INSTITUTE OF INFORMATION
AND COMMUNICATION TECHNOLOGIES
BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **26**, No 2
Sofia • 2026 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2026-0012

Privacy-Preserving Federated Learning with Galois Automorphism-Driven Linear Transformation with Brakerski-Fan-Vercauteren for Medical Data

C. R. Kavitha[1,2], *K. N. Sowmya*[3]

[1]*Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru, Amrita Vishwa Vidyapeetham, India*
[2]*Department of Computer Science and Engineering, JSS Academy of Technical Education, Bengaluru, Karnataka 560060, India*
[3]*Department of Information Science and Engineering, JSS Academy of Technical Education, Bengaluru, Karnataka 560060, India*
E-mails: cr_kavitha@blr.amrita.edu cr1.kavitha@gmail.com kn_sowmya@rediffmail.com

Abstract: *Healthcare data is frequently fragmented over diverse organizations because of its extremely complex and confidential nature. However, the existing Federated Learning* (*FL*) *approach through a central server creates various challenges within healthcare, such as privacy vulnerabilities and regulatory compliance. Thus, this research proposes the privacy-preserving FL approach with Fully Homomorphic Encryption* (*FHE*) *for protecting the patient's sensitive data in medical records. In the proposed framework, the Galois Automorphism-driven Linear Transformation with Brakerski-Fan-Vercauteren, named GALT-BFV, is proposed for improving the medical data privacy and security. Moreover, this research introduces the pre-trained model of XceptionNet for training the local and global models in FL. Finally, the Federated Proximal* (*FedProx*) *approach is introduced for the aggregation of local and global models. The experimental discoveries establish that the proposed GALT-BFV method reaches better accuracies of 0.98 and 0.88 on Coronavirus Disease 2019* (*COVID-19*) *X-ray and brain tumor Magnetic Resonance Imaging* (*MRI*) *datasets, compared to previous approaches.*

Keywords: *Brakerski-Fan-Vercauteren, Federated Learning, Fully Homomorphic Encryption* (*FHE*)*, Galois Automorphism-driven Linear Transformation, and XceptionNet.*

1. Introduction

Large-scale biomedical data plays an important role in advancing healthcare services, especially in supporting experts through precise diagnostics and effective treatment planning [1]. Through the fast growth of data-assisted advancements, the safeguarding of data privacy is emerging as a significant problem in various

applications. The large amount of confidential data often being developed and accessed makes it important to secure the data from third parties as well as probable fissures [2]. Acquiring and transmitting medical data, such as medical images, is becoming more effective and accessible. Nevertheless, it still needs improved security mechanisms to secure the patient's privacy [3]. The conventional data processing approaches depend on estimation and centralized storage, where information is integrated on central servers [4]. However, this centralized method is susceptible to privacy fissures while broadcasting as well as storing the data. The confidential data becomes uncovered when central storage or transmission procedures are compromised or attacked, causing crucial problems to the organizations and individuals [5, 6]. Machine Learning (ML) approaches become most significant through an expansion of the domain of Artificial Intelligence (AI) [7]. However, obtaining large-scale data becomes increasingly challenging due to privacy-preserving concerns and the presence of data-sharing barriers among organizations [8]. Thus, Federated Learning (FL) is a famous privacy-preserving solution for AI techniques because it enables users to share the model parameters through the server rather than sharing sensitive data [9, 10].

The FL approach is emerging as an important part of the joint learning approach, which is broadly studied in various areas such as medical imaging, blockchain, image classification, and computer vision [11, 12]. In conventional centralized learning, a large volume of user data is required for effective model training. Nevertheless, user data involves subtle privacy data, which results in user data leakage [13]. As an emerging distributed learning model, the FL approach trains the parameters of the model from diverse users through a lack of perception of their actual information [14]. This scheme is a privacy protection method that is attaining the trust of more participants. Though the FL approach solves some security issues of centralized systems, it still involves significant vulnerabilities [15, 16]. Even in a federated system, transmitting the updated model may inadvertently reveal information related to the local datasets. This determines the requirement for more expansion of privacy-preserving approaches in the FL method [17]. In this manner, the Fully Homomorphic Encryption (FHE) becomes the effective solution to improve privacy protection in FL [18]. FHE enables the analysis to be considered on encrypted data without requiring decryption, ensuring that subtle data remains safe over a comprehensive data processing framework. This capability makes the HE an optimal device for solving privacy vulnerabilities in the FL approach [19, 20].

Problem statement and objective. The existing Federated Learning (FL) approach through a central server creates various challenges within healthcare, such as privacy vulnerabilities and regulatory compliance. In the proposed approach for medical data, a collaboration of privacy-preserving FL and FHE becomes an important part in promising both confidentiality and safekeeping during model training over diverse edge nodes. FL allows decentralized training, while edge devices equally train a global model while protecting the actual data privacy. Rather than that, the model updates are transmitted to the federal server. This approach ensures confidentiality by keeping personal health data securely on each device.

Nevertheless, during this collaborative training process, preserving the privacy as well as truthfulness of model updates is significant, particularly when employing medical data. FHE provides problem-solving through enabling aggregation to be employed and ensures that data are securely transmitted to the server for aggregation without knowing any sensitive data. This research aims to address the challenges of privacy protection and secure collaborative learning in distributed medical data environments. Considering this problem, a privacy-preserving FL approach integrating homomorphic encryption and Deep Learning (DL) is developed. The proposed approach is evaluated through extensive experiments on benchmark datasets and compared with existing methods to demonstrate its effectiveness and practical applicability.

The key highlights of this research are provided as follows.

- The research proposes a Galois automorphism–driven linear transformation and key-switching mechanism within the BFV system for minimizing the computational overhead as well as noise accumulation. An incorporation of Galois automorphism operations with an efficient key-switching mechanism enhances the effectiveness of ciphertext manipulation in the BFV homomorphic encryption scheme. This improvement allows faster encryption, decryption, and bootstrapping processes, making the scheme suitable for real-time applications.
- The proposed GALT-BFV method is incorporated into FL to secure client-server communication without compromising model performance. Through minimizing the encryption and aggregation time, an approach allows efficient large-scale distributed training while preserving privacy for sensitive medical data. Therefore, the proposed approach allows effective collaborative training across diverse institutions while handling the privacy preservation for sensitive medical data.
- Extensive experiments on Coronavirus Disease 2019 Chest X-ray (COVID-19 X-ray), brain tumor Magnetic Resonance Imaging (MRI), and Medical Information Mart for Intensive Care III (MIMIC-III) datasets demonstrate the scalability and adaptability of the proposed approach. The estimation involves comparisons across different approaches, aggregation methods, and various numbers of clients, showing consistent improvements in accuracy and efficiency. The findings demonstrate reliable enhancements in both prediction accuracy and computational efficiency. These findings emphasize the adaptability of the proposed method for secure and consistent medical data analysis in distributed healthcare systems.

This research paper is structured as follows. Section 2 illustrates the literature survey, and Section 3 offers preliminaries. Section 4 represents the proposed methodology, and Section 5 presents experimental results. The conclusion is specified in Section 6.

2. Literature survey

With the initiation of the digital revolution, healthcare encourages the growth of different privacy-preserving approaches that combine ML and FL to ensure secure

healthcare applications. Through a review of existing studies, this survey highlights current advancements and delineates the scope of the proposed research within the broader field.

Firdaus, Larasati and Hyune-Rhee [21] implemented the FL approach through blockchain as well as Homomorphic Encryption (HE). This study aimed to reduce the part of a central server, allowing a collective model training over healthcare establishments, which improved the data privacy and security. The blockchain confirmed the truthfulness and transparency of processes, whereas HE made sure that the information remained secure. This implemented approach significantly allowed the establishments to supplement the medical skills while keeping patient information secure and facilitating the medical analytics in practical settings.

Walskaar, Tran and Catak [22] developed the privacy-preserving FL approach with respect to homomorphic multi-key encryption through the support of the Ring Learning With Error (RLWE) system and FL to secure the confidential information. Particularly, the problem-solving was improved through the development of the most secure HE method in the FL scheme. Moreover, the practical implementation of an encryption scheme for the Extended Multi-Key Cheon-Kim-Kim-Song (xMK-CKKS) Homomorphic Encryption Scheme was acquired and developed, and a hand-made communication between server and client was incorporated into the FL approach. This method ensured that the multi-key approach updates confidentiality HE approaches.

Abaoud, Almuqrin and Khan [23] presented a new method that solved the constraints by the development of a privacy-preserving FL approach. The presented approach allowed the medical organizations to mutually train an ML approach on decentralized data, simultaneously preserving the secrecy of the discrete patient's information. During the model combination stage, the proposed approach ensured the privacy of sensitive information by performing advanced privacy-preserving approaches, which involved secure multi-party estimation as well as discrepancy privacy. To authenticate the effectiveness of the presented approach, this study performed an array of complete simulations as well as estimations through various performance measures. The presented approach offered greater utility and ensured vigorous privacy promises.

Ali et al. [24] introduced the Blockchain-assisted FL (BFL) approach for an enhancement of privacy preservation in Electronic Health Records (EHR) tasks. The introduced approach utilized the Zero Knowledge Proofs (ZKP) for authentication as well as HE for privacy estimation, ensuring vigorous data security through the lack of revealing the actual patient's information. The FL approach allowed the decentralized model training over Internet of Things (IoT) devices, minimizing the privacy issues while keeping the utility of the data. Moreover, the blockchain advancement allowed the integrity as well as transparency of EHR transactions through the design of a tamper-proof ledger.

Li, Tan and Shin [25] developed the Cryptography Generative Adversarial Network (Crypto GAN), which integrated the GAN into the client's local network and aligned the generator's output distribution with the feature distribution of local

data distribution. Then, integrated the client's data by uploading homomorphically encrypted parameters of the generator. This approach not only prevented the leakage of local data features but also safeguarded the sensitive medical information contained within the generator parameters, thereby enhancing privacy in medical applications.

N a r e s h and R e d d i [26] solved the complex problem of privacy-preserving heart disease prediction through the development of the HE-assisted Logistic Regression (HELR) approach, which utilized a Cheon-Kim-Kim-Song (CKKS) encryption approach. A design of this developed approach comprised the HELR method applied to different healthcare datasets and compared its effectiveness through Support Vector Machine (SVM). A developed HELR approach illustrated the vigorous security privacy attacks at diverse ML phases.

G u p t a et al. [27] presented a communication-effective and privacy-preserving hybrid FL approach for mental healthcare applications. The different hybrid FL approaches, such as Clustered Federated Learning (CFL) and Quantum Federated Learning (QFL), were introduced in this study. The CFL focused on leveraging the learning behavior of clients, while QFL advanced federated learning by incorporating a Variational Quantum Classifier (VQC) for the classification process. Then, the angle encoding was leveraged for the quantum state preparation to increase the information encoding as well as learn the quantum model.

Research gap. While existing FL frameworks integrate conventional cryptographic methods, these approaches often suffer from high computational overhead, large encryption/decryption times, and inefficient handling of noise during bootstrapping. Moreover, prior works primarily focus on either model accuracy or data security in isolation, neglecting the trade-off between efficiency and strong privacy guarantees. This gap highlights the need for a scheme, namely, GALT-BFV, which addresses efficiency, scalability, and privacy preservation together in federated healthcare and IoT environments.

3. Preliminaries

This research introduces the computation of FL and the approaches utilized for privacy-preserving. The FHE is utilized for sharing and storing the arbitrary counts for securing the patient's sensitive medical data.

Fed prox. FL firmly allows the decentralized data sharing through managing the data acquisition, training, and integration over dispersed end devices, as well as a central server, and note the set of each node of size $|k| = N$ and D_k demonstrates every probable distribution of the data. Assume that $f_k(w; x_k)$ denotes the loss function of node k across modl w and instance x_k, and $F_k(w) \coloneqq E_{x_k \sim D_k}[f_k(w; x_k)]$ demonstrates the loss function of node k. An FL approach reduces the aim value by using the equation bellow:

$$\min_w \left\{ f(w) = \sum_{k \in K} \frac{n_k}{n} F_k(w) \right\}, \tag{1}$$

where $n = \sum_{k \in K} n_k$ illustrates the comprehensive value of every node's size. Every FL iteration utilizes the various sampling approaches for device collection with respect to minimizing the communication costs. Leveraging the local servers, the selected devices optimize the local aim function earlier, uploading an enhanced local model parameter to the federal server. A centralized server modifies a global model parameter by integrating a given particular update constraint. This research performs the statistical heterogeneity such that the information is non-Independent as well as Identically Distributed (non-IID). Once the causes of system heterogeneity are understood, most devices will be characteristically considered in every task of the iterative training process. Consequently, a larger number of devices can participate in local model updates, which helps reduce the divergence caused by numerical heterogeneity within the system. Thus, Federated Proximal Optimization (FedProx) includes the proximal value to constrain the unconventionality of local updates among the rounds while addressing a local function. Particularly, rather than solely updating model parameters by reducing a local function $F_k(w)$, the device performs its local selection solver and reduces the subsequent destination h_k, as illustrated in

$$\min_{w} \left\{ h_k\left(w; w^t\right) = F_k\left(w\right) + \frac{\mu}{2} w - w^{t2} \right\}. \tag{2}$$

The FedProx is extended from Federated Averaging (FedAvg) with respect to an inaccurate solution as well as a proximal term and converts it to FedAvg at: (i) a proximal value that is unraised, such that $\mu = 0$; (ii) system heterogeneousness is not taken into account; (iii) the local server is selected to be Stochastic Gradient Descent (SGD). Due to the ability to handle undesirable effects of system and statistical heterogeneity, FedProx is more commonly used in real-world settings than FedAvg.

4. Proposed methodology

This research proposes a secure FL method through leveraging FHE for solving the privacy-preserving issues in medical data.

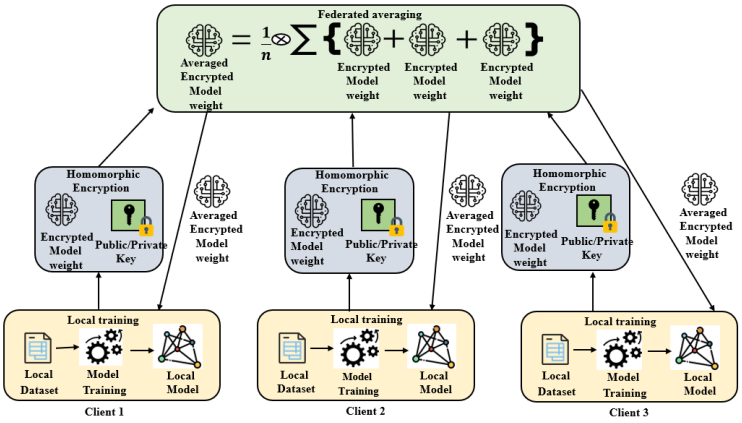

Fig. 1. Architecture of the proposed FL-assisted privacy-preserving

The proposed approach performs the FL background, which is appropriate for healthcare applications where organizations such as clinics remain steadily obtainable to participate in collaborative training during every estimation round. Simultaneously, the FHE secures data privacy through enabling the various participants, namely, healthcare units, to integrate in a collaborative FL approach while securing their encrypted data. Fig. 1 demonstrates the architecture of the proposed FL-assisted privacy-preserving.

4.1. System model

Before bestowing the design architecture, this research offers descriptions of appropriate relations utilized in this research.

(i) Users. They are involved in contributing to health organizations that have a greater amount of actual medical information. In this system, clinics are considered data providers who assess local model training through their individual information.

(ii) Local datasets. Information is deposited and locally processed at every contributing clinic. As compared to existing centralized ML, the proposed method controls the data in a dispersed way. Every clinic leverages its individual local dataset to locally train an approach that improves privacy as well as security to ensure that actual healthcare information, which involves personal data, does not remove the local hospital background.

(iii) Sensitive data. The FL approach aims to maintain data confidentiality to ensure that sensitive information remains within the local entities (e.g., hospitals), thereby reducing data exposure or unauthorized entry challenges. With respect to healthcare data sharing, confidential data involves Personally Identifiable Information (PII) such as names, genetic data, health data, addresses, treatment antiquities, diagnoses, and various health-assisted information.

(iv) Trained local model. Denotes an FL approach that is trained through data stored in the clinic. In this procedure, every clinic transmits a trained approach's parameters only to the edge server; this information is combined to design an improved global model.

(v) Clusters. The clinics are gathered into clusters to reduce transmission risks from users to an edge server. Moreover, clustering contributing clinics in terms of network constraints, data distribution, or geographic proximity minimizes the computational load as well as enhances system effectiveness. Importantly, every cluster is prepared with an edge server to gather a trained local model from the clinic.

(vi) Edge servers. This is applied to collect trained local models given through the clinic and employ a combination of protected approaches. Moreover, edge servers enable local storage, transmission, and dispensation competencies and minimize communication as well as estimation costs by applying computational operations closer to the clinic, which was previously performed by data providers.

(vii) Global model. Once the completion of training, every clinic transmits the updated parameters to an edge server in its cluster. Then, an edge server combines these updates to design an unknown global model. Through utilizing homomorphic encryption, the proposed method enables aggregation of encrypted local model

updates without requiring decryption; thus, the confidentiality improves in a system.

(viii) Trusted Authority (TA). They are accountable for preparing different security parameters, such as producing and maintaining cryptographic keys. These keys are utilized for decrypting the model updates replaced among clinics as well as the edge server. Furthermore, a reliable specialist validates the clinic's identity to ensure that only legitimate and authorized clinics contribute to the training procedure.

4.2. Threat model

In FL, both the client devices and the central server are considered untrustworthy entities, as they may potentially act maliciously, leak sensitive information, or fail to comply with the prescribed training. The devices and the centralized servers involved in FL significantly follow the created training protocol and do not vigorously insert fake data into the training procedure. Nevertheless, they attempt to infer isolated information from the targeted device and can potentially reconstruct sensitive information from the shared data during the training procedure. Access to shared model updates enables an opponent to present the rebuilt outbreak to redevelop an actual training dataset or utilize an implication attack to determine whether the data records occur in the actual training dataset. Thus, severe privacy promises are required to be provided for protecting against confidentiality attacks. A peripheral opponent eavesdrops on the communications transmitted at training and attempts to obtain private data of every competence; however, it cannot disrupt the transmission process or provide malicious data [28].

4.3. Design of privacy-preserving federated learning with homomorphic encryption

In the prior section, this research gives an outline of the general ideas of the proposed method. This portion describes the technical data over the problem-solving assisted training procedure of FL with FHE with respect to providing the optimal understanding.

4.3.1. Initialization of the system

Considering that there are n participants, where everyone is represented as $P_i (i \in [1, n])$. In an initialization stage, the trusted authority is required to finish an initialization of different parameters as well as produce keys as follows [29].

- **Initialization of model parameters.** Trusted authority initializes the model parameters, such as the model structure $n \times n$, learning rate η, and training rounds $epoch$.
- **Generation of asymmetric keys.** Trusted authority produces various public and private key pairs (pk_i, sk_i) for every participant. This research accepts the Paillier asymmetric key strategy, which is broadly utilized in the area of privacy protection as well as secure computation.
- **Generation of a real symmetric matrix.** The trusted authority arbitrarily produces an actual symmetric matrix $A_{n\times n}$ of size $n \times n$ and allocates the $i$the row $A_{n\times n}$ to participant P_i.

- **Generation of FHE.** The trusted authority produces the particular FHE function related to the discrete logarithm issue. This approach is utilized by applicants for estimating the exactness of aggregate results.

4.3.2. Local and global model

At this stage, every contributor is accountable for completing various key tasks. To solve the health data heterogeneousness on the accuracy of the global model, this research introduces the local training method of XceptionNet [30] in a privacy-preserving FL approach. Caption is a depth-wise separable variation of Inception, where nxn Spatially channel-wise convolution is represented as depthwise convolution. The Xception is a Convolutional Neural Network (CNN) approach that involves 71 depth layers. This pre-trained Xception method comprises 36 convolution layers, which provides development to the approach's extraction procedure. The convolutional layers are set as 14 modules for a total of 36 layers. Through an exclusion of primary and final modules, all these modules contain linear residual connections. An Xception involves a linear stack of depthwise separable convolution layers, which contains residual connections. Particularly, this research includes the limitation of influence on the local loss function of the contributor. This aspect limits the discrepancy between the local and global models, thereby guiding the training direction of the local model. To avoid a local model from conflicting with a global model when updated, the Kullback-Leibler (KL) divergence value of various predicted likelihoods is used as a restriction influence on the training loss.

4.3.3. Homomorphic encryption

HE is a cryptographic approach that allows computation on ciphertexts without requiring decryption, hence preserving data confidentiality [31]. The HE enables the firm transmission of data between investigators, hospitals, and assurance agencies. Encrypting the data before sharing helps ensure that unauthorized access is prohibited and also prevents information leaks significantly. FHE represents a significant advancement in data security, allowing estimations to be directly employed on encrypted data. FHE depends on vigorous crypto approaches that ensure both security and functional correctness [32]. BFV is accurately considered for helping with homomorphic addition and multiplication functioning on encrypted data. This competence enables a simple computation of complete exact operations on ciphertexts, significantly generating results identical to those obtained from decrypted plaintexts. The BFV mechanism is a leveled HE scheme that enables the employment of modular calculation on encrypted integers. A level count is described as the count of conceivable reproductions across an individual ciphertext in an arithmetic circuit. BFV performs through coded vector communications encoded and encrypted into multinomials.

The arrangement of BFV delivers the subsequent process.

- **Generation of key.** Provided a safekeeping parameter λ, a private key k_{pvt} is generated from undeviating dispersal across integers Θ. Through leveraging the private key as well as the integer coefficient modulus q, a development approach

estimates a public key in the form of $k_{\text{pub}} = \left(\left[-Xk_{\text{pvt}} + e\right]_q,\ X\right)$; X is acquired from Θ, and e is acquired from a discrete Gaussian distribution across the integers ϕ. Moreover, different significant keys are produced the estimation key k_{est}, which is utilized for re-linearizing the ciphertexts acquired from the development of size 2. Then, the Galois automorphism key k_{gal}, which enables the rotation of vectors of encrypted values to efficiently employ the homomorphic duplications.

- **Encoding.** A message vector m in the BFV system is encoded into plaintext p, and it involves a polynomial form whose space is a ring $R_\tau = Z_\tau^+[X]/(X^N + 1)$, where τ is an integer plaintext modulus and N is a polynomial modulus degree. An encoding function $f_{\text{e}}(.)$ obtained as input plaintext modulus τ, and message vector m, and returning the plaintext polynomial in the form of p is formulated in the equation,

$$p = \left[p_0\right]_\tau X^0 + \left[p_1\right]_\tau X^1 + \ldots + \left[p_{N-1}\right]_\tau X^{N-1}, \tag{3}$$

where p_0, p_1, and p_{N-1} demonstrate the coefficients of positive integers less than τ.

- **Encryption.** A polynomial space for ciphertext is described as $R_q^2 = Z_\tau^+[X]/(X^N + 1)$. Here, two demonstrates the tuple of different components. For encrypting a plaintext p, a public key k_{pub}, and different arbitrary polynomials v_0, v_1, v_2 through constants are acquired from ϕ and utilized for acquiring a ciphertext c, which is formulated in the next equations:

$$c = (c[0],\ c[1]), \tag{4}$$

$$c[0] = \left[\delta p + k_{\text{pub}}[0]v_0 + v_1\right]_q, \tag{5}$$

$$c[1] = \left[k_{\text{pub}}[1]v_0 + v_2\right]_q. \tag{6}$$

Here, $\delta = [q/\tau]$ and q are integer constant moduli satisfying $1 < \tau < q$.

- **Decryption.** For decrypting the ciphertext c, the decryption task utilizes the private key as input, k_{pvt}, and addresses through the equation

$$p = \left[\frac{\tau.\left[c[0]+c[1].k_{\text{pvt}}\right]_q}{q}\right]_\tau. \tag{7}$$

- **Decoding.** An actual message from a homomorphic process is received from c through decoding a plaintext p.

In the BFV scheme, linear transformation plays a crucial role in efficiently managing the encrypted data representation during homomorphic computations. By leveraging Galois automorphisms and key switching, it enables the rearrangement of coefficients and the movement of values between plaintext slots, thereby supporting Single Instruction Multiple Data (SIMD) parallelism and reducing the overhead of costly operations. This transformation is particularly vital in the bootstrapping process, where it facilitates digit extraction and modulus switching to refresh ciphertexts and control noise growth. Beyond bootstrapping, linear transformation can be applied in privacy-preserving machine learning, secure database querying, and encrypted IoT data aggregation, as it allows encrypted inputs to be aligned, packed, or restructured for efficient parallel processing.

4.3.4. Model aggregation

Once the completion of the local and global model training procedure, the FL-assisted edge servers E_i obtain an encrypted model updated $\text{Enc\_HE}(\Psi_h^t)$ from their applied clusters C_i of contributing clinics and employ the aggregation of the model. E_i offers the local computation competence for employing an aggregation operation on HE approaches. After that, E_i aggregates the model updated through averaging $\text{Enc\_HE}(\Psi_h^t)$ from all contributing hospitals to produce an unknown global model as

$$\Psi_{\text{gbl}}^t = \sum_{h=1}^{H} \frac{n_h}{N} \text{Enc\_HE}\left(\Psi_h^t\right), \tag{8}$$

where N demonstrates a comprehensive amount of data points. Subsequently, a model update is encrypted, and an edge server lacks admission to actual data or particular information of model updates; it combines encrypted updates. Through leveraging the FHE as a safeguard aggregation approach, an edge server aggregates the model updates without decrypting them. Moreover, an unknown global model Ψ_{gbl}^t is transmitted through each distributed server E_i in FL. A distributed system of edge servers supports ignoring the complexities of individual points of failure, thus improving the comprehensive privacy of the FL approach. Hence, contributing hospitals download the decrypted unknown global model $\text{dec}(\Psi_{\text{gbl}}^t)$ for a further round of local training at the iteration $t + 1$.

5. Simulation results

The proposed approach is implemented and tested in a Python 3 environment on a system equipped with 64 GB RAM, an Intel i5 processor, and a Windows 10 operating system. For experimentation, 1000 records are selected from real-world datasets related to COVID-19 and brain tumor MRI scans, with 800 samples allocated for training and 200 for testing. Key hyperparameters such as batch size, count of epochs, and learning rate are configured to 32, 10, and 0.001, respectively. The model's performance is estimated through diverse evaluation metrics named accuracy, precision, recall, and F1-score to comprehensively measure its effectiveness.

5.1. Datasets

This research considers various datasets to estimate the performance of the proposed method. These datasets are carefully chosen to represent complex and collaborative healthcare scenarios, including pandemic-related diseases and severe medical conditions requiring rapid diagnosis and intervention. The details of the datasets used are provided below.

5.1.1. COVID-19 X-ray dataset

In experimental evaluation, this research utilizes a publicly available COVID-19 radiography dataset, which plays a crucial role in addressing the global pandemic by supporting early and reliable diagnosis. The dataset contains chest X-ray images

categorized into COVID-19 positive, normal, and non-COVID lung infections, such as viral pneumonia, as well as lung opacity. In total, it includes 3616 COVID-19 positive samples along with various non-infected and other lung disease conditions. This research focuses on binary classification, distinguishing between normal and COVID-19 cases to enhance diagnostic accuracy and promote timely intervention.

5.1.2. Brain tumor MRI dataset

This dataset involves 7023 high-resolution MRIs of the human brain, encompassing different categories: glioma, meningioma, pituitary tumor, and no tumor. This dataset offers complete imaging information for the healthy as well as exaggerated regions. In this study, the analysis is restricted to binary classification, such as no tumor versus meningioma, to demonstrate the proposed model's capacity for accurate tumor identification, aiding in clinical diagnosis and treatment planning.

5.1.3. MIMIC-III dataset

This dataset is a benchmark database that involves de-identified EHRs of over 50,000 Intensive Care Unit (ICU) patients. It includes diverse real-time clinical information such as demographic details, laboratory findings, vital signs, and physician notes. This dataset is predominantly appropriate for evaluating FL models in privacy-preserving medical environments, as it provides a realistic setting for assessing the system's reliability and data protection capabilities.

5.1.4. Wearable Stress and Affect Detection (WESAD) dataset

The WESAD dataset is a valuable resource for detecting mental states and modeling the physiological signals from wearable sensors such as blood volume, pulse, body temperature, electrodermal activity, electromyogram, electrocardiogram, respiration, and three-axis acceleration. This dataset comprises data from wrist- as well as chest-worn devices of 15 subjects, offering multimodal physiological data. The dataset features multiple sensor modalities as well as various affective states (neutral, stress, amusement), enabling ML model training and evaluation. With 64 features and over 100,000 samples, it has consequences for mental health monitoring, stress management, and affective computing.

5.2. Performance analysis

Table 1 illustrates the performance analysis of the proposed method through various local and global model training methods using different datasets. The different local and global training methods, such as Residual Network with 50 layers (ResNet50), Mobile Neural Network Architecture (MobileNet), and 16-layer Visual Geometry Group Network (VGG16), are estimated and compared with the proposed XceptionNet. Among the models, XceptionNet consistently achieves the highest performance across datasets, with accuracy above 98% for COVID-19 X-rays and notable improvements over other architectures in the medical datasets.

Table 1. Performance analysis of the proposed method with different local and global model training methods using different datasets

Dataset	Methods	Accuracy	Precision	Recall	F1-score
COVID-19 X-ray	ResNet50	0.9618	0.9618	0.9618	0.9618
	MobileNet	0.9673	0.9673	0.9673	0.9673
	VGG16	0.9721	0.9721	0.9721	0.9721
	XceptionNet	0.9836	0.9852	0.9842	0.9846
Brain tumor MRI	ResNet50	0.8537	0.8537	0.8462	0.8362
	MobileNet	0.8641	0.8641	0.8641	0.8641
	VGG16	0.8728	0.8728	0.8728	0.8728
	XceptionNet	0.8847	0.8937	0.8736	0.8846
MIMIC-III	ResNet50	0.8351	0.8351	0.8351	0.8351
	MobileNet	0.8412	0.8412	0.8412	0.8412
	VGG16	0.8469	0.8469	0.8469	0.8469
	XceptionNet	0.8563	0.8647	0.8644	0.8864
WESAD dataset	ResNet50	0.8424	0.8582	0.8392	0.8592
	MobileNet	0.8562	0.8735	0.8459	0.8732
	VGG16	0.8746	0.8946	0.8655	0.8836
	XceptionNet	0.8963	0.9037	0.8793	0.9037

Table 2 demonstrates the performance analysis of the proposed FedProx approach through aggregation approaches. The different FL-assisted aggregation methods, such as conventional FL, FedAvg, and Federated Splitting (FedSplit), are estimated and compared with the proposed FedProx method. The results highlight that FedProx consistently outperforms the other approaches, achieving greater results across all datasets.

Table 2. Performance analysis of the proposed method with aggregation methods

Dataset	Methods	Accuracy	Precision	Recall	F1-score
COVID-19 X-ray	FL	0.9627	0.9635	0.9620	0.9628
	FedAvg	0.9684	0.9693	0.9672	0.9682
	FedSplit	0.9732	0.9746	0.9724	0.9734
	FedProx	0.9836	0.9852	0.9842	0.9846
Brain tumor MRI	FL	0.8538	0.8627	0.8541	0.8582
	FedAvg	0.8651	0.8728	0.8662	0.8695
	FedSplit	0.8743	0.8812	0.8729	0.8765
	FedProx	0.8847	0.8937	0.8736	0.8846
MIMIC-III	FL	0.8372	0.8461	0.8385	0.8419
	FedAvg	0.8446	0.8532	0.8462	0.8493
	FedSplit	0.8492	0.8574	0.8508	0.8540
	FedProx	0.8563	0.8647	0.8644	0.8864
WESAD	ResNet50	0.8636	0.8472	0.8174	0.8472
	MobileNet	0.8735	0.8562	0.8364	0.8764
	VGG16	0.8833	0.8936	0.8562	0.8947
	XceptionNet	0.8963	0.9037	0.8793	0.9037

Table 3 presents the performance analysis of the proposed approach for various numbers of clients. This table analyzes the impact of varying the number of federated clients (5, 10, 15, and 20) on model performance. The results reveal that as the number of clients increases, the model also improves, but only up to a certain threshold. For instance, with 20 clients, the performance is maximized across datasets, indicating that diversity of client data improves generalization.

Table 3. Performance analysis of the proposed method for different numbers of clients

Dataset	Number of clients	Accuracy	Precision	Recall	F1-score
COVID-19 X-ray	5	0.9681	0.9692	0.9675	0.9683
	10	0.9731	0.9743	0.9724	0.9732
	15	0.9795	0.9804	0.9798	0.9799
	20	0.9836	0.9852	0.9842	0.9846
Brain tumor MRI	5	0.8623	0.8714	0.8632	0.8672
	10	0.8692	0.8769	0.8698	0.8733
	15	0.8754	0.8837	0.8742	0.8787
	20	0.8847	0.8937	0.8736	0.8846
MIMIC-III	5	0.8396	0.8487	0.8408	0.8442
	10	0.8449	0.8536	0.8461	0.8497
	15	0.8512	0.8596	0.8527	0.8564
	20	0.8563	0.8647	0.8644	0.8864
WESAD	5	0.7836	0.8047	0.7946	0.8735
	10	0.8047	0.8264	0.8047	0.8623
	15	0.8474	0.8763	0.8483	0.8846
	20	0.8963	0.9037	0.8793	0.9037

This research configured the different clusters, such as C1 and C2, with almost standardized data distribution, whereas C4 and C5 demonstrate the most diverse data distribution, with C3 located in the center. This research continues the observation through the count of hospitals in each cluster: C1, C2, C3, and C4 with 2, 3, 4, and 5 Hospitals (H), respectively. This research employs estimation on the collected datasets through standardized data distributions. Table 4 exhibits the performance analysis of the proposed approach with diverse clusters through standardized data distributions.

Table 4. Performance analysis of the proposed method with different clusters using standardized data distributions

Dataset	Clusters	Accuracy	Precision	Recall	F1-score
COVID-19 X-ray	C1: H=2	0.8738	0.8747	0.8836	0.8537
	C2: H=3	0.8839	0.9083	0.8937	0.8703
	C3: H=4	0.9103	0.9337	0.9284	0.9472
	C4: H=5	0.9472	0.9583	0.9423	0.9682
Brain tumor MRI	C1: H=2	0.8472	0.8393	0.8583	0.8484
	C2: H=3	0.8632	0.8873	0.8746	0.8561
	C3: H=4	0.8762	0.8937	0.8873	0.8736
	C4: H=5	0.9037	0.9173	0.9247	0.9027
MIMIC-III	C1: H=2	0.8392	0.8573	0.8638	0.8738
	C2: H=3	0.8432	0.8682	0.8847	0.8836
	C3: H=4	0.8574	0.8737	0.8936	0.8973
	C4: H=5	0.8756	0.8973	0.9138	0.9023
WESAD	C1: H=2	0.8136	0.8462	0.8362	0.8562
	C2: H=3	0.8364	0.8735	0.8534	0.8634
	C3: H=4	0.8673	0.8863	0.8752	0.8735
	C4: H=5	0.8864	0.9037	0.8946	0.8864

Table 5 displays the performance analysis of the computational complexity of the proposed approach compared to previous approaches. The existing HE approaches, namely, Elliptic Curve Cryptography (ECC), Rivest Shamir Adleman (RSA), and BFV, are estimated and compared with the proposed method. The

results highlight that the proposed scheme achieves lower key generation time, encryption time, and decryption time, thus providing strong privacy guarantees while improving efficiency. The proposed GALT-BFV reduces computational complexity through linear transformation with Galois automorphisms, demonstrating a balance between security and performance.

Table 5. Performance analysis of the computational complexity of the proposed method through previous approaches

Dataset	Method	Encryption time (s)	Decryption time (s)	Aggregation time (s)	Total execution time (s)
COVID-19 X-ray	ECC	2594.38	19125.37	352.19	3214.42
	RSA	3047.19	21287.46	374.28	3556.34
	BFV	2173.26	18264.53	325.43	3012.45
	Proposed GALT-BFV	1466.38	15583.38	246.72	2361.38
Brain tumor MRI	ECC	2652.17	19748.63	361.28	3318.27
	RSA	3148.24	21872.38	387.53	3664.42
	BFV	2279.53	18834.71	333.14	3104.28
	Proposed GALT-BFV	1582.38	16284.37	252.39	2472.41
MIMIC-III	ECC	2718.46	20123.52	368.27	3412.39
	RSA	3214.32	22286.47	392.16	3718.42
	BFV	2351.19	19256.37	340.24	3186.42
	Proposed GALT-BFV	1683.47	16983.28	261.48	2586.39
WESAD	ECC	2389.57	2557.48	359.43	3037.58
	RSA	2146.48	2247.49	332.82	3258.47
	BFV	1894.47	2046.47	298.47	3047.38
	Proposed GALT-BFV	1588.48	1784.58	258.34	2787.48

5.3. Comparative analysis

Table 6 provides the comparative analysis of the proposed method with the existing method based on COVID-19 X-ray, brain tumor MRI, and WESAD datasets. The existing method of Cross-silo FL [21] and Hybrid FL, which involves CFL and QFL [22] approaches, is validated with the proposed method using various performance metrics. In this comparative analysis, the percentage value of the existing method [27] is converted into a decimal according to the proposed method for better understanding.

Table 6. Comparative analysis of the proposed method with the existing methods

Dataset	Method	Accuracy	Precision	Recall	F1-score
COVID-19 X-ray	Cross-silo FL [21]	0.9725	0.9735	0.9725	0.9725
	Proposed GALT-BFV	0.9836	0.9852	0.9842	0.9846
Brain tumor MRI	Cross-silo FL [21]	0.8625	0.8837	0.8625	0.8606
	Proposed GALT-BFV	0.8847	0.8937	0.8736	0.8846
WESAD	FL [27]	0.8733	0.8018	0.873	0.8790
	CFL [27]	0.7839	0.9500	0.7545	0.797
	QFL [27]	0.8425	0.7850	0.9275	0.8452
	Proposed GALT-BFV	0.8963	0.9037	0.8793	0.9037

5.4. Discussion

The experimental evaluation illustrates that the proposed GALT-BFV-based privacy-preserving federated learning framework achieves better performance over

different medical datasets. A combination of the Galois automorphism-driven linear transformation through the BFV encryption system efficiently minimizes the computational overhead and noise accumulation, allowing rapid key generation, encryption, and aggregation processes. Moreover, performing the XceptionNet model for local and global training improves diagnostic performance for large healthcare datasets such as COVID-19 X-rays and brain tumor MRI images. An integration of the FedProx aggregation approach ensures stability in training under heterogeneous data distributions, solving non-IID data challenges basically identified in federated environments. The experimental comparisons display that the proposed approach reliably outperforms existing FL and encryption-based approaches in both accuracy and execution time. An attained balance between privacy preservation and computational effectiveness highlights the framework's applicability for real-world healthcare systems. Overall, the research demonstrates that integrating homomorphic encryption and optimized federated strategies ensures secure, scalable, and high-performance medical data analysis. The experimental evaluation illustrates the effectiveness of the proposed GALT-BFV-based FL approach over diverse medical datasets. The findings demonstrate that the proposed method handles competitive prediction accuracy while ensuring effective privacy protection through homomorphic encryption. Comparative analysis with existing approaches confirms that the proposed method reaches enhanced effectiveness with respect to encryption and aggregation time. These findings demonstrate that the proposed approach provides a balanced trade-off between model performance and security in distributed healthcare environments.

Although the improvement in accuracy over existing approaches is relatively small (around 1-2%), such enhancements are effective in large benchmark issues where baseline performance is already high. The proposed pipeline enhances the secure understanding through incorporating homomorphic encryption with federated training, allowing privacy-preserving medical data analysis while handling competitive predictive effectiveness. Nevertheless, the usage of encryption mechanisms produces more computational overhead at model training and aggregation. Future work will concentrate on enhancing the computational efficiency and scalability for large-scale medical datasets. Furthermore, optimization of the secure aggregation mechanism supports minimizing communication overhead in federated settings. Also, the proposed method offers a development for improving privacy-preserving learning in other sensitive domains where secure distributed data analysis is important.

6. Conclusion

This research proposed a secure method for FL that leveraged homomorphic encryption for solving the security and privacy apprehensions in the healthcare system. Thus, this research proposed the privacy-preserving FL approach with FHE for protecting the patient's sensitive data in medical records. In the proposed framework, the GALT-BFV was proposed for improving the medical data privacy and security. Homomorphic encryption secured personal health data at cooperative

FL model training as well as accumulation, allowed calculations on encrypted data without decryption, and hence ensured privacy and security. The experimental results established that the proposed GALT-BFV method reached optimal outcomes as compared to the existing methods. An effective accumulation as well as substantiation system minimized the execution time and enhanced the scalability and practicality of FL for real-time healthcare applications. Future work will concentrate on acquiring lightweight encryption approaches to minimize computational complexity while preserving robust data security. In addition, future work will also incorporate AI-driven anomaly detection to effectively identify potential threats, ensuring resilient, privacy-preserving, and scalable FL frameworks appropriate for secure healthcare environments.

***Acknowledgements*:** The authors gratefully acknowledge Sri Mata Amritanandamayi Devi (Amma), Chancellor, Amrita Vishwa Vidyapeetham, for her inspiration and for providing financial support for the Article Processing Charges (APC) of this publication.

References

1. Guduri, M., C. Chakraborty, U. Maheswari, M. Margala. Blockchain-Based Federated Learning Technique for Privacy Preservation and Security of Smart Electronic Health Records. – IEEE Transactions on Consumer Electronics, Vol. **70**, 2024, No 1, pp. 2608-2617.
2. Kolawole, A. F., S. O. Rahmon, O. Akinnagbe. Designing Secure Data Pipelines for Medical Billing Fraud Detection Using Homomorphic Encryption and Federated Learning. – International Journal of Science and Research Archive, Vol. **10**, 2023, No 3, pp. 1210-1222.
3. El Kinani, K., F. Amounas, S. Bendaoud, M. Azrour, M. Badiy. New Image Crypto-Compression Scheme Based on ECC and Chaos Theory for High-Speed and Reliable Transmission of Medical Images in the IOMT. – Cybernetics and Information Technologies, Vol. **24**, 2024, No 4, pp. 108-125.
4. Yazdinejad, A., A. Dehghantanha, H. Karimipour, G. Srivastava, R. M. Parizi. A Robust Privacy-Preserving Federated Learning Model against Model Poisoning Attacks. – In: IEEE Transactions on Information Forensics and Security. Vol. **19**. 2024, pp. 6693-6708.
5. Dhasarathan, C., M. K. Hasan, S. Islam, S. Abdullah, S. Khapre, D. Singh, A. A. Alsulami, A. Alqahtani. User Privacy Prevention Model Using Supervised Federated Learning-Based Blockchain Approach for the Internet of Medical Things. – CAAI Transactions on Intelligent Technology, Vol. **2023**, 2023, pp. 1-15.
6. Gopalakrishnan, A., N. P. Kulkarni, C. B. Raghavendra, R. Manjappa, P. Honnavalli, S. Eswaran. PriMed: Private Federated Training and Encrypted Inference on Medical Images in Healthcare. – Expert Systems, Vol. **42**, 2025, No 1, e13283.
7. Aziz, R., S. Banerjee, S. Bouzefrane, T. Le Vinh. Exploring Homomorphic Encryption and Differential Privacy Techniques towards a Secure Federated Learning Paradigm. – Future Internet, Vol. **15**, 2023, No 9, 310.
8. Babu, K. M., M. Syed, S. Shaik, S. Thalari, U. Macha, A. Chatakondu. Fully Homomorphic Encryption Framework for Privacy Preserving in Healthcare through Decentralized Machine Learning, Challenges in Information. Communication and Computing Technology. CRC Press, 2024.
9. Chen, Y., B. Wang, H. Jiang, P. Duan, Y. Ping, Z. Hong. PEPFL: A Framework for a Practical and Efficient Privacy-Preserving Federated Learning. – Digital Communications and Networks, Vol. **10**, 2024, No 2, pp. 355-368.

10. Lin, J., J. Chen, J. Xiong, D. Jiao, W. Zhao, Y. Xiang. A Lightweight Privacy-Preserving Federated Learning Framework for Heterogeneity-Resilient Skin Cancer Diagnosis. – IEEE Journal of Biomedical and Health Informatics, 2025, pp. 1-13.
11. Muthalakshmi, M., K. Jeyapal, M. Vinoth, P. S. Dinesh, N. S. Murugan, K. S. Sheela. Federated Learning for Secure and Privacy-Preserving Medical Image Analysis in Decentralized Healthcare Systems. – In: Proc. of 5th International Conference on Electronics and Sustainable Communication Systems (ICESC'24), IEEE. Coimbatore, India, 2024, pp. 1442-1447.
12. Rahbari, D., M. Daneshtalab, M. Jenihhin. An Efficient Architecture for Edge AI Federated Learning with Homomorphic Encryption. – IEEE Access, Vol. **13**, 2025, pp. 97919-97929
13. Yang, X., C. Xing. Federated Medical Learning Framework Based on Blockchain and Homomorphic Encryption. – Wireless Communications and Mobile Computing, Vol. **2024**, 2024, No 1, 8138644.
14. Arazzi, M., S. Nicolazzo, A. Nocera. A Fully Privacy-Preserving Solution for Anomaly Detection in IoT Using Federated Learning and Homomorphic Encryption. – Information Systems Frontiers, Vol. **27**, 2023, pp. 367-390.
15. Pan, Y., Z. Chao, W. He, Y. Jing, L. Hongjia, W. Liming. Fedshe: Privacy-Preserving and Efficient Federated Learning with Adaptive Segmented CKKS Homomorphic Encryption. – Cybersecurity, Vol. **7**, 2024, 40.
16. Shi, Z., Z. Yang, A. Hassan, F. Li, X. Ding. A Privacy-Preserving Federated Learning Scheme Using Homomorphic Encryption and Secret Sharing. – Telecommunication Systems, Vol. **82**, 2022, pp. 419-433.
17. Mantey, E. A., C. Zhou, J. H. Anajemba, J. K. Arthur, Y. Hamid, A. Chowhan, O. O. Otuu. Federated Learning Approach for Secure Medical Recommendation in the Internet of Medical Things Using Homomorphic Encryption. – IEEE Journal of Biomedical and Health Informatics, Vol. **28**, 2024, No 6, pp. 3329-3340.
18. Anitha, R., M. Murugan. Privacy-Preserving Collaboration in Blockchain-Enabled IoT: The Synergy of Modified Homomorphic Encryption and Federated Learning. – International Journal of Communication Systems, Vol. **37**, 2024, No 18, e5955.
19. Kumbhar, H. R., S. S. Rao. Federated Learning Enabled Multi-Key Homomorphic Encryption. – Expert Systems with Applications, Vol. **268**, 2025, 126197.
20. Li, Q., R. Cai, Y. Zhu. GHPPFL: A Privacy-Preserving Federated Learning Based on Gradient Compression and Homomorphic Encryption in Consumer App Security. – IEEE Transactions on Consumer Electronics, Vol. **71**, 2025, No 2, pp. 5090-5099.
21. Firdaus, M., H. T. Larasati, K. Hyune-Rhee. Blockchain-Based Federated Learning with Homomorphic Encryption for Privacy-Preserving Healthcare Data Sharing. – Internet of Things, Vol. **31**, 2025, 101579.
22. Walskaar, I., M. C. Tran, F. O. Catak. A Practical Implementation of Medical Privacy-Preserving Federated Learning Using Multi-Key Homomorphic Encryption and Flower Framework. – Cryptography, Vol. **7**, 2023, No 4, 48.
23. Abaoud, M., M. A. Almuqrin, M. F. Khan. Advancing Federated Learning through a Novel Mechanism for Privacy Preservation in Healthcare Applications. – IEEE Access, Vol. **11**, 2023, pp. 83562-83579.
24. Ali, A. A., M. A. Gunavathie, V. Srinivasan, M. Aruna, R. Chennappan, M. Matheena. Securing Electronic Health Records Using Blockchain-Enabled Federated Learning for IoT-Based Smart Healthcare. – Clinical eHealth, Vol. **8**, 2025, pp. 125-133.
25. Li, Y., Q. Tan, B. S. Shin. CryptoGAN: Privacy-Preserving Federated Generative Adversarial Networks with Homomorphic Encryption in Healthcare Systems. – IEEE Transactions on Computational Social Systems, 2025, pp. 1-12.
26. Naresh, V. S., S. Reddi. Exploring the Future of Privacy-Preserving Heart Disease Prediction: A Fully Homomorphic Encryption-Driven Logistic Regression Approach. – Journal of Big Data, Vol. **12**, 2025, 52.
27. Gupta, A., M. K. Maurya, K. Dhere, V. K. Chaurasiya. Privacy-Preserving Hybrid Federated Learning Framework for Mental Healthcare Applications: Clustered and Quantum Approaches. – IEEE Access, Vol. **12**, 2024, pp. 145054-145068.

28. S o n g, C., Z. W a n g, W. P e n g, N. Y a n g. Secure and Efficient Federated Learning Schemes for Healthcare Systems. – Electronics, Vol. **13**, 2024, No 13, 2620.
29. W a n g, R., X. Y u a n, Z. Y a n g, Y. W a n, M. L u o, D. W u. RFLPV: A Robust Federated Learning Scheme with Privacy Preservation and Verifiable Aggregation in IoMT. – Information Fusion, Vol. **102**, 2024, 102029.
30. B a l a, D., M. S. H o s s a i n, M. A. H o s s a i n, M. I. A b d u l l a h, M. M. R a h m a n, B. M a n a v a l a n, N. G u, M. S. I s l a m, Z. H u a n g. MonkeyNet: A Robust Deep Convolutional Neural Network for Monkeypox Disease Detection and Classification. – Neural Networks, Vol. **161**, 2023, pp. 757-775.
31. S h e n, C., W. Z h a n g, T. Z h o u, L. Z h a n g. A Security-Enhanced Federated Learning Scheme Based on Homomorphic Encryption and Secret Sharing. – Mathematics, Vol. **12**, 2024, No 13, 1993.
32. N a r e s h, V. S., G. T. V a r m a. Privacy-Enhanced Heart Stroke Detection Using Federated Learning and Homomorphic Encryption. – Smart Health, Vol. **37**, 2025, 100594.
33. B a l a j i, V., S. K a n n a n, M. S u r y a m r i t h a, M. B e l w a l. A Homomorphic Encryption Compiler for Blood Pressure Analysis. – In: Proc. of 3-rd International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT'24), Trichirappalli, India, 2024, pp. 1-5. DOI: 10.1109/ICEEICT61591.2024.10718595.
34. B h a v i t h a, M., K. R a k s h i t h a, S. M. R a j a g o p a l. Performance Evaluation of AES, DES, RSA, and Paillier Homomorphic for Image Security. – In: Proc. of 9th IEEE International Conference for Convergence in Technology (I2CT'24), Pune, India, 2024, pp. 1-5. DOI: 10.1109/I2CT61223.2024.10544282.
35. K r i s h n a, A., A. A r u n k u m a r, J. W i l s o n, K. S r e e k a n t h, A. K u n j u m o n, G. S a r a t h. HE-FLAD: Homomorphic Encryption-Based Federated Learning with Autoencoder-Driven Anomaly Detection Using Latent Representations. – In: Proc. of 6th IEEE India Council International Subsections Conference (INDISCON'25), Rourkela, India, 2025, pp. 1-8. DOI: 10.1109/INDISCON66021.2025.11251557.

Received: 03.11.2025, Revised version: 17.03.2026, Accepted: 24.03.2026