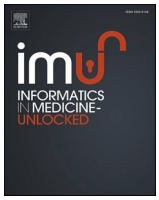
Informatics in Medicine Unlocked 49 (2024) 101547

Contents lists available at ScienceDirect

Informatics in Medicine Unlocked

journal homepage: www.elsevier.com/locate/imu



Distributed private preserving learning based chaotic encryption framework for cognitive healthcare IoT systems

Shaik Abdul Nabi [a], Ponugoti Kalpana [a], N. Subhash Chandra [b], L. Smitha [c], K. Naresh [d], Absalom E. Ezugwu [e,*], Laith Abualigah [f,g,h,i,j,k]

[a] Department of Computer Science and Engineering, AVN Institute of Engineering and Technology, Hyderabad, Telangana, 501510, India
[b] Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, Telangana, India
[c] Department of Information Technology, G Narayanamma Institute of Technology and Science, Hyderabad, Telangana, India
[d] Department of Computer Science and Engineering, TKR College of Engineering & Technology, Hyderabad, Telangana, 500097, India
[e] Unit for Data Science and Computing, North-West University, 11 Hofman Street, Potchefstroom, 2520, South Africa
[f] Computer Science Department, Al Al-Bayt University, Mafraq, 25113, Jordan
[g] MEU Research Unit, Middle East University, Amman, 11831, Jordan
[h] Applied Science Research Center, Applied Science Private University, Amman, 11931, Jordan
[i] Jadara Research Center, Jadara University, Irbid, 21110, Jordan
[j] Artificial Intelligence and Sensing Technologies (AIST) Research Center, University of Tabuk, Tabuk 71491, Saudi Arabia
[k] School of Engineering and Technology, Sunway University Malaysia, Petaling Jaya 27500, Malaysia

ARTICLE INFO

Keywords:
Cognitive health care
Internet of things
Privacy and security breaches
Distributed learning
Federated learning libraries
NIST

ABSTRACT

In the field of cognitive healthcare Internet of Things (CH-IoT), there is a strong demand for reliable and minimally intrusive smart gadgets that consistently acquire, analyse, and obtain the confidential health details of the individual. In fact, CH-IoT is empowered with artificial intelligence (AI) to transmute a fewer operational inputs into actionable, intelligent actions through the digitization of medical healthcare data. However, these systems consume more network complexity, interaction, and overhead costs, while inducing a blend of susceptibility and confidentiality issues. In support of this complexity, these cognitive systems need centralised data collection and to be gathered and analysed, which affects scalability issues and adds fuel to privacy and security breaches. Even though it possesses greater intricacy in its potential application, a substantial factor is maintaining the private preservation of healthcare data against the growing attacks. Thus, this paper presents a distributed privacy-preserving, chaotic encryption-based framework that can be deployed for CH-IoT systems to safeguard sensitive data against message modification, denial of service (DoS), and man-in-the-middle attacks (MIM), guaranteeing privacy and data integrity. The proposed framework integrated the federated learning layered hybrid chaotic encryption strategies by investigating through examination the learning infrastructure of convolutional neural networks (CNN). In the examination, the complete framework was carried out in the Tensorflow Federated Learning Libraries (FLL), and numerous performance metrics such as accuracy, precision, recall, f1-score, transmission efficiency, and overhead ratio were measured and contrasted with the various existing frameworks. For the intensive analysis, formal and informal security experiments were also conducted by NIST (National Institute of Science and Technology). The analytical results illustrate the importance of the proposed framework by achieving better security performance and outperforming the other existing models. Lastly, the proposed framework has more potential than the other existing frameworks and finds its place in real-time healthcare systems, but it needs to be improvised for real-time datasets.

* Corresponding author.
E-mail addresses: dr.nabi.cse@gmail.com (S.A. Nabi), drkalpanacse@gmail.com (P. Kalpana), subhashchandra@cvr.ac.in (N.S. Chandra), smitha2005sri@gnits.ac.in (L. Smitha), kuna48@gmail.com (K. Naresh), Absalom.ezugwu@nwu.ac.za (A.E. Ezugwu), aligah.2020@gmail.com (L. Abualigah).

https://doi.org/10.1016/j.imu.2024.101547
Received 29 April 2024; Received in revised form 4 July 2024; Accepted 4 July 2024
Available online 7 July 2024

1. Section-1

1.1. Introduction

However, these CH-IoT devices demand more complexities due to their resource-constrained and power consumption problems [1,2], and attract security and privacy problems [3,4] that even result in a fatal end in terms of the patient's side. As devices collect data from the cognitive healthcare environment, which consists of user behaviour and physical signals, These devices accumulate data that is dependent on network, communication, and dynamic environmental factors. These data are used to analyse and monitor the vital signs of the users and aid clinicians in the diagnosis and treatment process [5]. Moreover, the integration of artificial intelligence (AI) and deep learning algorithms in these devices makes it more intelligent to understand human cognition and environmental perceptions to identify the different risk levels of diseases in a real-time scenario [6,7,8].

In fact, these devices are now in everyone's life and put people in their comfort zone in terms of monitoring and the clinical treatment process. Fig. 1 illustrates the framework of the CH-'IoT framework of devices.

Fig. 1 illustrates how CH-IoT systems use artificial intelligence and IoT technologies to network hospitals and diagnostic centres. In this CH-IoT framework, IoT is used to collect any data format (video, images) from the diagnosis centre that contains the patient's sensitive information. These data formats are sent to hospital servers or the cloud, where AI algorithms are used to diagnose and treat patients more effectively, providing doctors with relevant information.

As a result, private-preserving machine learning models (PPML) [9] are formed to safeguard the confidentiality of the users whose information is meant for training the network. Private-preserving models are constructed based on Federated Learning techniques that offer an adaptive collaborative AI training approach and high degrees of user-level privacy without sharing information among individuals. These models are important as they protect the sensitive and personal information of the users [10,11].

1.1.1. Problem formulation

As discussed, the core problem is that the deployment of PPML in CH-IoT systems renders them susceptible and exposed to many growing cyber-attacks [12,13]. Moreover, applications of connected healthcare Internet of Things (CH-IoT) are intricately linked with sensitive services as they manage medical data concerning users. **The primary obstacle in this field pertains to safeguarding patient confidentiality and securing patients' data against attacks without degrading the performance or security level.** This System needs less memory to generate the same number of scroll as it takes the less component for generation [14]. Cognitive Healthcare-IoT belongs to the applications of the Internet of Things in health care applications [15]. Hence, novel and innovative security measures need to be implemented to ensure privacy and appropriate security for PPML in CH-IoT systems with less computational overhead, especially on CH-IoT devices [16,17]. The multi-scroll attractors are preferred over the other existing chaotic maps, such as sine, circle, tent, and logistic maps [18], due to their high randomness function and their ability to control their chaotic trajectories using the initial conditions. A significant benefit of Chaos-based encryption methods lies in their algorithmic effectiveness [19].

1.1.2. Contribution of the research

To meet the security and privacy requirements of CH-IoT systems, this paper designs the distributed PPML with hybrid chaotic encryption layers to protect the system features. In each experiment, this research proves the role of federated learning (FL) in PPML and chaotic encryption schemes in improving the ordinary performance metrics of learning networks for the participants and confirms the security levels against multiple attacks. As the first step, the framework incorporates the nature-inspired convolutional neural network (NI–CNN) suitable for the IoT devices that are used for the effective diagnosis of health care data.

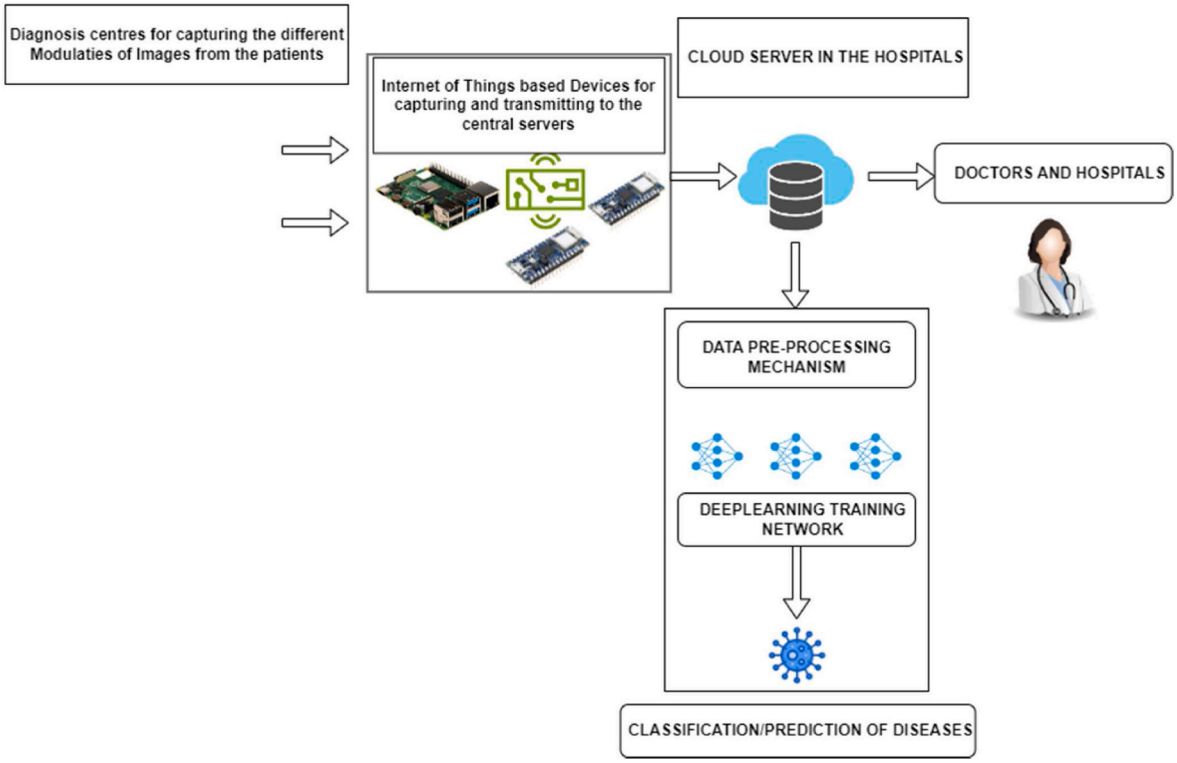


Fig. 1. General Description of CH-IoT systems.

This research study showed that the existing FL frameworks using CH-IoT need more improvisation strategies to protect system information using their own intelligence algorithms. The essential contribution of the suggested framework are as follows.

1. Proposed the nature-inspired convolutional neural network (NI–CNN) for an effective classification suitable for CH-IoT systems.
2. Deployment of **distributed privacy-preserving learning techniques** to mitigate potential attacks such as privileged-insider attacks and denial of service that often threaten the CH-IoT systems.
3. Incorporate the **principles of federated learning in DPPML and the hybrid chaotic encryption layer (HCEL),** which proactively manages the shared data in the CH-IoT networks, which guarantees to resist malicious behaviour with better credibility and robustness. Chaotic maps exhibit inherent intricacy and unpredictability, rendering them resilient against traditional cryptographic attacks. Moreover, their nonlinear behaviour augments their security. Furthermore, the deterministic attributes of chaotic maps render them an effective encryption technique.
4. **Extensive experimentation is conducted on real-time datasets** and various performance metrics are calculated, thereby comparing the results comprehensively with the existing state-of-the-art models.

1.1.3. Organization of the paper

The remainder of the document is formatted in the following manner.: 1) Section 2 briefly illustrates the existing FL frameworks for IoT and CH-IoT against the different threats. 2) Section 3 presents the phases of the proposed framework deployed in CH-IoT systems. 3)The experimental evaluation, analytical results and comprehensive comparisons are demonstrated in Section 4. 4) Ultimately, the research work is determined with the future advancements in Section 5.

2. Section-2

2.1. Related works

Chen et al. [20] proposed a lightweight security framework that is considered to be lightweight and uses low-power wearable sensors to analyse the key strengths of medical systems. Additionally, biometric authentication systems have been used to verify the fresh messages at every iteration via dedicated IoT gateways and systems.

Nair et al. [21] applied a federated learning architecture for constructing the privacy-preserving learning networks deployed for authentication and adopted the strategy of big-data analytics to analyse the functionalities of IoT systems with load reduction.

Lu et al. [22] developed a lightweight, privacy-preserving scheme for resource-constrained learning in an IoT-fog environment. In this scheme, three basic techniques, such as one-way hashing, Paillier cryptography, and the Chinese reminder problem, were applied to prevent data-related attacks at the edge of the networks. Examination results demonstrated that this system can mitigate computation and reduce communication costs.

Ma et al. [23] presented a multi-key holomorphic encryption protocol to design a novel privacy-preserving federated learning scheme to protect sensitive information by preventing data leakage while increasing bandwidth and communication costs. The experimental evaluation demonstrated that the model's accuracy still needs improvisation against conventional federated learning, while energy consumption and computation costs were reduced.

Zhang et al. [24] demonstrated the Privacy-Enhanced Momentum Federated Learning Framework to safeguard the privacy information of industrial agents. The above model combines differential privacy and momentum FL with chaos-based encryption to preserve privacy information and encrypt the weight of local models. The experimental results have demonstrated the excellence of model performance in terms of accuracy and privacy security.

Dharminder et al. [25] developed an efficient private-preserving framework based on Chebyshev chaotic maps to safeguard the management system against the vulnerabilities in the IoT systems. Results demonstrated that Chebyshev chaotic maps have produced considerable security requirements in the networks against privileged insider attacks.

Park et al. [26] demonstrated the privacy-preserving Federated Learning (PPFL) framework that uses a homomorphic encryption scheme at the centralised server to conduct arithmetic operations on encrypted texts. In this technique, the privacy-preserving technique uses the encrypted local model parameters but doesn't deploy the decryption for aggregation. This technique allows only encryption, which may be vulnerable to many attacks.

Zhao et al. [27] trained CNNs on MNIST, CIFAR-10, and speech commands datasets. They found that federated averaging reduced test accuracy for non-structured data.

Wang et al. [28] optimised Federated Learning on non-structured data using Reinforcement Learning.

Chen et al. [29] developed an asynchronous online FL system in which edge devices continuously transmit local non-IID data while a central server accumulates model parameters from clients.

3. Section-3

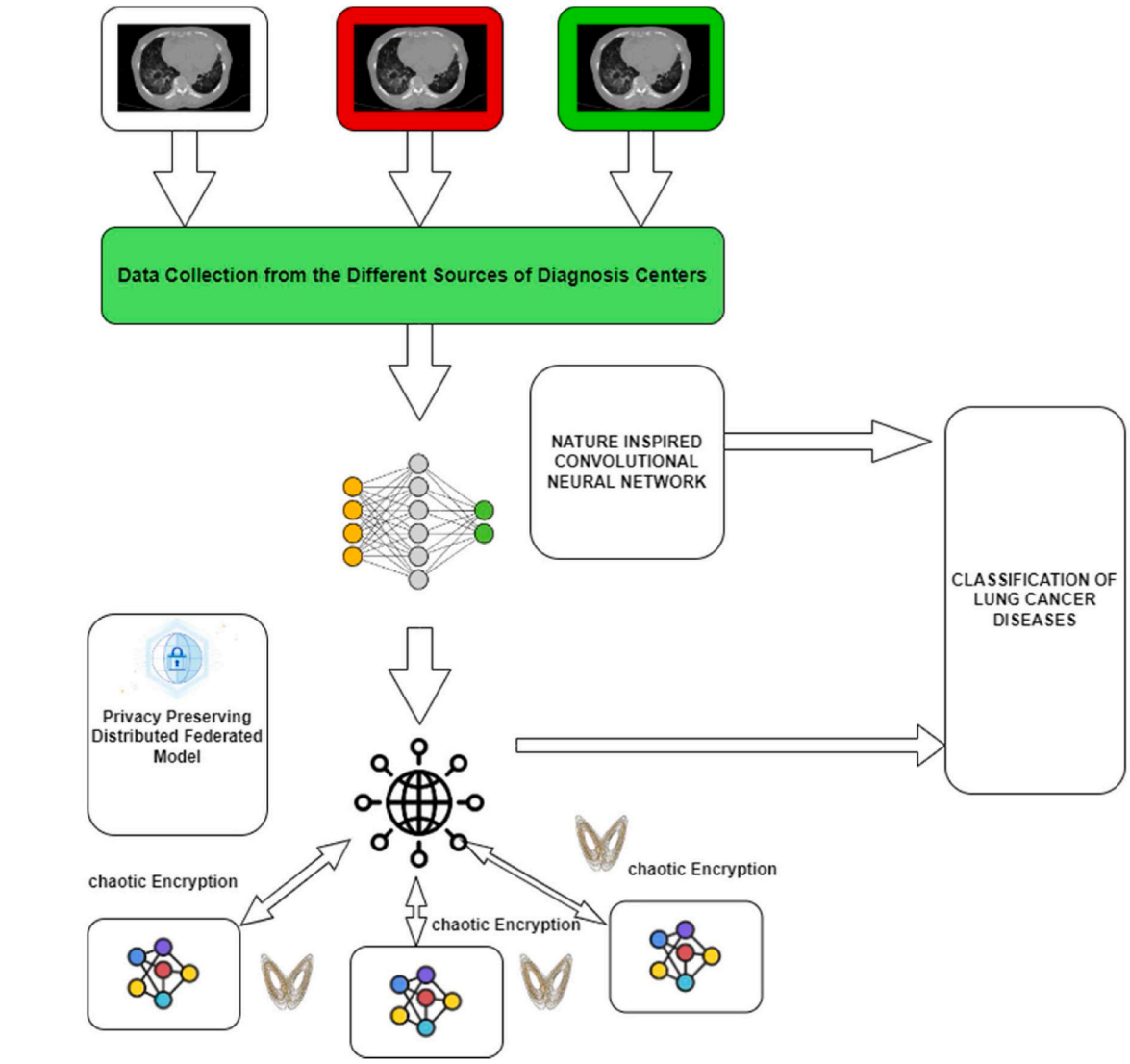
Fig. 2(a) and (b) illustrates the proposed framework which consists of four working phases: 1) Data Collection Systems(DCS). 2) Nature Inspired Deep learning framework(NIDLF). 3) Federated learning based private preserving NLDF models. 4) Effective Chaotic Encrypted Communication mechanism. 5) Effective Diagnosis and classification. The detailed description of each module is presented in preceding section.

3.1. Data Collection Systems

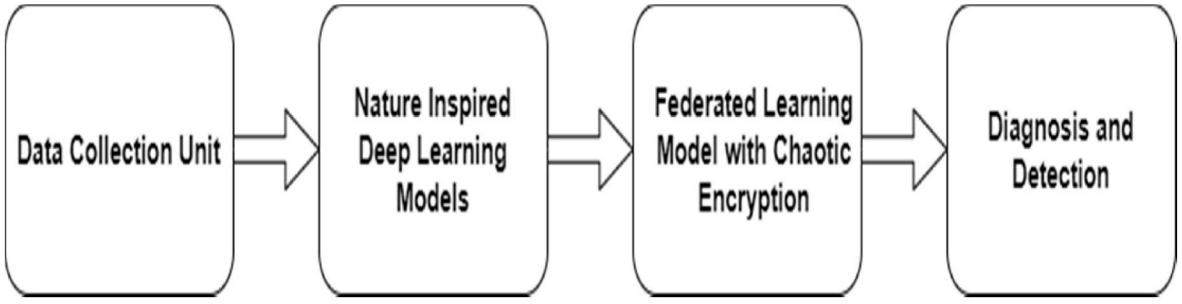
Since the CH-IoT systems transmit real-time images or videos, this research article employs CT lung cancer images collected from the TCIA databases [27]**.** Fig. 3 **shows the sample lung datasets.** The dataset comprises 1018 lung CT scans sourced from the National Cancer Institute, which are linked to proteomic and genomic clinical information in this study. All the training images are categorised as either malignant or benign nodules. A benign nodule is identified when scoring below 3, while a malignant nodule is identified when scoring above 3. The conversion of tcia format data to DICOM image data for subsequent processing is facilitated by a distinct software tool called the NBIA retriever. A encompassing overview of the testing datasets utilised is outlined in Ref. [28].

3.2. Nature Inspired Deep learning framework

To construct the Nature Inspired deep learning framework, conventional convolutional neural networks(CNN) are used in this research article. Then conventional CNN is converted into the nature inspired network by tuning the network hyper-parameters using the artificial



(a)



(b)

Fig. 2. (a)Comprehensive Framework for the Proposed Architecture (b) Step-by-Step technique for the Proposed Framework.

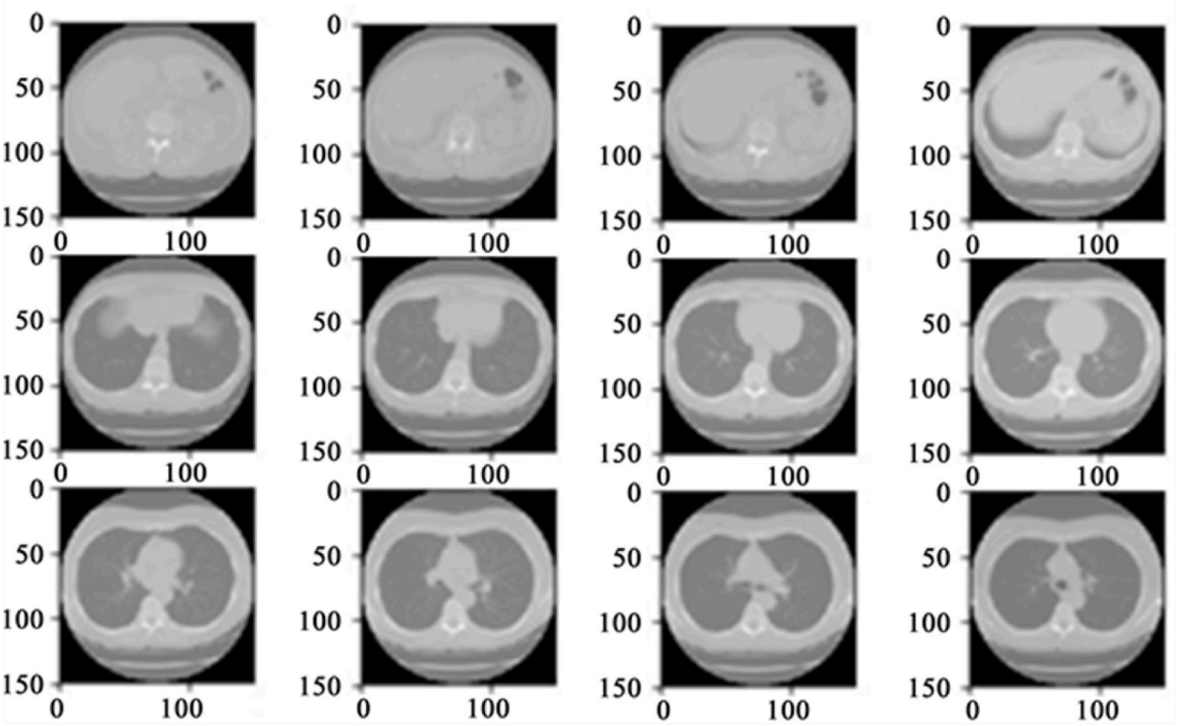


Fig. 3. Sample Lung Datasets used for Evaluating the Proposed Framework.

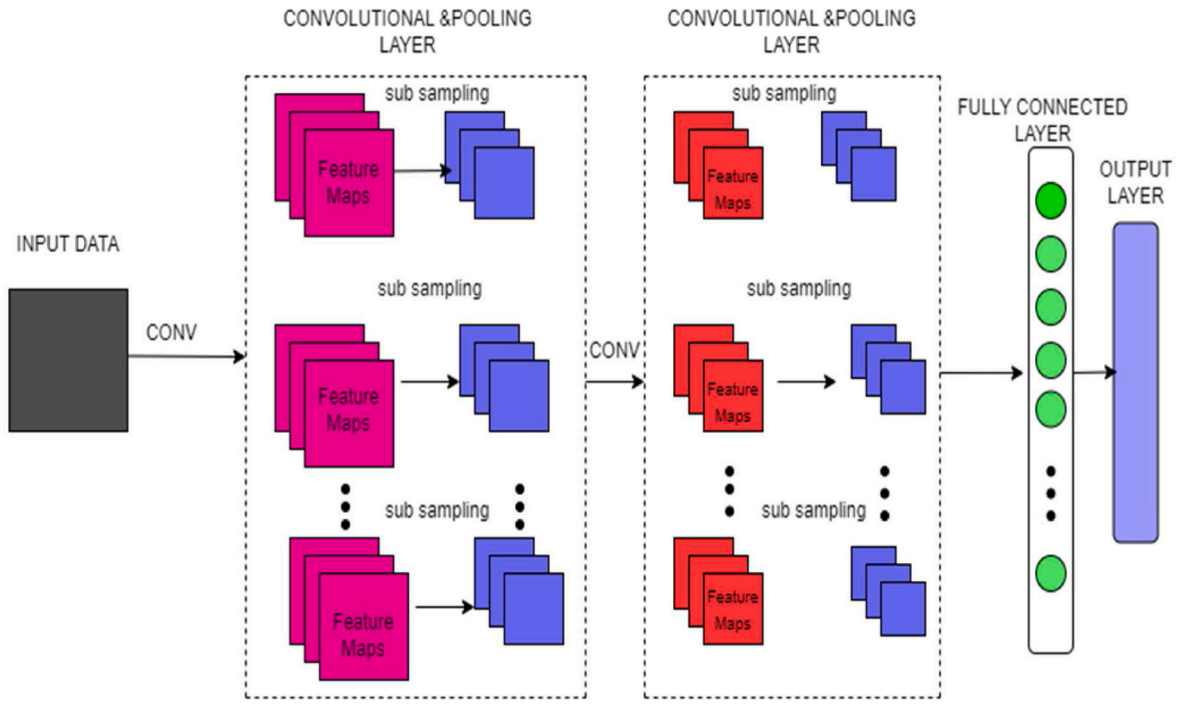


Fig. 4. Network architecture of convolutional neural networks.

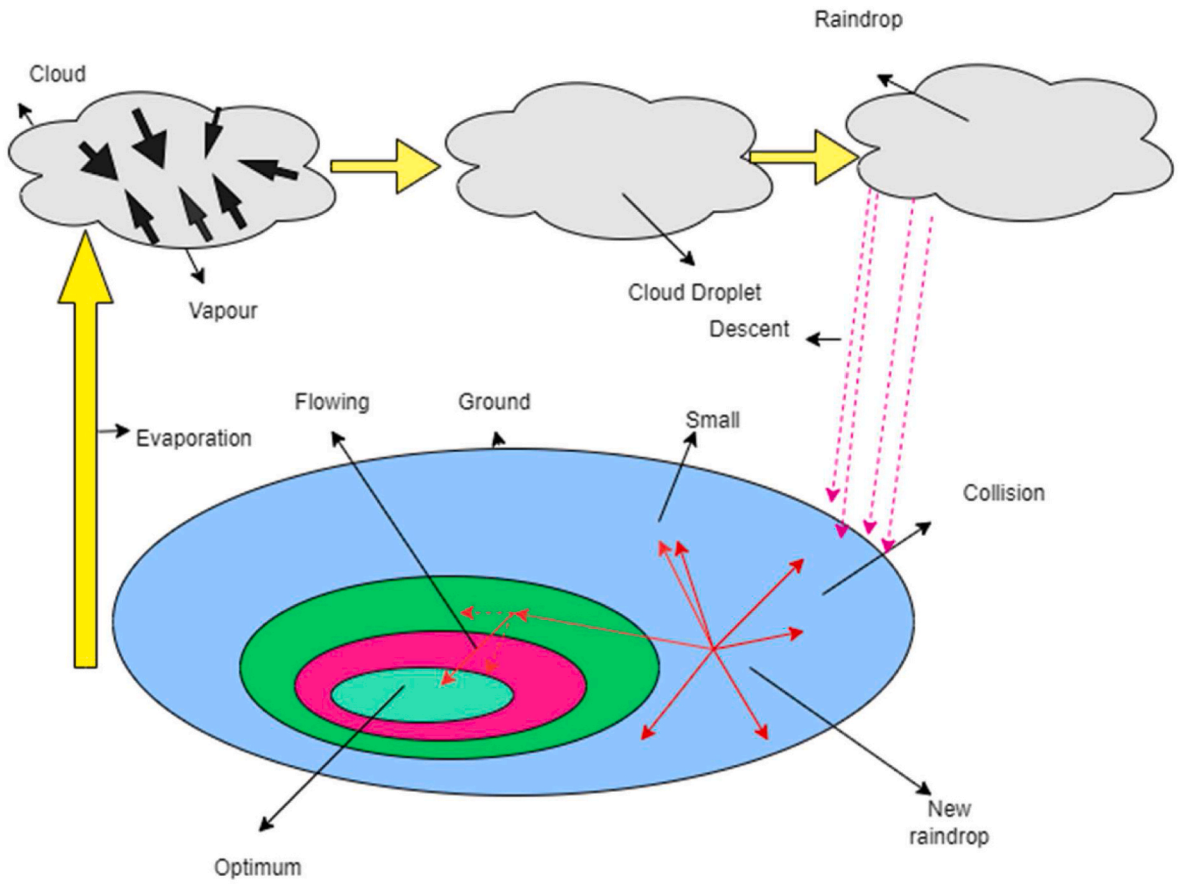


Fig. 5. Artificial Water Drop Optimisation Algorithm – its procedure.

water drop algorithm.

3.2.1. *Convolutional neural networks*

The Convolutional Neural Network (CNN) is an advanced iteration of the Multi-Layer Perceptron (MLP) that draws inspiration from biological systems. CNNs are extensively utilised in tasks such as image processing and video analysis. Fig. 4 illustrates the various layers utilised by CNNs for both feature extraction and classification. As pictured in Fig. 4, CNNs are supervised, feedforward networks consisting of multiple layers, including convolutional layers (CL), pooling layers (PL), and fully connected layers (FC). These layers are interconnected, facilitating a natural flow of information between them, wherein the output feature map of one layer serves as the input to the subsequent layer [29].

3.2.2. *Artificial water drop algorithm*

The Artificial Raindrop Algorithm (ARA) serves as a heuristic algorithm grounded in population dynamics. Emulating the natural rainfall process, it unfolds through five distinct stages: generation, descent, collision, raindrop flow, and vapour replacement. During the optimisation process, the positional data of water vapour or raindrops is evaluated based on altitude. The raindrop pool meticulously records locations at lower altitudes. A key advantage of employing ARA in the proposed network lies in its ability to reduce computational overhead, offer swift processing, and achieve faster convergence. Fig. 5 outlines the sequence of raindrop generation, where grey circles represent vapours and blue circles represent raindrops. In ARA, each vapour corresponds to a viable solution, and altitude serves as the fitness function, determining the fitness metric for both vapour and raindrop. The population consists of vapours and undergoes evolution through five operators, encompassing the primary raindrop operations. Table 2 presents the operators used in this optimisation algorithm. Algorithm-1 presents the pseudocode of the ARA optimisation methodology.

Algorithm-1. Input parameters include N, the population size; D, the dimensions of the optimisation problem; τ (tau), the step parameter for flowing; RP, the pool of raindrops; Max_Flow_Number, the maximum number of flows; and Max_FES, the maximum number of function evaluations. Ensure to cite any relevant references if available and correct as needed.

t=0;
Create an initial population: Pop (0) = {{Vapor}_1\left(0\right),\ {Vapor}_2\left(0\right),.., {Vapor}_N\left(0\right)} by selecting uniformly and randomly from the permissible solution domain
Evaluate the objective function values f $(Vapor_1(0)), f(Vapor_2(0)), \ldots, f\ (Vapor_N(0))$;
FES=N;
Find the best position best (0) of the initial population;
RP=gbest (0)
While FES≤Max_FES, **do**
$$Raindrop(t) = (\left(\frac{1}{N}\right)\sum_{i=1}^{N} Vapor_{i1}(t), \left(\frac{1}{N}\right)\sum_{i=1}^{N} Vapor_{i2}(t), \ldots\ldots, (1/N)\sum_{i=1}^{N} Vapor_{iD}(t));$$
Trail=Raindrop (t)
Randomly chosen indexes: $r_1, r_2, r_3, and\ r_4 \epsilon \{1,2, \ldots., D\}$;
$Trail_{i1} = Raindrop_{r2}(t) + \Phi * \left(Raindrop_{r3}(t) - Raindrop_{r4}(t)\right)$;
If f (Trail)<f(Raindrop (t))
New_Raindrop (t)= Trail;
Else
New_Raindrop (t) =Raindrop (t);
End if
FES=FES+2:
For j=1: N, do
Randomly chosen indexes: $k\epsilon\{, 2, \ldots, N\}$;
For $j = 1: D$,do
$c = \text{sign}\left(a_j - 0.5\right) * \log\left(\beta_j\right)$;
Small_Raindrop$_{ij}(t)$ =New_Raindrop$_j(t) + c *$ (New Raindrop$_j(t) -$ $Vapor_{kj}\ (t)$);
End for
FES=FES+1;
End for
For $i =; N,$ do
Flow_number=0;
While Flow_number≤Max_Flow_Number, **do**
$\lambda =$ round (rand)+1;
Choose $RP_{k1}\ and\ RP_{k2}(t)$ from RP by the tournament selection procedure;
$New\_small\_Raindrop_i(t)$= $Small\_Raindrop_i(t)$;+d(t,λ);
FES=FES+1;
$New\_small\_Raindrop_i(t) = Small\_Raindrop_i(t)$;+d(t,λ);
$Small\_Raindrop_i(t) = New\_small\_Raindrop_i(t)$;
Flow_number=Flow_number+1;
Else
Break;
End if
End while
End for
Update raindrop pool RP;
Update population Pop $(t + 1)$ = select (Pop(t)∪ Small_Raindrop(t));
$t = t + 1$;
End while
Output: The individual exhibiting the least value for the objective function among the population.

3.2.3. Nature inspired CNN model

Hyper Parameter Optimisation is the process of determining the best combination to tune the hyperparameters for obtaining the best performance in an adequate amount of time. This technique will also overcome the problem of overfitting, which maintains the stability of the model while training large datasets. This research article employs the artificial raindrop algorithm for model tuning to obtain the maximum performance from the network. The epochs, batch size, bias weights, momentum, hidden layers, and learning rate are called the hyperparameters, these are utilised for training the network. The initial selection of hyperparameters is randomly determined following the AWDO guidelines and subsequently utilised in training the NI–CNN network. The fitness function, as defined in equation (1), guides the optimisation process in AWDO. At each iteration, hyperparameters are computed using Algorithm 1. Iterations continue until the fitness function aligns with equation (1).

$$\textbf{\textit{Fitness Function}} > Max((1-A)+(1-P)+(1-R)) \quad (1)$$

For each cycle, the numerical values of hyperparameters are computed using the mathematical formulas outlined in Algorithm 1. These parameters are subsequently input into the network, where the fitness function is evaluated. If the fitness function matches the predefined threshold, the cycle halts; otherwise, it continues iterating. This approach results in AWDO exhibiting slower convergence compared to alternative meta-heuristic algorithms, which demonstrate faster optimisation and enhanced detection speed. Algorithm-2 provides the detailed pseudocode for this process for the proposed hyperparameter optimisation algorithm.

Algorithm-2. Pseudo-Code for the Hyper-parameter Optimisation using AWDO

1	**Input Population : Epochs, Batch size, Momentum, Learning rate, Layers**
2	**Outputs : Fitness Function**
3	While n= 1 to Max_iteration
4	Initialize the Input Populations using five operators as mentioned In **Algorithm-1**
5	Calculate the Output function from Proposed Framework using Eqn(14)
6	Determine the Fitness function using Eqn(20)
7	If fitness function == Eqn(20)
8	Assign the Best Global hyper parameters using Eqn(22)
9	Else
10	Go to step 3
11	End

3.2.4. Distributed NI–CNN model (federated NI–CNN)

As investigated in the existing research, federated learning is considered a decentralized machine learning approach with numerous clients, training a common global model by utilizing local data under the supervision of the central server or cloud. Unlike traditional centralised learning approaches, each node collaborates to educate a model using their confidential information and sends the update of the parameters to the central infrastructure (client or server). Next, the collected models are federated to create a universal model trained using the private data of participants. Federated Learning (FL) offers significant advantages, including enhanced accuracy, reduced latency, heightened privacy, and lower power consumption, by training a model on the private data of multiple participants, thus circumventing data-sharing issues. In this research, the proposed NI–CNN model is trained as a federated model in which the parameters are sent to the CH-IoT nodes. Algorithm-3 presents the procedure for the federated training for the proposed model.

Steps	Algorithm-3//Federated Learning for the Proposed Model
1	The Central infrastructure of CH-IoT sends a model to each user nodes of network.
2	Every Ch-IoT node conducts training on the model it receives using its individual private healthcare data.
3	Each CH-IoT transmit the model's parameters in a encrypted way (See the Encryption framework in Section-3.3)
4	The server in Ch-IoT systems combine the partial models by their parameters and construct the federated model.
5	The primary server evaluates a halting criterion condition by examining the fitness function defined by Equation (1). If the condition is met, the FL process concludes; otherwise, it recommences iteration from step 1.

3.3. Chaos based privacy preserving technique in proposed FL based NI–CNN model

As discussed in the previous section, the federated learning procedure ensures that sharing confidential information is not obligatory for training the federated model. But still, hazards are linked to the conveyance of such data is high and has adverse effects on the information. Therefore, chaotic preservation methods are used in Florida. In this research, chaotic algorithms are used to maintain privacy and encrypt the information from the CH-IoT nodes to the server. To construct the chaotic principles, hybrid Henon maps are used for the proposed framework. For the creation of high randomness and non-periodic sequences, this research article employs scroll maps, which work on the principle of multi-scroll attractors. The characteristics of the scroll maps used for the key generation are discussed in the preceding section.

3.4. Multi-scroll attractors

Dynamical systems with multiscroll attractors can state space equation for an automatic chaotic system that exhibits intricate dynamics surpassing those of general chaotic systems with mono-scroll attractors. Reformulating the equation using alternative language

$$: \dot{x}_1 = -ax_1 + bx_2x_3 \quad (2)$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (3)$$

$$\dot{x}_3 = ex_3 - fx_1x_2 \quad (4)$$

Top of equations (1)–(3) can be altered by integrating the hyperbolic equation $p_1\ tan\ h(x_2+g)$ which is given in eqn

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (5)$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (6)$$

$$\dot{x}_3 = ex_3 - fx_1x_2 + p_1\ tan\ h(x_2 + g) \quad (7)$$

Chaotic attractor is acquired when $a = 2, b = 6, c = 6, d = 3, e = 3, f = 1, p_1 = 1, g = 2$ and the predefined starting points are $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$.

When the hyperbolic function is initially incorporated with a parameter value of g = −3 in the first scenario, and given the commencement criterion [0.1,-0.1,-0.6], it exhibits a double scroll attractor as depicted in Fig. 1. Upon introducing it in the second scenario, with parameters p_1 = −1 and g = 3, and the same commencement criterion [0.1,-0.1,-0.6], it manifests a quadruple scroll, illustrated in Fig. 6. Transitioning to the third scenario with parameters p_1 = 1 and g = 3, alongside commencement criterion [0.1,0.1,0.6], it reveals a singular scroll as depicted in Fig. 6. Thus, we can ascertain the system's property of multiscroll behaviour (see Fig. 7).

To generate Multi-scroll 3D chaotic systems, equation (7) are adjusted using derivative properties outlined in Ref. [30]. The resulting chaotic system capable of showcasing multi-scroll characteristics is formulated as follows.(See.Fig. 8)

$$\frac{d^q x_1}{dt^q} = -ax_1 + bx_2x_3 \quad (8)$$

$$\frac{d^q x_2}{dt^q} = -cx_2^3 + dx_1x_3 \quad (9)$$

$$\frac{d^q x_3}{dt^q} = ex_3 - fx_1x_2 + p_1\ tan\ h(x_2 + g) \quad (10)$$

The bifurcation diagram for the proposed multi scroll integer order chaotic systems are shown in following Fig. 9.

3.4.1. Multi-scroll attractor – its advantages

The following are some benefits of the proposed scroll attractors used for encryption.

1. This System needs less memory to generate the same number of scroll as it takes the less component for generation [14].
2. To address overfitting and enhance generalisation, the paper employs the early stopping technique, as described in Ref. [31].
3. The random scroll can be generated by modifying any component of its any directions. This characteristic is much more different than the other chaotic systems.
4. Scroll maps are termed as the flexible maps in which the randomness doesn't depends in the scroll numbers, while that of other methods are closely related to the number of initial values.

3.5. Scroll based privacy preserving technique

Encryption with scroll maps is addition of security and privacy levels in the input parameter (Algorithm-4). In case of the encryption with scroll maps, diffusion operation is operated among every constituent of the input information and chaotic value generated by scroll maps. Diffusing the ith element of the plain data with the random value of scroll maps to form the strong encrypted data. Before encryption, all the scroll maps and data are scaled to common factor as 16(for reducing the complexity in the process). In the similar fashion, algorithm 5 involves a reversible operation, whereby the diffusion operation between the encrypted data and the identical encryption key (or parameter) results in the restoration of the input plain text data. The unique traits displayed by chaotic systems, such as determinism, ergodicity, and sensitivity to initial conditions, render them a compelling choice for building intelligent secured systems.

1	Input : Data Parameters (D)
2	Output : Encrypted Data (E)
3	Key generation Process using Scroll maps
4	Initial conditions selections
5	Generate the Scroll maps S
6	For i= 1 to n_iteration
7	E(i) = D(i) * S(i)
8	End
9	The output from the encryption process

Algorithm-5. Scroll based privacy Decryption Schemes

1	Input : Encrypted Data (E)
2	Output : Plain Data (P)
3	Key generation Process using Scroll maps
4	Initial conditions selections
5	Generate the Scroll maps S
6	For i= 1 to n_iteration
7	P(i) = E(i) * S(i)
8	End
9	The output from the decryption process

As mentioned in Algorithms 4 and 5, the encryption and decryption process involves the following phases: 1) Key generation process: The keys are generated by iterating over the different initial conditions of scroll maps. 2) A diffusion process is involved between the data and scroll keys to form the encrypted data. The main objective of the operation is to clear the non-linear connection between the initial and encoded information. Also in the encryption process, multiple iterations

Table 1
Summary of the different Works Suggested by the authors and its Pros and Cons.

Authors	Year of Publishing	Suggested Methodology	Pros	Cons
Chen et al. [20]	2023	Light weight Encryption Scheme for the IoT devices	Light weight suitable for IoT devices	High probability of in-secured data breaches
Nair.et al. [21]	2023	Ensures the privacy preserving models for the IoT devices	High end secured algorithms suitable for IoT devices	High Computational Overhead
Lu.et al. [22]	2023	Lightweight, privacy-preserving scheme with one-way hashing and other cryptographic mechanism	Strong encryption schemes	Computational overhead with less performance
Zhang.et al. [24]	2023	Privacy –Enhanced Momentum Federated learning framework	Decentralized training networks with the high end encryption scheme	Still needs for the improvisation in terms of security
Dharminder.et al. [25]	2022	Effective Privacy preserving Chebyshev chaotic encryption scheme	Proposed Chebyshev chaotic encryption technique for the IoT devices	Can be affected by more attacks
Ma.et al. [23]	2022	Multi-key Homomorhic encryption techniques for IoT devices	Light weight with the different layers of encryption	Less performance
Zhao.et al. [27]	2022	Federated learning Framework	Federated learning model for the unstructured data	Strong encryption algorithm is missing
Park et al. [26]	2021	Federated Learning model with the Homomorhic encryption technique	Decentralized training network	Suffers from the computational complexity

Table 2
Specific definition of the main raindrop operators.

Name	Detailed definition
Raindrop generation operator	$\varphi GR\ (Pop\ (t)) = \left(\sum Ni = 1 \frac{Vapor_{i1}(t)}{N}, \sum Ni = 1 \frac{Vapor_{i2}(t)}{N}, \ldots, \sum Ni = 1 \frac{Vapor_{i}(t)}{N}, \right.$
Raindrop descent operator	$\varphi DR\ (Raindrop\ (t) = Raindrop_{r2}\ (t) + \Phi * (Raindrop_{r3}\ (t) - Raindrop_{r4}\ (t)), k\varepsilon\{1,2,\ldots,N\}; \Phi\varepsilon(-1,1)$
Raindrop collision operator	$\varphi CR\ (New_{Raindrop}(t) \cup Pop\ (t))$
Raindrop flowing operator	$\varphi FR\ (Small_{Raindrop}(t)) = Small_{Raindrop_i}(t) + d(t,\lambda)$
Vapour replacement operator	$\varphi RV\ (Pop\ (t \cup Samll_{Raindrop}(t))$

are employed to update the scroll maps and keys, respectively. In every cycle, the key could be modified to introduce additional variability, thereby boosting the security of the encryption.4) The concluding encrypted result exhibits greater randomness and statistical autonomy from the initial data. 5) The process of decrypting involves applying the same chaotic map repeatedly to the encrypted data, utilizing identical starting criterion, parameters, and keys as in the encryption stage, in order to recover the initial plain text data.

3.6. Implementation methodology

As discussed, proposed encryption and decryption is applied to CH-IoT data which is considered as the encryption layers.

Steps	Algorithm-6//Chaotic Federated Learning for the Proposed Model
1	The Central infrastructure of CH-IoT sends a model to each user nodes of network.
2	Each Ch-IoT nodes trains the received model using their own private health care data.
3	Each CH-IoT sends the encrypted parameters of the model using the Algorithm-4
4	The server in Ch-IoT systems decrypts the data and aggregates the partial models through their parameters and builds the federated model.
5	The central server checks a halting criterion by checking the fitness function which is then given by Equation (.). If it is proficient, the FL process ends, otherwise it starts iterate from step 1.

4. Section-4

This section details the experimental approaches, results, and discussion, and finally concludes with a comprehensive assessment with the other state-of-the-art frameworks.

4.1. Experimental approaches

To generate and evaluate the results, experimental tests are conducted using TensorFlow 2.3.3, Keras 2.4.5, Python 3.10, Pandas 1.22, Numpy 1.20, Google Co-Lab with 16 GB RAM, and the NVIDIA Tesla T4. For implementing the federated learning model, the TensorFlow federated library Flower is utilised [31]. Nearly 1014 images are utilised for evaluation, in which 70 % of the total data was utilised for training, 20 % of the data was utilised for testing, and finally 10 % of the data was utilised for validation, respectively.

The experiments are conducted in the four-fold mechanism to demonstrate the efficiency of each module of the proposed framework. The elaborative analysis of the proposed model is depicted below.

4.2. Experiment-1

4.2.1. Model evaluation

Table 3 outlines the experimental configurations employed for training the novel network. Moreover, various performance metrics, including accuracy, precision, recall, specificity, and F1-score, are computed across different datasets. Additionally, AUC (area under ROC) is utilised to demonstrate the superiority of the proposed model. The mathematical formulations for measuring these performance metrics are provided in Table 3. Enhanced metrics in these metrics signify superior performances.

In the first experiment, different optimisation algorithms such as Ant Colony Optimisation (ACO), Spotted Hyena Optimisation (SHO), Genetic Algorithms (GA), Genetic Bee Colony Optimisation (GBO), Particle Swarm Optimisation (PSO), BAT Algorithm (BAT), Monkey Optimisation (MO), and Spider Optimisation Algorithm (SO) are integrated with the CNN to tune the hyper-parameters as similar to the proposed model. The execution of the proposed model is in contrast with the above-mentioned integrated models. Table 1 illustrates how the efficacy of various learning frameworks varies in their performance.

Table 4 illustrates the performance of the different nature-inspired CNN models in detecting lung cancer. From the table, it is very apparent that the proposed model has achieved the highest performance (accuracy of 0.9739, precision of 0.969, recall of 0.9589, and F1-score of 0.9695) and outperformed the other models. Table 5 depicts the execution of the federated learning models in the classification of lung cancers. It is found that the proposed federated model has attained similar performances, and error is very low between the federated and normal learning models. Hence, it is very apparent that the suggested

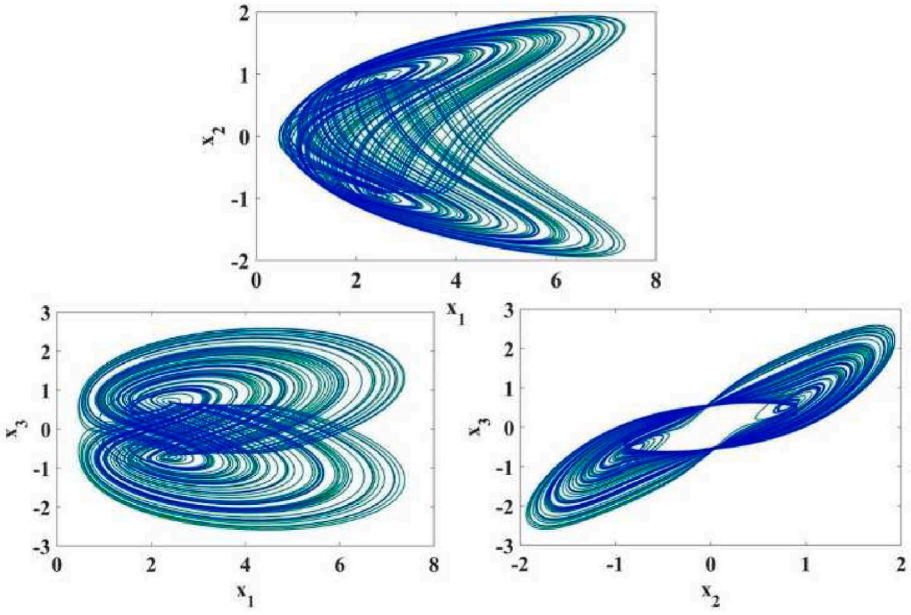


Fig. 6. Phase portraits of cubic nonlinear system with $p_1\ tan\,h(x_2+g)$ function in 1st state.

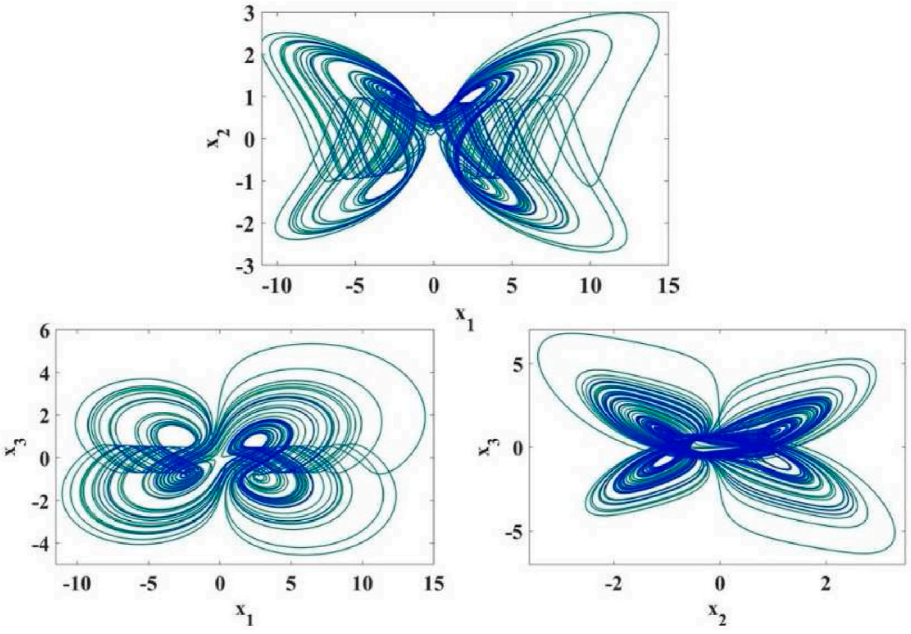


Fig. 7. Phase portraits of cubic nonlinear system with $p_1\ tan\,h(x_2+g)$ function in 2nd state.

federated model has achieved the best performance in identifying cancers. To validate the execution of the suggested federated learning model, ROC curves were plotted and analysed, as shown in Fig. 10.

With the picturization, it is apparent from the proposed federated model that the root mean square error (RMSE) between the training and validation sets is significantly low, measuring even less than 0.001. This experimentation underscores the superior performance of the distributed training model, which closely rivals that of the centralized training network.

4.3. Experiment-2

4.3.1. Statistical evaluation

This section covers the statistical performance of the different optimisation models and the proposed federated models, with their own advantages and disadvantages. The evaluation of classification results across various models is based on achieving the fitness function, delineated in terms of best, worst, mean, standard deviations and variance. Furthermore, the performance indicators from 50 trials are scrutinized

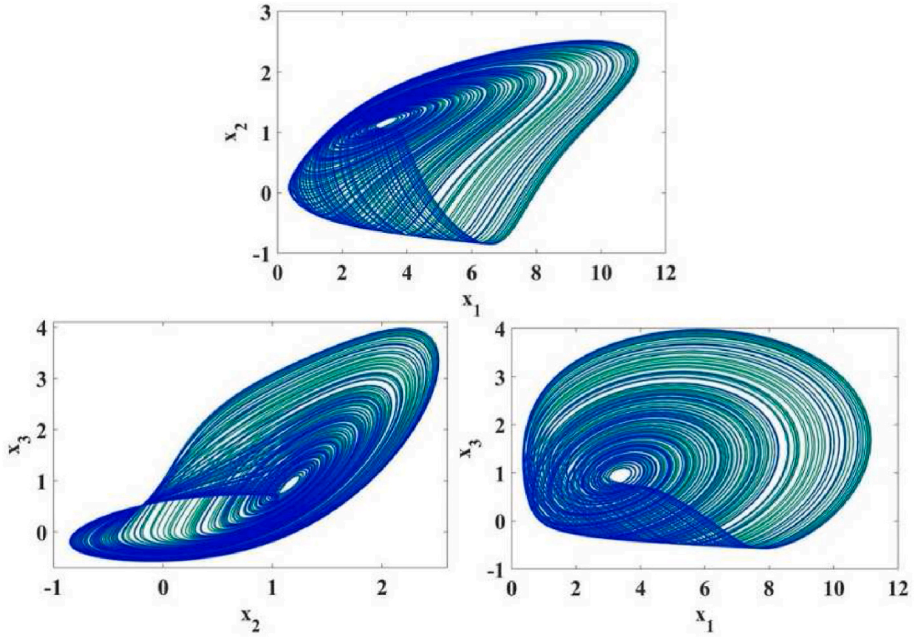


Fig. 8. Phase portraits of cubic nonlinear system with $p_1\ tan\ h(x_2+g)$ function in 3rd state.

for their consistency parameters. The classification results of diverse models alongside these specified metrics and their robustness indicators are presented in Tables 6 and 7, respectively.

Table 7 displays the results of various combinations of CNN networks. The data clearly indicates that the federated model proposed in this study outperformed other optimisation techniques. Fig. 11 illustrates the stability of this algorithm, showing that our proposed model achieved superior outcomes compared to existing models. If you have specific references or sources, please provide them for accurate citations.

4.4. Experiment −3

4.4.1. Model building time analysis

In this experiment, computational time is calculated in terms of model-building time (MBT). Model training times across various datasets are depicted in Fig. 12 concerning validation. Evaluating MBT is crucial due to the significant impact of computational time on model classification accuracy. This consideration directly affects resource utilization and model performance, highlighting the importance of MBT in achieving an optimal balance between computational load and classifier effectiveness. According to the data, the federated model requires only 20 % of the training time compared to traditional algorithms. This underscores the efficiency of the proposed decentralized model, which is particularly advantageous for resource-constrained CH-IoT devices.

4.5. Experiment −4

4.5.1. Security analysis

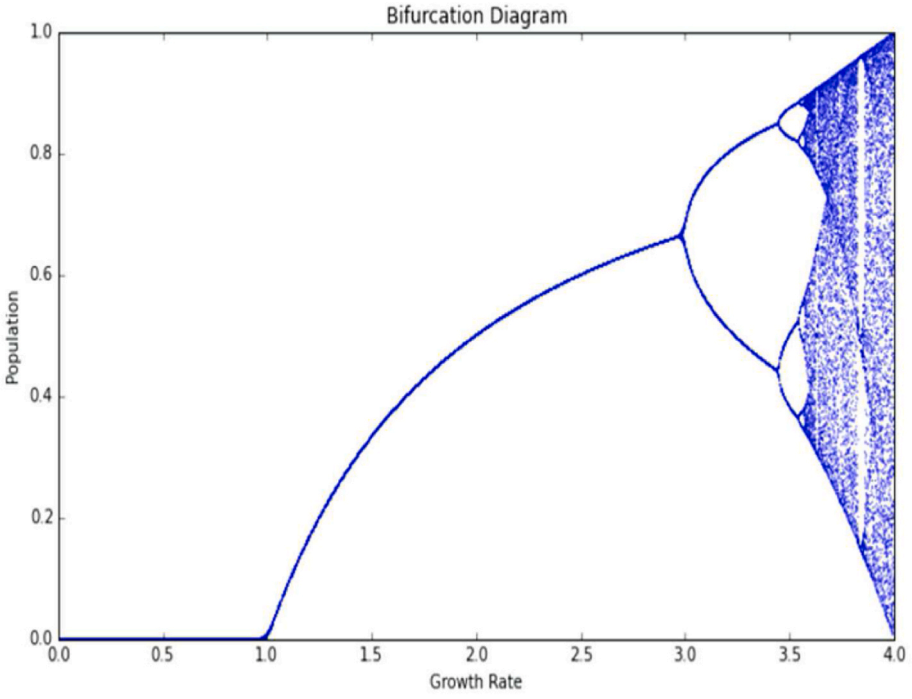
In this experiment, the security strength of encrypted bits is tested and evaluated. National Institute of Standards and Technology (NIST) tests are conducted to prove the randomness of the encrypted bits that can be used for the transmission of private models to the central servers. The 12 mandatory tests of NIST were conducted, and experimental outcomes are demonstrated in tabular form.

In Table 8, it is evident that the encrypted bits exhibit high randomness, which can make it harder for an intruder to modify the medical data during transmission.

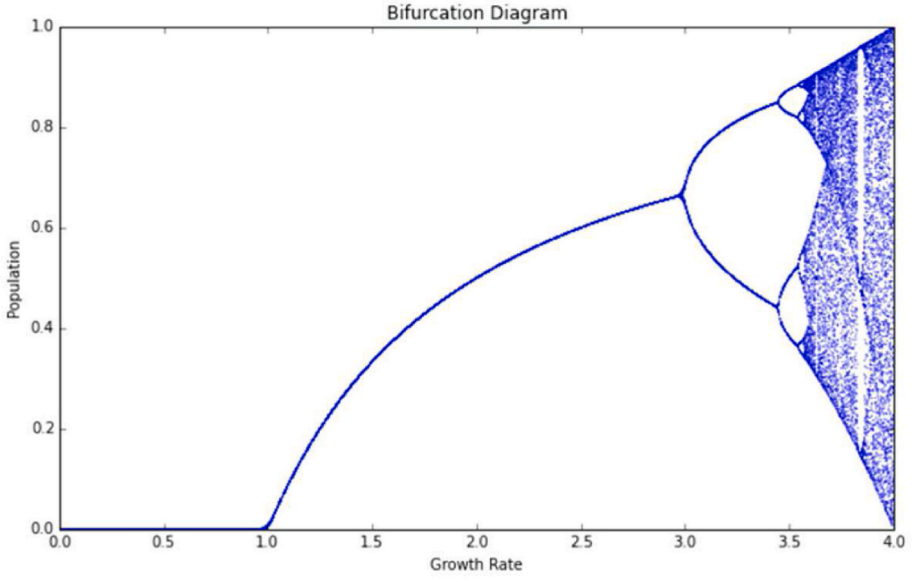
5. Section-5

5.1. Conclusion and future scope

In this research article, a proposed protocol has been presented for smart health care systems using CH-IoT devices. The nature-inspired CNN, which works on the principle of the artificial water drop algorithm, was proposed for an effective diagnosis of the medical image datasets. Later, optimised models are converted from traditional training into federated distributed networks for effective computation consumption and higher performance. Finally, the scroll chaotic maps are used for encrypting and decrypting the local models, thereby converting the distributed model into a privacy-preserving framework that can mitigate multiple attacks. The thorough testing has been computed using TCIA lung datasets, and various performance metrics were measured and analysed. In the first experiment, metrics such as accuracy, precision, recall, and f1-score were calculated for the proposed federated models and other existing state-of-the-art optimised CNN models. The performance of the proposed model has outperformed the other models in producing the highest accuracy of 0.97, 0.96 precision, 0.96 recall, and 0.965 F1-score, respectively. In the second phase, various statistical tests were conducted for the different models, and the federated model exhibited more stability than the other algorithms. The computation time was analysed, and the distributed model exhibited less time than the other models, thereby making it suitable for CH-IoT



(a)



(b)

Fig. 9. Fractional bifurcation diagrams for the proposed multi scroll chaotic systems.

Table 3
Mathematical expressions for the performance metrics' calculation.

SL.NO	Performance Metrics	Mathematical Expression
01	Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
02	Recall	$\frac{\mathrm{TP}}{\mathrm{T\,P+FN}}$ x100
03	Specificity	$\frac{TN}{TN+FP}$
04	Precision	$\frac{TN}{TP+FP}$
05	F1-Score	$2.\frac{Precison*Recall}{Precision+Recall}$

devices. Finally, the privacy of the model is proven by conducting NIST standard tests. In all experiments, the proposed distributed learning models have shown superior performances to the other frameworks and find a strong place in CH-IoT systems.

In the future, light-weight operations will need to be incorporated for different Edge/Fog gateway devices to optimise system effectiveness, encompassing computational, communicative, and securely stored data. Furthermore, complete models need to be improvised for handling real-time datasets.

Table 4
Performance Analysis of the Nature-Inspired CNN model in detecting the lung cancers.

Algorithm	Performance metrics				
	Accuracy	Precision	Recall	Specificity	F1-Score
CNN	0.73	0.71	0.703	0.698	0.702
CNN + PSO	0.76	0.72	0.712	0.690	0.713
CNN + ACO	0.765	0.753	0.743	0.722	0.754
CNN + GA	0.774	0.763	0.755	0.732	0.758
CNN + SHO	0.802	0.80	0.792	0.782	0.797
CNN + GBO	0.812	0.80	0.783	0.782	0.80
CNN + BAT	0.85	0.84	0.821	0.802	0.832
CNN + MO	0.873	0.862	0.832	0.820	0.843
CNN + SO	0.890	0.882	0.863	0.854	0.875
Proposed Model	0.974	0.968	0.960	0.972	0.969

Table 5
Performance Analysis of the Nature-Inspired CNN model (federated learning) in detecting the lung cancers.

Algorithm	Performance metrics				
	Accuracy	Precision	Recall	Specificity	F1-Score
CNN	0.729	0.702	0.700	0.6984	0.701
CNN + PSO	0.753	0.733	0.710	0.689	0.720
CNN + ACO	0.743	0.721	0.739	0.720	0.710
CNN + GA	0.78	0.754	0.750	0.727	0.750
CNN + SHO	0.80	0.793	0.782	0.771	0.790
CNN + GBO	0.81	0.799	0.781	0.775	0.784
CNN + BAT	0.843	0.832	0.820	0.79	0.812
CNN + MO	0.863	0.845	0.8292	0.81	0.834
CNN + SO	0.885	0.883	0.855	0.843	0.873
Proposed Model	0.9739	0.969	0.9589	0.971	0.9695

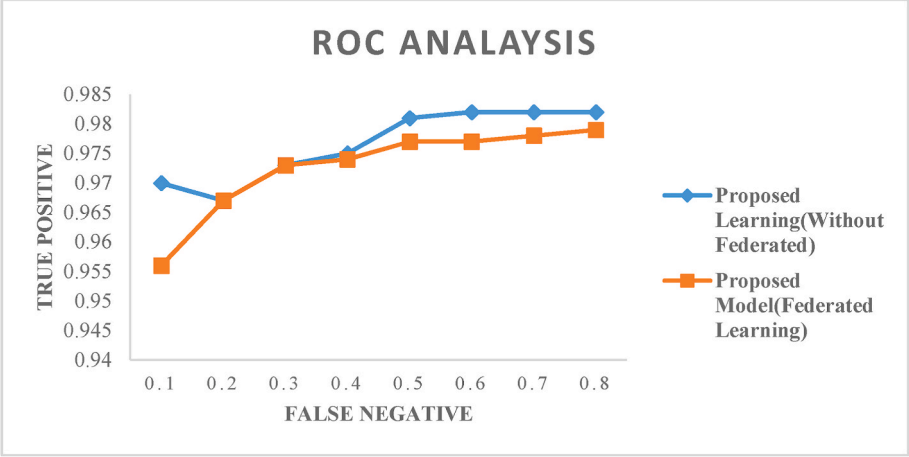


Fig. 10. ROC assessment of the Proposed Model (with Federated & Without Federated learning model).

Table 6
Fitness Function based Outcomes for the different combinations of CNN.

Algorithm	Best	Worst	Mean	Median	SD	Variance
CNN	0.73	0.6453	0.722	0.02892	0.06734	6.3×10^{-6}
CNN + PSO	0.76	0.6202	0.68	0.01903	0.07032	8.2×10^{-6}
CNN + ACO	0.765	0.6102	0.673	0.02390	0.06932	4.0×10^{-5}
CNN + GA	0.774	0.6044	0.6425	0.023450	0.052029	3.20×10^{-4}
CNN + SHO	0.802	0.743	0.7542	0.039403	0.054389	2.89×10^{-4}
CNN + GBO	0.812	0.733	0.7522	0.043930	0.046373	2.043×10^{-4}
CNN + BAT	0.85	0.8023	0.825	0.0567839	0.067340	2.002×10^{-4}
CNN + MO	0.873	**0.834**	**0.73**	**0.07203**	**0.067350**	**1.9045×10^{-4}**
CNN + SO	0.890	**0.874**	**0.7363**	**0.078455**	**0.045360**	**1.890×10^{-4}**
Proposed federated Model(With Nature Inspired Optimzation)	0.975	**0.864**	**0.902**	**0.08932**	**0.07563**	**1.2892×10^{-4}**

Table 7
Indicator Outcome Analysis for the different combinations of CNN.

Algorithm	Best	Worst	Mean	Median	SD	Variance
CNN	0.73	0.6453	0.722	0.02892	0.06734	6.3×10^{-6}
CNN + PSO	0.76	0.6202	0.68	0.01903	0.07032	8.2×10^{-6}
CNN + ACO	0.765	0.6102	0.673	0.02390	0.06932	4.0×10^{-5}
CNN + GA	0.774	0.6044	0.6425	0.023450	0.052029	3.20×10^{-4}
CNN + SHO	0.802	0.743	0.7542	0.039403	0.054389	2.89×10^{-4}
CNN + GBO	0.812	0.733	0.7522	0.043930	0.046373	2.043×10^{-4}
CNN + BAT	0.85	0.8023	0.825	0.0567839	0.067340	2.002×10^{-4}
CNN + MO	0.873	**0.834**	**0.73**	**0.07203**	**0.067350**	**1.9045×10^{-4}**
CNN + SO	0.890	**0.874**	**0.7363**	**0.078455**	**0.045360**	**1.890×10^{-4}**
Proposed federated Model(With Nature Inspired Optimzation)	0.975	**0.864**	**0.902**	**0.08932**	**0.07563**	**1.2892×10^{-4}**

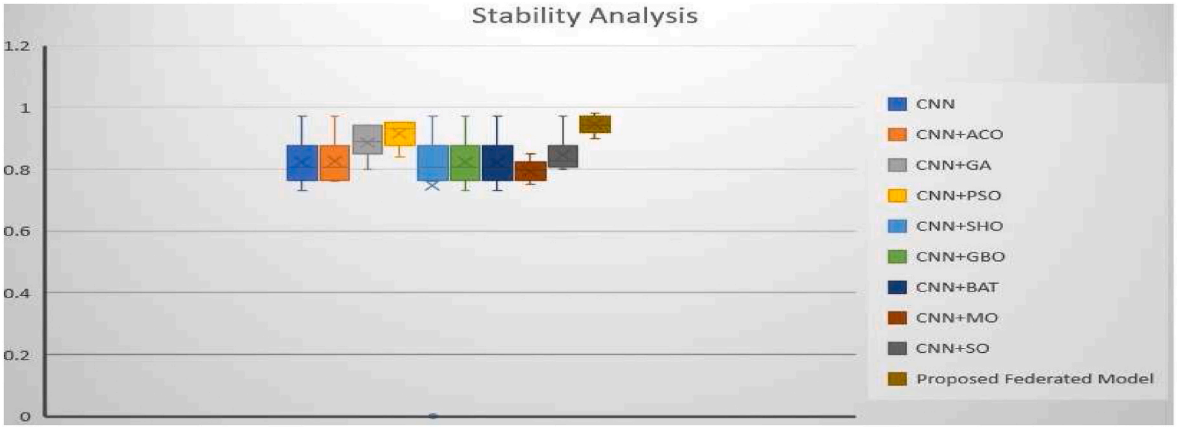


Fig. 11. Stability Analysis for the Different Models for used for Evaluation Process.

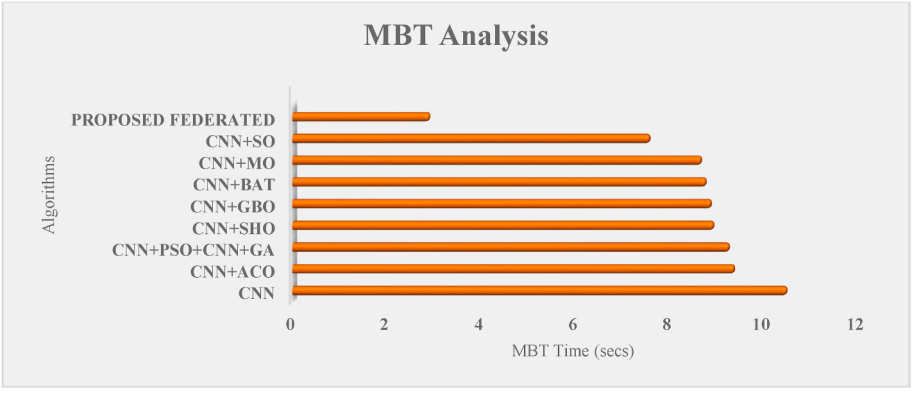


Fig. 12. Mbt analysis for the different algorithms and federated learning models.

Table 8
NIST standard test performance of the proposed algorithm.

Sl.No	NIST Test Specification	Status of test
1	DFT Test	PASS
2	RunTest	PASS
3	Long Run Test	PASS
4	Frequency Test	PASS
5	Block Frequency Test	PASS
6	Frequency MonoTest	PASS
7	Overlapping Template of all One's test	PASS
8	Linear Complexity Test	PASS
9	Matrix Rank Test	PASS
10	Lempel-ZIV Compression Test	PASS
11	Random Excursion Test	PASS
12	Universal Statistical Test	PASS

Ethical approval

This article does not involve any studies with human participants or animals conducted by any of the authors.

Informed consent

Informed consent was obtained from all individual participants included in the study.

Data availability

The data can be made available by contacting the corresponding authors upon reasonable request.

Funding

Not applicable.

CRediT authorship contribution statement

Shaik Abdul Nabi: Conceptualization. **Ponugoti Kalpana:** Conceptualization. **N. Subhash Chandra:** Conceptualization. **L. Smitha:** Conceptualization. **K. Naresh:** Conceptualization. **Absalom E. Ezugwu:** Conceptualization. **Laith Abualigah:** Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

Not applicable.

References

[1] Mavrogiorgou Argyro, et al. FAME: federated decentralized trusted data marketplace for embedded finance. In: 2023 international conference on smart applications, communications and networking (SmartNets). IEEE; 2023. https://doi.org/10.1109/SmartNets58706.2023.10215814.
[2] García Santaclara Pablo, Fernandez Vilas Ana, Redondo Rebeca P Díaz. Prototype of deployment of federated learning with iot devices. In: Proceedings of the 19th ACM international symposium on performance evaluation of wireless ad hoc, sensor, & ubiquitous networks; 2022. p. 9–16. https://doi.org/10.1145/3551663.3558681.
[3] Kumar Mohit, et al. A smart privacy preserving framework for industrial IoT using hybrid meta-heuristic algorithm. Sci Rep 2023;13(1):5372. https://doi.org/10.1038/s41598-023-32098-2.
[4] Iwendi Celestine, et al. N-sanitization: a semantic privacy-preserving framework for unstructured medical datasets. Comput Commun 2020;161:160–71. https://doi.org/10.1016/j.comcom.2020.07.032.
[5] Zhang Tuo, Gao Lei, He Chaoyang, Zhang Mi, Krishnamachari Bhaskar, Salman Avestimehr A. Federated learning for the internet of things: applications, challenges, and opportunities. IEEE Internet of Things Magazine 2022;5(1):24–9. https://doi.org/10.1109/IOTM.004.2100182.
[6] Tahir Mehreen, Ali Muhammad Intizar. On the performance of federated learning algorithms for iot. IoT 2022;3(2):273–84. https://doi.org/10.3390/iot3020016.
[7] Yaacoub Jean-Paul A, Noura Hassan N, Salman Ola, Ali Chehab. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. Int J Inf Secur 2022;21(1):115–58. https://doi.org/10.1007/s10207-021-00545-8.
[8] Jean-Paul Yaacoub, Hassan Noura, Salman Ola, Ali Chehab. Security analysis of drones systems: attacks, limitations, and recommendations. Internet of Things 2020;11(2542–6605):100218. https://doi.org/10.1016/j.iot.2020.100218.
[9] Jiang Yupeng. Sybil attacks on differential privacy based federated learning. Macquarie University; 2022. PhD Thesis.
[10] Nguyen Thien Duc, Rieger Phillip, De Viti Roberta, Chen Huili, Brandenburg Bjorn Є B, Yalame Hossein, Mollering Helen, Fereidooni Hossein, Marchal Є Samuel, Miettinen Markus, et al. FLAME: taming backdoors in federated learning. In: 31st USENIX security symposium, vol. 22; 2022. p. 1415–32. https://doi.org/10.48550/arXiv.2101.02281. USENIX Security.
[11] Manna Arpan, Kasyap Harsh, Tripathy Somanath. Moat: model agnostic defense against targeted poisoning attacks in federated learning. In: Information and communications security: 23rd international conference, ICICS 2021, chongqing, China; 2021. p. 38–55. https://doi.org/10.1007/978-3-030-86890-1_3. Part I.
[12] Moharram Jebreel Najeeb, Domingo-Ferrer Josep, Sanchez David, BlancoJusticia Alberto. Defending against the label-flipping attack in federated learning. arXiv preprint arXiv:2207.01982, https://doi.org/10.48550/arXiv.2207.01982; 2022.
[13] Andreina Sebastien, Marson Giorgia Azzurra, Mollering Helen, Karame Ghassan. Baffle: backdoor detection via feedback-based federated learning. In: IEEE 41st international conference on distributed computing systems (ICDCS). IEEE; 2021. p. 852–63. https://doi.org/10.1109/ICDCS51616.2021.00086.
[14] Ehui BrouBernard, Han Yiran, Guo Hua, Liu Jianwei. A lightweight mutual authentication protocol for IoT. Journal of Communications and Information Networks 2022;7(2):181–91. https://doi.org/10.23919/JCIN.2022.9815201.
[15] Nguyen Dinh C, Ding Ming, Pathirana Pubudu N, Seneviratne Aruna, Jun Li H. Vincent Poor. Federated learning for internet of things: a comprehensive survey. IEEE Communications Surveys & Tutorials 2021;23(3):1622–58. https://doi.org/10.1109/COMST.2021.3075439.
[16] Li Dongcheng, Wong W Eric, Wang Wei, Yao Yao, Chau Matthew. Detection and mitigation of label-flipping attacks in federated learning systems with kpca and kmeans. In: 2021 8th international conference on dependable systems and their applications (DSA). IEEE; 2021. p. 551–9. https://doi.org/10.1109/DSA52907.2021.00081.
[17] Vale Tolpegin, Truex Stacey, Emre Gursoy Mehmet, Liu Ling. Data poisoning attacks against federated learning systems. In: European symposium on research in computer security. Springer; 2020. p. 480–501. https://doi.org/10.1007/978-3-030-58951-6_24.
[18] Chen CM, Liu Shuangshuang. Improved secure and lightweight authentication scheme for next-generation IoT infrastructure. Secur Commun Network 2021;(5):1–13. https://doi.org/10.1155/2021/6537678.
[19] Chen CM, Liu Shuangshuang. Improved secure and lightweight authentication scheme for next-generation IoT infrastructure. Secur Commun Network 2021;(5):1–13. https://doi.org/10.1155/2021/6537678.
[20] Chen CM, Liu S, Li X, Islam SH, Das AK. A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT. J Syst Architect 2023;136. https://doi.org/10.1016/j.sysarc.2023.102831.
[21] Nair AK, Sahoo J, Raj ED. Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. Comput Stand Interfac 2023;86. https://doi.org/10.1016/j.csi.2023.103720.
[22] Gupta DS, Mazumdar N, Nag A, Singh JP. Secure data authentication and access control protocol for industrial healthcare system. J Ambient Intell Hum Comput 2023;14(5):4853–64. https://doi.org/10.1007/s12652-022-04370-2.
[23] Wang Chen, Wu Xinkui, Liu Gaoyang, Deng Tianping, Peng Kai, Wan Shaohua. Safeguarding cross-silo federated learning with local differential privacy. Digital Communications and Network 2022;8(4):446–54. https://doi.org/10.1016/j.dcan.2021.11.006.
[24] Zhang Zehui, Zhang Linlin, Li Qingdan, Wang Kunshu, He Ningxin, Gao Tiegang. Privacy-enhanced momentum federated learning via differential privacy and chaotic system in industrial cyber–physical systems. ISA Trans 2022;128(A):7–31. https://doi.org/10.1016/j.isatra.2021.09.007.
[25] Dharminder D, Kumar U, Gupta P. A construction of a conformal Chebyshev chaotic map-based authentication protocol for healthcare telemedicine services. Complex Intell. Syst 2021;7(5):2531–42. https://doi.org/10.1007/s40747-021-00441-7.
[26] Kang Wei, Jun Li, Ding Ming, Ma Chuan, Yang Howard H, Farhad Farokhi, Shi Jin, Tony QS, Quek H. Vincent Poor. Federated learning with differential privacy: algorithms and performance analysis. IEEE Trans Inf Forensics Secur 2020;15:3454–69. https://doi.org/10.1109/TIFS.2020.2988575.
[27] Yu H, Zhou Z, Wang Q. Deep learning assisted predict of lung cancer on computed tomography images using the adaptive hierarchical heuristic mathematical model. IEEE Access 2020;8:86400–10. https://doi.org/10.1109/ACCESS.2020.2992645.
[28] Asuntha A, Srinivasan A. Deep learning for lung Cancer detection and classification. Multimed Tool Appl 2020;79:7731–62. https://doi.org/10.1007/s11042-019-08394-3.

[29] Cengïl E, Cinar A. A deep learning based approach to lung cancer identification. In: 2018 international conference on artificial intelligence and data processing (IDAP); 2018. p. 1–5. https://doi.org/10.1109/IDAP.2018.8620723.
[30] Zargar S, Ali Shahidinejad, Ghobaei-Arani Mostafa. A lightweight authentication protocol for IoT-based cloud environment. Int J Commun Syst 2021:1–17. https://doi.org/10.1002/dac.4849.
[31] Zargar S, Ali Shahidinejad, Ghobaei-Arani Mostafa. A lightweight authentication protocol for IoT-based cloud environment. Int J Commun Syst 2021. https://doi.org/10.1002/dac.4849.