Mesopotamian journal of Cybersecurity
Vol. 5, No.2, **pp**. 703-720
DOI: https://doi.org/10.58496/MJCS/2025/042; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Ensure Privacy-Preserving Using Deep Learning

Abeer D. Salman [1, *], Ruqayah R. Al-Dahhan[2]

[1] *Electronic Computer Center, University of Anbar, Ramadi, Iraq*

[2] *Computer Science Department, College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq*

ARTICLEINFO

Article History

Received 19 Nov 2024

Revised: 17 Apr 2025

Accepted 7 Jul 2025

Published 19 Jul 2025

Keywords

Security

Homomorphic

Deep Learning

Neural Network

Predication

ABSTRACT

Deep learning has emerged as a powerful approach for treating complex real-world challenges. However, the performance of the deep learning models is heavily reliant on access to large volumes of high-quality training data—an aspect often constrained by privacy concerns. Ensuring data availability while preserving user confidentiality remains a pressing issue. In response, cryptographic techniques like homomorphic encryption (HE), which are grounded in strict mathematical principles, present hopeful solutions for securing data on digital platforms without compromising its usability for learning models. It performs computations on encrypted data without revealing the underlying plaintext. The main attractive feature of this technique is its ability to protect sensitive information in a variety of settings. Moreover, it guarantees the data's trustworthiness and keeps data from being altered or tampered with. In this paper, sensitive data are encrypted via homomorphic algorithms and then input into deep learning to evaluate the feasibility of privacy-preserving deep learning. The aim is to examine the performance and security implications of fully homomorphic encryption (by the Learning With Errors (LWE) scheme) and partially homomorphic encryption (by the Rivest, Shamir, and Adleman (RSA) algorithms). Both methods were applied to three datasets for osteoporosis diagnosis. The experimental results show that LWE maintains high accuracy, reaching 88.01%, compared with unencrypted models. In contrast, RSA showed lower accuracy with minimum resource consumption. The findings showed that LWE is a more secure and reliable option for privacy-preserving deep learning in medical applications.

1. INTRODUCTION

Machine learning has recently received much interest in the healthcare industry for cutting-edge outcomes in numerous domains. Algorithms, particularly deep neural networks, have produced astonishing personalized medical solutions, allowing tailored treatment, prevention, and diagnosis. Deep neural networks are frequently utilized to blend medical professionals' expertise and knowledge into computer-aided diagnostic solutions because of their ability to learn from previous experiences [1]. Deep learning has yielded promising achievements in industry and academic fields. In some cases, deep learning systems produce accuracies comparable to, if not surpassing, those of human experts. This is due to the computational innovations and physical parallel technology used in the processing of neural networks [2] [3]. However, collecting massive amounts of data is necessary for deep learning. This highlights privacy concerns due to the storing of gathered data on an untrusted cloud server that is out of the owner's control [5]. As a result, medical research institutes and hospitals prevent the sharing of sensitive data and thus do not take advantage of the benefits of deep learning techniques [1] [2] [4]. Therefore, anonymizing sensitive data helps preserve its secrecy and privacy, which are critical requirements before transmitting it to the cloud server. However, using anonymized data limits the ability of deep learning to extract important knowledge and insight from the data [6]. Patients' medical information includes health conditions, diagnoses, medications, and even patients' medical history. If the data are not encrypted, they can be easily accessed by unauthorized parties. This poses a significant risk to patient privacy, especially if the data are related to sensitive diseases. The risk of tampering with patient information can lead to incorrect results in medical tests or diagnoses, which can lead to incorrect treatments, putting patients' lives at risk. Unencrypted data are also vulnerable to illegal use, such as blackmail, where sensitive medical information can be used to pressure individuals or companies, or it may be used for marketing or commercial purposes without patient consent. Unencrypted data are an attractive target for hackers, who may exploit vulnerabilities to access medical information and exploit it for financial gain or sell it in black markets.

*Corresponding author. Email: abeer.dawood@uoanbar.edu.iq

Encryption is an essential security barrier to protect data from this type of attack. Additionally, encryption is considered a fundamental mechanism for preserving the confidentiality of sensitive data. However, conventional encryption algorithms cannot work properly without first decrypting the data. ***Homomorphism*** is proposed as a possible solution for computation without decrypting the data. In terms of deep learning, its algorithms could be used on data that were encrypted while they were still encrypted, giving almost the same results when applied to plain data. Homomorphic encryption (HE) techniques offer a way out of this impasse [7] [8][9]. HE allows users to upload encrypted datasets to a cloud service securely [10] [9] [11].

This study aims to bridge a lacuna by applying HE techniques. Specifically, fully homomorphic encryption (FHE), which is based on the Learning With Errors (LWE) scheme, and partially homomorphic encryption (PHE), which use Rivest, Shamir, and Adleman (RSA), are performed separately on multiple datasets related to osteoporosis diseases, and then a deep learning framework for osteoporosis prediction is applied, thus preserving the privacy of patients. To decide the effectiveness of each HE technique, the study implements and evaluates it independently. In this case, the scope of its efficacy will be determined by securing sensitive data through an artificial neural network (ANN) model that is used to predict the disease.

The following lists the contributions of this work:

- An integrated system predicts osteoporosis via an ANN based on three different databases (comma-separated values (CSVs) and images). These data are encrypted via LWE and RSA to maintain patient privacy during the prediction process.
- An evaluation of the encrypted ANN models, comparing their prediction performance on encrypted versus unencrypted data via standard classification metrics such as accuracy, precision, recall, and F1 score, as well as system-level metrics such as prediction time, memory usage, and model size.
- Metrics (computing cost, energy consumption, and storage overhead) are used to compare and analyse the performance of the used encryption algorithms and determine the possibility of using FHE and PHE in global diagnostic systems.

On the basis of available information, this is the first study to implement and compare both LWE-based FHE and RSA-based PHE in the context of encrypted disease prediction via an ANN. The results revealed that secure and effective medical prediction can be achieved on encrypted data without revealing patient information. Thus, this will lead to advancements in the integration of privacy-preserving techniques into artificial intelligence-driven healthcare applications.

In this paper, osteoporosis disease prediction is adopted as a case study. It is a chronic disease that affects bones as a result of their low mineral density, making the bones brittle and easy to break. It is also called silent disease because patients do not feel it unless they are exposed to a fracture. Studies have shown that it is possible to predict this disease by measuring some proteins, such as osteopontin (OPN), and some biochemical factors [12].

The structure of this article is as follows. Some of the related works are described in Section 2. Section 3 introduces deep learning and ANNs. HE and its classification are shown in Section 4. The details of the proposed system are presented in Section 5. Section 6 presents the results and discussion of the work, and the security evaluation is introduced in Section 7. Section 8 shows a comparison of our work with others. The final section includes the conclusion of the work and some suggestions for future work.

2. RELATED WORKS

Hassan Takabi et al. [13] proposed a model to run deep neural networks on encrypted information via PHE methods. Chebyshev low-degree polynomials are used to approximate continuous functions (e.g., sigmoid functions) in addition to enhancing the performance of neural networks. The modified Chebyshev basis is used. Moreover, the authors evaluate the effectiveness of the proposed algorithms. However, in this research, less communication is needed between the client and the server. Ping Li et al. [14] presented two approaches to reduce communication and computational expenses for data owners, who store their data on the cloud server after securely encrypting it with various keys. Whereas in the first basic case, they employed multikey FHE, they combined FHE and the double decryption mechanism; both schemes handle the challenge of creating shared deep learning ciphertexts by protecting privacy via several public keys. Unlike the basic system, the advanced method eliminates the requirements for data owners to interact among themselves during the decryption of the resulting data.

On the other hand, another study used additive HE to protect data stored on the cloud before using deep learning [2]. The study enhances security by preventing information from leaking to the cloud server. Furthermore, Xiaoqiang's study [15] improved FHE to be suitable for the private classification of machine learning. Moreover, decision-based classification, naïve Bayes classification, and a homomorphic comparison protocol were implemented via enhanced FHE. However, the work in [4] investigated the feasibility of deep learning via a convolutional neural network (CNN) by preserving privacy. This study focuses on bootstrap FHEs to enable the evaluation of complex functions. For a bootstrap

FHE implementation, the operations of the deep learning methods are encrypted for use in image classification applications. How logic circuits and security factors affect system performance were examined. Relatedly, Anamaria Vizitiu et al. [1] proposed a method depend on FHE to process personal health information without revealing sensitive data. This method is named MORE (matrix operation for randomization or encryption). It enables calculations within neural network models directly on floating-point data with relatively low computing cost. This study adopts the National Institute of Standards and Technology (MNIST) digit recognition dataset to evaluate the viability of the suggested strategy, and they demonstrated that using deep learning to handle homomorphic data does not impair performance. Table 1 summarizes recent studies on the use of homomorphic algorithms with deep learning.

TABLE 1: SURVEY ABOUT DEEP LEARNING OVER ENCRYPTED DATA

citation	Year	Technique used	Dataset used	result
[13]	2016	Leveled or somewhat homomorphic systems combined with neural networks (NNs) that use polynomial approximation as their activation function.	15 datasets from UC Irvine Machine Learning Repository	The findings demonstrate that polynomial approximation can obtain the best accuracy when the appropriate interval is selected, depending on the dataset. The cost increased when the connection between the cloud server and the learning participants increased.
[14]	2017	This work presents a fundamental technique based on MK-FHE, and a cutting-edge method using a hybrid structure is suggested. This hybrid structure combines a twofold decryption mechanism with FHE.	No mention	When decrypting the learning result, the advanced approach does not require communication between data owners. It is possible to maintain the confidentiality of sensitive data, interim results, and the training model. However, the fundamental architecture calls for communication between various data owners.
[2]	2017	protects privacy by combining HE (LWE and Paillier) with asynchronous stochastic gradient descent	Street View House Numbers (SVHN) and (MNIST) datasets	There is no data breach on the server. Allowing several users to implement deep learning using NNs on a single aggregated dataset without giving a central server access to their local data. Compared to a typical system of deep learning applied to the pooled dataset, accuracy is maintained. The price of greater connectivity between the cloud server and learners
[15]	2018	The FHE approach proposed in this research is an enhancement of Helevi's FHE library. The multiplicative ciphertext's size is first reduced using the relinearization approach, and the modulus and decryption noise are subsequently reduced using the modulus switching technique. Concerning this framework, FHE uses private decision trees, private naïve Bayes classification assessments, as well as private hyperplane decision-based classification.	No mention	This system is more effective than Khedr's FHE scheme and HElib with SIMD. Furthermore, implementing private decision trees is superior to using HElib with SIMD and Khedr's FHE method.
[4]	2019	Demonstrate the creation of privacy-preserving FHE using deep learning CNNs. To encrypt the operations of this Deep Learning technique for image classification applications, deploy bootstrapped FHE.	adapted dataset from the National Institute of Standards and Technology	With the very minimum-security parameters, training takes approximately 36 hours for images from the MNIST dataset. FHE can be substituted with LFHE to control operations and noise. It is advisable to have a small CNN to reduce the number of calculations due to the vast size of ciphertexts introduced by the fully homomorphic cipher. By multiple orders of magnitude, the bootstrapping operation requires most of the time.
[16]	2020	This essay utilized MORE. It uses regression, binary classification, and multiclass classification as three different deep learning applications.	An internal database was used to save 3378 coronary angiographies with a resolution of 512 by 512 pixels from the 70,000 greyscale images in the MNIST collection, which has a 28 by 28-pixel dimension.	The process is nondeterministic and noise-free. The four fundamental arithmetic operations can be performed over encrypted data. The MORE encryption method provides less security than conventional methods, but it does provide floating-point arithmetic to meet the privacy-preserving floating-point precision requirement. The technique is then open to well-known ciphertext attacks.

[17]	2023	The aim is to use a Siamese neural network and HE to process data securely.	Custom Monte Carlo-generated datasets.	Achieving accuracy is 93.8% for 2D scene and 93.4% for encrypted inference for single-point spectral.
[18]	2025	The paper aims to utilize Privacy-preserving machine learning (PPML) HE. Solve the challenges of implementing Sigmoid, Tanh activation functions in encrypted neural networks.	The MNIST dataset, which contains images for handwritten digits	This work achieves an accuracy of 87.10% for Sigmoid and 85.60% for Tanh. The computational efficiency was ~5.69 seconds per inference.

3. DEEP LEARNING WITH ANN

Nowadays, deep learning has acquired popularity due to its being one of the best machine learning and pattern recognition methods. It can activate the data's representation to a higher, more abstract level. Moreover, complex functions can be learned by combining many simple functions via these transformations[19] [20]. The learning process is defined as finding weights that enable the neural network (NN) to display the required action, like driving a car. Such activity may comprise time-consuming computational phases depending on the issue and how the neurons are connected (since a standard NN consists of a large number of fully connected processors) [21]. ANNs imitate brain activity to create artificial systems that can handle complicated prediction issues. It was initially trained via the backpropagation algorithm (BP). Multiple neurons (nodes) are arranged in layers of an ANN (input, hidden, and output), and synaptic weights are used to identify the connections between the neurons. These weights are utilized by an ANN to predict and train the corresponding input class. BP adjusts the weights of the ANN based on error calculations from the resulting feedback of previous layers [22]. An attractive feature of an ANN is its ability to accept an unlimited amount of data as input, where it can be trained with millions of data records. Fig. 1 shows the main structure of an ANN.

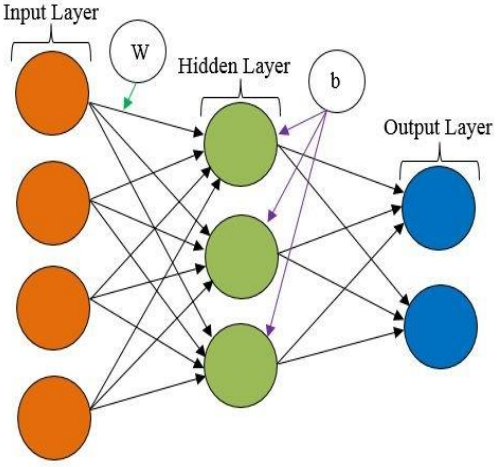

Fig. 1. ANN structure [23]

To grasp the relationships among the inputs, the necessary features for the model must be learned. Eq. 1 shows the method for obtaining the output of the neuron by taking vectors of real-valued inputs and applying a nonlinear activation function to the whole input value [24].

$$X_k = f(X_k - 1 * W_k + b) \qquad (1)$$

where W_k is the weight matrix of hidden layer k, which outlines how each input contributes to the result, and *f* is the activation function. The bias parameter (b) ensures that the sum of the inputs is greater than 0 [22]. This study evaluated the potential of deep neural networks as predictors of several osteoporosis disease symptoms [25].

4. HOMOMORPHIC ENCRYPTION (HE)

A kind of encryption known as homomorphic encryption (HE) maintains the characteristics of the format and function of the encrypted material while permitting a third party to perform some computational operations on the encrypted data (such as a cloud provider or service provider). A mapping in abstract algebra corresponds to this HE. Permitting addition and multiplication operations may be applied to evolve an encryption system that enables the homomorphic evaluation of any function [7]. The standard four processes of HE systems are as follows:

- ***Creation of keys**:* The clients generate a secret key (s_k) and a public key (p_k).
- ***Encryption***: a method of encrypting data that transforms plain text (M) into ciphertext (C) via the public key. $C=E_{pk}$ (M)
- ***Evaluation***: The public key is employed to apply a function *f* to a ciphertext C. $C^*=Eval_{pk}$ (*f*, C). The Eval operation receives ciphertexts as input and generates a ciphertext that corresponds to a functioned plaintext, although it only supports HE. Without viewing the messages (m_1,m_2), Eval applies the function *f* across the ciphertexts (c_1,c_2) [9]. where *f* may be Addition and/or multiplication.
- ***Decryption***: a technique for decryption that reveals the plain text M via the secret key and the ciphertext C. $M=D_{sk}$ (c) [8]

The following characteristics must be verified for an HE method [8].

- *Additive homomorphism (AH):* HE is additive if

$$D_{sk}\left(E_{pk}(M_1)+E_{pk}(M_2)\right)=M_1+M_2 \quad (2)$$

- *Multiplicative homomorphism (MH):* HE is multiplicative if

$$D_k\left(C_p(M_1)*C_k(M_2)\right)=M_1*M_2 \quad (3)$$

A simple, compelling HE example is shown in Figure 2.

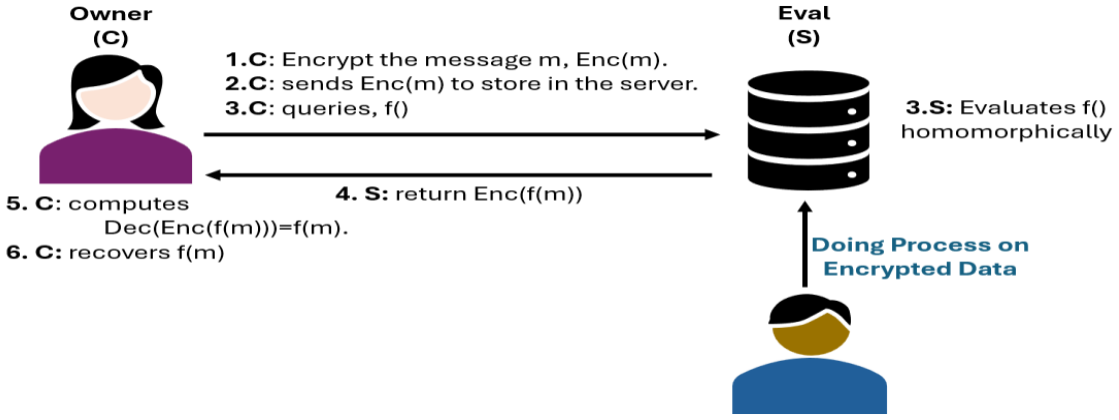

Fig. 2. Simple Homomorphic Example

The main requirement of the homomorphic technique is that the HE must be successfully decoded while preserving the format of the ciphertexts after an evaluation procedure. Also, the size of the ciphertext must be set to support eternal operations. If the ciphertext size is raised without utilizing more resources, the total number of operations will be constrained [9][26]. Three different kinds of HEs exist, as shown in Figure 3.

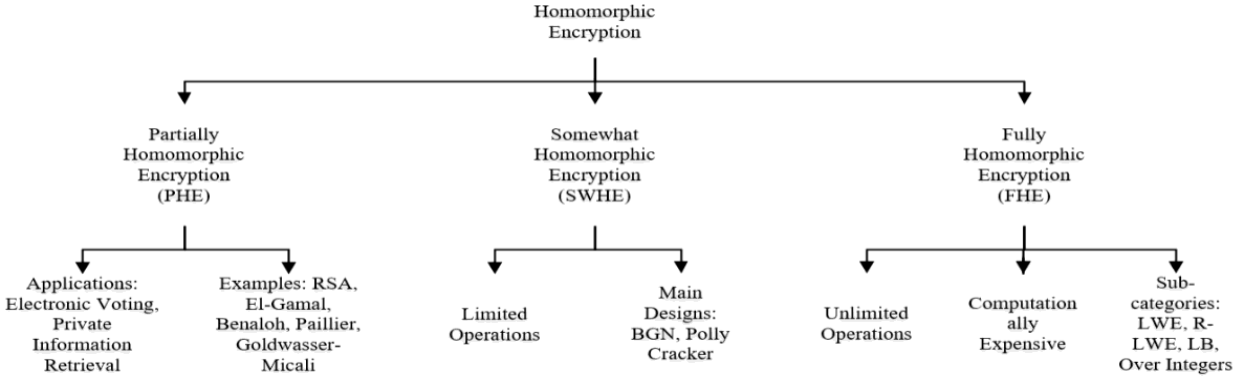

Fig. 3. Types of Homomorphic

Partially homomorphic encryption (PHE) only permits addition or multiplication, both of which can be performed an endless number of times (no cap on the number of uses, in other words) [8] [16]. Some applications take advantage of

PHE methods including electronic voting and private information retrieval (PIR). RSA, El-Gamal, Benaloh, Paillier, and Goldwasser-Micali are methods of PHE whease they use addition or multiplication operations [8][9] [10].

Somewhat homomorphic encryption (SWHE) makes several methods for addition and multiplication possible; however, the total number of homomorphic operations that may be carried out is restricted since the size of the ciphertexts grows with each homomorphic action. These issues add a cap to the utilization of PHE and SWHE schemes in practical applications [10][8]. Examples of SWHE techniques include the Boneh-Goh-Nissim (BGN) and the Polly Cracker [9].

Fully homomorphic encryption (FHE) is the expansion of HE schemes that can handle an endless number of homomorphic operations with random functions and has finally accelerated because cloud-based services are becoming widespread, i.e., FHE schemes allow the evaluation of any function, such as searching, sorting, max, min, etc., across ciphertexts an endless number of times. The accurate features of the SWHE and PHE are merged in FHE, permitting for indefinite multiplication and addition operations. FHE, however, costs a lot to compute. The few subcategories of FHE schemes that are now in use include the LWE, Ring-LWE, lattice-based (LB), and Over Integers FHE methods [10] [8][9]. In this study, data stored in the cloud were encrypted via LEW and RSA. A straightforward comparison will be made.

a) RSA Algorithm

In 1978, the RSA algorithm was designed to be one of the most widely used asymmetric encryption methods to secure data during transmission. RSA is used for many purposes, such as encrypting data, making digital signatures, and key exchange. The RSA is an asymmetric encryption algorithm that differs from symmetric encryption in that it uses two keys, one public key used for encryption and the other secret key used for decryption, whereas symmetric encryption uses one key for encryption and decryption, as shown in Fig. 4.

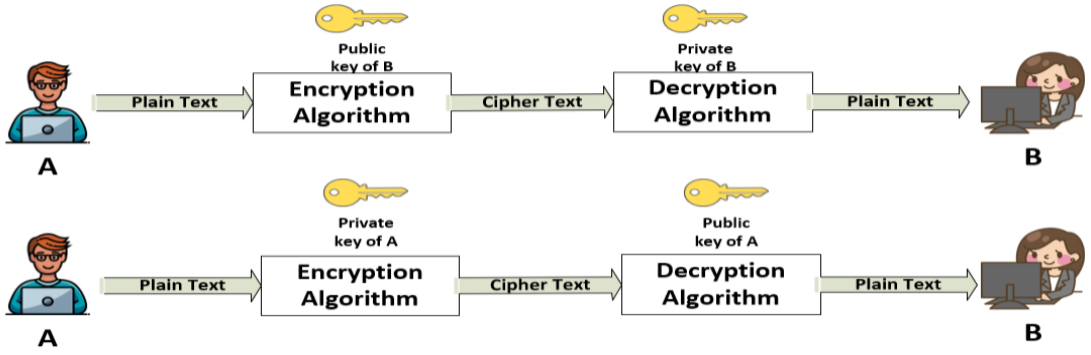

Fig. 4. Asymmetric Cryptosystem

The strength of the key used for the encryption process makes the process of decrypting and recovering the original text difficult for the hacker because he/she will need to guess the key. The RSA consists of three stages: key generation, encryption, and decryption, as explained in Algorithm 1.

Algorithm 1: RSA Procedure

1: Select two prime numbers, p and q
2: Calculate n = p * q
3: Find$\emptyset(n) = (p-1)(q-1)$
4: Pick an integer e, $\gcd(\emptyset(n), e) = 1; 1 < e < \emptyset(n)$, Public key PU = {e, n},
5: Calculate d, $d \equiv e^{-1} mod(\emptyset(n))$, private key PR = {d, n}
6: Encryption: Plaintext: M < n Ciphertext C:

$$Cipher = Message^{e} mod\ n \quad (4)$$

7: Decryption: Ciphertext: C, message M:

$$Message = Cipher^{d} mod\ n \quad (5)$$

of a multiplicative partial homomorphic encryption technique.

$$Cipher1 = message_1^{e} \bmod n, \quad Cipher2 = message_2^{e} \bmod n$$

$$Cipher1 \cdot Cipher2 = (message_1^{e} \cdot message_2^{e}) \bmod n$$

For m1, m2, and M, the homomorphic property is

$$E(m_1)\ E(m_2) = (m_1^{e} \pmod n)\ (m_2^{e} \pmod n) = E(m_1\ m_2). \quad (6)$$

The homomorphic characteristic of RSA demonstrates that without decrypting the inputs, $E(m_1\ m_2)$ may be assessed via $E(m_1)$ and $E(m_2)$. In other words, only multiplication is homomorphic to RSA. The homomorphic addition of ciphertexts is therefore prohibited. (m is the message)

The strong point of the algorithm depends on the choice of two prime numbers, p and q. The encryption process is very weak when the values are small, as the hacker can guess the key easily, e.g., via probability theory. On the other hand, if the values are very large, this leads to time consumption during the encryption process, so it is better to choose values of p and q with similar lengths. In terms of security, the RSA algorithm relies on two keys, the public and the secret keys; breaking this algorithm requires guessing the values of p and q. There is no efficient way to factorize two prime numbers from n that are declared as a public key [27] [28] [29].

b) *LWE Algorithm*

An algorithm called ***Learning With Errors (LWE)*** was introduced in 2005 and has received widespread attention in recent decades. For lattice-based cryptography, LWE is considered one of the most important algorithms in this field. LWE has many great advantages that have led to its use in many applications, such as its efficiency, versatility, and theoretical reduction to standard lattice problems, which allow it to be a highly versatile cryptographic construction. LWE is one of the basic structures of quantum cryptography. It is used in the following areas: attribute-based encryption (ABE), FHE, function encryption (FE), key exchange protocols, and digital signatures [30]. Algorithm 2 explains the detailed steps of this algorithm.

Algorithm 2: LWE Procedure

The inner product of vectors a and b is denoted by the widely popular notation <a,b>.
Moreover, Z[x]/(f(x)) symbolizes the ring of all polynomials modulo f(x), and d<--D indicates that d is allocated at random by an element from the distribution D. Rq≡=Zq [x]/(f(x)) denotes the ring of polynomials modulo f(x) with coefficients in q. Denotes an error distribution over the ring Rq to finish.

The underlying scheme is provided in its symmetric form as follows:
Key generation: The error distribution is used to select a ring component as a secret key, i.e., $s \leftarrow \chi$. The secret key vector is described as $\vec{s} = (1, s, s^2, \ldots, s^D)$ for an integer D.
Encryption: The message m is encrypted by selecting the noise e ← χ and a random vector a ← R_q^n.

$$\vec{c} = (c_0, c_1) = (as + te + m, -a), \qquad (7)$$

where $\vec{c} \in R_q^2$.
Decryption: It is easy to calculate that to retrieve the message from the ciphertext,

$$m = \langle \vec{c}, \vec{s} \rangle \pmod{t} \qquad (8)$$

Decryption is successful if $\langle \vec{c}, \vec{s} \rangle$, and s is less than $q/2$. Moreover, it is necessary to create a random set of pairings (a, as + te) in order to make the scheme asymmetric.
Homomorphism over addition

$$E(m) + E(m') = (c_0 + c_0', c_1 + c_1') = \big((a + a')s + t(e + e') + (m + m'), -(a + a')\big) \qquad (9)$$

Homomorphism over multiplication:

$$E(m) + E(m') = (c_0 c_0', c_1 c_1') = \big((-a's^2) + (c_0'a + c_0 a')s + t(2ee' + em' + e'm) + (mm')\big) \qquad (10)$$

5. PROPOSED PRIVACY-PRESERVING PREDICTION SYSTEM

This study proposes a privacy-preserving system as a secure disease prediction system that combines homomorphic encryption and artificial neural networks. The inputs of the ANN are encrypted medical data used to predict disease without the need for decryption, making the sensitive data less vulnerable to detection. To evaluate the proposed system, the following algorithms were applied:

- The FHE scheme-LWE allows for the implementation of arbitrary computations on encrypted data.
- PHE-RSA, which allows a limited number of operations to be applied.

As mentioned before, to evaluate the effectiveness of the above proposed method, osteoporosis was used as a case study. Three osteoporosis datasets, two structured (CSV) and one unstructured (image) medical dataset, are used to train an ANN model for disease prediction. The proposed privacy-preserving system consists of many stages. It begins by obtaining datasets and ends with system evaluation, passing through encryption and ANN prediction stages, as illustrated in Fig. 5. The details of each stage are explained as follows:

5.1 Dataset collection stage

To test the proposed system, three *datasets were used* to predict osteoporosis. The data were downloaded from Kaggle. The details of each dataset are explained in Table 2. Dataset 1 consists of 16 features used for prediction (ID, Age, Gender,

Hormonal Changes, Family History, Race/Ethnicity, Body Weight, Calcium Intake, Vitamin D Intake, Physical Activity, Smoking, Alcohol Consumption, Medical Conditions, Medications, Prior Fractures, and classes).

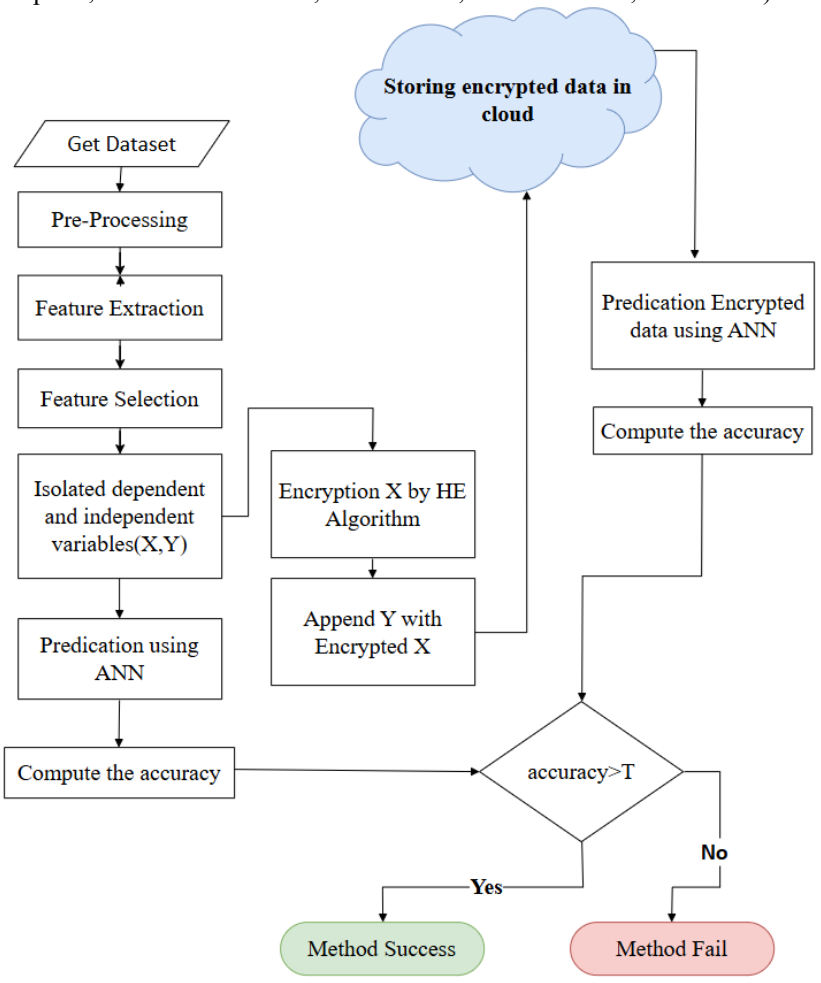

Fig. 5. Proposed Privacy-Preserving System

The images in dataset 2 are grouped into 372 images for the normal person and 372 images for osteoporosis. Dataset 3 contains the following features: S.No., Patient Id., Joint Pain, Gender Age, Menopause Age, Height (meter), Weight (KG), Smoker, Alcoholic, Diabetic, Hypothyroidism, Number of Pregnancies, Seizer Disorder, Estrogen Use, Occupation, History of Fracture, Dialysis, Family History of Osteoporosis, Maximum, Walking distance (km), Daily Eating habits, Medical History, T score Value, Z Score Value, BMI, Site, Obesity, and class. There are three classes in this dataset: 36 files for normal, 154 files for osteopenia, and 49 files for osteoporosis.

TABLE 2: DATASET DETAILS

No.	Dataset Name	Type of Data	No. of columns	No. of files	No. of classes	size
1	Osteoporosis Risk Prediction, [31]	CSV	16	1958	Two Osteoporosis and Normal	(235.69 KB)
2	Osteoporosis [32]	RGB Image	256	744	Two Osteoporosis and Normal	(299.83 MB)
3	Knee Osteoporosis Dataset multiclasses [33]	CSV	28	240	Three Normal, Osteopenia, and Osteoporosis	(48 KB)

5.2 Preprocessing Stage

First, the system splits the dataset into dependent variables and independent variables. The data are pre-processed before the encrypting stage, including converting categorical values into numeric forms, such as (male 0 and female 1). Additionally, in the preprocessing stage, we convert the floating-point numbers into integers via a rounding process; these steps are more important for the encryption and prediction process. The red, green, and blue (RGB) color image of dataset 2 must be converted into a grayscale image for feature extraction later. The ANN divides the data into training and testing

sets, 80% for training and 20% for testing, and then the normalization process is performed on the training and testing sets. This step is necessary due to the features of the data have different scales, which affects the ANN's performance, so normalization ensures that each feature has an equal effect on the results.

5.3 Feature Extraction and Selection

As mentioned earlier, the system will be applied to various databases (CSVs and images). For CSV data, a set of rows and columns is used. The rows represent the number of patients, and the columns represent the features of each patient. Some features, such as the patient's ID number, are excluded during the training process because they do not contribute to the prediction process. Many missing value features are also removed to avoid bias or reduce the reliability of the model. The rest corresponds to the features that were input into the ANN after being encoded.

A technique is required for extracting features from the images for the database containing bone X-ray images. In this study, pretrained visual geometry group (VGG-16)-CNNs were used for this purpose. Each image is passed through the network, and 512 features are output, the features representing high-level visual patterns.

To reduce the computational complexity, not all 512 features are used. Rather, the best and most informative features are selected to train the ANN while maintaining a high level of classification. Principal component analysis (PCA) was used to reduce the dimensionality by selecting the best 150 features to move on to the next stage.

5.4 Encryption Stage

Separately, the datasets are encrypted via homomorphic techniques (RSA or LWE), as illustrated in Fig. 6 and Fig. 7, respectively. The challenge when using LWE is that the volume of the data is increased compared with its original size because each value needs to be converted into binary format and encrypted each bit separately. The result of the encryption of each bit is two values, and each number can be represented with a different binary bit number. Resolving this problem is maintained by equalizing all the numbers to one length of the result by taking the maximum output of one column and filling the rest of the numbers with zeros. The size of the ciphertext that is encrypted via RSA is fixed and equal to the plaintext size. Finally, the encrypted data as well as the decision variable are merged and then stored on the cloud server.

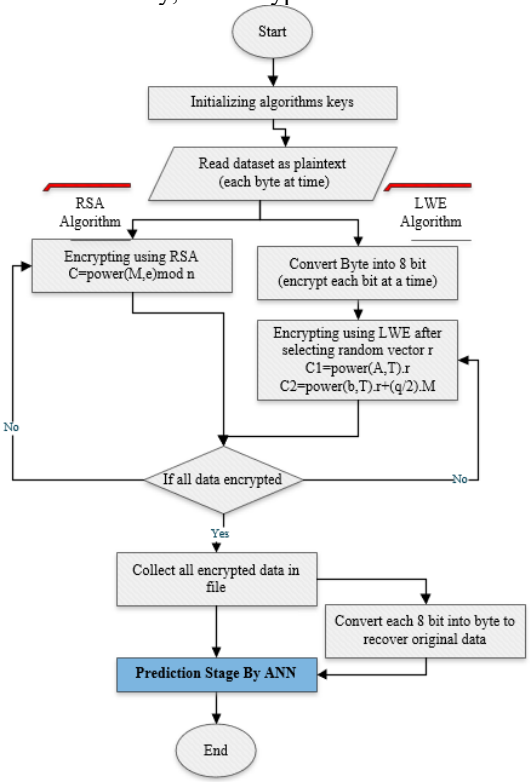

Fig. 6. Encryption Process

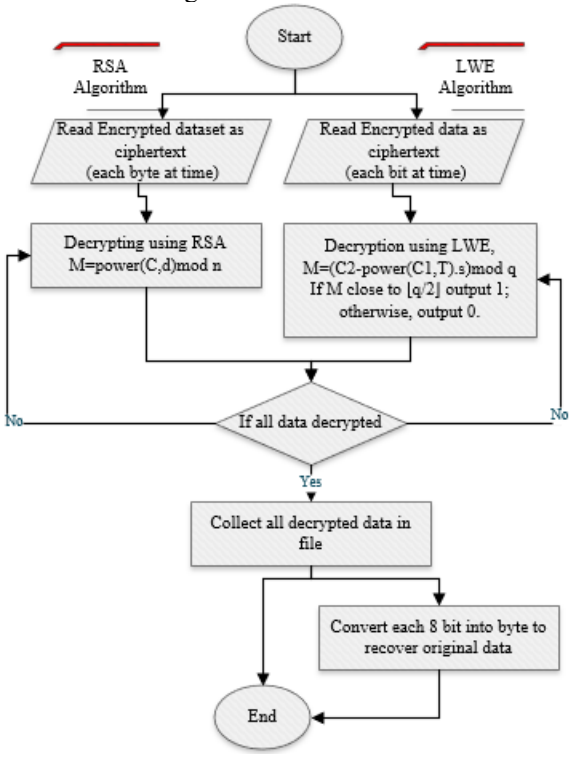

Fig. 7. Decryption Process

Example 1: Consider the number 8. When encrypted using RSA, it becomes: **182322**, for n=191483 and e =7
While the result of number 8, if LWE encrypts it, is

63 12 11 62 66 14 60 13

Because it is represented in binary format with 4 digits (1000), each digit is encrypted with 2 decimal numbers, so the result is 8 numbers.

Example 2: If m= **4**, the m encrypted by RSA is **16384**. The m encrypted by LWE is as follows:

64 58 13 60 12 17

It is represented by 3 digits only in binary format (100).

5.5 Prediction Stage

For the prediction process, an ANN is used to predict whether a person suffers from osteoporosis disease, depending on the encrypted dependent variables without prior information about the original data. The ANN consists of an input layer that depends on the number of input features, two second (hidden) layers with 128 and 46 neurons, and one output layer. Table 3 explains the details of the ANN structure. The researchers employ an output layer with sigmoid and softmax activation functions, whereas the hidden layers use ReLU as the activation function.

TABLE 3. ANN STRUCTURE

Component	Details
Model Type	Sequential model used for both binary and multiclass classification.
Input Layer	Dense to process the input features
Dropout Layer 1	Dropout(0.3) to reduce overfitting.
Hidden Layer	Dense for feature transformation and nonlinearity.
Dropout Layer 2	Dropout(0.2) to improve generalization.
Output Layer	'sigmoid' as activation function for binary classification and 'softmax' for 3-class output.
Loss Function	Binary crossentropy is suitable for binary targets. In addition, sparse categorical crossentropy for multiclass.
Optimizer	Adam optimizer
Evaluation Metric	Accuracy is used to evaluate models during training and testing.

6. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed system implements two different HE techniques along with an ANN. This helps to decrease outside third-party interference or any intruders' involvement during communication. Two homomorphic encryption/decryption approaches were taken into consideration to increase the secrecy, privacy and security of the data kept on the cloud. Microsoft Windows 11, HP Core i7, and 16 GB RAM are the personal computer (PC) specifications that are used for implementing the systems. Python 3.12.7 is a programming language used for writing code. The system was evaluated on the two-sided prediction side and the security side as follows:

6.1 Encryption System Results and Discussion

To measure the performance of the security side, time, memory consumption (RAM), and storage overhead of the encryption and decryption process for the LWE and RSA algorithms are computed. Eq. (11) is used to calculate the storage overhead in bytes.

$$storage\ overhead = \frac{ciphertext_{size} - plaintext_{size}}{plaintext_{size}} * 100 \qquad (11)$$

Table 4 shows the difference in resource consumption between the LWE and RSA encryption schemes, which are used to maintain the privacy of patient data in three databases used later to predict osteoporosis.

TABLE 4. ENCRYPTION SYSTEM RESOURCE CONSUMPTION

Metrics		Dataset 1		Dataset2		Dataset3	
		LWE	RSA	LWE	RSA	LWE	RSA
Time (sec)	Encryption	2.7	2.7	43.98	11.08	0.14	0.06
	Decryption	0.224	2.81	1.85	11.33	0.01	0.05
Memory Consumption (RAM)	Encryption	2.57 MB	0.31 MB	33.15 MB	2.98 MB	0.04 MB	0.02 MB
	Decryption	0.36 MB	0.39 MB	3.32 MB	3.46 MB	0.00 MB	0.02 MB
Storage Overhead	Size of Original	0.22 MB	0.22 MB	2.91 MB	2.91 MB	0.04 MB	0.04 MB
	Size of Encrypted	0.34 MB	0.22 MB	8.92 MB	2.91 MB	0.18 MB	0.04 MB
	Storage Overhead	53.26%	0%	206.22%	0%	332.97%	0%

Databases 1 and 3 contain categorical data. Encrypting Database 3 (image features) using FHE (via LWE) consumed more RAM, 33.15 MB, and had a time consumption of 43.9s, which was comparable to that of the other databases; however, it was very efficient at decrypting data, where it took 0.01s for Dataset 3 and 1.85 s for Dataset 2. Although the algorithm requires somewhat large resources, it offers high security by allowing encrypted data to be processed without the need to

decrypt it. This makes it efficiently applied to medical diagnostic systems to prevent sensitive patient data from being exposed publicly. The encryption using PHE (via RSA) offers efficient RAM and time consumption, where it takes only 2.98 MB RAM and 11.08 seconds for Dataset 2.

LWE causes an additional storage overhead (53.26% in Dataset 1, 206.22% in Dataset 2, and 332.97% in Dataset 3) because LWE increases the size of the encrypted text, as shown in Table 4. However, this storage cost is acceptable when dealing with medical contexts because protecting patient data is a top priority. However, RSA does not incur any storage cost.

Notably, despite the high efficiency demonstrated by the RSA algorithm in terms of resource consumption, it lacks some features due to limitations, including dealing with binary features (0 and 1), as found in database 1 and database 3. Where it was observed that the ciphertext is the same as the plaintext, which jeopardizes data confidentiality. The solution to this problem is the use of padding technologies, including optimal asymmetric encryption padding (OAEP). It works by adding randomness to the text, improving semantic security, but increasing the size of the encrypted text causes increasing the computing cost. Therefore, the application of the RSA algorithm in real-time medical applications is limited.

After the results of the encryption systems are analysed, the following conclusions are drawn:

- It can be said that LWE is highly suitable for privacy preservation during the diagnosis of osteoporosis and can be integrated practically and securely with the requirements of cloud-based healthcare.
- RSAs can be used for light or semi sensitive applications that do not involve categorical data and do not require high confidentiality.

The bottom line is that HE is ready to handle clinical AI applications that require data privacy.

6.2 Prediction System Results and Discussion

The proposed prediction system was evaluated using performance metrics, namely, accuracy, precision, recall, and F score, which are computed according to equations (12), (13), (14), and (15), respectively. The training time, memory storage, and model size are also computed for all the datasets.

$$\text{Accuracy} = \frac{\text{TruePositives} + \text{TrueNegatives}}{(\text{TruePositives} + \text{FalseNegatives} + \text{TrueNegative FalsePositive})} \quad (12)$$

$$\text{Precision} = TruePositive/(TruePositive + FalsePositive \quad (13)$$

$$\text{Recall} = \text{TruePositive}/(\text{TruePositives} + \text{FalseNega tives} \quad (14)$$

$$\text{Fscore} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (15)$$

Each dataset is split into two sections that are utilized for training and testing: 80% and 20%, respectively. After the system experiments, we obtain the results explained in Table 5 and Fig. 8. The evaluation of prediction system performance across three osteoporosis-related datasets—under three settings—without encryption, with LWE encryption, and with RSA encryption—demonstrates valuable insights into the balance between accuracy, security, and computational resource demands.

TABLE 5. PREDICTION SYSTEM RESOURCE CONSUMPTION

Metrics	Dataset1			Dataset2			Dataset3		
	Without Encryption	LWE	RSA	Without Encryption	LWE	RSA	Without Encryption	LWE	RSA
Precision	0.955975	0.963855	0.527473	0.8971	0.8267	0.7312	0.9459	0.8051	0.7507
Recall	0.756219	0.79602	0.592593	0.8243	0.8267	0.9067	0.924	0.7896	0.7842
F1 score	0.844444	0.871935	0.55814	0.8592	0.8267	0.8095	0.934	0.7967	0.7657
Accuracy%	85.71%	88.01%	61.22%	86.58%	82.55%	78.52%	93.75%	87.50%	81.25%
Time of Predication	10.389 sec	11.614 sec	10.595 sec	7.21 sec	10.13 sec	1.94 sec	5.39 sec	4.76 sec	4.52 sec
Memory Usage	67.39 MB	63.55 MB	63.336 MB	66.2 MB	62.72	54.75	60.99 MB	63.203 MB	64.01MB
Model Size	0.06 MB	0.06 MB	0.06 MB	0.35 MB	0.35 MB	0.35 MB	0.06 MB	0.27 MB	0.16 MB

The results showed that LWE demonstrated strong performance in accurately predicting disease while maintaining reasonable resource consumption, enabling its use in real-world medical applications. When LWE was applied to all the databases, high prediction performance was achieved. For instance, in Dataset 1, the LWE-encrypted model achieves a precision of 0.9639, surpassing the unencrypted model (0.9560) and significantly outperforming RSA (0.5275).

The same applies to the F score value, which was 0.8719, which was completely consistent with the value for the unencrypted data. The resulting accuracy was 88.01%, the highest value ever achieved for disease prediction using encrypted data. In contrast, RSA's accuracy dropped sharply to 61.22%, primarily due to its poor handling of categorical-like or low-entropy features in Datasets 1 and 3, where encrypted messages often remain unchanged.

The results computed for database 2, which consisted of features extracted from X-ray images via a pretrained VGG-16 model, were as follows: the prediction accuracy without encryption was 86.58%. When the data were encrypted using LWE, it dropped slightly to 82.55%, but it still outperformed the accuracy achieved using RSA-encrypted data, which was 78.52%. The prediction time with LWE was marginally longer than the prediction time with RSA. Nevertheless, this increase is acceptable, especially when dealing with clinical data where patient privacy is a priority. The reduced time consumed by RSA came at the expense of accuracy and the F score.

The results demonstrated on databases 1 and 2 were confirmed when the systems were applied to database 3. Despite the memory consumption of the LWE-based model (e.g., LWE: 63.203 MB vs. no encryption: 60.99 MB), the model maintained a high accuracy of 87.50% and an F1 score of 0.7967. As expected, the RSA-based model achieved lower performance than LWE did, with an accuracy of 81.25% and an F score of 0.7657.

In conclusion, the LWE algorithm was able to preserve patient privacy with minimal sacrifices in time and resource consumption.

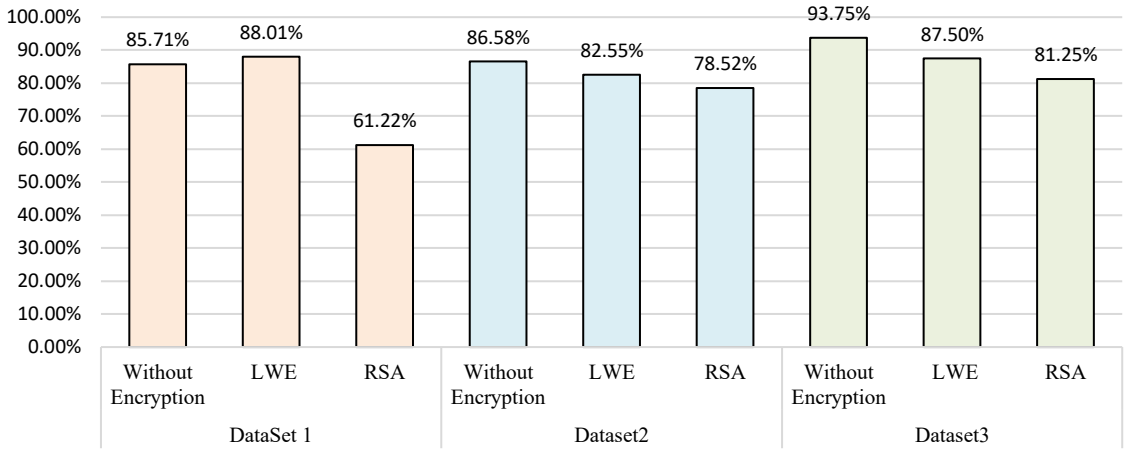

Fig. 8. Accuracies of the applied systems

Fig. 9 shows the trade-offs between time consumption for the prediction of osteoporosis between the three applied models for all the databases used.

For database1, the prediction time for normal data was 10.389 sec, which is slightly less than the prediction time for using data that are encrypted by LWE, which was 11.614 sec and 10.595 sec for RSA-encrypted data. The slight time variance is normal due to the calculations involved in the encryption. RSA-based prediction model for the second database achieved the lowest time of just 1.94 sec compared to the remaining models, where the prediction time for the model based on the LWE was 10.13 sec and the prediction time without encryption was 7.21 sec. This superiority is due to the nature of the data for the second set. The prediction time was almost the same for database3, with RSA slightly ahead by 4.52 sec, while with LWE, it was 4.76 sec, and prediction without encryption was 5.39sec.

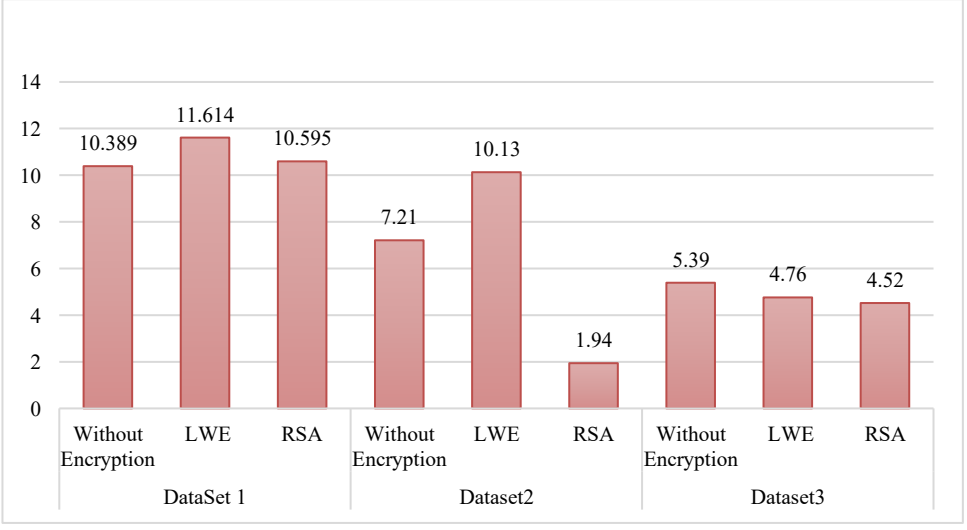

Fig. 9. Average time of prediction with and without encryption

Table 6 explains the trade-off between the training process across all three datasets and the models' performance. The validation accuracy metric is used as the main measure of generalization. According to the database, the results were as follows:

- Database 1: The model with LWE outperformed the model with RSA at epoch 15, where the validation accuracy was 88.53%, whereas the RSA accuracy was 85.35%. The validation accuracy converged after epoch 30. The model with LWE keep a small variation between the validation accuracy and training accuracy.
- Database 2: Applying prediction models to this dataset achieved a training accuracy of >97% at epoch 30, with stable validation accuracy. The RSA validation accuracy decreased to 69.33% at epoch 50 due to overfitting. The model with LWE maintains stable validation accuracy (~76.5%).
- Database 3: Applying osteoporosis prediction models to this dataset yielded a high accuracy of 92.3% for the unencrypted model, whereas LWE maintained a validation accuracy of 87.1% at epoch 50. The RSA-based model slightly lags its validation accuracy while demonstrating competitive training accuracy.

These results confirm that the verification accuracy measure is a reliable measure for assessing the effectiveness of real-world models in medical prediction applications. The results also showed that the model (via LWE) had strong generalizability with minimal deterioration in verification accuracy, making it practical and safe for use in healthcare.

TABLE 6. EPOCHES VS. ACCURACY

Dataset 1						
Without Encryption			**LWE**		**RSA**	
Epochs	**Train Accuracy**	**Validation Accuracy**	**Train Accuracy**	**Validation Accuracy**	**Train Accuracy**	**Validation Accuracy**
5	0.851438	0.818471	0.818182	0.847134	0.818182	0.847134
10	0.850639	0.821656	0.882102	0.866242	0.882102	0.866242
15	0.865016	0.821656	0.890625	0.88535	0.890625	0.88535
30	0.872204	0.812102	0.909091	0.878981	0.909091	0.878981
40	0.888179	0.812102	0.90767	0.872611	0.90767	0.872611
50	0.884984	0.812102	0.920455	0.853503	0.920455	0.853503
Dataset 2						
Epochs	**Train Accuracy**	**Validation Accuracy**	**Train Accuracy**	**Validation Accuracy**	**Train Accuracy**	**Validation Accuracy**
5	0.889387	0.8	0.86532	0.724832	0.826087	0.813333
10	0.946188	0.786667	0.919192	0.812081	0.943029	0.76
15	0.962631	0.813333	0.957912	0.812081	0.956522	0.786667
30	0.976084	0.8	0.973064	0.812081	0.971514	0.68
40	0.96562	0.813333	0.981481	0.778524	0.973014	0.706667
50	0.976084	0.84	0.974747	0.765101	0.974513	0.693333
Dataset 3						
Epochs	**Train Accuracy**	**Validation Accuracy**	**Train Accuracy**	**Validation Accuracy**	**Train Accuracy**	**Validation Accuracy**
5	0.736842	0.74359	0.907895	0.794872	0.743421	0.717949
10	0.894737	0.871795	0.986842	0.846154	0.921053	0.769231
15	0.947368	0.923077	0.993421	0.846154	0.980263	0.794872
30	1	0.923077	1	0.846154	0.993421	0.820513
40	1	0.897436	1	0.871795	0.993421	0.794872
50	1	0.897436	0.993421	0.871795	0.993421	0.820513

Fig. 10 shows the results of changing the size of a dataset on validation accuracy for osteoporosis prediction using the datasets under three scenarios: the plaintext-based model, the LWE-based model, and the RSA-based model across increasing dataset sizes (10%–90%). In the no encryption scenario of dataset 1, changing the size of the trained data decreases the validation accuracy from 0.86% to 0.76%. The case is interpreted as follows: increasing the batch size causes overfitting or gradient plateaus, whereas smaller batches make the weight update frequently and thus improve the generalizability. When privacy preservation is not constrained, the model maintains relatively stable performance, this is ensuring its baseline learning capacity. The model with the RSA algorithm showed little performance; the validation accuracy decreased from 0.66% to 0.52% as the number of batches grow. This degradation is due to the encryption algorithm, which introduces much noise that affects the model's ability to learn medical features. The noise can be decreased by frequent gradient updates that happen with small batches (e.g., 10%), which achieve a validation accuracy of 0.66%. An RSA in this form is unsuitable for application in medical classification. Under LWE encryption, the model demonstrates comparatively stable performance, with accuracy declining from 0.88 to 0.74 as the dataset size increases. The validation accuracy of the prediction with LWE is better than RSA due to LWE keeping the integrity of the encrypted features effectively. However, at higher dataset sizes, the accuracy degradation is likely to stem from the computational cost associated with LWE's homomorphic operations.

For Dataset 2, the model without encryption realizes an accuracy ranging moderately from 0.86% to 0.74%. The model with LWE encryption initially outperforms the baseline (0.87 at 10%), possibly due to regularization from encryption noise,

but the accuracy decreases sharply to 0.70 at 90%, indicating noise interference at scale. The accuracy fell from 0.74% to 0.66% with the RSA model, indicating feature distortion, which makes the model unable to predict correctly and unsuitable for application in medical prediction tasks. Lastly, for dataset 3, the figure shows that the accuracy varies from ~0.95% to ~0.70%, indicating better generalizability with more unencrypted data. In the LWE-based model, the performance improves at the middle size of batches, and the accuracy is moderate (~0.90% to ~0.70%). The RSA-based model was inefficient in the healthcare area because it performed worse, starting at ~0.80% and decreasing to ~0.60%.

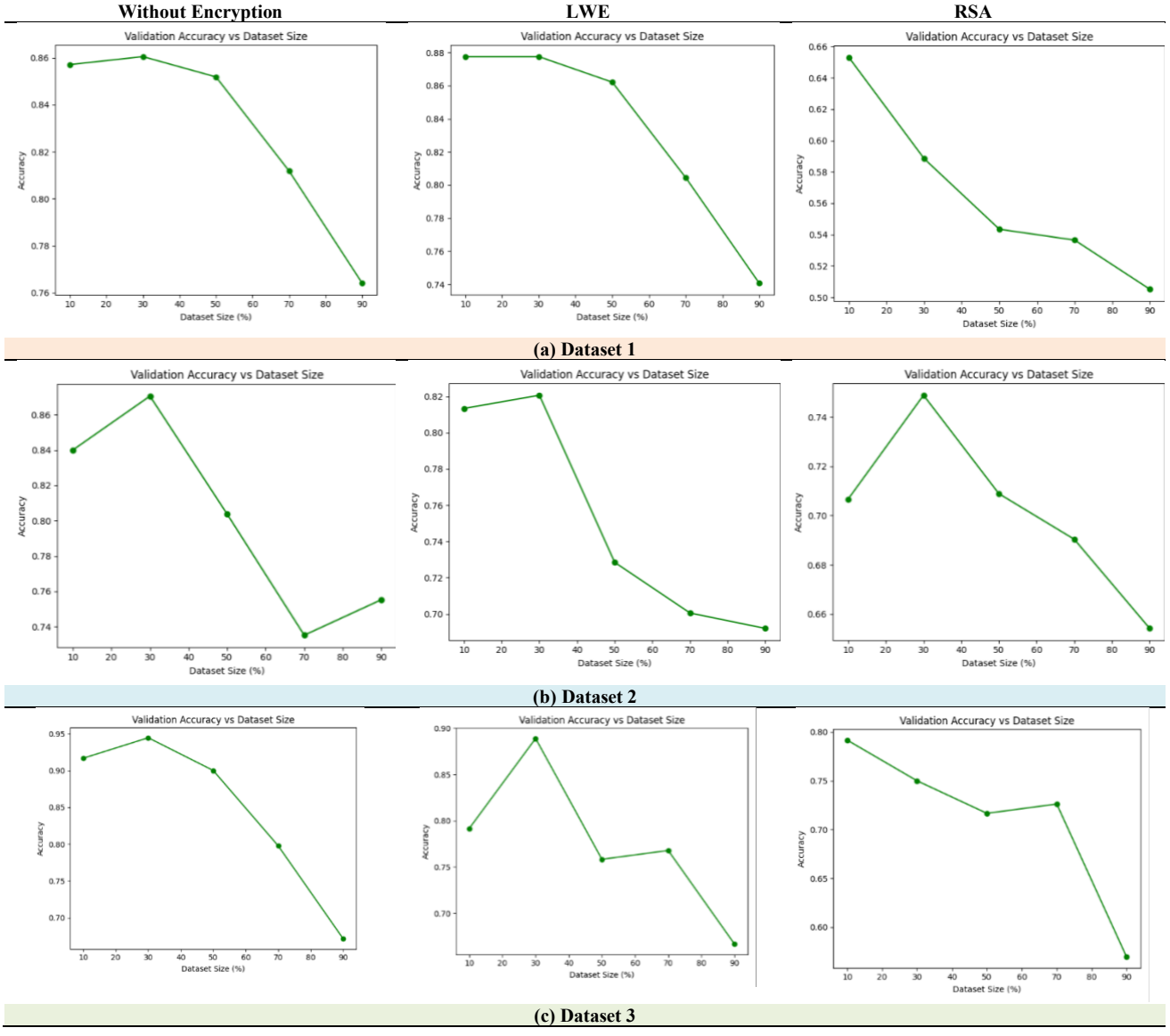

Fig 10. Batch size vs. validation accuracy.

7. SECURITY EVALUATION

In this study, it was assumed that patient data are kept on cloud servers to ensure the privacy of the data when a third party applies the prediction. So, homomorphic techniques are used, which allow third parties to apply the prediction to the encrypted data without the need to discover the patient's data. By using the PHE, which is represented by the RSA algorithm, to communicate secretly with the cloud, the data are encrypted using the public key of the cloud. Since only the cloud would have access to the appropriate private key, only the cloud would be able to decrypt such a message. The mathematical attack against RSA that makes it necessary to determine the prime components p and q of modulus n has drawn more interest due to of its security implications of an RSA-specific nature. The attacker will, of course, be fit to

determine the exponent d for decryption if they know p and q. A distinct approach would be to say that the attacker would try to determine the ∅n of the modulus n. As already mentioned, knowing p and q is equivalent to knowing n. Attackers will be able to construct the equation $(p-1)*(q-1) = \emptyset n$ and use it together with the equation $p*q = n$ to calculate the values for p and q if they can somehow find n.

Increasing the key size of RSA makes the algorithm stronger because the attacker needs to guess the prime numbers, which means that solving the factorization problem, which consumes more computational resources, but RSA remains vulnerable to quantum attacks that use quantum computers to efficiently factor numbers. Thus, RSA usage is limited to applications that do not require a high level of security. Therefore, FHE is applied and evaluated on the basis of the LWE algorithm to overcome the limitation of PHE and enhance cryptographic robustness. The LWE assumption is believed to be hard even for quantum adversaries, making it a promising foundation for postquantum cryptography [34] [35] [36]. This depends on the difficulty of solving specific noisy linear equations, which have been rigorously proven to be as hard as worst-case lattice problems. Unlike RSA, whose security depends on the number-theoretic assumption, LWE provides a wide and more adjustable security model. Furthermore, LWE allows homomorphic operations (additions and multiplication) on encrypted data, which is necessary for privacy-preserving deep learning. From a security perspective, LWE-based encryption offers significant advantages:

(1) Both conventional and quantum computers are unable to attack the program, which makes it a strong choice for postquantum cryptography.

(2) Its ability to change parameter-specific variables to control the level of security required for the application

(3) LWE can also be used to provide other security services, such as key exchanges and digital signatures [37].

In addition to the above security properties, LWE is also considered an effective and flexible homomorphic encryption algorithm that can execute calculations on encrypted data without the need for decryption. This is profitable in situations where sensitive data must be handled and examined without uncovering their contents. This makes LWE a suitable and proven solution for medical applications requiring rigid data confidentiality.
In summary, the dual use of RSA and LWE in the current study handles both immediate and long-term security concerns. RSA provides efficient encryption with lower computational overhead for applications that do not require full homomorphism, whereas LWE encloses robust, quantum-resistant security with guarantees of privacy during the entire prediction process.

8. COMPARISON WITH OTHER WORKS

First, the proposed work is the first to implement both FHE and PHE schemes on real-world medical datasets related to osteoporosis. Previous studies have relied primarily on synthetic datasets, such as Monte Carlo-generated samples [17] or widely used benchmark datasets like MNIST and CIFAR-10 [18] [17] [38] [38]. These datasets include both structured tabular records (CSV format) and diagnostic imaging (X-ray scans), significantly enhancing the clinical relevance and applicability of the findings, whereas prior research generally employs a single homomorphic encryption scheme in isolation—for example, Brakerski/Fan-Vercauteren (BFV) [18], Cheon-Kim-Song (CKKS) [18], or TFHE [39]. This work uniquely applies and directly compares both LWE-based FHE and RSA-based PHE within the same predictive framework and across the same medical datasets. This dual evaluation provides a rare and valuable trade-off analysis between model performance, computational cost, and encryption strength that is not available in the literature.

The proposed framework not only evaluates model performance in terms of classification accuracy, precision, recall, and F1 score but also includes crucial system-level metrics such as prediction latency, memory usage, and model size. Such holistic evaluation metrics are typically omitted in prior works and represent a step forward in making privacy-preserving models feasible for deployment in real-world diagnostic systems. Despite the computational overhead of homomorphic encryption, the experimental results demonstrate that the encrypted ANN model retains a high level of diagnostic accuracy, achieving, for instance, 88.01% accuracy using LWE on one dataset. Privacy preservation does not come at the expense of diagnostic performance. This is what happens in [18], where the ANN with CKKS achieves an accuracy of 87.10% and the CNN with BFV on CIFAR-10 achieves an accuracy of 69% in [17], which are both lower than the accuracy achieved. Finally, in this paper, it was implemented an encryption, training, and evaluation pipeline that supports both numerical and image-based input types with illustrating the epoch-level performance tracking. This end-to-end design explains the viability of the proposed framework not merely as a theoretical contribution but also as a practical system that can be appropriate for other diseases or medical datasets. Table 7 shows a comparison with other related works.

TABLE 7: COMPARISON WITH OTHER WORKS

Feature/Metric	Prior Works ([18], [17], [39], [38])	This Study
Real medical data	✗ (mostly MNIST, CIFAR, synthetic)	Osteoporosis datasets (CSV + X-ray)
Use of both FHE and PHE	✖	LWE + RSA
System-level metrics (time, memory)	✖	✓
Comparative encryption analysis	✖	✓
High accuracy on encrypted data	Some (on toy datasets)	On clinical data
Generalizability to healthcare	Limited	High

9. CONCLUSION AND SUGGESTION OF FUTURE WORKS

This study presented a structure that preserves the privacy of osteoporosis prediction through deep learning by combining HE techniques with neural network. This study also evaluated and contrasted the FHE (via the LWE) algorithm with the PHE (via RSA) algorithm, which was applied across various medical datasets, including structured CSVs and image-based data. The results ensured that using LWE-based prediction achieved high accuracy in disease prediction, reaching 88%. Patients' confidentiality was maintained during cloud storage. RSA-based prediction demonstrated weaknesses or limitations in generalization, robustness, and handling of categorical data, which LWE could overcome despite the high storage and computation costs.

The results also revealed that RSA prediction was efficient in terms of time and resource consumption, but its security capabilities declined when dealing with categorical data, which limits its use in medical applications without using the padding method, increasing its consumption of time and computational resources. This study promotes the secure and encrypted use of data during AI-based diagnostics. The idea reinforces the importance of using LWE in healthcare systems, as it has proven effective in preserving patient privacy during diagnostics, thus opening the way for many future medical projects related to the application of HE with machine learning.

FHE-based LWE lacks computational overhead, which can be solved in the future via some optimization techniques, such as ciphertext packing or the use of approximate homomorphic encryption schemes like CKKS. To reduce the processing time, hardware acceleration (e.g., using GPUs or FPGAs) can be used, thus improving scalability in medical applications. The scope of this study was to prove the effectiveness of applying homomorphic encryption schemes for privacy-preserving osteoporosis prediction using deep learning. It was not to evaluate the system's resilience against adversarial threats, such as side-channel attacks and chosen-ciphertext attacks. Assessment of these attacks requires specialized testing environments and methodologies that can be used in the future.

Future optimization can enhance the computational efficiency of homomorphic operations to be applied in real-time encrypted predictions, especially in time-sensitive medical environments. For future work, Explainable AI (XAI) techniques such as SHapley Additive exPlanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME) will be incorporated to reinforce the interpretability of both encrypted and nonencrypted ANN models, particularly in the context of the medical area, where transparency is critical.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Acknowledgment:

None.

References

[1] A. Vizitiu, C. I. Niţă, A. Puiu, C. Suciu, and L. M. Itu, "Applying deep neural networks over homomorphic encrypted medical data," *Comput Math Methods Med*, vol. 2020, no. 1, p. 3910250, 2020.

[2] Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE transactions on information forensics and security*, vol. 13, no. 5, pp. 1333–1345, 2017.

[3] Z. Salam, "A One Day Workshop on 'Preparing High Quality Journal Article'SESSION 1 MOTIVATION. TITLE, ABSTRACT AND INTRODUCTION," *Centre of Electrical Energy Systems, UTM Johor Bahru, Malaysia*, Nov. 2019.

[4] N. J. H. Marcano, M. Moller, S. Hansen, and R. H. Jacobsen, "On fully homomorphic encryption for privacy-preserving deep learning," in *2019 IEEE Globecom Workshops (GC Wkshps)*, IEEE, 2019, pp. 1–6.
[5] G. Ali and M. M. Mijwil, "Cybersecurity for sustainable smart healthcare: state of the art, taxonomy, mechanisms, and essential roles," *Mesopotamian journal of Cybersecurity*, vol. 4, pp. 20–62, May 2024, doi: https://doi.org/10.58496/MJCS/2024/006.
[6] A. D. Salman and E. H. Hasan, "Survey Study of Digital Forensics: Challenges, Applications and Tools," in *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, IEEE, 2023, pp. 788–793.
[7] B. Pulido-Gaytan *et al.*, "Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities," *Peer Peer Netw Appl*, vol. 14, no. 3, pp. 1666–1691, 2021.
[8] Z. H. Mahmood and M. K. Ibrahem, "New fully homomorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing," in *2018 1st Annual international conference on information and sciences (AiCIS)*, IEEE, 2018, pp. 182–186.
[9] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (Csur)*, vol. 51, no. 4, pp. 1–35, 2018.
[10] J. Bird and L. Eleftheriou, "Homomorphic Encryption Survey Paper," 2018.
[11] Z. Salam, "A One Day Workshop on 'Preparing High Quality Journal Article'Session 2: Methods, Results, Discussions, and Conclusion," *Centre of Electrical Energy Systems, UTM Johor Bahru, Malaysia*, Nov. 2019.
[12] A. D. Salman and M. J. Al-Shammaa, "Effect of Osteopontin and Other Biochemical Markers on Iraqi Women with Osteoporosis," *Ann Rom Soc Cell Biol*, vol. 25, no. 3, pp. 2264–2268, 2021.
[13] H. Takabi, E. Hesamifard, and M. Ghasemi, "Privacy preserving multi-party machine learning with homomorphic encryption," in *29th Annual Conference on Neural Information Processing Systems (NIPS)*, 2016, p. 4.
[14] P. Li *et al.*, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, pp. 76–85, 2017.
[15] X. Sun, P. Zhang, J. K. Liu, J. Yu, and W. Xie, "Private machine learning classification based on fully homomorphic encryption," *IEEE Trans Emerg Top Comput*, vol. 8, no. 2, pp. 352–364, 2018.
[16] M. S. I. Alsumaidaie, A. A. Nafea, A. A. Mukhlif, R. D. Jalal, and M. M. AL-Ani, "Intelligent System for Student Performance Prediction Using Machine Learning," *Baghdad Science Journal*, 2024.
[17] W. Legiest, F. Turan, M. Van Beirendonck, J.-P. D'Anvers, and I. Verbauwhede, "Neural network quantisation for faster homomorphic encryption," in *2023 IEEE 29th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, IEEE, 2023, pp. 1–3.
[18] M. R. Abou Harb and B. Celiktas, "Privacy-Preserving Machine Learning: ANN Activation Function Estimators for Homomorphic Encrypted Inference," *Authorea Preprints*, 2025.
[19] R. Q. Mohammed, M. M. Abdulrazzaq, A. J. Mohammed, K. Mardikyan, and M. Çevık, "Enhancing smart grid efficiency: a modified ANN-LSTM approach for energy storage and distribution optimization," in *2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, IEEE, 2023, pp. 1–5.
[20] A. M. Salman, B. T. Al-Nuaimi, A. A. Subhi, H. Alkattan, and R. H. C. Alfilh, "Enhancing cybersecurity with machine learning: A hybrid approach for anomaly detection and threat prediction," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 1, pp. 202–215, 2025.
[21] M. A. S. Al Zakitat, M. M. Abdulrazzaq, N. T. A. Ramaha, Y. A. Mukhlif, and O. A. Ismael, "Harnessing advanced techniques for image steganography: sequential and random encoding with deep learning detection," in *International Conference on Emerging Trends and Applications in Artificial Intelligence*, Springer, 2023, pp. 456–470.
[22] A. H. Alsaeedi, A. H. Aljanabi, M. E. Manna, and A. L. Albukhnefis, "A proactive metaheuristic model for optimizing weights of artificial neural network," *Indones. J. Electr. Eng. Comput. Sci*, vol. 20, no. 2, pp. 976–984, 2020.
[23] M. A. Rahman, R. C. Muniyandi, K. T. Islam, and M. M. Rahman, "Ovarian cancer classification accuracy analysis using 15-neuron artificial neural networks model," in *2019 IEEE Student Conference on Research and Development (SCOReD)*, IEEE, 2019, pp. 33–38.
[24] A. A. Nafea, A. L. Manar, K. M. A. Alheeti, M. S. I. Alsumaidaie, and M. M. AL-Ani, "A Hybrid Method of 1D-CNN and Machine Learning Algorithms for Breast Cancer Detection," *Baghdad Science Journal*, vol. 21, no. 10, 2024.
[25] S. S. Roy, A. Mallik, R. Gulati, M. S. Obaidat, and P. V. Krishna, "A deep learning based artificial neural network approach for intrusion detection," in *Mathematics and Computing: Third International Conference, ICMC 2017, Haldia, India, January 17-21, 2017, Proceedings 3*, Springer, 2017, pp. 44–53.

[26] Z. M. Muneef, H. Bahjat, and A. J. Abdulhoseen, "Image Encryption Paillier Homomorphic Cryptosystem," *Iraqi Journal Of Computers, Communications, Control And Systems Engineering*, vol. 21, no. 4, pp. 29–36, 2021.
[27] R. Sood and H. Kaur, "A literature review on rsa, des and aes encryption algorithms," *Emerging Trends in Engineering and Management*, pp. 57–63, 2023.
[28] F. Mallouli, A. Hellal, N. S. Saeed, and F. A. Alzahrani, "A survey on cryptography: comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, IEEE, 2019, pp. 173–176.
[29] Y. Salami, V. Khajevand, and E. Zeinali, "Cryptographic algorithms: a review of the literature, weaknesses and open challenges," *J. Comput. Robot*, vol. 16, no. 2, pp. 46–56, 2023.
[30] Y. Wei, L. Bi, X. Lu, and K. Wang, "Security estimation of LWE via BKW algorithms," *Cybersecurity*, vol. 6, no. 1, p. 24, 2023.
[31] Amit Kulkarni, "Osteoporosis Risk Prediction," https://www.kaggle.com/datasets/amitvkulkarni/lifestyle-factors-influencing-osteoporosis.
[32] "Osteoporosis," https://www.kaggle.com/datasets/mrmann007/osteoporosis.
[33] "Knee Osteoporosis Dataset multiclasses," https://www.kaggle.com/datasets/mohamedgobara/osteoporosis-database.
[34] B. G. Kim, D. Wong, and Y. S. Yang, "Private and secure post-quantum verifiable random function with nizk proof and ring-lwe encryption in blockchain," *arXiv preprint arXiv:2311.11734*, 2023.
[35] T. T. Nguyen, Q. B. Phan, T. X. Nghiem, M. Gowanlock, and B. Cambou, "A video surveillance-based face image security system using post-quantum cryptography," in *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2023*, SPIE, 2023, pp. 147–154.
[36] T. Bao, P. He, and J. Xie, "Systolic acceleration of polynomial multiplication for KEM saber and binary ring-LWE post-quantum cryptography," in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, IEEE, 2022, pp. 157–160.
[37] K. Zhang, Y. Liu, L. Wang, and L. Li, "Identity-Based Proxy Re-Encryption Based on LWE with Short Parameters," in *2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS)*, IEEE, 2023, pp. 118–124.
[38] A. Madi, R. Sirdey, and O. Stan, "Computing neural networks with homomorphic encryption and verifiable computing," in *Applied Cryptography and Network Security Workshops: ACNS 2020 Satellite Workshops, AIBlock, AIHWS, AIoTS, Cloud S&P, SCI, SecMT, and SiMLA, Rome, Italy, October 19–22, 2020, Proceedings 18*, Springer, 2020, pp. 295–317.
[39] G. V Turturica and V. Iancu, "Homomorphic inference of deep neural networks for zero-knowledge verification of nuclear warheads," *Sci Rep*, vol. 13, no. 1, p. 7464, 2023.