Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.063242

ARTICLE

Enhancing Healthcare Data Privacy in Cloud IoT Networks Using Anomaly Detection and Optimization with Explainable AI (ExAI)

Jitendra Kumar Samriya[1], Virendra Singh[2], Gourav Bathla[3], Meena Malik[4], Varsha Arya[5,6], Wadee Alhalabi[7] and Brij B. Gupta[8,9,10,11,*]

[1]Department of CSE, Indian Institute of Information Technology, Sonepat, 131001, Haryana, India
[2]Department of Computer Application, Integral University, Lucknow, 226026, Uttar Pradesh, India
[3]Department of Computer Science and Engineering, GLA University, Mathura, 281406, Uttar Pradesh, India
[4]Department of Computer Science Engineering, Chandigarh University, Mohali, 140143, Punjab, India
[5]Department of Electronic Engineering and Computer Science, Hong Kong Metropolitan University, Hong Kong SAR, 999077, China
[6]Center for Interdisciplinary Research, University of Petroleum and Energy Studies (UPES), Dehradun, 248007, Uttarakhand, India
[7]Immersive Virtual Reality Research Group, Department of Computer Science, King Abdulaziz University, Jeddah, 22254, Saudi Arabia
[8]Department of Computer Science and Information Engineering, Asia University, Taichung, 41354, Taiwan
[9]Symbiosis Centre for Information Technology (SCIT), Symbiosis International University, Pune, 412115, Maharashtra, India
[10]School of Cybersecurity, Korea University, Seoul, 02841, Repbulic of Korea
[11]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, 404327, Taiwan

*Corresponding Author: Brij B. Gupta. Email: bbgupta@asia.edu.tw

Received: 09 January 2025; Accepted: 29 May 2025; Published: 03 July 2025

ABSTRACT: The integration of the Internet of Things (IoT) into healthcare systems improves patient care, boosts operational efficiency, and contributes to cost-effective healthcare delivery. However, overcoming several associated challenges, such as data security, interoperability, and ethical concerns, is crucial to realizing the full potential of IoT in healthcare. Real-time anomaly detection plays a key role in protecting patient data and maintaining device integrity amidst the additional security risks posed by interconnected systems. In this context, this paper presents a novel method for healthcare data privacy analysis. The technique is based on the identification of anomalies in cloud-based Internet of Things (IoT) networks, and it is optimized using explainable artificial intelligence. For anomaly detection, the Radial Boltzmann Gaussian Temporal Fuzzy Network (RBGTFN) is used in the process of doing information privacy analysis for healthcare data. Remora Colony Swarm Optimization is then used to carry out the optimization of the network. The performance of the model in identifying anomalies across a variety of healthcare data is evaluated by an experimental study. This evaluation suggested that the model measures the accuracy, precision, latency, Quality of Service (QoS), and scalability of the model. A remarkable 95% precision, 93% latency, 89% quality of service, 98% detection accuracy, and 96% scalability were obtained by the suggested model, as shown by the subsequent findings.

KEYWORDS: Healthcare; data privacy analysis; anomaly detection; cloud IoT network; explainable artificial intelligence; temporal fuzzy network

1 Introduction

Nowadays, the healthcare industry has shifted from a hospital-centric model to a patient-centric approach, to empower individuals to control their health decisions for better management. Trending features in cloud and edge networks along with advancements in AI, IoT, and big data, derive and facilitate this

transformation. Precisely, digital health are equipped with smart sensors that can produce better business insights with the help of real-time predictive models. Healthcare 4.0 focuses on a patient-centric approach leveraging a sensor-based technology to provide continuous health monitoring to collect real-time data followed by analysis using advanced tools. This empowers healthcare providers to offer more personalized care, making informed decisions through precise and current insights into the patient's health status.

While this industry has aligned patient care activities with the Healthcare 4.0 vision, it is developing new standards [1]. Healthcare 5.0 integrates intelligent control systems, augmented and virtual reality with various identifiable healthcare analytics and 3-D view models. Therefore, personalized analytics and comprehensive healthcare would drive ingenious business proposals in the medical domain. Medical science technology anticipates that millions of Internet of Things (IoT)-based sensors will be networked and interact over fifth-generation (5G) network infrastructure to enable digital wellness, smart healthcare, enhanced healthcare metrics in the context of Healthcare 5.0. Intelligent wearables are connected with mobile communication as well as medical methods for convenient and inaccessible healthcare deliverance in a scenario made possible by 5G, IoT, and AI [2]. Major methods such as IoT from the foundation for a number of emerging applications in the fields of smart manufacturing, transportation systems, and health care. IoT uses various sensors to collect data about people, things, and the environment. This data is regularly sent to the cloud server, enabling application managers to take a variety of actions aimed at enhancing application performance. Based on the gathered data, AI approaches can also be used to operate the apps. One of the main uses of IoT is in healthcare, where patients wear devices to collect vital signs data [3,4]. Body measurements like blood pressure, sugar level, heart rate, oxygen saturation, and so on are examples of this type of data. These crucial measurements cannot be continuously collected and delivered to the cloud for processing without the use of IoT. Consequently, IoT-enabled health care is a significant use case that has a profound effect on people's lives. Healthcare predictive modeling can be intricate, counterintuitive, and frequently difficult to understand. Artificial intelligence can now function swiftly and well and is widely utilized in various fields. The influence of machine learning algorithms' evolving processes and optimization to tackle a variety of issues in the healthcare industry, that enables AI usage in medical imaging as a central domain for research attention transforms diagnostic procedures, for more accurate disease detection like cancer, neurological disorders, and cardiovascular diseases [5]. Nevertheless, deep learning algorithm-based AI lacks transparency, leaving doctors confused about the symptoms of a diagnosis. So, how to present strong proof of the answers is a crucial query. However, a gap still exists between AI models and human understanding termed "black-box" transparency. Significant research is ongoing to improve clinical reliance on the use of AI models. For instance, in 2015, the US Defence Advanced Research Projects Agency (DARPA) created the explainable AI (ExAI) concept. Subsequently, in 2021, a trust AI project demonstrated that the ExAI may be applied to interdisciplinary application challenges in computer science, psychology, and statistics and may offer answers that boost users' trust [6]. A robust scheme is essential to improvise predictive methods for explainability in the healthcare domains that may result in advanced patient care. In certain therapeutic settings, such as radiology, AI cna facilitate doctors in optimal choice and may better overtake human intelligence. By collaborating with healthcare professionals to develop relevant clinical questions, advanced AI algorithms can reveal clinically important information hidden within large volumes of healthcare data. AI applications are trained to predict particular results for a set of characteristics. This method helps to gain deep insights to get significant attention to recent advances in deep learning. In DL, NN with multiple hidden layers examines higher convoluted patterns to improve prognostic accuracy.

Several challenges may arise while interpreting the prediction outcomes and a functional explanation of artificial intelligence applications. It is challenging to monitor Deep Learning due to the lack of transparency in the decision-making stage and frequently described as an opaque model [7,8].

This work provides the following significant contributions:

To suggest a unique technique for identifying anomalies in cloud IoT networks utilize explainable artificial intelligence and integrate privacy analysis of healthcare data. Here, the radial Boltzmann Gaussian temporal fuzzy network was used for anomaly detection in the healthcare data privacy invextigation. Next, remora colony swarm optimization was used to assess network optimization.

2 Literature Review

Numerous medical diseases and applications use predictive modeling using sophisticated AI and ML techniques. To optimize long-term outcomes for the patients with type 1 diabetes, work [9] suggested using reinforcement learning to learn and suggest a sequential course of treatment that includes insulin and oral antidiabetic medications. Author [10] suggested modeling the intricate relationships between diseases using high-order networks. The suggested approach is utilized to replicate disease trajectories as well as forecast disease states in type 2 diabetes. It outperforms first-order network, according to the results. Rathee et al. [11] present a Zero Trust Blockchain Architecture designed for decentralized e-health Cyber-Physical Systems (CPS) to enhance security, storage, and real-time patient monitoring. A dilated recurrent neural network (DRNN) was proposed in study [12] to predict type 1 diabetes patients' future blood glucose levels. To identify diabetic retinopathy from retinal fundus images, work [13] built DL algorithms and discovered that they achieved great sensitivity and specificity. Using an annotation tool, a panel of ophthalmologists rated the photographs. Yaqoob et al. [14] looked at the safety concerns related to treating sepsis and used the deep reinforcement learning approach to find the best course of action. To determine the optimal reward functions out of a set of seemingly optimal treatment trajectories, the work proposed in [15] provides a Mini-Tree (DIRL-MT) method using deep inverse reinforcement learning. The simultaneity of organ dysfunction was identified by the author [16] using a network-based model, which helps forecasting sepsis as well as the survival of those who experience it. A common metric for assessing the effectiveness of health services is the hospital readmission rate. Enhancing communication and care coordination is the aim of the Hospital Readmissions Reduction Program (HRRP) to lower preventable readmission rates. To predict the hospital readmission of diabetic patients, work [17] presented a deep learning model that combines deep forest and wavelet transform. Wei et al. [18] introduce SM-UNet, a deep learning model designed for real-time medical image segmentation by integrating CNN and MLP architectures. A generalized taxonomy of ExAI is presented by the authors in [19] based on present issues and potential future developments. The suggested taxonomy combines the examined taxonomies, ExAI database methods, and decision tree methods to determine which taxonomy is most appropriate for the intended uses. A cloud-based, DL multi-modal method for ECG pattern detection using a 6G communication network is proposed by authors in [20]. Authors in [21] suggest an intrusion detection technique based on Sequential Online ELM. ELM is a NN with strong generalisability and high training speed. An advancement of ELM networks, known as OS-ELM, was created expressly to handle cloud services, incorporating multi-category detection into the process. Sadly, this makes it more difficult to detect attacks such as privilege escalation and probing. Convolutional neural networks (CNNs) were first designed to classify images; however, reference [22] proposed employing CNNs as an in-router multi-category network attack classifier. The approach was validated using public data from NSL-KDD and UNSW-NB15. Nevertheless, the suggested study does not address the IoT environment. Tewari & Gupta [23] resent a secure and low-cost mutual authentication protocol for IoT-based healthcare systems, ensuring strong location privacy. Inuwa & Das [24] proposed Vector Convolutional Deep Learning, a CNN variation, to detect anomalies in IoT data. Two novel qualities, Correlated-Set Thresholding and DT were introduced by [25]. They are based on ML and were developed specifically for the Raspberry Pi. The approach is evaluated using the available Bot-IoT dataset, no conclusions are drawn regarding benign

classification. Hossain et al. [26] introduced a new attribute selection technique. The new method uses a wrapper strategy to choose relevant attributes for the machine learning approach and accurately filters them using the AUC. The proposed strategy is validated using four distinct ML techniques and the Bot-IoT dataset. Gupta et al. [27] examine the challenges of big data management in B2B-based healthcare systems and explore its potential benefits, such as improved patient access, efficiency in data transmission, and enhanced care quality. 98.8% classification accuracy has been achieved in the detection as well as physiological data classification, like ECG, for heartbeat using a support vector machine (SVM) along with discrete wavelet transform (DWT) [28]. Vector size is the work's limitation in such cases. The shift-invariance aspect of the DWT approach, which influences classification accuracy and performance, is absent from this work. Encrypted approaches like watermarking have been investigated about other elements, such as the security of industrial IoT-based healthcare, to prevent theft. This work does not emphasize the effective data management strategy. In IoT-based healthcare, a significant volume of data gathered by body sensors needs to be appropriately managed. Big data analytics approaches have been implemented in healthcare organizations as a result. R-peak is identified from an ECG signal to detect arrhythmias in a related study. Techniques from random forests and CNN have been used for categorization. Combining the frequency domain (FS2) and temporal (FS1) data has increased classification accuracy of automatic arrhythmia identification [29]. DTCWT as well as random forest classifier were used for classification. In this work, the accurate labeling of ECG data is crucial to the training process. To identify any irregularities in heartbeats, a hybrid deep CNN method can identify as well as categorise various heartbeats using real-time ECG data. Three neural network architectures have been trained using an ECG dataset for an entropy-based ECG categorization. To improve computational efficiency, there are three types of architectures: CNN-based, SincNet-based, and CNN-based with entropy induction. A method for increasing classification accuracy when there is a shortage of training data is provided in reference [30]. They used a two-dimensional residual network (2D-ResNet) in conjunction with the Stockwell transform (ST) approach.

3 Proposed Healthcare Data Privacy Analysis Based Anomaly Detection in Cloud IoT Network

ExAI is a branch of AI that strives to ensure the decisions made by AI systems are expliciate and aligned with human reasoning. The main priority in this context is building an AI system that ensures transparent and clear results, a factor that becomes particularly important in healthcare. Knowing the logic behind decisions is essential for impacting patient care and building trust effectively. ExAI helps to supply an apprehensible description to provide simplified knowledge for all the stakeholders like patients, doctors, etc. Its main strategy is to identify multiple methods for designing a collection of models that will help future innovators to minimize the trade off between system performance and its explainability.

As the healthcare database expands, it opens up several possibilities for AI solutions. Errors in medical procedures pose a significant challenge in this field due to the reliance on numerous medical devices, and various algorithms have been deployed to recognize and resolve these errors like erratic readings, deviant health conditions, etc. However, these methods fail to address the reason for considering it an anomaly. AI-based anomaly detection improves patient outcomes by identifying of several issues at an early stage and facilitates fast intercession along with controlling bogus anomaly alarms.

The suggested Anomaly Detection (AD) paradigm based on a cloud IoT network is shown in Fig. 1. To implement the proposed model for anomaly detection and privacy preservation, we used three datasets, the DARPA dataset [31], the CAIDAS dataset [32], and the DEFCON [33] dataset in the healthcare sector. Wearable glucose meters and smartwatches are only two examples of smart IoT devices that collect data, and each of the N participants has their own locally stored dataset. The dataset's samples are labeled to distinguish between "normal" and "abnormal" findings. After each participant trains a local model, the federated cloud

server receives the model weights. Consequently, the weights from each participant's local model are sent to this server. It then compiles these weights according to specific criteria (such as the user's age or the name of their ailment) and returns the results to the participants as a global weight.

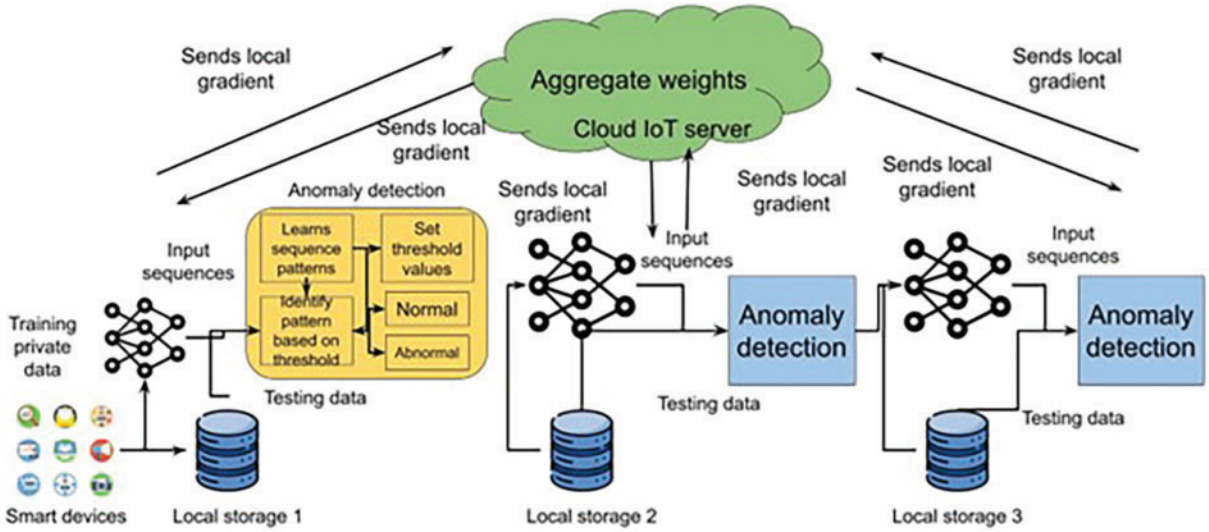


Figure 1: Proposed healthcare data privacy analysis based anomaly detection in cloud IoT network

The system works as follows: it is made up of edge devices, gateways, a cloud database with users, and a remote IoT platform. For decentralized optimization, a collection of IoT devices initially communicates with the gateway. Transmission frequencies are iteratively determined throughout the optimization process considering the system resource limitations defined at the gateway. Transmitting data streams from devices to a cloud database by determining optimal transmission frequency via gateway as well as IoT platform after transmission frequencies have converged and been allotted locally. Using particular cloud-based applications, users can visualize data flows. We took into account the following description of the problem mathematically (1) and Table 1 presents the abbreviations used in the paper:

$$\max_{x_1 x_2 \ldots x_N} \sum_{i=1}^{N} h_i\left(x_t\right)$$
$$\text{such that } \sum_{t=1}^{N} x_t \leq c, \sum_{t=1}^{N} a_i x_t \leq d, x_t \geq 0 \tag{1}$$

where a_i indicates the amount to be transmitted by device 'i', in a specific period, c presents the highest writing frequency (MWF) to the database, 'd' refers to available storage capacity in a specific period, the utility function $h_i(x_i)$ presents flow writing frequency as x_i for i^{th} device. Here, d and c both are finite resources where set having N different devices want to solve optimization problems cooperatively in order to determine their optimal x_i. The best possible solution for every given device in the network depends on a combination of various system-level factors (N, c, and d) and user-defined information (h_i and a_i). This work develops and offers an innovative anomaly detection model termed Radial Boltzmann Gaussian temporal fuzzy network (RBGTFN) in Section 4 to secure healthcare data. In the next phase, the Swordfish algorithm is applied to optimize the network performance in Section 5. The simulation analysis and results comparison are present in Sections 6 and 7, showcasing primary outcomes and implications of the study.

Table 1: Abbreviation table

Abbreviation	Full form
x_i	Decision variable for device i
c	Maximum writing frequency (MWF) to the database
d	Available storage capacity in a specific period
$h_i(x)$	Utility function of device i
a_i	Amount of data to be transmitted by device i
$Z(\theta)$	Partition function in the probability distribution
$E(x)$	Energy function in Deep Boltzmann Machine (DBM)
$P(x)$	Probability distribution function
W	Weight matrix in neural network models
b	Bias term in neural network models
σ	Activation function
$\Delta h_i^{(1)}$	Weight update term for first hidden layer in DBM
$\Delta h_i^{(2)}$	Weight update term for second hidden layer in DBM
D	Food separation distance in Remora Colony Swarm Optimization
a	Random number for position update in Remora algorithm
b	Coefficient for controlling position update in Remora algorithm
τ_{ij}	Pheromone level between city i and city j in ACO
η_{ij}	Heuristic value in Ant Colony Optimization (ACO)
ρ	Pheromone evaporation rate in ACO
Q	Constant in ACO for pheromone update
L_k	Tour length in ACO for kth ant
v_i	Velocity of particle i in PSO
x_i	Position of particle i in PSO
w	Inertia weight in PSO
c_1, c_2	Acceleration coefficients in PSO
$\text{rand}_1, \text{rand}_2$	Random numbers in PSO
λ_1, λ_2	Lagrange multipliers
$g_1(x), g_2(x)$	Constraint functions in the optimization problem

4 Radial Boltzmann Gaussian Temporal Fuzzy Network (RBGTFN) in Anomaly Detection

Due to the duplication, polymorphism, and incompleteness in health big data, the conventional supervised learning technique must perform feature selection and preprocessing before training the classifier. The process of analyzing data from the viewpoint of observation space is known as manifold analysis. To reduce the impact of specific isolated points on the AP algorithm, the data set is clustered according to the concept of neighborhood and the threshold of the gap between classes. The clusters with fewer samples in the class are then deleted. The following illustrates the RBF network design and training strategy created for the categorization of bipolar disorder. Within this approach, we have created two classes: BD for bipolar disorders, and CN for control patients. The structure consists of three layers: an input layer, a linear output layer, hidden layer including a non-linear RBF activation function. Eq. (2) displays the sth node's activity,

s(p), which stands for the Euclidean norm.

$$a_s(p) = \|p - \widehat{p}_s\| = \sqrt{\sum_{m=1}^{M} (p_m - \widehat{p}_{s,m})^2} \tag{2}$$

where the input vector is denoted by pT = [p1, p2, . . . , pM], and the center of the sth node is represented by pn T s = h pn T s,1, pn, T s,2, . . . pn T s, M i. A radial symmetric function was applied to the node output. Moreover, a Gaussian function may be used:

$y(v) = e^{\frac{z}{\varepsilon_i}}$ where the node's width is represented by w 2 s. A set of well-known inputs as well as outputs presented as (pk; fk) where (k = 1, 2, . . . , K) were utilized to train NN. The neural network in the suggested system was trained in two stages: 1. Hidden layer's parameters, cs(p), were first computed; 2. The hidden layer's parameters are derived from junction weights connecting the hidden layer and to the output. Input space's FP, where several fuzzy sets were described for every input variable, was employed by the suggested approach. For its input pj (j = 1, 2, . . . , M), the novel RBF approach applied a uniform split of discourse universe into cj fuzzy sets F 1 j, F 1 j, . . . , F cj j with functions of form as follows by Eq. (3).

$$F_j^s\left(p_j\right) = \begin{cases} 1 - \frac{\left|a_j - v_j^s\right|}{F_j} & \text{if } p \in \left[v_j^s - I_j^s, v_j^s + I_j^s\right] \left(s = 1, \ldots, c_j\right) \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

where I_j^s is half of the corresponding width and v_j^s is vital, and the membership value of the unit is set. For every input variable, the correspondence degrees at each given location in context to approaches 1. After exanimating the $k-1$ input vectors, S diffuse subspaces are created, where $1 \le S \le k-1$. After inserting the k^{th} input vector, $p(k)$, Euclidean relative distances $zls\ (p(k))$ (s = 1, . . . , S) between $p(k)$ and each fuzzy subspace S generated by Eq. (4) are determined.

$$zl_j^s r(p(k)) = \begin{cases} \frac{\left[\sum_{j-1}^{M}\left(v_j^p - p_j(k)\right)^2\right]^{1/2}}{\left[\sum_{j=1}^{M}(F_j)^2\right]^{1/2}} & \text{if } \left[\sum_{j=1}^{M}\left(v_j^s - p_j(k)\right)^2\right. \\ 1 & \text{otherwise} \end{cases} \tag{4}$$

Examine the combined probability distribution of the energy function E for the DBM that comprises two hidden layers, $h^{(1)}, h^{(2)}$, and one visible layer. Below is the probability distribution by Eq. (5).

$$P\left(V, h^{(1)}, h^{(2)}\right) = \frac{1}{Z(\theta)} exp - E\left(V, h^{(1)}, h^{(2)}; \theta\right)$$

$$P\left(V, h^{(1)}, h^{(2)}\right) = -V^T W^{(1)} h^{(1)} - V^T W^{(2)} h^{(2)} + b \tag{5}$$

By contrasting with alternative generative models, DBM offers a bipartition structure for the categorization of spectral-spatial images. Each neighboring layer uses the Bernoulli parameter to determine the DBM condition distribution, causing each unit's distribution to be active. Most classification in deep learning models involves an autoencoder for feature extraction. It includes encoders as well as decoders in its structure and matrix multiplication is applied in both. The normalizing function is the encoder's gradient function. Following the correction of weights and biases in the autoencoder, the network's training is carried out by Eq. (6).

$$h^{(n)} = a\left(b^{(n)} + V^T W^{(n)}\right)$$

$$h^{(n)} = \sigma\left(b_i^{(n)} + h^{(n-1)T} W^{(n)}\right) \text{ where } n = 1, 2, 3, \ldots, m \tag{6}$$

Examine the following example of training an HSI datacube that has two hidden layers by Eq. (7).

$$P\left(V_i = n; h^{(1)}, h^{(2)}\right) = \alpha W_i h^{(1)} + \alpha W_i h^{(2)} \tag{7}$$

Below is the mean-field value by Eq. (8).

$$P(x) = \sum_{h=1,2} Q\left(h^{(1)}, h^{(2)}\right) log\left(\frac{h^{(1)}, h^{(2)}}{P\left(h^{(1)}, h^{(2)}\right)}\right) \tag{8}$$

where the following is the Gibbs energy by Eq. (9).

$$E(x) = \frac{1}{Z(D)} exp(-P(x)) \tag{9}$$

Eqs. (10) and (11) provide the weight change and are used to calculate the new weight value. Every layer uses the bias b = 0.

$$\Delta h_i^{(1)} = \alpha \sum_i V_i W^{(1)} \tag{10}$$

$$\Delta h_i^{(2)} = \alpha \sum_i V_i W^{(2)} \tag{11}$$

The DBM's suggested bipartition structure enables Gibbs sampling, which updates a single variable at a time, contrasting CNN. Accurate classification of images in spatial-spectral variations is thus made possible. Two update blocks can be created from one image patch using Gibbs sampling. It requires n = L + 1 maximum possible limits for each image patch in the l layer. There are two hidden processing layers. Therefore, each layer was sampled independently and concurrently. First, we investigate the scenario when $g(\cdot)$ and $l(i)(\cdot)$ follow Gaussian Processes as a realistic illustration of the framework (1). Please take note that this formulation only serves to connect our framework to current multi-task general practitioners that each patient uses a unique GP. By the end of this subsection, it should be evident that when the number of patients increases, this direction of individualization will need nearly unmanageable computations. In particular, the two halves are shown as follows by Eq. (12).

$$g\left(x_t\right) \sim GP\left(0, kg(x1, x1')\right), \; l(i)(x2) \sim GP\left(0, kp(x1, x1')\right) \tag{12}$$

where $kg(\cdot,\cdot)$ and $k(i)(\cdot,\cdot)$ are appropriate covariance functions, such as the squared exponential kernel (RBF), and we assume that both GPs have a zero mean for simplicity. Knowledge sharing takes place using the global GP covariance function $kg(\cdot,\cdot)$. Assuming further that $g(\cdot)$ and $l(i)(\cdot)$ are independent for every patient, we can construct the overall covariance function as follows by Eq. (13).

$$\dot{k}\left(x_t^{(i)}, x_{i'}^{(j)}\right) = k_g\left(x_t^{(i)}, x_{i'}^{(j)}\right) + \delta_{ij} \cdot k^{(i)}\left(x_t^{(i)}, x_{t'}^{(j)}\right) \tag{13}$$

where the Kronecker delta function, denoted by δ_{ij}, is as follows: $\delta_{ij} = 1$ for the same patient if $i = j$, and 0 otherwise. It's interesting to note that for all function variables f(1), $\cdots$, and f(P), personalized GPs from this

construction really reduce to a single GP with the covariance function $\tilde{k}(\cdot,\cdot)$ by Eq. (14).

$$\begin{bmatrix} \mathbf{f}^{(1)} \\ \vdots \\ \mathbf{f}^{(P)} \end{bmatrix} \sim \mathcal{GP}\left(\mathbf{0}, \begin{bmatrix} K_{14}^{g}+K^{(1)} & \cdots & K_{1P}^{g} \\ \vdots & \ddots & \vdots \\ K_{P1}^{g} & \cdots & K_{PP}^{g}+K^{(P)} \end{bmatrix}\right) \tag{14}$$

To be more precise, we consider $l^{(i)}$ to be GP and $g(\cdot)$ to be a deep network as follows by Eq. (15).

$$g\left(x_t\right)=\mu\left(x_t\right), l^{(i)}\left(x_t\right) \sim \mathcal{GP}\left(0, k^{(i)}\left(x_t, x_{t'}\right)\right) \tag{15}$$

Both the individual function $l^{(i)}(\cdot)$ and the shared function $g(\cdot)$ have desired qualities of their own. $X=\{x1, x2, \cdots, xn\}$ indicates vector set of n elements and X indicates a random vector. A feature vector with k dimensions, or each x_h, is taken from the patient data that was submitted. There is statistical independence among those vectors. Given the model λ, the probability distribution of the set X can be written as Eq. (16).

$$logp(X/\lambda)=\sum_{h=1}^{n} logp\left(x_h/\lambda\right) \tag{16}$$

Due to the fact that these vectors' distributions are unknown. Thus, a combination of Gaussian probability distributions, that is calculated as weighted sum of l component densities using the Eq. (17).

$$p\left(x_h/\lambda\right)=\sum_{i=1}^{l} w_i N\left(x_h, \mu_i, \Sigma_i\right) \tag{17}$$

As $\lambda=\{w_i, \mu_i, \sum_i\}$, where w_i denotes the mixture weight and $N(x_i, \mu_i, \sum_i)$ represents the density of the k-th Gaussian component with mean vector μ_i and covariance matrix $\sum_i$, λ serves as the prototype composed of a set of model parameters. For the random vector X or the extracted feature vectors, the probability distribution is given by Eq. (18).

$$p(X/\lambda)=\sum_{e^{h=1}}^{n}\sum_{i=1}^{l} w_i \frac{exp\left\{-\frac{1}{2}\left(x_h-\mu_i\right)^{-1}\sum_i\left(x_h-\mu_i\right)\right.}{(2\Pi)^{k/2}\left|\sum_i\right|^{\frac{1}{2}}} \tag{18}$$

$0 \le x_h \le \infty$ and $1 \le i \le n$ in this case The component $(x_h-\mu_i)$ is now transposed as $(x_h-\mu_i)/$, while the inverse of $(\sum i)$ is $\sum i-1$. In contrast, the doctor cluster $\{C1, C2, \cdots, C_{m-1}\}$ is represented by the typical GMM model $\{G1, G2, \ldots, G_{m-1}\}$, i.e., the Gi model, which describes Ci cluster. Let G* represent the Gaussian Mixture Model (GMM) for each patient whose data was entered via the Android app. $L(\frac{\lambda}{X}) \approx p(\frac{X}{\lambda})$ is the probability function that stock parameter vector as well as data vector. Initialization will work for components like the convolutional and fuzzy neural networks. The weights between each layer are found at the bottom. We will then prepare the classification function as well as the hybridization. Every node's bias (b) is set to zero. Following this, the weight between the layers is initialized according to the rule, and it is provided as Eq. (19).

$$Un\left[-\frac{1}{\sqrt{m^{(l-1)}}}, \frac{1}{\sqrt{m^{(l-1)}}}\right] \tag{19}$$

m^{l-1} is the $(l-1)^{th}$ level, and Un is the even dispersal. m^{l-1} determines number of nodules on final levels of fuzzy as well as convolutional features for the hybridization level.

5 Remora Colony Swarm Optimization (RCSO)

The global search is carried out by the ROA using the SFO approach, which is based on the elite technique employed in the swordfish algorithm. The following is an expression for the position updating Formula (20):

$$V_i\left(t+1\right) = X_{\text{best}}\left(t\right) - \left(rand \times \left(\frac{X_{\text{best}}\left(t\right) + X_{\text{rand}}\left(t\right)}{2}\right) - X_{\text{rand}}\left(t\right)\right) \tag{20}$$

And $V_i(t+1)$ indicates the position of ith remora's candidate. The best position as of right now is $X_{\text{best}}(t)$. Remora's random position is denoted by $X_{\text{rand}}(t)$. Iteration number t is what we're talking about. A random number between 0 and 1 is called a rand. Furthermore, remora can to switch hosts based on its experiences by Eq. (21):

$$V_i'(t+1) = V_i(t+1) + randn \times \left(V_i(t+1) - X_i(t)\right) \tag{21}$$

And $V_i'(t+1)$, indicates the position of ith remora's candidate. Its prior location is represented using $X_i(t)$. Also, 'randn' is used to generate an accurately distributed random number. The WOA bubble-net assault technique is utilized. These are the updated position updating formulas with modifications by Eq. (22):

$$\begin{aligned} V_i(t+1) &= D \times e^a \times cos(2\pi a) + X_{\text{best}}\left(t\right) \\ D &= \left|X_{\text{best}}\left(t\right) - X_i(t)\right| \\ a &= rand \times \left(b-1\right) + 1 \\ b &= -\left(1 + \frac{t}{T}\right) \end{aligned} \tag{22}$$

where D indicates food separation from the remora. It is evident from Eq. (22) that an is a random number between −2 and 1. Additionally, b drops linearly from −1 to −2. Ants use their avarice to choose which towns to visit according to the number and distance of pheromones between them. The shortest path is considered to be the optimal answer in this iterative procedure. Eq. (23) is used to select the city j that an ant in city i will travel to in iteration t.

$$P_{ij}^k = \begin{cases} \frac{\left[\tau_{ij}(t)\right]^\alpha \left[\eta_{ij}\right]^\beta}{\Sigma_0 \left[\tau_{ij}(t)\right]^\alpha \left[\eta_{ij}\right]^\beta}, & \text{if } j \text{ is allowed city} \\ 0, & \text{otherwise} \end{cases} \tag{23}$$

Eq. (24) uses ij and $(1/dij)$ to represent the number of pheromones and distance respectively between i and j cities, j to illustrate the cities that may be travelled by k^{th} ant. Ants in the typical ACO updates pheromones on their trail to a food source before making a probabilistic decision based on transition probability. The transition probability for k^{th} ant at time step t from City i to City j in the TSP problem is written as follows:

$$PROB_{ij}^k(t) = \begin{cases} \frac{\left[\tau_{ij}(t)\right]^\alpha \cdot \left[\eta_{ij}\right]^\beta}{\Sigma_{j \in l_i^k} \left[\tau_{ij}(t)\right]^\alpha \cdot \left[\eta_{ij}\right]^\beta} & \text{if } j \in I_i^k \\ 0 & \text{otherwise} \end{cases} \tag{24}$$

The pheromone trails are updated once each ant has finished a tour by first decreasing them at a consistent rate of evaporation and then enabling every ant to drop pheromone over the arcs belonging to its

tour, shown in Eq. (25):

$$\tau_{ij} = (1-\rho)\cdot\tau_{ij} + \sum_{k=1}^{M}\Delta\tau_{ij}^{k} \tag{25}$$

where ρ is the rate at which the pheromone trail evaporates ($0 << 1$) and M is the total number of ants. ρ value allows the algorithm to "forget" past incorrect decisions and prevent the pheromone trails from building up infinitely. The corresponding pheromone strength on arcs that are not chosen by the ants decreases exponentially with many iterations. The amount of trial substance placed on edge *(i, j)* by k^{th} ant, expressed as a quantity per unit of length $\Delta\tau_{ij}^{k}$, is described as follows by Eq. (26):

$$\Delta\tau_{ij}^{k} = \begin{cases} \frac{Q}{L_k} & \text{if ant } k \text{ uses edge } (i,j) \text{ in its tour} \\ 0 & \text{otherwise} \end{cases} \tag{26}$$

where Q is a preset constant and L_k represents tour length. PSO the algorithm runs iteration by iteration, comparing the solutions generated in each iteration against the global best of the swarm and the self-local best. The following equations are utilized to evaluate the new position of the particle given its velocity (V), number (N), and vector (X) of particles by Eq. (27):

$$v_i(t+1) = w\cdot v_i(t) + c_1\cdot rand_1\cdot\left(pbset_i(t) - x_i(t)\right) + c_2\cdot rand_2\cdot\left(gbest_i(t) - x_i(t)\right)$$

$$x_i(t+1) = x_i(t) + v_i(t+1)(i = 1\cdots N) \tag{27}$$

In the interval $[0,1]$, two random numbers are evenly distributed, and $rand_1$ and $rand_2$ reflect the relative influence of the social and cognitive components (learning elements) based on these determinations. The inertia weight, or w, parameter regulates how much the velocities from before affect the current one. We now recast the original optimization issue (28) in the following way to adhere to mathematical conventions:

$$\begin{aligned} &\min_{x_1,x_2\cdots x_N}\sum_{t=1}^{N} f_t\left(x_t\right), \\ &\text{s. t. } \sum_{i=1}^{N} x_i \le c, \sum_{i=1}^{N} a_i x_i \le d, x_t \ge 0 \end{aligned} \tag{28}$$

where the function $f_i(x_i) = -h_i(x_i)$ is convex. The following is how (3)'s Lagrange equation is displayed in Eq. (29):

$$\mathbf{L}\left(x,\lambda_1,\lambda_2\right) = \sum_{t=1}^{N} f_i\left(x_t\right) + \lambda_1 g_1(x) + \lambda_2 g_2(x) \tag{29}$$

and for optimality, the KKT criteria demand that the following hold true by Eq. (30):

$$\begin{aligned} &\frac{\partial\mathbf{L}}{\partial x_t} = \frac{\partial f_1\left(x_1\right)}{\partial x_t} + \lambda_1\frac{\partial g_1(x)}{\partial x_t} + \lambda_2\frac{\partial g_2(x)}{\partial x_t} = 0 \\ &\lambda_1,\lambda_2 \ge 0, \\ &\lambda_1 g_1(x), \lambda_2 g_2(x) = 0 \end{aligned} \tag{30}$$

where ∂ is operation of partial derivative, λ_1. λ_2 are Lagrange coefficients for $g_1(x) = \sum_{i=1}^{N} x_i - c$ and $g_2(x) = \sum_{i=1}^{N} a_i x_i - d$ which represents constraint in issue with Eq. (31):

$$\frac{dg_1(x)}{\partial x_t} = 1$$
$$\frac{\partial_{g2}(x)}{\partial x_t} = a_t \tag{31}$$

Due to system limitations, the optimal converged solution will fall into any of the subsequent scenarios.

6 Simulation Analysis

Experimental setup-Version 3.1 was used to examine and monitor the situation, and the configuration was done using virtual machines-based open-source broker software packages. Oracle Virtual Box (Oracle, 2018) housed in Windows 10 PC having three virtual machines and Intel Core i7-5820K, 64 GB RAM, 3.30 GHz, 6 physical CPUs, and 12vCPU for installing broker setup. Each virtual computer contains 8 GB RAM, 15 GB hard drive, and a single CPU.

Dataset description Deep learning-based intrusion detection systems require access to a dataset to assess intrusions. Properly produced data is crucial and difficult to train the model because it includes labeled regular and abnormal communication along with extra factors like IP address. Furthermore, for security concerns, few network packet-based analytic datasets are released publicly. Freely available datasets described in this section are commonly used. The Defence Advanced Research Project Agency (DARPA) produced the dataset in 1998. The test data for network-based assaults spanning two weeks is included along with network traffic and audit records spanning seven weeks. However, a drawback of the DARPA dataset is its lack of real network activity. The KDD CUP (Knowledge Discovery and Data Mining) dataset originated with the original DARPA dataset, which disclosed approximately 5 million suspicious behavior evaluations of network traffic within seven weeks.

Versions DEFCON-8 and DEFCON-10 of the DEFCON Dataset were suggested in 2000 and 2002, respectively. One version of DEFCON-8 contains attacks based on buffer overflows and port scanning, while another version includes attacks related to the FTP protocol, malformed packets, port scanning, and sweeps. The difference between regular and real-time traffic during the CTF (Capture the Flag) tournament, which results in IDS evaluation limits the size of this dataset. Three distinct datasets are covered under the Centre of Applied Internet Data Analysis's (CAIDAs) dataset: RSDoS Attack Metadata (2018-09), CAIDA DDOS, and CAIDA Internet traces (2016).

7 Comparative Analysis

The hidden Markov models (HMMs) and an LR- multilayer perceptron (MLP) based classifier are used as a comparative experimental result with the proposed Explainable AI (ExAI) fuzzy network-based technique RBGTFN blended approach RCSO with all three datasets in Tables 2–4 helps to explain its false detection:

Tables 2–4 present a Cross-comparison of smart grid security using a variety of datasets. The datasets analyzed are MIMIC-IV, DEFCON, and CAIDAS datasets in terms of detection accuracy, QOS, precision, latency, and scalability.

Table 2: Comparative analysis of DARPA dataset

Technique	Detection accuracy	QOS	Precision	Latency	Scalability
HMM	82	80	73	70	79
LR-MLP	87	84	80	79	85
RBGTFN_RCSO	94	89	90	87	91

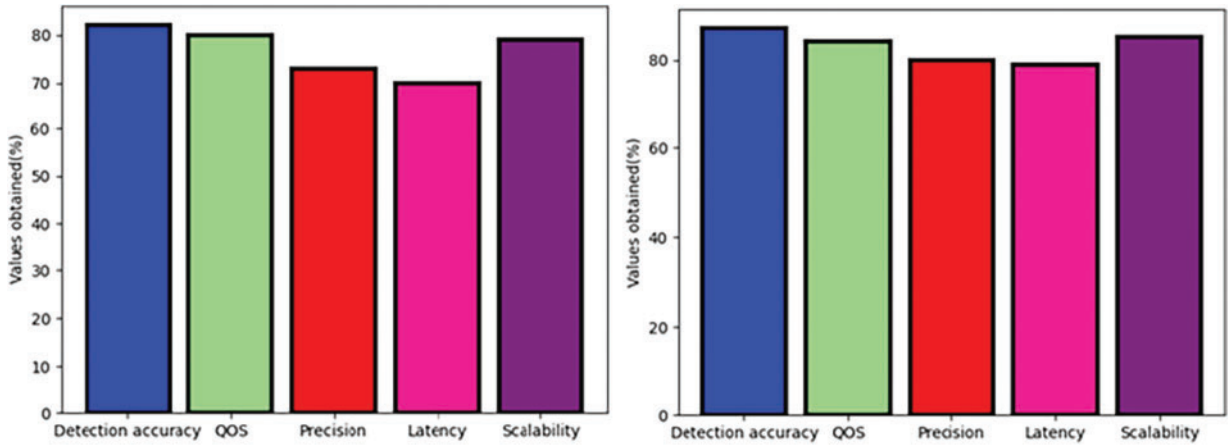
Table 3: Comparative analysis of DEFCON dataset

Technique	Detection accuracy	QOS	Precision	Latency	Scalability
HMM	74	77	78	80	76
LR-MLP	82	79	82	87	78
RBGTFN_RCSO	92	87	94	96	90

Table 4: Comparative analysis of the CAIDAS dataset

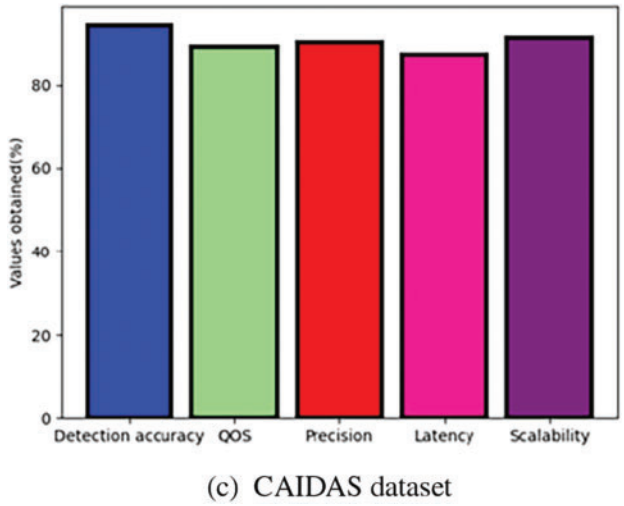
Technique	Detection accuracy	QOS	Precision	Latency	Scalability
HMM	82	79	74	78	81
LR-MLP	90	83	80	84	85
RBGTFN_RCSO	98	89	95	93	96

Fig. 2a–c shows an analysis of the existing parameters of HMM in the DARPA dataset. For the DARPA dataset existing HMM precision is 73%, latency 70%, QOS 80%, detection accuracy 82%, and scalability 79%. precision 78%, latency 80%, QOS 77%, detection accuracy 74%, scalability 76% for DEFCON; existing HMM attained precision of 74%, latency of 78%, QOS of 79%, detection accuracy of 82%, and scalability of 81% for the CAIDAS dataset.



(a) DARPA dataset (b) DEFCON

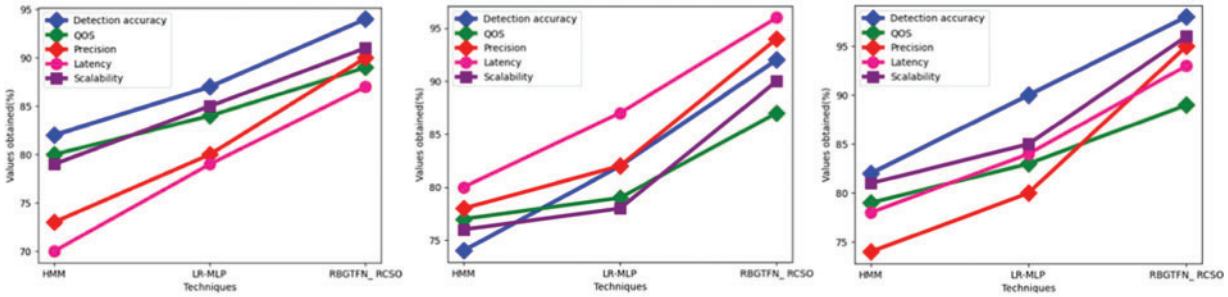
Figure 2: (Continued)



(c) CAIDAS dataset

Figure 2: Analysis of existing parameters of HMM for (**a**) MIMIC-IV, (**b**) DEFCON, (**c**) CAIDAS dataset

Fig. 3a–c indicates the analysis of existing parameters of LR-MLP that are currently in use in the DARPA dataset. Current LR-MLP achieved precision 80%, latency 85%, QOS 84%, detection accuracy 87%, and scalability 85% on the DARPA dataset. For DEFCON, existing LR-MLP precision 82%, latency 87%, QOS 79%, detection accuracy 82%, scalability 78%; precision 80%, latency 84%, QOS 83%, detection accuracy 90%, scalability 85% for the CAIDAS dataset.



(a) DARPA dataset (b) DEFCON (c) CAIDAS dataset

Figure 3: Analysis of existing parameters of LR-MLP for (**a**) MIMIC-IV, (**b**) DEFCON, (**c**) CAIDAS dataset

The analysis of existing parameters of RBGTFN_RCSO in DARPA dataset is displayed in Fig. 4a–c. RBGTFN_RCSO 90% precision, 87% latency, 89% QOS, 94% detection accuracy, and 91% scalability for the DARPA dataset. For the DEFCON, precision was 94%, latency was 96%, QOS was 87%, detection accuracy was 92%, scalability was 90%. For CAIDAS dataset, precision was 95%, latency was 93%, QOS was 89%, detection accuracy was 98%, and scalability was 96%.

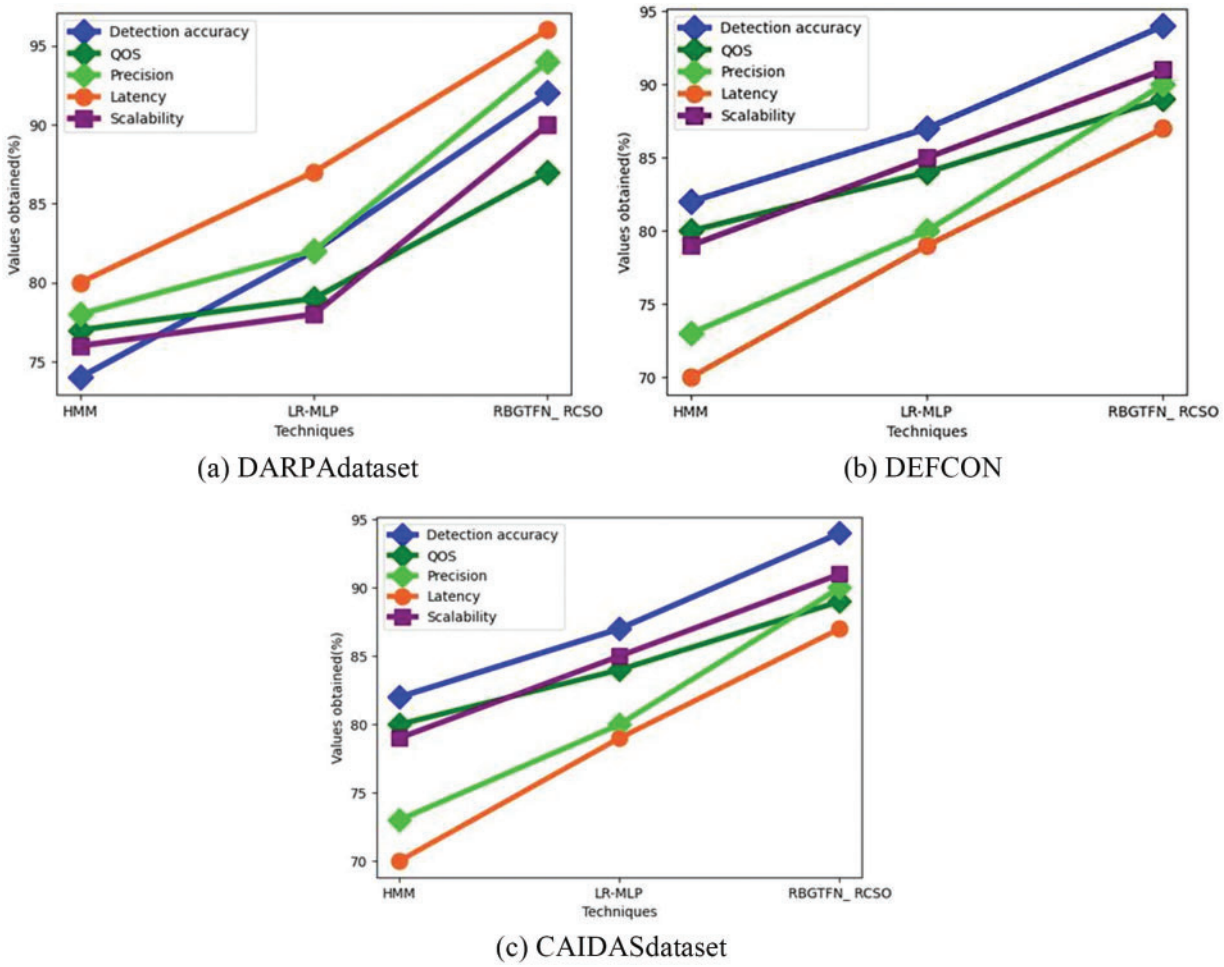


Figure 4: Analysis of existing parameters of RBGTFN_RCSO for (**a**) MIMIC-IV, (**b**) DEFCON, (**c**) CAIDAS dataset

8 Discussion

In the proposed data security technique, a random hash value and signature pattern of the data matrix are used to generate a random key for the input data stream. As a result, it facilitates quicker and less time-consuming data encryption and decryption. Keep in mind that anomalies can occur on any device, and we base our evaluation of the anomaly detection on the abnormalities that have happened on device number one. This takes into account a plausible situation in an actual Internet of Things network, in which a small number of devices in our method, for example, are outperformed the ones that were published. Because of the initial imbalance in the dataset, the models produced have low recall values. The enhanced recall values can be attributed to the data samples being evenly distributed throughout the various categorization jobs. These tables demonstrate how much better the suggested solution is than the current schemes in terms of accuracy in anomaly detection, system throughput and scheme efficiency. It is not necessary to classify this communivation because it has already been identified as intrusive and can be stopped without repercussions. Traffic identified as harmful at the first level may be routed to the cloud for a more thorough investigation, which would relieve demand on edge resources, thanks to the second level's customizable reaction time.

9 Conclusion

This study proposes a novel method for anomaly detection in cloud-based IoT networks utilizing explainable artificial intelligence and privacy analysis of healthcare data. A Radial Boltzmann Gaussian temporal fuzzy network has been used in anomaly detection to assess the privacy of healthcare data in this case. Remora colony swarm optimization was then used to examine network optimization. The suggested AI-based security mechanism offers several important benefits, including less computational complexity, a quick and easy process, low time consumption, precise attack detection, and optimal performance results. During performance analysis, suggested AI-based security method outcomes are verified as well as contrasted using a variety of assessment metrics with feature learning, classification, and data security models. The acquired results indicate that the suggested technique performs better than other techniques. Attackers may modify the transmission frequency of IoT edge devices and transmit data streams at an irregular cadence. Given the variety of manipulations available to alter transmission frequency, the rule-based method illustrates internal workings during an anomaly event but is not able to accurately identify anomalies in real-world settings.

Acknowledgement: The authors thank the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah for supporting this study.

Funding Statement: This project was funded by Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah under grant No. (RG-6-611-43), the authors, therefore, acknowledge with thanks DSR technical and financial support.

Author Contributions: Final manuscript revision, funding, supervision: Brij B. Gupta, Wadee Alhalabi; study conception and design, analysis and interpretation of results, methodology development: Jitendra Kumar Samriya, Virendra Singh; data collection, draft manuscript preparation, figures and tables: Gourav Bathla, Meena Malik, Varsha Arya. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data generated or analysed during this study are included in this published article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Saraswat D, Bhattacharya P, Verma A, Prasad VK, Tanwar S, Sharma G, et al. Explainable AI for Healthcare 5.0: opportunities and challenges. IEEE Access. 2022;13:84486–517. doi:10.1109/ACCESS.2022.3197671.
2. Albahri AS, Duhaim AM, Fadhel MA, Alnoor A, Baqer NS, Alzubaidi L, et al. A systematic review of trustworthy and explainable artificial intelligence in healthcare: assessment of quality, bias risk, and data fusion. Inf Fusion. 2023;96:156–91. doi:10.1016/j.inffus.2023.03.008.
3. Yang CC. Explainable artificial intelligence for predictive modeling in healthcare. J Healthcare Inform Res. 2022;6(2):228–39. doi:10.1007/s41666-022-00114-1.
4. Gupta BB, Gaurav A, Attar RW, Arya V, Alhomoud A, Chui KT. A sustainable W-RLG model for attack detection in healthcare IoT systems. Sustainability. 2024;16(8):3103. doi:10.3390/su16083103.
5. Liu W, Zhao F, Shankar A, Maple C, Peter JD, Kim B-G, et al. Explainable AI for medical image analysis in medical cyber-physical systems: enhancing transparency and trustworthiness of iomt. IEEE J Biomed Health Inform. 2023;29(4):2365–76. doi:10.1109/jbhi.2023.3336721.
6. Sangaiah AK, Rezaei S, Javadpour A, Zhang W. Explainable AI in big data intelligence of community detection for digitalization e-healthcare services. Appl Soft Comput. 2023;136:110119. doi:10.1016/j.asoc.2023.110119.

7. Ahmed M, Zubair S. Explainable artificial intelligence in sustainable smart healthcare. In: Explainable artificial intelligence for cyber security: next generation artificial intelligenc. Cham, Switzerland: Springer International Publishing; 2022. p. 265–80.
8. Gupta BB, Lytras MD. Fog-enabled secure and efficient fine-grained searchable data sharing and management scheme for IoT-based healthcare systems. IEEE Trans Eng Manag. 2022;71:12566–78. doi:10.1109/tem.2022.3143661.
9. Raza A, Tran KP, Koehl L, Li S. Designing ECG monitoring healthcare system with federated transfer learning and explainable AI. Knowl Based Syst. 2022;236(4):107763. doi:10.1016/j.knosys.2021.107763.
10. Alsalman D. A comparative study of anomaly detection techniques for IoT security using AMoT (adaptive machine learning for IoT threats). IEEE Access. 2024;12:14719–30. doi:10.1109/access.2024.3359033.
11. Rathee G, Saini H, Garg S, Choi BJ, Hassan MM. A secure data e-governance for healthcare application in cyber physical systems. Int J Sem Web Inform Syst. 2024;20(1):1–17. doi:10.4018/IJSWIS.345934.
12. Samriya JK, Chakraborty C, Sharma A, Kumar M. Adversarial ML-based secured cloud architecture for consumer Internet of Things of smart healthcare. IEEE Transact Consum Electr. 2023;70:2058–65. doi:10.1109/TCE.2023.3341696.
13. Xu H, Sun Z, Cao Y, Bilal H. A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. Soft Comput. 2023;32(19):14469–81. doi:10.1007/s00500-023-09037-4.
14. Yaqoob S, Hussain A, Subhan F, Pappalardo G, Awais M. Deep learning based anomaly detection for fog-assisted IoVs network. IEEE Access. 2023;14:19024–38. doi:10.1109/ACCESS.2023.3246660.
15. Patel SK. Improving intrusion detection in cloud-based healthcare using neural network. Biomed Signal Process Control. 2023;83(1):104680. doi:10.1016/j.bspc.2023.104680.
16. Khatun MA, Memon SF, Eising C, Dhirani LL. Machine learning for healthcare-IoT security: a review and risk mitigation. IEEE Access. 2023;11:145869–96. doi:10.1109/ACCESS.2023.3346320.
17. Bezanjani BR, Ghafouri SH, Gholamrezaei R. Fusion of machine learning and blockchain-based privacy-preserving approach for healthcare data in the Internet of Things. J Supercomput. 2024;80(17):24975–5003. doi:10.1007/s11227-024-06392-3.
18. Wei Z, Liu J, Yao Y. Semantic-based optimization of deep learning for efficient real-time medical image segmentation. Int J Sem Web Informat Syst (IJSWIS). 2024;20(1):1–16. doi:10.4018/IJSWIS.340938.
19. Rai AK, Verma DK, Dwivedi RK. Detecting deviations: anomaly detection in healthcare IoT data streams using advanced machine learning techniques. In: International Conference on Emerging Trends in Expert Applications & Security; 2024; Singapore: Springer Nature Singapore. p. 427–39.
20. Namratha M, Anusree MK, Niha, Pooja S, Arpana MR. Anomaly detection in medical IoT devices using federated learning. In: International Conference on Smart Trends in Computing and Communications; 2023; Singapore: Springer Nature Singapore. p. 259–70.
21. Krishnamoorthy R, Gupta M, Swathi G, Tanaka K, Raja C, Ramesh JVN. An intelligent IoT-based smart healthcare monitoring system using machine learning. In: 5G-based smart hospitals and healthcare systems. Boca Raton, FL, USA: CRC Press; 2023. p. 230–47.
22. Ioannou I, Nagaradjane P, Angin P, Balasubramanian P, Kavitha KJ, Murugan P, et al. GEMLIDS-MIOT: a green effective machine learning intrusion detection system based on federated learning for medical IoT network security hardening. Comput Commun. 2024;218(6):209–39. doi:10.1016/j.comcom.2024.02.023.
23. Tewari A, Gupta BB. An internet-of-things-based security scheme for healthcare environment for robust location privacy. Int J Computat Sci Eng. 2020;21(2):298–303. doi:10.1504/ijcse.2020.10574.
24. Inuwa MM, Das R. A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. Int Things. 2024;31(71):101162. doi:10.1016/j.iot.2024.101162.
25. Khan F, Jan MA, Alturki R, Alshehri MD, Shah ST, ur Rehman A. A secure ensemble learning-based fog-cloud approach for cyberattack detection in IoMT. IEEE Trans Ind Inform. 2023;19(10):10125–32. doi:10.1109/TII.2022.3231424.
26. Hossain MS, Muhammad G, Guizani N. Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics. IEEE Netw. 2020;34(4):126–32. doi:10.1109/mnet.011.2000458.

27. Gupta BB, Gaurav A, Panigrahi PK. Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. J Bus Res. 2023;162:113859. doi:10.1016/j.jbusres.2023.113859.
28. Srinivasu PN, Sandhya N, Jhaveri RH, Raut R. From blackbox to explainable AI in healthcare: existing tools and case studies. Mob Inf Syst. 2022;2022(1):8167821.
29. Nazar M, Alam MM, Yafi E, Su'ud MM. A systematic review of human-computer interaction and explainable artificial intelligence in healthcare with artificial intelligence techniques. IEEE Access. 2021;9:153316–48. doi:10.1109/access.2021.3127881.
30. Patel N, Ramoliya F, Jadav NK, Gupta R, Tanwar S, Aujla GS. X-NET: explainable AI-based network data security framework for Healthcare 4.0. In: 2024 IEEE International Conference on Communications Workshops (ICC Workshops); 2024 Jun 9–13; Denver, CO, USA. p. 481–6.
31. Lippmann R, Cunningham RK, Fried DJ, Graf I, Kendall KR, Webster SE, et al. Results of the darpa 1998 offline intrusion detection evaluation. In: Recent Advances in Intrusion Detection, RAID 99 Conference; 1999 Sep 7–9; West Lafayette, IN, USA. p. 829–35.
32. Shirsath V. CAIDA UCSD DDoS 2007 Attack Dataset. IEEE Dataport. 2023. doi:10.21227/dvp9-s124.
33. Nehinbe JO. A simple method for improving intrusion detections in corporate networks. In: Information security and digital forensics (ISDF 2009). Berlin/Heidelberg, Germany: Springer; 2009. p. 111–22. doi:10.1007/978-3-642-11530-1_13.