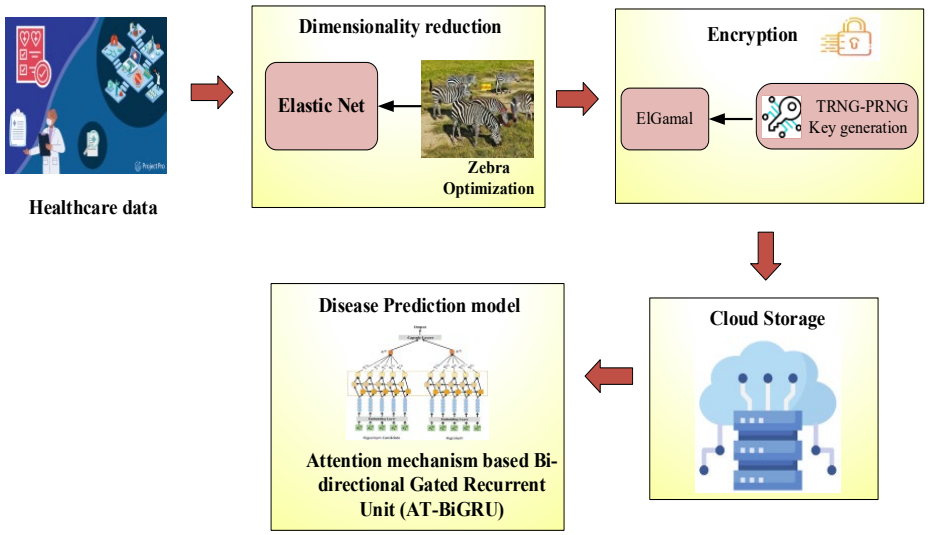


Fig. 1. Overview of the Secure Data Processing and Heart Disease Prediction.

Medical records are regarded as private inputs for disease prediction in this framework which protects patient privacy. Using the Elastic Net, the dimension of an input raw data set is first decreased without sacrificing the information itself. An Elastic Net's hyperparameters may be optimally selected through a technique called Zebra Optimization Algorithm (ZOA). After dimensionality reduction, the selected data are encrypted using homomorphic encryption called ElGamal approach. In the encryption algorithm, the secret key is generated using True Random

Number Generator-Pseudo Random Number Generator (TRNG-PRNG) encryption algorithm. Next, data is transformed into ciphertext using homomorphic functions including addition, multiplication, and rescaling. This enables data to be used and examined as though it were still in its original format. These data are encrypted and kept in the cloud. After that, attention-mechanism-based Bi-directional Gated Recurrent Unit (AT-BiGRU) approach is utilized to predict the heart disease.

### *3.1. Dimensionality Reduction*

One technique for converting high-dimensional data into low-dimensional representations is called "dimensionality reduction." As high-dimensional data (HDDs) have grown in popularity, several dimensionality reduction techniques (DRTs) are now widely used in many applications. DRTs solve the problem of the curse of dimensionality by transforming the data into a low-dimensional representation while maintaining the original semantics of the data. Low-dimensional data is a useful tool in many disciplines since it is simpler to handle, evaluate, and visualize. To reduce the dimensions of the input healthcare data, the Zebra optimization (ZOA)-based Elastic Net is applied.

#### *3.1.1. Elastic Net*

Large datasets with more predictors (features-N) than observations (subjects-K) are typically better suited for the LASSO model. Because of the strong correlations among the predictors, it is not resilient. A novel feature selection technique called Elastic Net (EN) often performs better than LASSO. The EN technique balances the L1 and L2 regularization norms, while the LASSO method solely considers the L1 norm of$L^1L^2L^1$ β. When there are many more predictors (features) than observations, this approach performs exceptionally well [16].

The problem is solved for non-negative $\lambda$ values by the EN by introducing a penalty term depending on $\alpha$, with a value of $0 < \alpha < 1$,

$$\min_{\beta_0,\beta}\left(\frac{1}{2k}\sum_{i=1}^{K} y_i - \beta_0 - x_i^T\beta\right)^2 + \lambda D_\alpha(\beta) \tag{1}$$

Where,

$$D_\alpha(\beta) = \frac{1-\alpha}{2}\|\beta\|_2^2 + \alpha\|\beta\|_1 \tag{2}$$

Between the square of the $L^2$ norm of β and the $L^1$ norm, the penalty term $D_\alpha(\beta)$ interpolates. The best hyperparameter is chosen using ZOA in order to minimize error. Zebra Optimization Algorithm

Zebras are equine mammals native to eastern and southern Africa, notable for their black-and-white striped coats. It helps to hide from attackers and discourage biting insects since these stripes are positioned vertically on the neck and body. Zebras range in size from 110 to 160 cm in the shoulders, 210–300 cm in body length, and weigh 175–450 kg. Their head is made to consume grass, while they possess long, skinny legs, a single toe on every foot, and a lengthy neck. Zebras engage in two primary social behaviors: foraging and predator protection. By leading the herd across the plains, a pioneer zebra makes room for additional zebras to migrate and graze [17]. Zebras' primary defense against predators is to flee in a zigzag manner. However, they might group to mislead or intimidate the predator. The ZOA design depends on computational simulations of two forms of smart zebra behavior: the zebras' protection mechanism against predator assaults and their foraging activity.

Mathematical model for the Zebra Optimization is given below:

*Step 1: Initialization*

The population of the ZOA has been replaced with hyperparameter alpha. Equation (3) provides the necessary formula to represent the initialized procedure.

$$\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \tag{3}$$

Where, $\alpha$ represents the alpha it controls the strength of regularization.

*Step 2: Fitness Function*

The error is calculated in order to assess the fitness value. Its conceptual representation is shown in equation (4).

$$fitness\ function = minimise\ (E) \tag{4}$$

$$E = \frac{1}{2}\sum_{n=1}^{N}(y_n - z_n)^2 \tag{5}$$

Where E denotes Mean Squared Error (MSE), $z_n$ as actual value, and $y_n$ is the displayed value.

*Step 3: Update*

The value is changed for every population member's position until it reaches an ideal value. Thus, zebras' positions are updated by two of their normal actions, such as foraging and predator-defence maneuvers.

Zebra positions during the foraging phase can be updated mathematically by employing equations (6) and (7).

$$x_{i,j}^{new,P1} = x_{i,j} + r.(PZ_j - I.x_{i,j}) \tag{6}$$

$$X_i = \begin{cases} X_i^{new,P1}, F_i^{new,P1} < F_i; \\ X_i, else, \end{cases} \tag{7}$$

In this case, $x_{i,j}^{new,P1}$ is the ith zebra's new position based on the first phase. $PZ$ is the initial zebra, regarded as the most superior member. $PZ_j$ is their jth dimension. $r$ is an arbitrary number in the interval [0, 1]. $I = round\ (1 + rand)$, where rand is a random value in the interval [0, 1]. Its objective function value is represented as $F_i^{new,P1}$. Thus,$I \in \{1, 2\}$ as a result, and there are much more variations in population movement if parameter $I = 2$.

Using equations (8) and (9), the location of the ZOA population is updated by the use of zebra defensive mechanisms against predator assaults.

$$x_{i,j}^{new,P2} = \begin{cases} S_1: x_{i,j} + R.(2r - 1) \\ .\left(1 - \frac{t}{T}\right).x_{i,j,} \ \ P_s \le 0.5; \\ S_1: x_{i,j} + r.\left(AZ_j - I.x_{i,j}\right), else, \end{cases} \tag{8}$$

$$X_i = \begin{cases} X_i^{new,P2}, F_i^{new,P2} < F_i; \\ X_i, else, \end{cases} \tag{9}$$

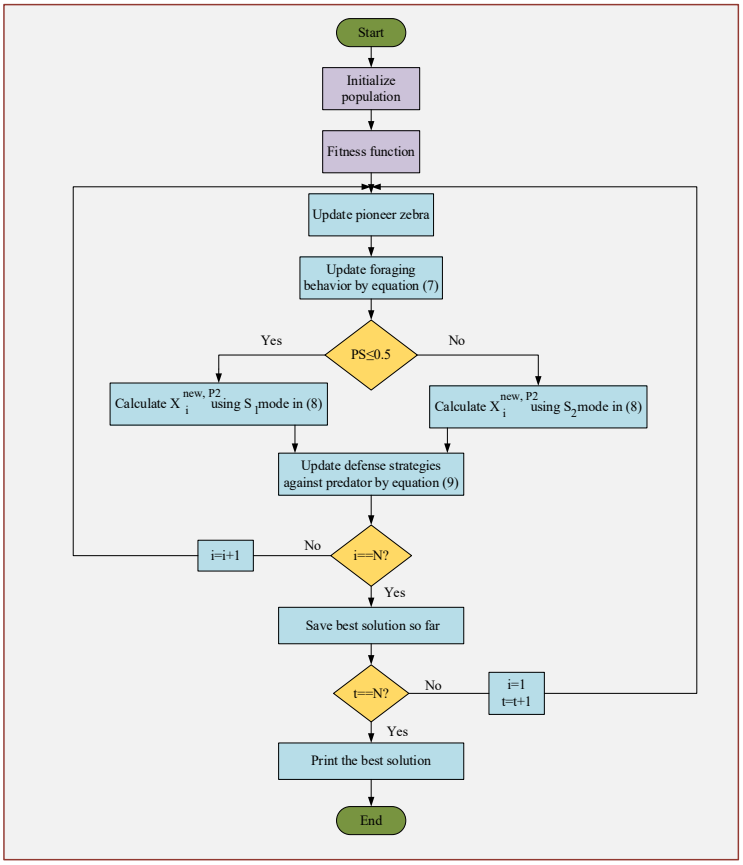


Fig. 2. Process Flow of the Zebra Optimization Algorithm.

In this case, t represents the current iteration, T represents the maximum number of iterations, R represents a constant value of 0.01, $P_s$ represents the probability of selecting one of two randomly generated strategies in the interval [0, 1], AZ represents the targeted zebra's status, and $AZ_j$ represents the jth dimension value. $x_{i,j}^{new,P2}$ represents the ith zebra's new state from the second phase.

*Step 4: Termination*

The process of selecting options ends after the best choice has been determined. After dimensionality reduction, the selected data are encrypted using homomorphic encryption called ElGamal approach. The flow chart for ZOA algorithm is given in Figure 2.

### *3.2. Encryption Process*

The process of converting plain text data (plaintext) into something that seems random and meaningless (ciphertext) is known as encryption. For encrypting the selected features, ElGamal based homomorphic encryption algorithm is employed.

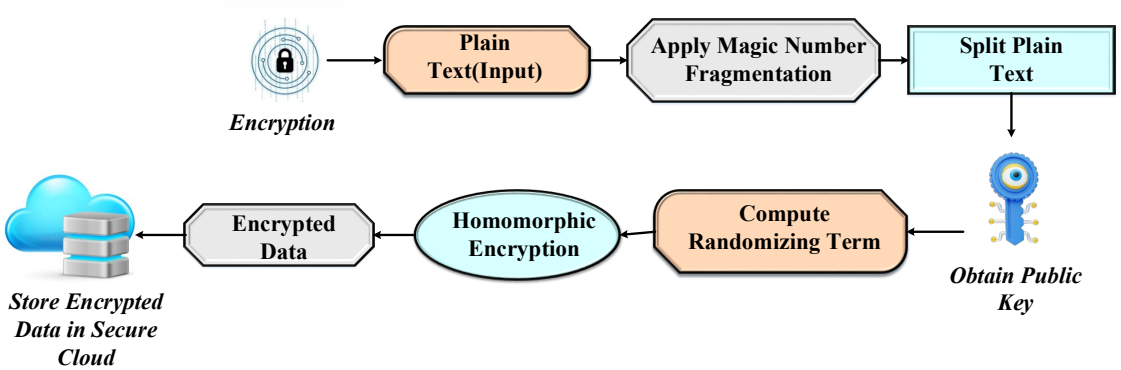


Fig. 3. Architecture for the Encryption Model.

Figure 3 shows a secure encryption process where plain text is fragmented using a magic number, split, and then encrypted using homomorphic encryption with a public key and randomizing term. This encrypted data is securely stored in the cloud, enabling privacy-preserving computation without exposing the original information.

### *3.2.1. ElGamal based homomorphic encryption*

An FHE encryption technique with unlimited homomorphic additions and multiplications is presented in this section. The two components of the method, which use El-Gamal encryption principles, are a multiplicative encryption scheme for multiplicative property and a linear encryption strategy for homomorphic addition [18]. El-Gamal encryption uses generator g, independent of public key $y$, and random number $r$. Power of $g$ equals $m$, speeding up the power computation of large integers.

While homomorphic multiplication is possible with RSA, El-Gamal is the main emphasis because of its message integrity characteristic. El-Gamal has $m + m'$ on both sides, hence in order to decode the second component, the first section must first be decrypted. Private channels present a major sharing challenge for symmetric FHE schemes, notwithstanding their efficiency in accelerating and allocating resources. By tackling the problem of lengthy encryption durations brought on by exponentially complicated computation, the MNF-G technique seeks to simplify and allocate resources in asymmetric FHE. For safe and lightweight protection, the scheme's main goal is to provide linear cyclic asymmetric encryption.

$$c = (m + r \times \rho) mod\ n \tag{10}$$

Where $n = p \times q$. Equation (10) are improved to mitigate the vulnerability to plain text assaults and other forms of attacks.

$$c = (m \times k + r \times \rho) mod\ n \tag{11}$$

Elgamal's El-Gamal encryption mode originated from this method, but Equation (11) is weak as obtaining two plain texts can lead to the recovery of all ciphered entities. The proposed encryption scheme hides plain text by randomly fragmenting m into $m'$ and $m''$, making it difficult for attackers to extract $p$, using the following equation (12).

$$c = (m' + m'' \times k + r \times \rho) mod\ n \tag{12}$$

Verification of homomorphic multiplication is challenging due to $k^2$ multiplication. Encryption involves ciphered text $c_+$ and $c_\times$. The Diffie-Hellman key exchange is the foundation of the safe and effective El-Gamal cryptosystem. It generates keys using a finite cyclic group, encrypts using a random integer, and decrypts using a one-way function. Variations include quotient rings, classical, $Z_n$, Gaussian integers, and bilinear encryption for data aggregation that protects privacy.

*i) Fundamental elements for the FHE method design*

MNF-G (Magic Number Fragmentation and El-Gamal encryption) shall be covered entirely in the subsection that follows. The cyclic group $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{0,1, \dots, p-1\}$ and the primitives P,C,K, Enc(), Dec() are considered.

- P as a simple text ring $\mathbb{Z}_p$
- C representing an encrypted text ring$\mathbb{Z}_n$
- K the pivot ring
- Utilizing $pk \in K$ and encrypting data with enc(),$Enc_{pk}: P \to C$
- Dec() as the decrypt method $Dec_{sk}: C \to P\ with\ Sk \in K$

Fully homomorphic encryption approach consists of three steps:

- KeyGen: yields a public key $pk$ and a secret key $sk$, respectively, $(sk, pk) = (k, k + r \times p, g)$.
- Enc(m): a plain text $m \in P$ employs the public key for encryption $pk$,$c_+ = (m' + m'' \times pk) mod\ n$, $c_\times = (m \times g^m) mod\ n$
- Dec(c): Using the secret key $sk$, a ciphered text is decoded, $m = (c_+ mod p) mod (k-1), m = c_\times \times (g^m)^{-1} mod\ p$

Two main topics of this proposal are the magic fragmentation of m and the difficulties of the number factorization.

*Encryption*

The proposed scheme uses asymmetric encryption to send ciphered text to Bob using a shared public key. The

encryption process involves a shared public key, with $m' < p \rightarrow cmodp = m' + (m'' \times k)modp$ and $m'' < p \rightarrow (m'' \times k \times k^{-1})modp = m''$.

*Decryption*

Decryption recovers the plaintext from the ciphertext using the formula and $.c = c_+, c_\times c_+ = m' + m'' \times k + r \times p$ It is first extracted from $c_+$, then $c_+ modp = m' + m'' \times k$, and since $m \times kmod(k-1) = m\ then\ Dec\ (c_+) = m$.

*ii) Homomorphic additive property*

$Enc(m_1) + Enc(m_2) = m_1' + m_1'' \times pk + m_2' + m_2'' \times pk = (m_1' + m_2') + (m_1'' + m_2'') \times pk = E\ (m_1 + m_2)$ and $c = c_1 + c_2 + \cdots + c_i = (m_1' + m_1'' \times pk) + (m_2' + m_2'' \times pk) + \cdots + (m_i' + m_i'' \times pk) = \left(m_1' + m_2' + \cdots + m_i'\right) + \left(m_1'' + m_2'' + \cdots + m_i''\right) \times pk = m' + m'' \times pk$, where $m' + m'' < p$ from encryption and decryption. Hence, the additive property holds. Typically, the additive property is obtained$Dec\ (c) = m_1 + m_2 + \cdots m_i = m$

$$\sum_{i=1}^{t} Enc(m_i) = Enc(\sum_{i=1}^{t} m_i) \tag{13}$$

*iii) Homomorphic multiplicative property*

Let $c_1$ and $c_2$ be two encrypted characters with ciphers from $m_1 = m_1' + m_1''$ and $m_2 = m_2' + m_2''$, respectively. Enc $(m_1) \times$ Enc $(m_2) = (m_1 \times g^{m_1} \times m_2 \times g^{m_2}) = (m_1 \times m_2 \times g^{m_1} \times g^{m_2}) = (m_1 \times m_2 \times g^{m_1 + m_2}) = (m \times g^s)$ where $s = m_1 + m_2$. To ensure the property of multiplication, it is necessary to guarantee the decryption of $m \times g^s$, which can be achieved by adding the first part, resulting in $Enc\ (m_1) \times Enc(m_2) = (c_{1+} + c_{2+}, m_1 \times m_2 \times g^{m_1 + m_2}$.

$$\prod_{i=1}^{t} Enc(m_i) = Enc(\prod_{i=1}^{t} m_1) \tag{14}$$

The private key is created using the TRNG-PRNG key generation mechanism.

*Key Generation Using TRNG-PRNG Module*

To increase security, every clock cycle and plaintext character creates a key value for this TRNG-PRNG module. Figure 4 shows the general design with 80-bit key generation system. Typically, digital circuits are used in the construction of the TRNG to provide real randomness through unexpected effects. Here, the $random function is used to produce the TRNG. Additionally, the general circuit architecture that generates the 80-bit key is known as PRNG [19].

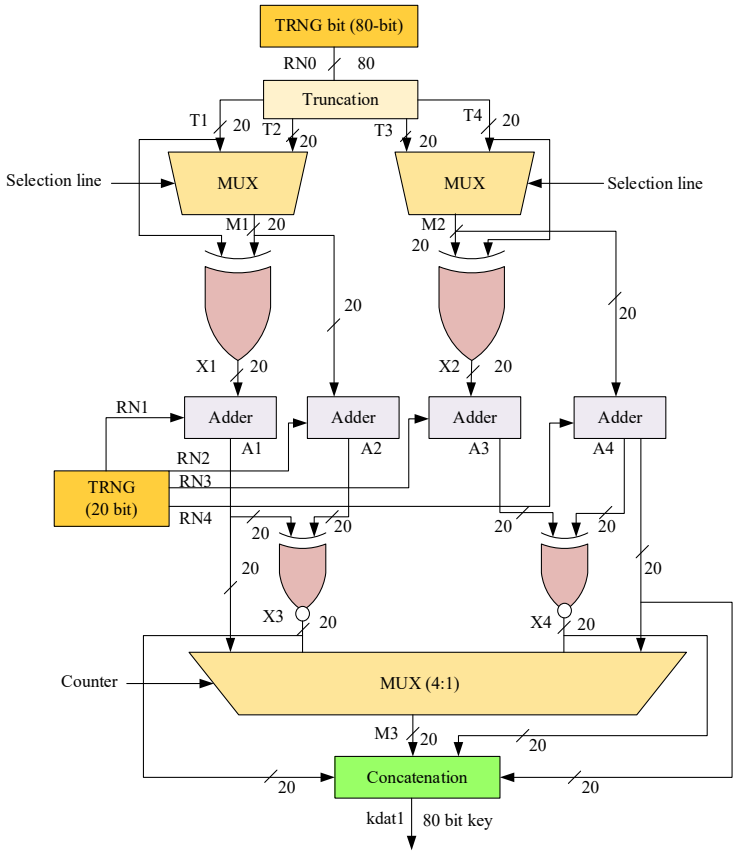


Fig. 4. Architecture of TRNG-PRNG module.

The following steps are involved in the key generation process.

a. TRNG-PRNG module first generates the actual random number, represented as RN0, which is an 80-bit value. Next, four 20-bit values, T1, T2, T3, and T4, are created by truncating this 80-bit RN0 value, which is shown in equation (15).

$$\begin{aligned} T1 &= RN0[0:19] \\ T2 &= RN0[20:39] \\ T3 &= RN0[40:59] \\ T4 &= RN0[60:79] \end{aligned} \tag{15}$$

b. Equation (16) illustrates how the selection line is used to operate the MUX's output.

$$\begin{aligned} M1 &= MUX(T1, T2) \\ M2 &= MUX(T3, T4) \end{aligned} \tag{16}$$

Where M1 and M2 stand for the MUX function levels within the pairs of T1−T2 and T3−T4, respectively.

c. Equation (17) states that X1 and X2, accordingly, reflect the XOR action involving the pairings of M1−T1 and M2−T4.

$$\begin{aligned} X1 &= XOR(M1, T1) \\ X2 &= XOR(M2, T4) \end{aligned} \tag{17}$$

d. One TRNG is used in the procedure for creating keys to generate four 20-bit values, which are subsequently added by four different adders, as shown in equation (18).

$$\begin{aligned} A1 &= X1 + RN1 \\ A2 &= M1 + RN2 \\ A3 &= X2 + RN3 \\ A4 &= M2 + RN4 \end{aligned} \tag{18}$$

e. As shown in equation (19), the numbers of A1-A2 and A3-A4 are processed using the XNOR procedure following the addition for both pairs.

$$X3 = XNOR(A1, A2) \\ X4 = XNOR(A3, A4) \tag{19}$$

f. The MUX operation uses four inputs, with output determined by counter values. The output is A1 when the counter value is 0, X3, A4, and X4.
g. The TRNG-PRNG module's result is used in the encryption procedure, an 80-bit key for kdat1 through a concatenation operation between X3, M3, X4, and A4, as input for the encryption process.

In order to achieve high operating frequency and low space use, the PRESENT architecture optimizes hardware components utilizing DROM. A stronger defense against attackers is provided by key creation for every round and plaintext, because of this, it is challenging to decode the initial plain text without understanding the key value. These data are encrypted and stored in the cloud. Using these encrypted data, the heart disease is detected by attention mechanism based Bi-directional Gated Recurrent Unit (Bi-GRU).

### *3.3. Classification*

Selected encrypted data are used as input for a classification procedure developed for privacy-preserving heart disease prediction. The model uses an attention-mechanism-based Bi-directional Gated Recurrent Unit (AT-BiGRU) to predict heart disease.

GRU must be configured to function with the recursive network architecture by modifying the standard GRU memory unit to accept the input from two child nodes. From now on, researchers will refer to this extended dual-input GRU as BiGRU [20]. Given a BiGRU node unit $j$, its output is $h_j$, and its left and right child nodes' outputs are $h_j^L \; and \; h_j^R$, respectively. An example of the $h_j$ calculating method is given in equation (20).

$$h_j = z_j\left(\omega^L h_j^L + \omega^R h_j^R\right) + \left(1 - z_j\right)h_j \tag{20}$$

In this case, $\omega^L + \omega^R = 1$, $\omega^L \; and \; \omega^R$ indicate the weights for both of the GRU unit's top and bottom nodes, respectively.

For BiGRU node $j \; is \; z_j$ as the update function. As it primarily controls whether the BiGRU is updated, its purpose resembles that of a command gate, hence it is additionally referred to as a change gate at times. A child node's output $h_j^L, h_j^R$ is determined by the input vector$x_j$. The gate used for updating determines if it needs to modify the cell's internal state. An example of the exact method used to determine the update gate $z_j$ of the BiGRU is provided by equation (21).

$$z_j = \sigma\left(W_z x_j + U_z\left(\omega^L h_j^L + \; \omega^R h_j^R\right)\right) \tag{21}$$

BiGRU node $j$ candidate output, $\tilde{h}_j$ is computed as shown in equation (22). Here, $W \; and \; U$ are parameter matrices, $x_j \in R^d$ denotes a term represented as a d-dimensional vector, and stands for the Gaussian curve $f$. $\odot$ is the symbol for the multiplying of dots.

$$\tilde{h}_j = f\left(W_h x_j \; + \; U_h\left(r_j \odot \left(\omega^L h_j^L + \omega^R h_j^R\right)\right)\right) \tag{22}$$

Mainly controlling whether or not restore gateway resets the data storage unit $r_j$. In order to avoid permanent dependency, the GRU is capable of ignoring previous data whenever the restore function's output is close to zero. Equation (23) illustrates this specific computation of the resetting function:

$$r_j = \sigma\left(W_Z x_j + U_r\left(\omega^L h_j^L + \; \omega^R h_j^R\right)\right) \tag{23}$$

For the nonlinear function $\sigma$, one often uses the $tanh$ function. When the dimensions of the input word vector are $h_j, r_j, z_j \in R^d \; and \; d$, it is feasible to predict disease categories using softmax for the BiGRU.

*i) Attention Mechanism:*

It is acceptable to assume that the source in this attention mechanism consists of many data pairs. Value, key, and query are the three fundamental components of the attention mechanism. The following is a summary of the way the attention value is determined. Equation (24) can be used to characterize the basic concept of the attention mechanism as the conversion of a query into a series of keys and values:

$$Attention\ (Query, Source) = \sum_{i=1}^{L_x} Similarity\ (Query, key_i) * Value_i \tag{24}$$

Where $L_x = \|Source\|$ is the total length from the data source. The AT-BiGRU model's detailed design is shown in Figure 5.

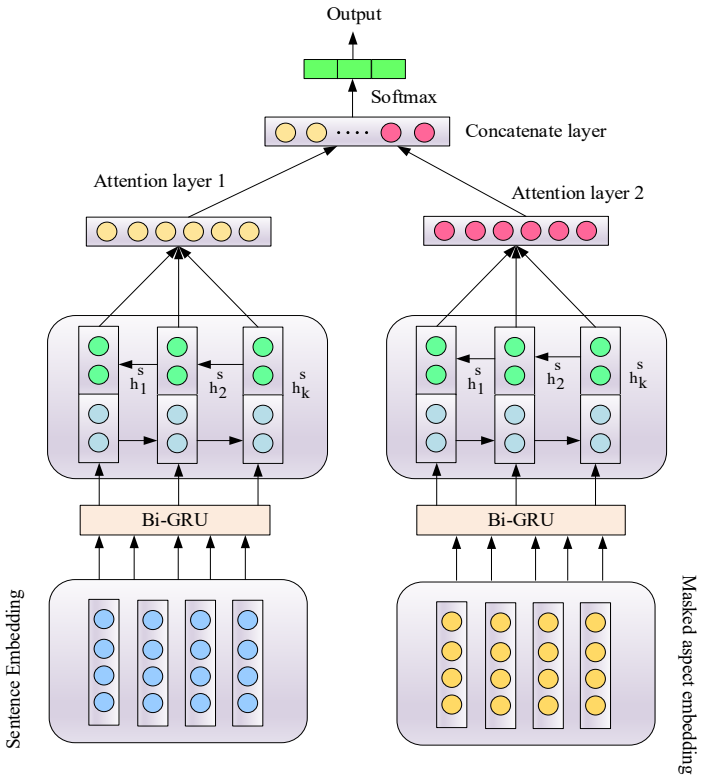


Fig. 5. Architecture of the Attention Mechanism Based Bi-Directional Gated Recurrent Unit.

The specialized calculation approach of the attention mechanism may be abstracted in three phases. Based on the association among each Query and each Key, this initial stage calculates the weight factor for every feature that matches the query. The subsequent stage uses the identical softmax function to emphasize the weights of important components and equalize the weights. Equation (25) presents the specific computation for the weight coefficient associated with Value, denoted by $a_i$.

$$a_i = Soft\max(Sim_i) = \frac{e^{Sim_i}}{\sum_{j=1}^{L_x} e^{Sim_j}} \tag{25}$$

In the final step, the weight and the corresponding key score are combined to produce the final attentive value. Therefore, AT-BiGRU is developed for privacy preserving disease prediction. The Pseudo code of this privacy preserving disease prediction method is given in Algorithm 1.

**Algorithm 1**. Pseudocode for privacy preserving disease prediction

**Input:** D= Healthcare data
# Dimensionality reduction
{
EN = Elastic net (D) // To reduce the dimensions of the input healthcare data using equation (1) and (2)
ZOA = Zebra optimization (EN) // To select the hyperparameters of Elastic Net optimally using equations (6) to (9)
}
# Encryption process
{
EG = ElGamal based homomorphic encryption (EN) // For encrypting the selected data
TRNG-PRNG = True Random Number Generator-Pseudo Random Number Generator (EG)// For generating the key in

the encryption algorithm
}
#Classification
{
AT-BiGRU = Attention- Bidirectional Gated Recurrent Unit (EG) // To detect the heart disease from encrypted data
}
Output: privacy preserving disease prediction
End

## 4. Results and Discussion

Cloud-based healthcare services have grown in popularity as a result of centralized electronic healthcare records (EHR) and remote patient services. However, the expanding Healthcare 4.0 business necessitates the maintenance of security and privacy. In order to overcome these issues, the proposed system uses an efficient and privacy-preserving classification scheme for the health monitoring system. Healthcare data are considered to be input private data. Initially, input raw data are reduced using a dimensionality reduction technique called Elastic Net. The Zebra Optimization Algorithm (ZOA) is used to optimize Elastic Net's hyper parameter. The ElGamal approach is used for encrypting the selected data, where the secret key is generated using the TRNG-PRNG encryption algorithm. The secured data are fed into AT-BiGRU to detect heart disease. The entire model is designed and implemented in Python, and an NVidia GeForce GTX 1650 GPU, an Intel Core i5 CPU, a 64-bit operating system, and 16GB of RAM are among the system specifications.

*i) Dataset 1*

The heart failure prediction dataset is collected from Kaggle [21]. Cardiovascular diseases are the main cause of mortality globally, accounting for 17.9 million fatalities per year. Heart attacks and strokes are prevalent causes, accounting for one-third of early deaths in those under the age of 70. A dataset including 11 indicators can predict cardiac disease, allowing for early identification and care in high-risk patients. Records include the patient's age, sex, kind of chest pain, resting blood pressure, cholesterol, blood sugar levels after fasting, findings of the resting ECG, exercise-induced angina, ST_Slope, and heart disease.

*ii) Dataset 2*

The dataset, collected over a 2-month period in India, consists of 400 rows and 25 features, including red blood cells, pedal edema, sugar levels, and more. The objective is to classify whether a patient has chronic kidney disease (CKD) or not, based on the "classification" attribute, which can either be 'ckd' (chronic kidney disease) or 'notckd'. Data cleaning was performed, including mapping textual values to numerical ones and other necessary transformations. Exploratory Data Analysis (EDA) was conducted to better understand the dataset. After splitting the data into training and testing sets, machine learning models were applied. The initial results were not satisfactory. Instead of dropping rows with missing (NaN) values, a lambda function was used to replace them with the mode of each respective column [22]. The dataset was split into training and testing sets, with 320 rows used for training and 80 rows for testing. The process was repeated, and the models were applied again. The results significantly improved, with Random Forest and Decision Tree models emerging as the top performers, achieving an accuracy of 1.0 and zero misclassifications. Model performance was assessed using the confusion matrix, classification report, and accuracy metrics. The dataset is 48.55 KB in size.

*iii) Dataset 3*

The dataset contains comprehensive health information for 2,149 patients, each identified by unique patient IDs ranging from 4751 to 6900. A total of 1,709 rows were used for training the model, and 430 rows were used for testing. It includes demographic details, lifestyle factors, medical history, clinical measurements, cognitive and functional assessments, symptoms, and a diagnosis of Alzheimer's Disease [23]. The dataset is ideal for researchers and data scientists aiming to explore factors associated with Alzheimer's, develop predictive models, and conduct statistical analyses.

*iv) Dataset 4*

The UCI Heart Disease dataset is a widely used medical dataset designed to predict the presence of heart disease in patients based on 14 key clinical attributes such as age, sex, chest pain type, resting blood pressure, cholesterol levels, fasting blood sugar, electrocardiographic results, maximum heart rate, exercise-induced angina, ST depression, slope of the ST segment, number of major blood vessels, and thalassemia status [24]. The target variable indicates whether a patient has heart disease, often simplified into a binary classification of presence or absence.

*v) Dataset 5*

The MIMIC-III dataset is a large, publicly available clinical database containing detailed information from over 61,000 intensive care admissions, including 47 features related to demographics, vital signs, and lab results of sepsis patients. This project explores the use of offline deep reinforcement learning (RL) to develop a Clinical Decision Support System aimed at optimizing sepsis treatment strategies in emergency care[25].

Table 1. Parameters of Zebra Optimization.

| Hyperparameter | Selection |
|---|---|
| Max.Iteration | 100 |
| Searching agent | 10 |
| Lower bound | 0 |
| Upper bound | 1 |

Table 2. Specifications of AT-BiGRU.

| Hyper parameter | Selection |
|---|---|
| Learning rate | 0.001 |
| Optimizer | RMSprop |
| GRU | 20 layers |
| Attention | 1 layer |
| Activation | Sigmoid for all layer |

Simulation parameters of the Zebra Optimization Algorithm are given in Table 1. For ZOA, the number of iterations was varied between 50 and 200 in increments of 25. Results showed that performance improvements plateaued around 100 iterations, beyond which computational cost increased without significant gains. Thus, 100 iterations were selected as the optimal value, balancing efficiency and optimization quality. Likewise, the classification algorithm AT-BiGRU is given in Table 2. In the case of the GRU layers, configurations ranging from 5 to 25 layers were tested. The highest classification accuracy and precision were achieved at 20 layers. Fewer layers resulted in underfitting, while additional layers introduced overfitting and increased training time without performance benefits. Regarding the learning rate, a range of values including 0.01, 0.005, 0.001, and 0.0005 were explored using the RMSprop optimizer. A learning rate of 0.001 provided the most stable convergence and optimal predictive accuracy. Higher rates led to unstable training, while lower rates significantly slowed convergence with minimal accuracy improvement. These findings confirm that the chosen hyperparameters (ZOA iterations = 100, GRU layers = 20, learning rate = 0.001) represent the most effective configuration for the proposed system, ensuring both reliable performance and practical training efficiency.

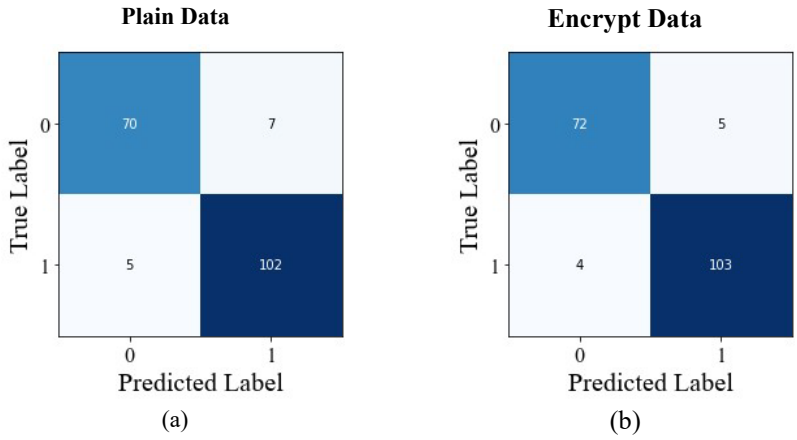


Fig. 6. Confusion matrix for plain data and encrypted data.

The confusion matrix for the proposed plain data model is shown in Figure 6(a). It is used to ascertain if a classification machine can distinguish between predictions that are correct and those that are not. For classes 0 and 1, the estimated plain data is 70 and 102. Figure 6 (B) shows the confusion matrix for the encrypted data. Based on the given data, the technique's class categorization contains both successful and inaccurate classifications. The predicted values for classes 0 and 1 are 72 and 103, respectively.

**Plain Data** **Encrypt Data**

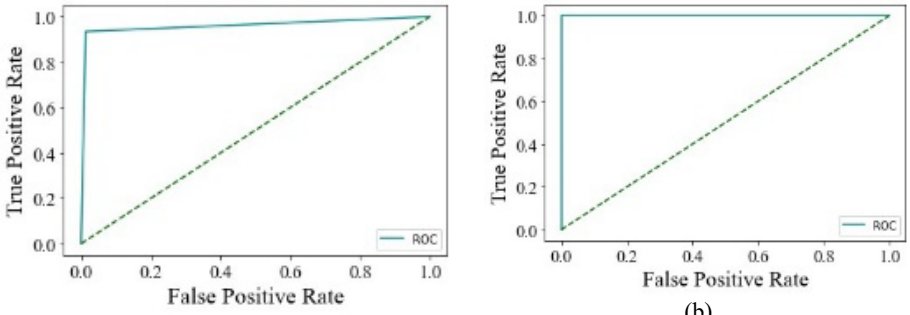


Fig. 7. ROC plot.

The ROC curve for the suggested model is displayed for both plain and encrypted data in Figures 7(a) and 7(b). The receiver operating characteristic curve is a plot that illustrates the performance of a classification model. The link among the percentage of FPR and TPR can be represented using ROC curves in a prediction model with different probability thresholds used.

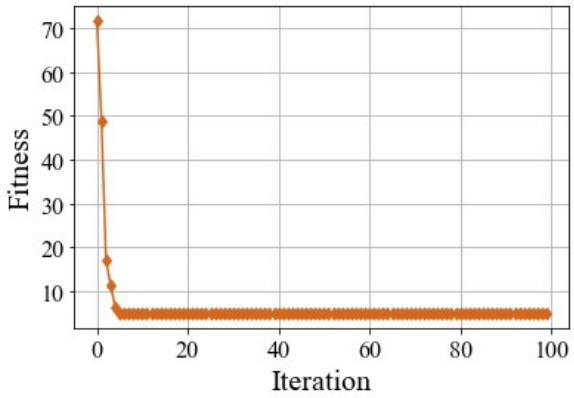


Fig. 8. Graph of convergence for the ZOA algorithm.

Figure 8 shows the convergence graph of the optimization technique. The zebra optimization's fitness value is measured using mean square error. It measures difference between expected and actual values of the entire training set. In the hundredth iteration, the zebra optimization's fitness is 0.1%.

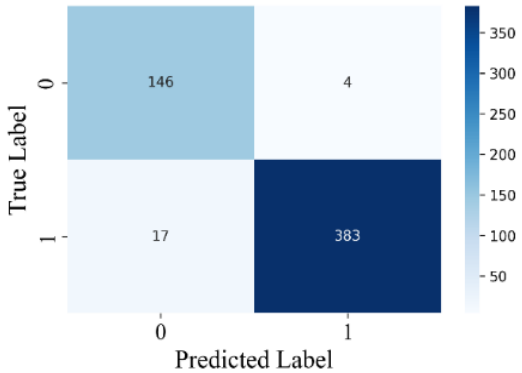


Fig. 9. Confusion matrix of the Dataset 2.

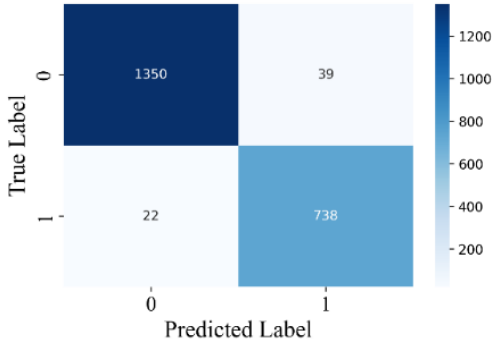


Fig. 10. Confusion matrix of Dataset 3.

Dataset 2 is used to represent chronic kidney disease (CKD) cases. It consists of two classes: class 0 (146 instances) represents “no disease”, and class 1 (383 instances) represents kidney disease, as shown in Figure 9.Figure 10 represents the confusion matrix for Alzheimer's disease prediction. It includes two classes: 1,350 instances of individuals not affected by Alzheimer's disease and 738 instances of individuals diagnosed with Alzheimer's disease.

### *4.1. Performance analysis of encryption process*

The ElGamal- True Random Number Generator-Pseudo Random Number Generator (ElGamal-TRNG-PRNG) is compared with some existing post quantum cryptography algorithms. fully homomorphic encryption (FHE) [26], threshold fully homomorphic encryption (TFHE) [27], Quasi Oppositional Sail Fish Optimizer with Homomorphic Encryption (QOSFO-HE) [28], and Cheon-Kim-Kim-Song (CKKS) [29] are the existing approaches used to compare performance. The statistics used to compare the models' efficiencies are encryption time, and decryption time.

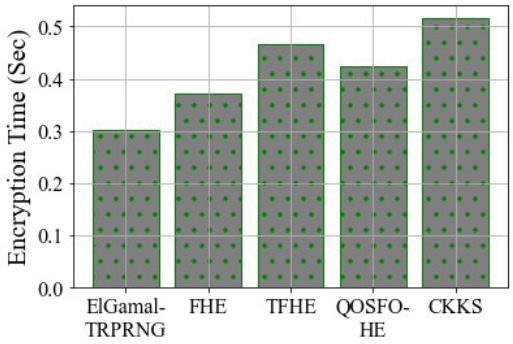


Fig. 11. Evaluation of encryption time.

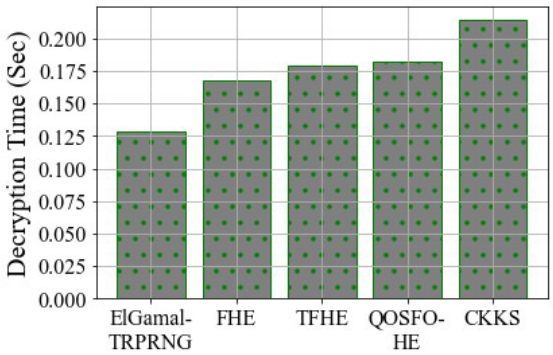


Fig. 12. Evaluation of decryption time.

An analysis of encryption times for various encryption techniques is presented in Figure 11. An encryption time of 0.30 sec is produced by the ElGamal-TRNG-PRNG. It takes less time to encrypted data than other techniques as the FHE, TFHE, QOSFO-HE, and CKKS algorithms, which require 0.37, 0.46, 0.42, and 0.51 sec. Decryption time data for various encryption algorithms are also compared in Figure 12. The decryptions are generated at 0.12 sec, 0.16 sec, 0.17 sec, 0.18 sec, and 0.21 sec, by ElGamal-TRNG-PRNG, FHE, TFHE, QOSFO-HE, and CKKS

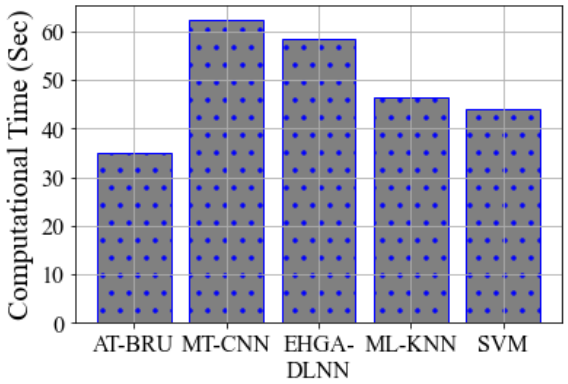


Fig. 13. Evaluation of the Proposed and Current Algorithms in Computational Time.

Figure 13 compares the computational time of five algorithms. AT-BiGRU is the fastest at around 35 seconds, while MT-CNN is the slowest at about 63 seconds. EHGA-DLNN, ML-KNN, and SVM.

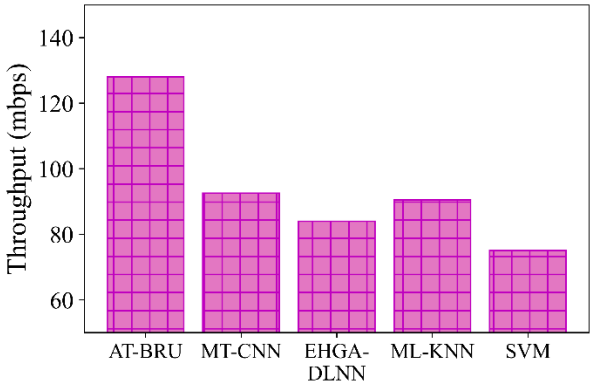


Fig. 14. Evaluation of the Proposed and Current Algorithms in throughput.

The figure 14 shows that AT-BiGRU has the highest throughput at about 128 Mbps, outperforming MT-CNN, ML-KNN, EHGA-DLNN, and SVM. SVM has the lowest throughput around 75 Mbps, making AT-BiGRU the most efficient method among the five. This demonstrates its superior capability to manage large-scale data processing with minimal latency.

### *4.2. Comparison Analysis for the Proposed Model*

A number of metrics were used to calculate the proposed prediction system's performance. The evaluation includes the following metrics: false negative rate (FNR), accuracy, recall, precision, specificity, memory overhead and error. Attention- Bidirectional Gated Recurrent Unit (AT-BiGRU) technique is compared with existing strategies such as MT-CNN [30], EHGA-DLNN [12], ML-KNN [13], and SVM [31].

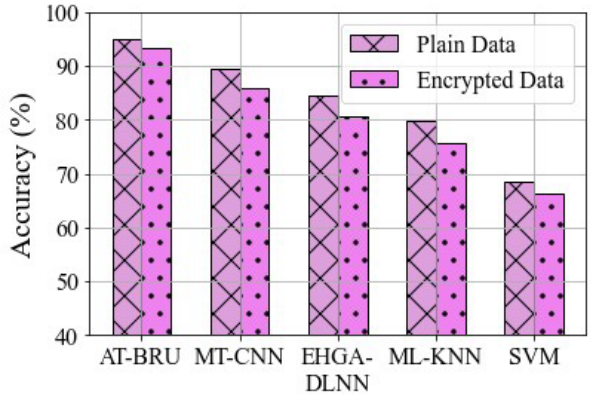


Fig. 15. Evaluation of the accuracy.

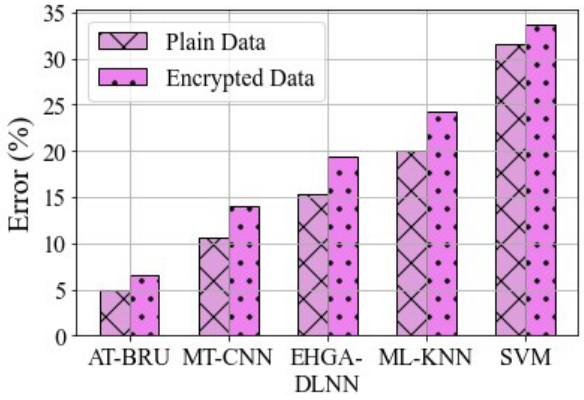


Fig. 16. Evaluation of the error of plain and encrypted data.

Evaluation of plain and encrypted data for both proposed and existing systems is shown in Figure 15. Accuracy in the assessment dataset is the proportion of properly categorized individuals. By comparing the AT-BiGRU with the existing MT-CNN, EHGA-DLNN, ML-KNN and SVM, the accuracy of the approach is evaluated. The plain data accuracy values for AT-BiGRU, MT-CNN, EHGA-DLNN, ML-KNN and SVM are 95.10%, 89.40%, 84.64%, 79.89% and 68.47%, in that order. Likewise, the accuracy values for encrypted data for AT-BiGRU, MT-CNN, EHGA-DLNN, ML-KNN and SVM are 93.47%, 86%, 80.57%, 75.71% and 66.36%. The AT-BiGRU offers higher plain data accuracy than encrypted data, despite the importance of encryption for healthcare data security. Figure 16 illustrates the error testing process for the AT-BiGRU strategy with the existing algorithms for both plain and encrypted data. For AT-BiGRU, MT-CNN, EHGA-DLNN, ML-KNN and SVM, the plain data error values are 4.9%, 10.6%, 15.36%, 20.11%, and 31.53%, respectively. Similarly, the error values for AT-BiGRU, MT-CNN, EHGA-DLNN, ML-KNN and SVM with encrypted data are 6.53%, 14%, 19.43%, 24.29%, and 33.61%. The AT-BiGRU has a lower error than the existing methods.

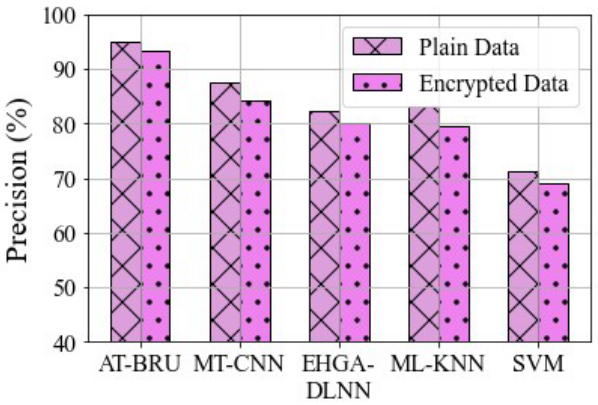


Fig. 17. Evaluation of the precision.

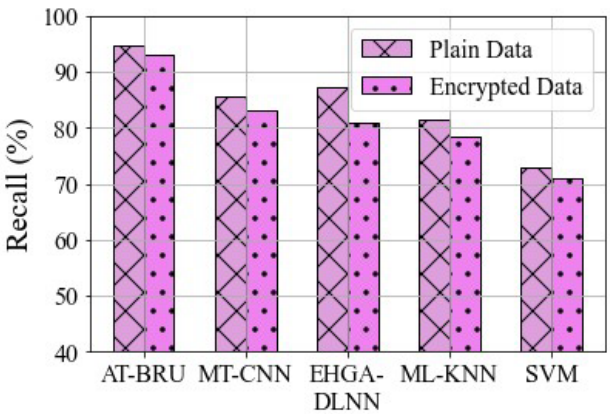


Fig. 18. Evaluation of the recall.

Figure 17 shows the results of the precision evaluation of plain and encrypted data for both the suggested and current approaches. The precision of the AT-BiGRU model is assessed by contrasting it with the cutting-edge methods MT-CNN, EHGA-DLNN, ML-KNN and SVM. The precision values for the AT-BiGRU, MT-CNN, EHGA-DLNN, ML-KNN and SVM derived from the plain data are 95.05%, 87.44%, 82.22%, 83.17% and 71.29%, respectively, while for the encrypted data are 93.45%, 84.39%, 80.09%, 79.43%, and 69.15%. The recall evaluation of existing and proposed approaches is shown in Figure 18. By comparing the AT-BiGRU with the existing techniques MT-CNN, EHGA-DLNN, ML-KNN and SVM, recall is estimated. The plain data yielded recall values of 94.88%, 85.58%, 87.29%, 81.60% and 73.06% for the AT-BiGRU, MT-CNN, EHGA-DLNN, ML-KNN and SVM, respectively. 93.12%, 83.15%, 81.01%, 78.40%, and 71.04% are the recall values that were discovered for encrypted data.

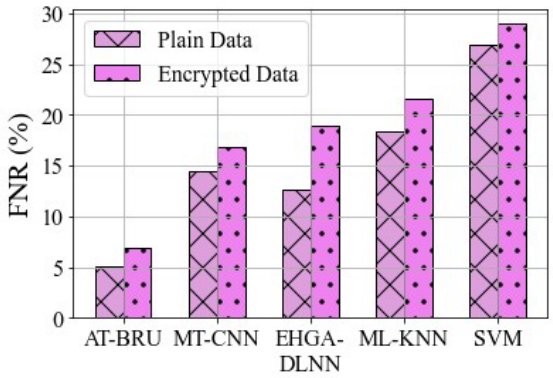


Fig. 19. Evaluation of the FNR.

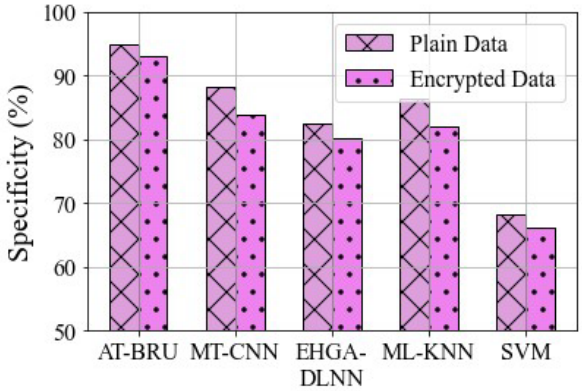


Fig. 20. Evaluation of the specificity.

Figure 19 shows the False Negative Rate (FNR) analysis of the proposed and existing approaches. The AT-BiGRU is compared with MT-CNN, EHGA-DLNN, ML-KNN and SVM, in order to determine the FNR. The obtained FNR value for plain data of AT-BiGRU is 5.12%, 14.42%, 12.71%, 18.4% and 26.94%, respectively, for the existing techniques, MT-CNN, EHGA-DLNN, ML-KNN and SVM. For encrypted data, the FNR values found are 6.88%,

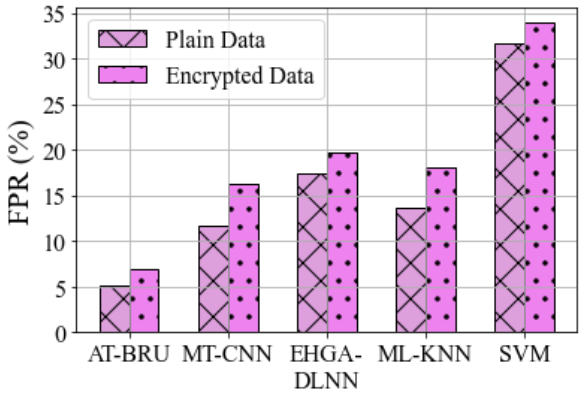


Fig. 21. Evaluation of the FPR.

16.85%, 18.99%, 21.6%, and 28.96%. The AT-BiGRU which applies to both plain and encrypted data, is shown in Figure 20. Plain data specificity values for AT-BiGRU, MT-CNN, EHGA-DLNN, ML-KNN and SVM are 94.85%, 88.24%, 82.54%, 86.34%, and 68.31%, respectively. Comparable specificity values of 93.11%, 83.80%, 80.26%, 81.94%, and 66.11% are found for AT-BiGRU, MT-CNN, EHGA-DLNN, ML-KNN and SVM with encrypted data. Compared to existing approaches, the AT-BiGRU has a higher degree of specificity for both plain and encrypted data.

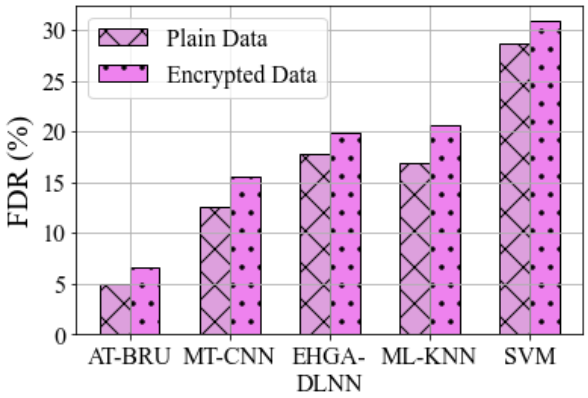


Fig. 22. Evaluation of the FDR.

The AT-BiGRU method shows the lowest FPR (around 5% for plain data and 7% for encrypted), while SVM has the highest FPR (around 32% for plain and 35% for encrypted). The other methods have intermediate values, with FPR increasing noticeably when encryption is applied in Figure 21. Figure 22 shows that all methods have higher false detection rates (FDR) with encrypted data compared to plain data. AT-BiGRU has the lowest FDR, while SVM has the highest. Encryption increases false detections across all methods.

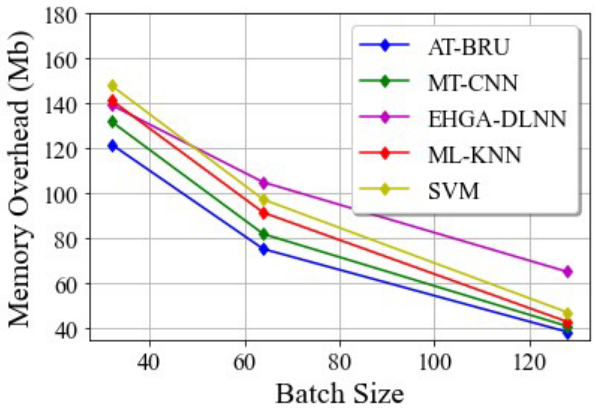


Fig. 23. Memory overhead analysis.

Figure 23 illustrates that the memory overhead stabilizes once the data is stored in memory. It is anticipated that the batch size ranges from 40 to 120. Memory overhead decreases with higher batch size values. At batch size 100, the AT-BiGRU method achieves 55 MB. Compared with existing techniques like MT-CNN, EHGA-DLNN, ML-KNN and SVM, AT-BiGRU takes low overhead ratio.

Table 3. Ablation Analysis Based on Model.

| | Accuracy | Precision | Recall | FNR |
|---|---|---|---|---|
| Elastic Net+ BiGRU | 88.9 | 88.60 | 87.5 | 11.04 |
| Elastic Net+ Encryption+ BiGRU | 91.63 | 90.5 | 90.7 | 8.55 |
| Elastic Net+ Encryption | 88.6 | 88.5 | 86 | 9.6 |
| Elastic Net + Zebra Optimization + Encryption + AT-BiGRU | 93.47 | 93.45 | 93.12 | 6.88 |

The ablation study shows that each added component improves model performance in table 3. Starting with Elastic Net + BiGRU, the addition of encryption enhances recall and reduces the false negative rate. Removing BiGRU leads to lower accuracy, confirming its importance in handling sequential data. The best results are achieved when both Zebra Optimization and an attention mechanism are added, leading to the highest accuracy (93.47%) and lowest FNR (6.88%).

Table 4. Comparison of the Proposed and Existing Systems with the State of the Art.

| **Comparison of Proposed and Existing System for Encryption** | | | |
|---|---|---|---|
| **Author** | **Techniques** | **Performances Analysis** | |
| Proposed | ElGamal-TRNG-PRNG | Encryption:0.30ms | Decryption times:0.53ms |
| Ma et al., [11] | Privacy-preserving and highly accurate outsourced disease predictor on random forest, called PHPR. PHPR system can perform secure training on data. | Encrypted:7.54ms | Decrypted : 7.70ms |
| Yin et al.[32] | Decentralized ciphertext-policy attribute-based encryption (DCP-ABSE) | Encryption: 15 ms | Decryption: 12 ms |
| Mahajan et al.[33] | Lightweight cryptography | Encryption:3.25 ms | Decryption times:2.0ms |
| **Comparison of Proposed and Existing System for Classification** | | | |
| **Author** | **Techniques** | **Performances Analysis** | |
| Proposed | AT-BiGRU | **specificity** | **precision** |
| Elsedimy et al. [34] | Quantum-behaved particle swarm optimization (QPSO) algorithm and support vector machine (SVM) | 93.56% | 94.23% |
| Dubey et al.[35] | Crow Search Optimization Algorithm (CSOA) with Deep learning | - | 91% |
| Ramesh et al.[36] | Optimal Scrutiny Boosted Graph Convolutional LSTM (O-SBGC-LSTM) with Eurygaster Optimization Algorithm (EOA) | - | 89% |

Table 4 illustrates the comparison between the proposed system and the state-of-the-art methods in encryption and classification. In encryption, for lightweight cryptography, the encryption time is 325 ms and the decryption time is 20 ms. In classification, the existing systems include the Quantum-behaved Particle Swarm Optimization (QPSO) algorithm and the Support Vector Machine (SVM). The specificity value for these existing systems is 93.56%, and the precision value is 94.23%. The proposed system achieves a specificity value of 95.05%.

Table 5. Proposed and Existing Systems for Datasets 2, 3, 4, and 5.

| | **Methods** | **Accuracy** | **Precision** | **Recall** | **Specificity** | **FNR** | **F1-Score** |
|---|---|---|---|---|---|---|---|
| **Dataset 2** | AT-BiGRU(Proposed) | 96.1% | 94.2% | 96.5% | 96.5% | 3.4% | 95.3% |
| | MT-CNN | 94% | 90% | 89% | 84% | 2.3% | 93% |
| | EHGA-DLNN | 91% | 85% | 90% | 89% | 1.2% | 84% |
| | ML-KNN | 93% | 89% | 85% | 90% | 3% | 92% |
| | SVM | 89% | 84% | 79% | 85% | 2.1% | 86% |
| **Dataset 3** | AT-BiGRU(Proposed) | 97.1% | 96.2% | 97.1% | 96.1% | 2.8% | 96.6% |
| | MT-CNN | 93% | 94% | 91% | 82% | 3.1% | 87% |
| | EHGA-DLNN | 90% | 87% | 82% | 85% | 3.5% | 88% |
| | ML-KNN | 93% | 89% | 85% | 90% | 3% | 92% |
| | SVM | 91% | 75% | 90% | 89% | 1.2% | 84% |
| **Dataset 4** | AT-BiGRU(Proposed) | 96.4% | 89% | 85% | 90% | 3% | 92% |
| | MT-CNN | 89% | 84% | 79% | 94.2% | 96.5% | 96.5% |
| | EHGA-DLNN | 90% | 89% | 84% | | | |
| | ML-KNN | 89% | 84% | 79% | 94.2% | 96.5% | 96.5% |
| | SVM | 90% | 89% | 84% | 96.5% | 96.5% | 85% |
| **Dataset 5** | AT-BiGRU(Proposed) | 96.3% | 89% | 84% | 79% | 96.5% | 96.5% |
| | MT-CNN | 89% | 84% | 79% | | | |
| | EHGA-DLNN | | | | 94.2% | 96.5% | 96.5% |
| | ML-KNN | 90% | 89% | 84% | | | |
| | SVM | 89% | 84% | 79% | 94.2% | 96.5% | 96.5% |

Table 5 presents a comparison between the proposed and existing systems for Dataset 2, Dataset 3, dataset 4, dataset 5 Dataset 2, which contains chronic kidney disease data, shows that the proposed system achieves an accuracy of 96.1%, precision of 94.2%, recall of 96.5%, specificity of 96.5%, FNR (False Negative Rate) of 3.4%, F1-Score of 95.3%, and .Dataset 3 shows the Alzheimer's disease prediction, comparing the current systems, including MT-CNN, EHGA-DLNN, ML-KNN, and SVM, with the proposed system, AT-BiGRU, which achieves an accuracy of 97.1%.

Table 6. Statistical Test Results on the Datasets.

| Dataset | Friedman chi-square | | Wilcoxon | |
|---|---|---|---|---|
| | Statistic | P-Values | Statistic | P-Values |
| Dataset 1 | 4.0 | 0.4060 | 10.0 | 0.0625 |
| Dataset 2 | 4.1 | 0.5171 | 10.4 | 0.2736 |
| Dataset 3 | 4.23 | 0.6891 | 10.6 | 0.3695 |
| Dataset 4 | 4.20 | 0.6728 | 10.5 | 0.3294 |
| Dataset 5 | 4.19 | 0.6625 | 10.3 | 0.3394 |

The statistical tests in the dataset shown in table 6 are as follows: Dataset 1, Dataset 2, Dataset 3, Dataset 4, and Dataset 5. In dataset 1, the Friedman chi-square statistic is 4.0 with a p-value of 0.4060, and the Wilcoxon statistic is 10.0 with a p-value of 0.0625. In dataset 2, the Friedman chi-square statistic is 4.1 with a p-value of 0.5171.

Table 7. Analysis of the proposed Model with various attacks.

| | Side-Channel Attack | Key Leakage Attack | Unauthorized Access | Replay Attack |
|---|---|---|---|---|
| Proposed | 3.7 ms | 0.99 | - | - |
| FHE | 13.2 ms | 0.94 | 3.7% | 94% |
| TFHE | 11.2 ms | 0.95 | 2.8% | 95% |
| QOSFO-HE | 9.7 ms | 0.97 | 1.7% | 98% |
| CKKS | 12.4 | 0.93 | 2.3% | 97% |

Table 7 shows that the proposed model outperforms other HE schemes with the fastest side-channel response (3.7 ms), highest key leakage protection (0.99), and complete resistance to unauthorized access and replay attacks. In contrast, other methods are slower and vulnerable to multiple security threats.

### *4.3. Discussion*

The proposed model effectively addresses several critical security threats commonly encountered in IoT-based healthcare systems. Side-channel attacks, which exploit physical information leakage such as timing or power consumption during cryptographic operations, are mitigated by employing the ElGamal encryption scheme with carefully designed operations that minimize data-dependent timing variations, thereby reducing vulnerability to such exploits. Key leakage attacks, often arising from weak or predictable key generation, are countered through the use of the True Random Number Generator–Pseudo Random Number Generator (TRNG-PRNG) approach, which produces highly unpredictable and robust encryption keys, significantly lowering the risk of key compromise. Additionally, the model safeguards against unauthorized data access whether from external attackers or malicious insiders by encrypting sensitive patient data before storage in the cloud, ensuring that data remains unintelligible without the appropriate keys. Furthermore, to reduce the potential attack surface presented by high-dimensional datasets, the model integrates an optimized Elastic Net dimensionality reduction method that condenses data complexity while preserving critical information. Collectively, these components provide a comprehensive defense mechanism that secures patient healthcare data against a range of sophisticated attacks, all while maintaining high predictive accuracy and operational efficiency in the healthcare environment.

## 5. Conclusion

Modern healthcare systems have considerably increased life expectancy by utilizing medications, medical services, and patient health data management. However, issues such as insufficient medical information, avoidable mistakes, data breaches, misdiagnosis, and delayed transmission continue. Computerized medical information systems, such as CDSS, EHR, and DPS, are critical for early detection and decision-making. The significance of clinical decision support systems has grown as a result of medical sensors and IoT. However, IoT-based healthcare systems face security and privacy challenges, as they collect and transmit personal information over open networks. Privacy issues occur as a result of the possible physical, psychological, and financial consequences of disclosing personal information during data gathering and dissemination, necessitating strict data protection measures. Personal information can be effectively protected by encryption-based privacy protection techniques, but they are less appropriate for Internet of Things applications because of their complexity of computation and data functionality. To address the aforementioned problems, an efficient privacy-preserving disease prediction system using machine learning algorithms is developed. By employing this, patients can get privacy preserving disease prediction services. Healthcare data were employed as an input here. Initially, input raw data dimensionality was reduced by Elastic Net. The hyperparameters were optimized using the Zebra Optimization Algorithm (ZOA). Reduced data were then encrypted using the ElGamal approach, which generated secret key as TRNG-PRNG encryption. These encrypted data were then stored in the cloud. The Attention Mechanism-Based Bi-directional Gated Recurrent Unit (AT-BiGRU) approach was then employed to predict heart disease. The system's efficiency was compared using performance analysis for both classification and secure data transmission. The ElGamal-TRNG-PRNG performance is initially assessed against existing FHE, TFHE, QOSFO-HE, and CKKS algorithms in terms of encryption time of 0.30 seconds and decryption time of 0.12 seconds. The suggested

AT-BiGRU classifier was then validated and compared to various techniques, including MT-CNN, EHGA-DLNN, ML-KNN, and SVM, for both plain and encrypted information. 93.47% accuracy, 93.11% specificity, 6.53% error, 6.88% FNR, 93.12% recall, and 93.45% precision are the outcomes for the suggested encryption model. The results of the experiment show that the recommended approach outperforms current disease prediction techniques and offers superior privacy and security. Future work will focus on creating a privacy-aware model that maintains security features while predicting diseases at minimal computational and communication costs.

## All the Declarations and Statements

### Author Contributions Statement

Bhawana S. Dakhare – performed Conceptualization, Methodology, Formal analysis, Data curation, Funding acquisition, Project administration; Resources; Software, Validation; Visualization, Roles/Writing - original draft; Writing.
Lata L. Ragha – performed Supervision, Investigation, Writing - Original Draft, Reviewing and Editing.

All authors have read and agreed to the published version of the manuscript.

### Conflict of Interest Statement

The authors declared that they have no conflicts of interest in this work. We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

### Funding Declaration

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

### Data Availability Statement

Not Applicable.

### Ethical Declarations

This article is a completely original work of its authors; it has not been published before and will not be sent to other publications until the journal's editorial board decides not to accept it for publication.

### Acknowledgments

We sincerely thank the experts for their professional evaluation and valuable recommendations, which have contributed to improving the quality of the experiment and the reliability of its results.

### Declaration of Generative AI in Scholarly Writing

Not Applicable.

### Abbreviations

The following abbreviations are used in this manuscript:

IoT - Internet of Things
IoMT - Internet of Medical Things
DPS - Disease Prediction System
EN - Elastic Net
ZOA - Zebra Optimization Algorithm
TRNG - True Random Number Generator
PRNG - Pseudo Random Number Generator
TRNG-PRNG - True Random Number Generator–Pseudo Random Number Generator
AT-BiGRU - Attention Mechanism based Bi-directional Gated Recurrent Unit
BiGRU - Bi-directional Gated Recurrent Unit
GRU - Gated Recurrent Unit
AES - Advanced Encryption Standard
RSA - Rivest–Shamir–Adleman
ECC - Elliptic Curve Cryptography
RF - Random Forest
KNN - K-Nearest Neighbor
SVM - Support Vector Machine

ANN - Artificial Neural Network
DT - Decision Tree
DBN - Deep Belief Network
ML - Machine Learning
HE - Homomorphic Encryption
CPU - Central Processing Unit
AI - Artificial Intelligence
CNN - Convolutional Neural Network
RNN - Recurrent Neural Network
TP - True Positive
TN - True Negative
FP - False Positive
FN - False Negative

## References

[1] H. Ullah, S. Manickam, M. Obaidat, S. U. A. Laghari, and M. Uddin, (2023). Exploring the potential of metaverse technology in healthcare: Applications, challenges, and future directions. IEEE Access, 11, 69686-69707.
[2] S. Bansal, and D. Kumar, (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. International Journal of Wireless Information Networks, 27(3), 340-364.
[3] A. Cirne, P. R. Sousa, J. S. Resende, and L. Antunes, (2022). IoT security certifications: Challenges and potential approaches. Computers & Security, 116, 102669.
[4] S. Karthick, (2018). TDP: A Novel Secure and Energy Aware Routing Protocol for Wireless Sensor Networks. International Journal of Intelligent Engineering and Systems, 11(2), 76-84.
[5] A. B. Kathole, and D. N. Chaudhari, (2021, October). Securing the Adhoc Network Data Using Hybrid Malicious Node Detection Approach. In International Conference on Intelligent Vision and Computing (pp. 447-457). Cham: Springer International Publishing.
[6] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, (2022). Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices. IEEE Journal of Biomedical and Health Informatics, 27(2), 710-721.
[7] B. Tahir, A. Jolfaei, and M. Tariq, "A Novel Experience-Driven and Federated Intelligent Threat-Defense Framework in IoMT," IEEE Journal of Biomedical and Health Informatics, 29(4), 2345–2352, 2025.
[8] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access, 7, 74361-74382.
[9] P. Sharma, S. Jain, S. Gupta, and V. Chamola, (2021). Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. Ad Hoc Networks, 123, 102685.
[10] S. Ali, and F. Anwer, (2024). Secure IoT framework for authentication and confidentiality using hybrid cryptographic schemes. International Journal of Information Technology, 16(4), 2053-2067.
[11] Z. Ma, J. Ma, Y. Miao, and X. Liu, (2019). Privacy-preserving and highly accurate outsourced disease predictor on random forest. Information Sciences, 496, 225-241.
[12] S. Padinjappurathu Gopalan, C. L. Chowdhary, C. Iwendi, M. A. Farid, and L. K. Ramasamy, (2022). An efficient and privacy-preserving scheme for disease prediction in modern healthcare systems. Sensors, 22(15), 5574.
[13] D. Zhu, H. Zhu, X. Liu, H. Li, F. Wang, H. Li, and D. Feng, (2020). CREDO: Efficient and privacy-preserving multi-level medical pre-diagnosis based on ML-kNN. Information Sciences, 514, 244-262.
[14] A. Alabdulkarim, M. Al-Rodhaan, T. Ma, and Y. Tian, (2019). PPSDT: A novel privacy-preserving single decision tree algorithm for clinical decision-support systems using IoT devices. Sensors, 19(1), 142.
[15] R. Jayaram, and S. Prabakaran, (2021). Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. Egyptian Informatics Journal, 22(4), 401-410.
[16] K. K. Patro, A. Jaya Prakash, M. Jayamanmadha Rao, and P. Rajesh Kumar, (2022). An efficient optimized feature selection with machine learning approach for ECG biometric recognition. IETE Journal of Research, 68(4), 2743-2754.
[17] E. Trojovská, M. Dehghani, and P. Trojovský, (2022). Zebra optimization algorithm: A new bio-inspired optimization algorithm for solving optimization algorithm. IEEE Access, 10, 49445-49473.
[18] M. Kara, A. Laouid, M. A. Yagoub, R. Euler, S. Medileh, M. Hammoudeh, and A. Bounceur, (2022). A fully homomorphic encryption based on magic number fragmentation and ElGamal encryption: Smart healthcare use case. Expert Systems, 39(5), e12767.
[19] T. Kowsalya, R. G. Babu, B. D. Parameshachari, A. Nayyar, and R. M. Mehmood, (2021). Low Area PRESENT Cryptography in FPGA Using TRNG-PRNG Key Generation. Computers, Materials & Continua, 68(2), 1447-1465.
[20] X. Lu, and H. Zhang, (2021). Sentiment analysis method of network text based on improved AT-BiGRU model. Scientific Programming, 2021(1), 6669664.
[21] Dataset 1: Fedesoriano, 2021, Heart failure prediction dataset, https://www.kaggle.com/datasets/fedesoriano/heart-failure-prediction, accessed on 03-05-2024.
[22] Dataset 2: Kidney Disease Dataset, https://www.kaggle.com/datasets/akshayksingh/kidney-disease-dataset, accessed on 03-05-2024.

[23] Dataset 3: Alzheimer's Disease Dataset, https://www.kaggle.com/datasets/rabieelkharoua/alzheimers-disease-dataset, accessed on 03-05-2024.
[24] Dataset 4: MIMIC-III - Deep Reinforcement Learning Dataset, https://www.kaggle.com/datasets/asjad99/mimiciii, accessed on 03-05-2024.
[25] Dataset 5: UCI Heart Disease Data, https://www.kaggle.com/datasets/redwankarimsony/heart-disease-data, accessed on 03-05-2024.
[26] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. Fitzek, and N. Aaraj, (2022). Survey on fully homomorphic encryption, theory, and applications. Proceedings of the IEEE, 110(10), 1572-1609.
[27] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, (2020). TFHE: fast fully homomorphic encryption over the torus. Journal of Cryptology, 33(1), 34-91.
[28] D. Venu, A. V. R. Mayuri, S. Neelakandan, G. L. N. Murthy, N. Arulkumar, and N. Shelke, (2022). An efficient low complexity compression based optimal homomorphic encryption for secure fiber optic communication. Optik, 252, 168545.
[29] Y. Rahulamathavan, (2022). Privacy-preserving similarity calculation of speaker features using fully homomorphic encryption. arXiv preprint arXiv:2202.07994.
[30] M. Alawad, H. J. Yoon, S. Gao, B. Mumphrey, X. C. Wu, E. B. Durbin, and G. Tourassi, (2020). Privacy-preserving deep learning NLP models for cancer registries. IEEE Transactions on Emerging Topics in Computing, 9(3), 1219-1230.
[31] R. Zhao, Y. Xie, X. Jia, H. Wang, and N. Kumar, (2022). Practical Privacy Preserving-Aided Disease Diagnosis with Multiclass SVM in an Outsourced Environment. Security and Communication Networks, 2022(1), 7751845.
[32] H. Yin, Y. Zhao, L. Zhang, B. Qiao, W. Chen, and H. Wang, "Attribute-Based Searchable Encryption with Decentralized Key Management for Healthcare Data Sharing," Journal of Systems Architecture, 148, 103081, 2024.
[33] H. Mahajan and K. T. V. Reddy, "Secure Gene Profile Data Processing Using Lightweight Cryptography and Blockchain," Cluster Computing, 27(3), 2785-2803, 2024.
[34] E. I. Elsedimy, S. M. AboHashish, and F. Algarni, "New Cardiovascular Disease Prediction Approach Using Support Vector Machine and Quantum-Behaved Particle Swarm Optimization," Multimedia Tools and Applications, 83(8), 23901-23928, 2024.
[35] A. K. Dubey, A. K. Sinhal, and R. Sharma, "Heart Disease Classification Through Crow Intelligence Optimization-Based Deep Learning Approach," International Journal of Information Technology, 16(3), 1815-1830, 2024.
[36] B. Ramesh and K. Lakshmanna, "A Novel Early Detection and Prevention of Coronary Heart Disease Framework Using Hybrid Deep Learning Model and Neural Fuzzy Inference System," IEEE Access, 12, 26683-26695, 2024.

## Authors' Profiles

**Bhawana S. Dakhare** is a Ph.D. candidate at Terna Engineering College, in the University of Mumbai. She has an M.E. degree in Computer Engineering (2014) and B. E. in Information Technology (2005). She has experience in Information Technology with emphasis on databases, data structures, algorithm analysis, artificial intelligence and machine learning. She currently works as an assistant professor in Information Technology Department at Bharati Vidyapeeth College of Engineering, Navi Mumbai, Mumbai University. Mumbai, Maharashtra, India.

**Lata L. Ragha** has received her Ph. D. degree from Jadavpur University, Kolkata in 2011. She received her B. E. and M.Tech degree in Computer Science and Engineering from Karnatak University in 1987 and Visvesvaraya Technological University, Karnataka, in 2000 respectively. She is currently working as Principal at Xavier Institute of Engineering, Mumbai. Her research interests include Networking, Security, Internet Routing, and Data Mining. She has more than 160 research publications in International Journals and conferences.

## How to cite this paper:

Bhawana S. Dakhare, Lata L. Ragha, "ElGamal Based Homomorphic Encryption Using AT-BiGRU for Efficient Privacy Preserving Disease Prediction Scheme in Healthcare Data", International Journal of Computer Network and Information Security (IJCNIS), Vol.18, No.4, pp. 210-232, 2026. DOI:10.5815/ijcnis.2026.04.11