Journal of Integrated
SCIENCE & TECHNOLOGY

Securing the patient healthcare data using Deep Inception-ResNet based CPABPP model in Internet of Things

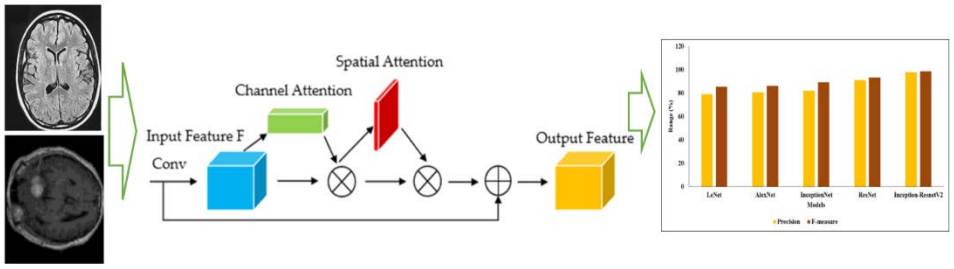
N.V. Raja Sekhar Reddy,[1*] Swathi Baswaraju,[2] P. Mary Kamala Kumari,[3] Phanikanth Chintamaneni,[4] B. Raveendra Naick,[5] B. Gunapriya Pradhan[2]

[1]Department of Information Technology, MLR Institute of Technology, Hyderabad-500043, India. [2]New Horizon College of Engineering, Ring Road, Bellandur Post, Bengaluru, India. [3]Department of Computer Science and Engineering, Lakireddy Bali Reddy College of engineering, Mylavaram 521230, India. [4]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur-520002, India. [5]Department of AI & ML, School of Computing, Mohan Babu University, Tirupati, India.

Received on: 08-Oct-2023, Accepted and Published on: 07-Feb-2024

Article

ABSTRACT



The IoT is transforming healthcare by enabling extensive connectivity between medical professionals, equipment, staff, and patients, facilitating real-time monitoring. While the network's scale and diversity offer advantages for data exchange, they also pose challenges for privacy and security, particularly with sensitive medical information. To address this, deep learning-based cryptographic and biometric systems are utilized for authentication and anomaly detection in medical systems. However, power constraints on network sensors necessitate efficient security schemes. Thus, the authors propose a novel framework, the deep Inception-ResNetV2 with privacy preservation, to secure data transmission while minimizing encryption and decryption time. Implementing this method reduces the network's burden, saving time and costs in communication. Compared to alternatives like private biometric-based authentication, this model demonstrates superior performance.

Keywords: Healthcare; Patient data; Security; Inception-ResnetV2; Cryptographic Techniques; Internet of Things.

INTRODUCTION

A patient's medical history is documented in a patient health record (PHR), containing essential information. Health records are often sent and received via the digital healthcare system. However, current digital healthcare systems rely on central servers, which are susceptible to hacking.[1] Due to its versatility and enhanced security, blockchain technology stands out as the most obvious choice for integrating the digital healthcare system. Additionally, blockchain enables P2P and decentralized network architectures.[2] Private blockchains, public blockchains, and consortium blockchains are the three main types. Since all network participants are known to one another in permissioned blockchains administered by a consortium, everyone involved feels safer and more confident. Hyperledger Fabric allows developers of contracts and network applications to use languages like Java, Go, Node.js, etc.

Organizations can meet their Information and Communication Technology (ICT) needs at a lower cost with cloud services, avoiding investments in costly and time-consuming in-house IT infrastructure or software installations.[3] Medical institutions now have access to automatic computer-assisted diagnostic (CAD) systems thanks to recent advancements in Machine Learning (ML) for computer vision.[4] Deep Learning (DL), a branch of ML, notably delivers superior results to human experts in picture categorization. However, training DL models requires state-of-the-art hardware and a large amount of processing resources. By utilizing cloud-computing services, healthcare organizations access cutting-edge technology, speeding up the training process and allowing DL models to scale efficiently at lower capital costs.[5] Additionally, a large amount of sample data is needed for DL model training, which can be difficult and expensive to gather in fields like medicine.[6] A community cloud, where services are shared by organizations with

*Corresponding Author: N V Raja Sekhar Reddy
Email: rajasekhar.nv1@gmail.com

Cite as: *J. Integr. Sci. Technol., 2024, 12(5), 805.*
URN:NBN:sciencein.jist.2024.v12.805

common interests, can help healthcare organizations address this problem.[7] When multiple companies need to collaborate on a project, they can use cloud storage services as a centralized data repository. However, data leakage is always a possibility, and there's a need for significant bandwidth when outsourcing data for cloud services.[8]

In an Internet of Things (IoT) setting, patient data privacy and security are paramount.[9] Secure data storage and transit ensure the integrity, authenticity, and validity of data, while data privacy is ensured by restricting access to authorized users. Reasonable precautionary measures can be formulated based on requirements, goals, and necessities.[10] While widespread usage of IoT devices has the potential to improve patient care, it's crucial to ensure the safety of sensitive personal data.[11] Attacks on next-generation schemes have increased, making IoT devices vulnerable to both new and old threats. The data that travels from the Internet of Things to the cloud and visualization domains undergo numerous transformations along the way. Data compression and encryption meet the challenges of sending information across public networks with limited capacity. Compression reduces the number of bits needed to save the image by condensing its representation. Lossless and lossy compression implementations exist for this purpose. Lossless compression maintains or improves the original picture quality during restoration, while lossy compression degrades the image quality.[12] Lossy compression provides cost savings, but quality loss isn't always acceptable, especially in fields like medicine, where accurate diagnoses depend on detailed data preservation. Popular methods for achieving this include lossless compression of the diagnostically-relevant region-of-interest (ROI) and lossy compression of the remaining data. However, these techniques require picture segmentation, which is computationally costly and ideally suited for cloud-based computing power. Consequently, region-of-interest (ROI)-based approaches aren't optimal for quickly sharing picture data. When picture data is encrypted, it becomes incoherent and can only be retrieved through the corresponding decryption procedure. Encryption techniques based on number theory and chaos theory are effective in protecting picture data, but they're only suitable for encrypting raw photos, as they conduct stream values.[13]

Since new types of threats constantly emerge, traditional solutions relying on signature or machine-learning methods are inadequate.[14] Deep neural networks (DNNs) can identify malfunctions in virtualized communication networks with greater precision by learning to recognize typical data flows and rebuilding them.[15] However, a significant challenge with these models is that sophisticated DNNs in the core clouds require more time to train than currently available classical approaches. Therefore, finding new ways to reduce training time without sacrificing detection precision is essential.

The paper's original contributions include:

- Constructing a standardized framework for patient data processing using deep learning (Inception-ResNet) to further reduce network traffic.
- Public key (PK) and master key (MK) generation using ciphertext-policy attribute-based privacy preservation (CPABPP).
- Validating the efficacy of the CPABPP model across various criteria, including MRI data verification.

RELATED WORK

Kumar et al.[16] proposed a Blockchain-directed Deep learning tactic (henceforth "BDSDT") for secure data transfer in an IoT-enabled healthcare system. To ensure data integrity and safe transmission of information, we first propose a novel, scalable blockchain design that employs the Zero Knowledge Proof (ZKP) method. Then, an Ethereum smart contract and the off-chain storage IPFS are included in BDSDT to address issues with data storage costs and data security. An intrusion detection system for HS networks is then built using the verified data. The latter utilizes Bidirectional Long Short-Term Memory (BiLSTM) in conjunction with Deep Sparse AutoEncoder (DSAE) to provide a highly effective intrusion detection solution. Experiments conducted on two publicly accessible data sources (CICIDS-2017 and ToN-IoT) demonstrate that the proposed BDSDT achieves an accuracy close to 99% in both non-blockchain and blockchain situations.

Consultative Transaction Key Generation and Management (CTKGM) is a method proposed by Selvarajan and Mouratidis[17] to facilitate safe exchange of medical records. Using random values, multiplication, and timestamps, it creates a unique key pair. The blockchain system then securely stores the patient information in encrypted blocks of hash values. The Quantum Trust Reconciliation Agreement Model (QTRAM) enables safe and trustworthy data transmission by calculating the trust score based on feedback data. The suggested framework is novel because it promotes secure patient-healthcare provider communication via feedback analysis and trust value utilization. Furthermore, nonce verification messages are authenticated during communication using the Tuna Swarm Optimization (TSO) technique. QTRAM's nonce message verification feature aids in authenticating senders and receivers in transit. After analyzing a number of evaluation metrics to assess the performance of this security model, it has been shown that the proposed scheme is effective by comparing the acquired findings with other existing state-of-the-art representations.

The deep framework is presented by Lakhan et al.[18] as a potential new solution to the aforementioned problems. Healthcare applications benefit from DRLBTS's secure and time-efficient scheduling. After initial validation, it transfers valid and secure data across connected network nodes. Statistical evidence demonstrates that DRLBTS is adaptable and satisfies the security, privacy, and makespan criteria of healthcare requests running on a dispersed network.

Energy-Efficient Networks is an issue that Mohammed et al.[19] have researched for medical use cases. This research offers the Energy-Efficient Distributed Federated Learning Offloading and Scheduling (EDFOS) system for blockchain-based networks as a potential solution to the aforementioned issue. EDFOS comprises many energy-efficient offloading and scheduling mechanisms that work together to ensure all running applications receive the necessary quality of service (QoS). Simulation findings reveal that compared to conventional healthcare systems, EDFOS significantly decreases energy usage (39%), training and testing time (29%), and

resource leakage and deadlines (36%). When it comes to healthcare applications, the challenges of power consumption and data protection, the EDFOS platform provides an efficient answer.

To protect healthcare networks against poisoning assaults, Kalapaaking et al.[20] suggest using blockchain technology to provide federated learning, with SMPC model verification. We begin by removing any compromised machine learning models from the FL participants using a secure inference method. After each participant's local model has been validated, it is transmitted to the blockchain node where it is aggregated securely. To test the efficacy of our suggested approach, we ran a series of experiments on various medical datasets.

A method called Lionised Golden Eagle Homomorphic Elapid Security (LGE-HES) was proposed by Miriam et al.[21] to ensure the safety of blockchains used in healthcare networks. The hash function performed by the blockchain algorithm keeps the medical picture secure. The MATLAB program is used to carry out the research. Simulation findings using Computed Tumour (CT) images and MRI image datasets confirmed the usefulness of the proposed system. Overall, the simulation resulted in a successful recognition and identification of 94.9% of malicious transmissions. Root measures are used to contrast the proposed model's performance with those of conventional methods.

To combat the coronavirus pandemic, Ahmed et al.[22] proposed a smart blockchain and AI-enabled solution for the healthcare industry. A new deep learning-based architecture is being developed to detect the virus in x-ray pictures, further using Blockchain technology. This means the proposed system has the potential to provide trustworthy data-gathering solutions, ensuring the superior quality of COVID-19 data analytics. Using a reference dataset, we developed a multi-layered sequential deep learning architecture. We also applied the Gradient-based color visualization technique to all experiments to make the proposed deep learning accessible and interpretable. Therefore, the design achieves a 96% accuracy in categorization, which is quite satisfying.

DESIGNED MODEL

The designed non-invasive technique for cancer diagnosis works in tandem with current diagnostic tools and mechanisms to improve the accuracy and precision of cancer diagnoses. This dataset will be used in the current study[23] and comprises 4,800 verified MRI pictures. Normal MRI scans of a patient seem different than those in which a tumour is visible. Figure 1 shows how the cancer appears in MRI scans with varying degrees of colour intensity.

Both training pictures and test images have been prepared. All radiographs were inspected for quality control before MRI analysis began, and those of poor quality or those could not be read were omitted. After that, the photographs were evaluated by two experts before being added to the AI database. Finally, a third specialist checked the evaluation pool to make sure there were no problems with the grades.

The purpose of this suggested endeavour is to differentiate between healthy individuals and those with cancer by classifying them into distinct groups. This sorting is arrived at by evaluating how well classifications work. Magnetic resonance imaging (MRI)

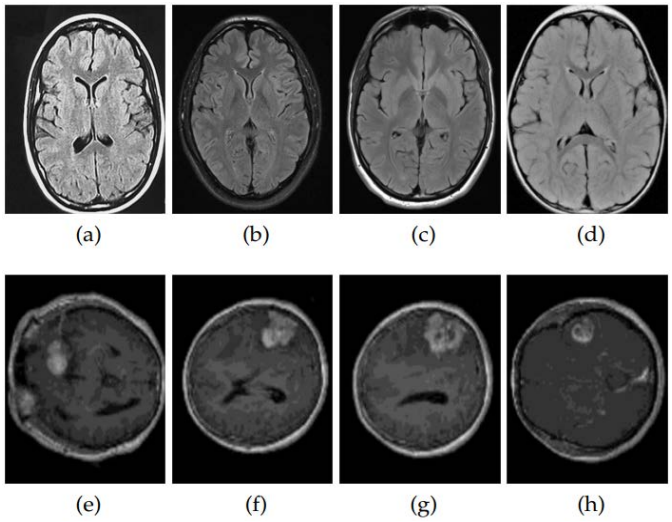


Figure 1:(a-d) Normal patient imageries (e-h) Cancer duplicate patient.

scans are used to collect the information. Different MRI scans have different pixel dimensions, denoted by the letters A and B.

Image Preprocessing: Preprocessing photos is a vital step in achieving high image quality. Image categorization is made possible by the preprocessing stage. Data augmentation was the first and primary method employed. This process performs many transformations on the input, which adds to the overall volume growth of the dataset. Translation, symmetry, and rotation were among the many transformations used to create a copy of the input. The steps of preprocessing and enhancement are outlined below.

Translation: Both the picture size and orientation were adjusted to meet the requirements. Centering Each picture has its rows and columns cropped out of the borders. This means that it's possible to get photographs in a range of sizes. The total number of pictures is then counted after the row and column widths have been cut.

Segmentation: It is necessary for picture extraction and classification. Segmenting the high-resolution photos led to spectrum confusion, poor delineation, and blurrier final images. In addition, this was improved by using the object-oriented picture segmentation method, which employed object structure and spectral signatures to eliminate salt and noise from the image and boost its precision.

Feature extraction: To obtain features, we use the built-in filters of each layer. Low-level features are retrieved using the filters in the initial layers (convolution and pooling), whereas high-level features are extracted using the filters in the top convolutional layer.

• Distinct feature vectors ($Z.Vs$) for each X-ray image were made: $Z.V = Z_1, Z_2, Z_3 \cdots Z_{14}$.

• Only vectors representing MRI scan statistics are included in the given matrix (Z.Vs). Equation 19 demonstrates that it is possible to describe such characteristics inside a single dataset.

$$\begin{pmatrix} Z.V_1 = Z_1, Z_2, Z_3 \ldots . Z_{14} \\ Z.V_2 = Z_1, Z_2, Z_3 \ldots . Z_{14} \\ Z.V_3 = Z_1, Z_2, Z_3 \ldots . Z_{14} \\ \vdots \\ Z.V_n = Z_1, Z_2, Z_3 \ldots . Z_{14} \end{pmatrix} \quad (1)$$

• Using fully connected layers, the classifier received the recovered characteristics and made a determination based on them.

3.2. Prediction of Disease using Inception-ResnetV2 Model

Szegedy combined Inception and Resnet for the Inception-Resnet[24] design for network backbones. By performing numerous convolution or pooling operations in parallel on the input picture, the Inception topology. It doesn't employ just one size of convolution kernel, but rather many sizes at once, and combines the outputs of these kernels to create a more nuanced feature map. Using such to your advantage can enhance your image representations. Kaiming, He designed Resnet,[25] a 152-layer residual neural network architecture, for use in the ImageNet challenge. In the neural network, he implemented a time-saving shortcut design. This is done by include the transfer and convolution outputs from the input layer, which mitigates common neural network issues such gradient dispersion at high depth.

To improve its picture identification performance, the Inception-ResnetV2 network, seen in Figure 2, adjusts the *input image size to* 299 299 3.

.

Figure 2. The construction of Inception-ResnetV2.

The Stem architecture takes the InceptionV3[26] model's notion of a parallel structure and decomposition to cut down on computation while maintaining high accuracy. Dimensionality reduction is achieved with the help of the built-in 1 1 convolution kernel. All three of the InceptionResnet variants (InceptionResnet-A, InceptionResnet-B, and InceptionResnet-C) use the Inception design, but with ever more layers, channels, and complexity in their topologies and feature maps. To cut down on computation and feature map size, we have three designs at our disposal: Reduction-A, Reduction-B, and Reduction-C. By combining the strengths of network structure, the Inception-ResnetV2 model not only has the potential to expand the network's depth and breadth, but also to prevent the gradients' disappearance. Inception-Resnet-A's architecture is seen in Figure 3; the similarity between the networks ends there.

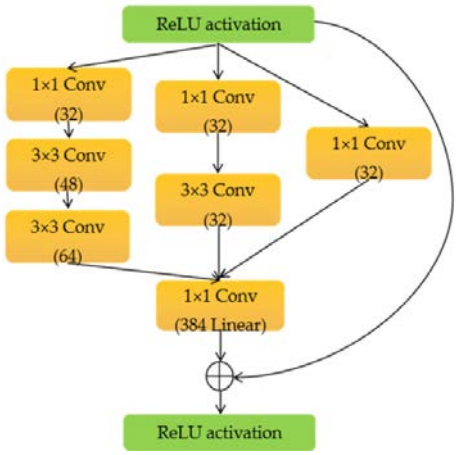


Figure 3. The construction of Inception-Resnet-A.

3.2.1. The CBAM Attention Mechanism

In order to increase neural networks' feature extraction capabilities while minimising costs and maximising efficiency, the attention mechanism has emerged as a powerful tool. It can automatically tune out irrelevant data and concentrate on the relevant data. In the Inception-ResnetV2 network, mechanism module to improve defect feature extraction and classification accuracy in $Inception - Resnet - A, Inception - Resnet - B, and\ Inception - Resnet - C$. Figure 4 depicts the detailed architecture.

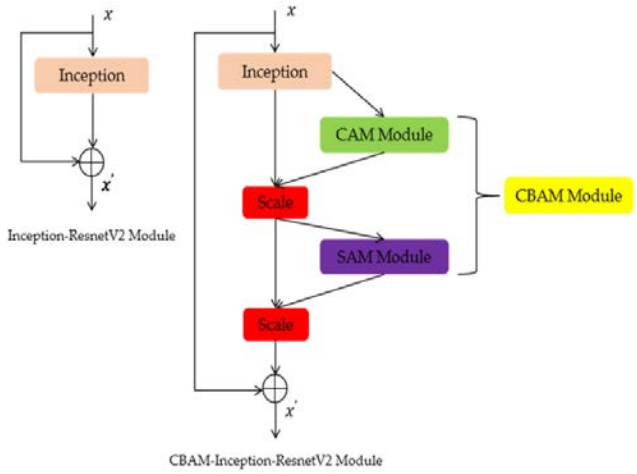


Figure 4. The constructions of Inception-ResnetV2.

Figure 5 shows that CBAM is made up of two distinct parts: Channel and spatial attention are employed to highlight relevant

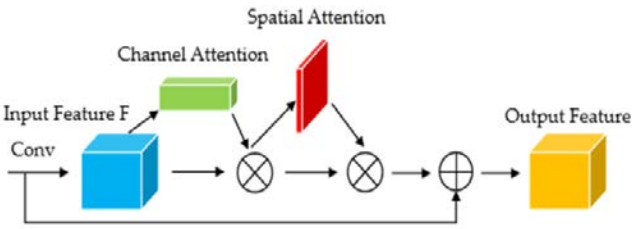


Figure 5. The construction of the CBAM component.

elements while downplaying irrelevant ones, hence enhancing the target detection effect. As a result, not only are limitations and processing power conserved,[27] but the module may be simply plugged into the preexisting network structure.

The CAM computation procedure is depicted in Figure 6a. Length (H), width (W), and number of channels (C) describe the input feature map. Using this formula, we can determine how much emphasis should be placed on each channel.

$$M_c(F) = \sigma\big(MLP\big(AvgPool(F)\big) + MLP(MaxPool(F))\big) = \sigma\left(W_1\left(W_0\left(F^c_{avg}\right)\right) + W_1(W_0\left(F^c_{avg}\right))\right) (2)$$

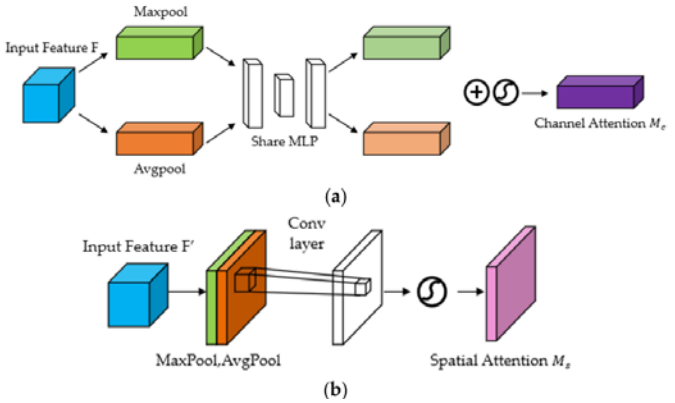


Figure 6. The constructions of the CAM and SAM components. (a) SAM component. (b) CAM unit.

Apiece channel of pooling F^c_{max} and regular pooling F^c_{avg} at the same period, and then passes through a Multilayer Perceptron (MLP). The MLP's output feature vector is then element-wise added, and function s is applied. By following these steps, we may capture the focus of the relevant channel.

The steps involved in determining SAM are depicted in Figure 6b. The CAM module's output feature map is used as input for a series of max pooling and average pooling operations, followed by a convolution on the resulting intermediate vector. The spatial attention is obtained by passing the results of the convolution through a sigmoid activation function s, as given in Equation (3).

$$M_s(F) = \sigma\big(f^{7\times7}\big(AvgPool(F)\big); (MaxPool(F))\big) = \sigma\big(f^{7\times7}(F^c_{avg}; F^c_{max})\big) (3)$$

3.2.2. Optimization of Model Parameters

(1) We simplified the model by reducing $Reduction - A, Reduction - B, and\ Reduction - C$ from six parameters, respectively. The last layer is a Softmax layer, although the size of the output is problem-dependent. This article presents two methods for predicting cancer using MRI scans.

(2) The cost function we choose is the cross-entropy loss function.[28] From what has been said, however, it is clear that illness similarities are rather high and are frequently not visible, making overfitting during training a common occurrence. To prevent this and make the model more stable in a healthcare setting, we blended L1 and L2 regularisation into the loss function.

Loss function optimisation the formula for L_{loss} is:

$$cross_{loss} = H(p,q) = -\sum_x p(x)1nq(x) (4)$$

$$L_{loss} = cross_{loss} + \sum_i(\alpha|w_i| + (1-\alpha)w_i^2) (5)$$

where p is the true probability of x, q is the circulation based on the model's predictions, w_i are the model's weights, and is the regularisation parameter. Overfitting is mitigated using L1 and L2 mixed regularisation, after which the batch-average cross entropy is used to derive $cross_{loss}$.

For the purposes of dataset was split in half. The model was trained using the suggested methodology, and the training data set contained both healthy and pneumonia-infected individuals. Almost 80% of training purposes, including both clean and dirty examples. There is some flexibility in how much data is used for each purpose (training vs. testing).

To further enhance the precision of the projected model, we employed transfer learning and fine-tuning. After some tweaking, we found that the model was 98% accurate. The proposed model's accuracy was further increased to 99.7 percent with the use of K-fold analysis and voting methods.

3.3. K-Fold Analysis

The suggested model is put through its paces using the K-fold validation purpose with several values validation approach selects various training data from the entire dataset to teach the model. If K is set to 10, for instance, ten iterations will be run, each time selecting 10% of the data set for evaluation. That is, we will only utilise the top 10% of the dataset for our initial round of testing. In the same way, the second 1/10th of the data will be utilised for testing in the next iteration, while the training. It has a mathematical expression of:

$$\begin{cases} if \\ Total\ test\ instance\ T = 5000 \\ Training\ \ instance\ (Total\ \ instance) - (5000) \end{cases} (6)$$

When K = 10, the dataset must be split into ten parts so that the model may be evaluated. Each section will serve as a test dataset in each cycle. The probabilities of each class occuring may be calculated using Equations 7–10.

$$Class\ cancer\ (C) = \frac{Po(C)_1 + Po(C)_2 + \cdots + Po(C)_N}{N} (7)$$

$$Class\ normal(N) = \frac{(N)_1 + Po(N)_2 + \cdots + Po(N)_N}{N} (8)$$

$$Class(C) = \frac{0.70+0.45+0.55+0.65+0.40}{4} \times 100 = 55 (9)$$

$$Class(N) = \frac{0.30+0.55+0.45+0.35+0.60}{5} \times 100 = 45\% (10)$$

3.4. System Model for Security

After an illness has been predicted, the information will be saved in the cloud. Medical record datasets are secure and patient and hospital privacy is protected prior to uploading to the cloud. A trusted authority (TA), users (patients), a server, and hospitals staffed by medical experts make up this paradigm.

Each entity's function in the modelled system is explained in further detail below.

- Parameters are generated by TA, and registration is handled by TA as well.
- The medical records of their patients are provided to the databases by the hospitals.

- The patient sends a query to the physicians with their starting and ending locations.
- Part of the clinical route is generated through server interaction and then returned to the user. By allowing many exchanges to take place amongst themselves rather than the hospital and the user, we can significantly cut down on the local communiqué overhead and processing cost. Patient information such as name, age, gender, costs, other indices, medicine, and appointment time are included in the medical datasets in this model. The ciphertext-policy attribute-based privacy preservation technique is used to exchange and secure these facts. The server builds the network in a way that respects these privacy settings.

3.4.1. Key Generation on Ciphertext-Policy Attribute-Based Privacy Protection (CPABPP)

The data owner initiates the three-stage setup procedure.

Step 1: Input security settings are used to run the CP-ABE setup algorithm, which produces both a public key (PK) and a master key (MK).
Step 2: A functional master key (MKF) are generated using a minimal amount of security inputs using the functional encryption setup procedure.
Step 3: A functional SK[f(i)] is generated using the functional encryption key-generation algorithm KeyGen(MK,S), where f(i) is defined as fi(S) = ssi(KeyGen(MK,S)), where ssi(s) is a purpose secrets. After the initialization process completes its run, the data owner sends the PKF and SK [fi] to authority, correspondingly, through the secure channel. A high number of precomputed subkeys are employed in this method for both encryption and decryption. P1, P2,..., P18 are all subkeys in the P-array, which spans 18 to 32 bits.

Algorithm 1 for making subkeys:

Algorithm 1 Procedure for generating subkeys

1: $Input — plain\ text$
3: $Strings(x) = P1, P2, P3 \ldots Pn$
5: $A = P1(XOR)\ P2$
6: $(n = P1;\ n + 1 > P1)$
7: $B = P2(XOR)\ P3$
8: (P2 = n; P2 < n + 1)
9: $C = P3(XOR)\ P4$
10: $(n = P1;\ n + 1 > P1)$
11: $N = Pn(XOR)\ Pn$
12: $(P1 = n;\ P1 < n + 1)$
13: $end\ if$
14: $Y * Z * (A\ mod\ E) = K1$
17: $\alpha^2(Y * Z * (A\ mod\ E)) = \beta K1$
18: $\alpha^2(X * Z * (B\ mod\ F)) = \beta K2$
19: $\alpha^2(Y * X * (C\ mod\ G)) = \beta K3$
20: end

3.4.2. Encryption Process

The parameter A is given a positive integer value of the form Ak 257, where k can take on any positive integer value between 1 and n. Let's pretend we have an array T with 256 distinct numbers (0–255). Using the linear mapping given by Equation (11), a new array R is constructed from A and T.:

$$R(i) = mod((A \times (T(i) + 1)), 257) \quad (11)$$

where i is an integer between 1 and 256. The range of T(i) is from 0 to 255, and any positive integer A fulfils the expression Ak257, where k is an integer bigger than 0. The results of the division by 257 of (A/257) and (T(i + 1)/257) are not integers. $Mod\ ((A\ (T(i) + 1)), 257)$ is therefore not equal to zero. When R(i) = R(i) - 1, R(i) is in the range [0,255], where [i] is in the range [1,256]. The original S-box, represented by the 1D array R = R(i), is converted to the 2D matrix Rb. A chaotic sequence of length L is produced by iteratively applying the tent-logistic map L times. By excluding the initial (L-256) items of the true chaotic series, we create a new chaotic series of length 256, designated as X, which improves the sensitivity of the chaotic series. $X, J = J(1), J(2), \ldots, J(256)$ is an index array produced by sorting X. As the chaotic sequence is nonperiodic and ergodic, it surely gives $J(i) \neq J(j)$, providing that $I \neq j$.

3.4.3. Communication with diagnosed patients

Each medical centre creates its own identifier using the following formula (Equation 12) based on logic and node distance:

$$d_i(H_i, H_j) = \frac{\sum_{p,q\in\{H_i\cup H_j - H_i\cap H_j\}}\left(X_{pq}^{H_i} + X_{pq}^{H_j}\right)}{\sum_{pq\in H_i\cup H_j}\left(X_{pq}^{H_i} + X_{pq}^{H_j}\right)} \quad (12)$$

where H_i and H_j are nodes with IDs of $H_i(id)$ and $H_j(id)$, correspondingly; p is the source. As stated in Equation (13), two hospital nodes' data privacy is tenable in a decentralised fashion using a randomised tactic:

$$Hr[(R0) \in S] \leq exp(\in) \cdot Hr[(R') \in O] \quad (13)$$

where R and R_0 are two data records next to each other and O is the data set that was output. Although RS successfully protects patient information, Laplace is implemented in a local training model mi for a number of healthcare facilities, as indicated in Equation (14).

$$\vec{m}_1 = m_i + Laplace(s/\in) \quad (14)$$

where s represents sensitivities and represents overall transmission costs. All patient information is encrypted using a combination of public and private keys. (PK_i, SK_i). MAE provides an estimate for each exchange and announces it through m_i and H_j. The distributed ledger contains a record of every transaction that has been validated. Equation (15) provides the MAE:

$$MAE(m_i) = \frac{1}{n}\sum_{i=1}^{n}|y_i - f(X_i)| \quad (15)$$

where n represents the total sum of users and X_i represents the individual costs of communicating with and making a transaction with each user. Some specialised security attacks pose a threat to data providers if their customers' personal information is shared. The problem can be solved by protecting the holders' data while yet providing it to the user with all relevant information. Provided data, such as hospitals, can instead trade trained models just with the requester.

RESULTS AND DISCUSSION

PYTHON was used to carry out the employment of the suggested model. The computer has an Intel CPU, 8 GB of RAM, and Windows 10, among other features. The proposed model was evaluated with respect to its precision, sensitivity, and generalizability. Existing models were compared with the proposed framework. In the paragraph that follows, we will discuss the criteria used for grading.:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (16)$$

$$Precision = \frac{TP}{TP+FP} \quad (17)$$

$$Recall = \frac{TP+TN}{TP+TN+FP+FN} \quad (18)$$

$$F1_{score} = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (19)$$

Table 1: Classifier Analysis

Methodology	Parameter Evaluation			
	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
LeNet	88.89	79.12	80.92	85.27
AlexNet	72.32	80.53	83.69	86.07
InceptionNet	81.43	82.07	90.06	89.28
ResNet	77.16	91.04	94.17	93.08
Inception-ResnetV2	**96.20**	**97.84**	**98.20**	**98.67**

In the Table 1 provided, the Classifier Analysis is characterized as follows:

In this investigation, the LeNet model achieved an accuracy of 88.89%, with a precision range of 79.12%, recall of 80.92%, and an F1-score of 85.27%. The AlexNet model achieved an accuracy of 72.32%, with a precision range of 80.53%, recall of 83.69%, and an F1-score of 86.07%. The InceptionNet model achieved an accuracy of 81.43%, with a precision range of 82.07%, recall of 90.06%, and an F1-score of 89.28%. The ResNet model achieved an accuracy of 77.16%, with a precision range of 91.04%, recall of 94.17%, and an F1-score of 93.08%. The Inception-ResNet V2 model achieved an accuracy of 96.20%, with a precision range of 97.84%, recall of 98.20%, and an F1-score of 98.67%.

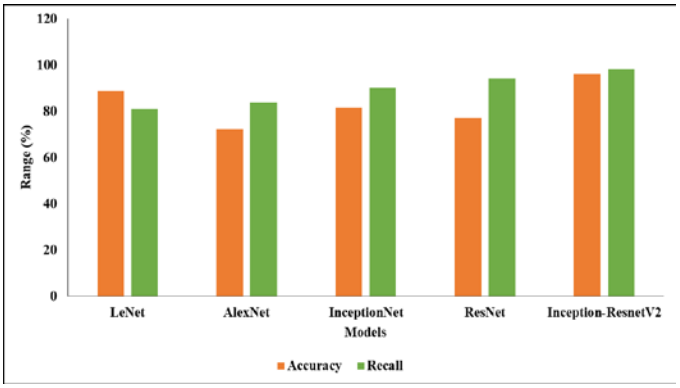


Figure 7: Graphical Illustration of projected model

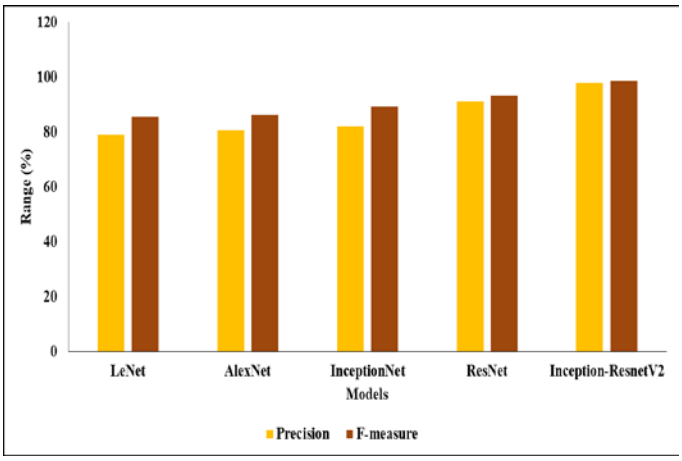


Figure 8: Analysis of different models for prediction process.

4.2. Performance Analysis for proposed encryption model

Metrics like encryption and decryption times can be used to assess the efficacy of the proposed CPABPP approach.

4.2.1 Encryption Time

Encryption Period is the time taken for transporting an input text to ciphertext.

Table 2: Encryption time comparison

Key Sizes	64	128	256	512	1024
RSA	9	100	150	410	720
Blowfish	7	10	100	220	650
CPABPP	1	2	5	80	350

In the analysis of Table 2 characterizing the Encryption time comparison: The RSA encryption time for key sizes of 128 was 9, for 256 it was 100, for 512 it was 150, for 256 it was 410, and for 1024 it was 720, respectively. The Blowfish encryption time for key sizes of 128 was 7, for 256 it was 10, for 256 it was 100, for 256 it was 220, and for 256 it was 650, respectively. The CPABPP encryption time for key sizes of 64 was 1, for 256 it was 2, for 256 it was 5, for 512 it was 80, and for 1024 it was 350, respectively.

4.2.2 Decryption Time

Decryption period is the period taken for transporting encrypted text to unique text

Table 3: Decryption time comparison

Key Sizes	64	128	256	512	1024
RSA	70	145	280	520	830
Blowfish	60	120	270	400	710
CPABPP	0	8	10	90	400

In Table 3, the Decryption time comparison is characterized as follows: The RSA model reached decryption times of 70 for key size 64, 145 for key size 256, 280 for key size 512, and 830 for key size 1024, respectively. The Blowfish model reached decryption times of 60 for key size 64, 120 for key size 256, 270 for key size

512, 400 for key size 512, and 710 for key size 1024, respectively. The CPABPP model reached decryption times of 8 for key size 64, 10 for key size 256, 90 for key size 512, and 400 for key size 1024, respectively.

CONCLUSION

When it comes to using the IoT for healthcare, privacy is one of the biggest concerns. Existing security methods are inadequate for the IoT due to its restricted resources. Threats to security and privacy are overcome by the suggested Inception-ResNet model, which incorporates a privacy preservation approach in its design. For the purpose of building a patient-control strategy utilized in electronic medical subdivisions, this research offered innovative ciphertext-policy attribute-keys. Researchers and scientists dealing with private healthcare data in distributed computing environments may find this study valuable. The suggested model achieves competitive performance by making use of both strategies, but at the cost of major trade-offs in execution time and client count. Using both encrypted and plain data, the classification metrics (accuracy, F1, precision, and recall) achieve over 96% in every scenario. The aforementioned studies show that there is a wide range in image quality both within and across categories. It's easy to confuse one for the other during the identification phase. Therefore, additional improvements to the recognition accuracy can be achieved through appropriate data augmentation and other methods in future studies.

CONFLICT OF INTEREST

Authors declare that there is no conflict of interest (financial or academic) for publication of this work.

REFERENCES

1. Q.X. Huang, W.L. Yap, M.Y. Chiu, H.M. Sun. Privacy-Preserving Deep Learning With Learnable Image Encryption on Medical Images. *IEEE Access* **2022**, 10, 66345–66355.
2. M. Alawad, H.J. Yoon, S. Gao, et al. Privacy-Preserving Deep Learning NLP Models for Cancer Registries. *IEEE Trans. Emerg. Top. Comput.* **2021**, 9 (3), 1219–1230.
3. S. Kumari, E. Ranjith, A. Gujjar, S. Narasimman, H.S. Aadil Sha Zeelani. Comparative analysis of deep learning models for COVID-19 detection. *Glob. Transitions Proc.* **2021**, 2 (2), 559–565.
4. M.V. Rao, Y. Sreeraman, S.V. Mantena, et al. Brinjal crop yield prediction using shuffled shepherd optimization algorithm based ACNN-OBDLSTM model in smart agriculture. *J. Integr. Sci. Technol.* **2024**, 12 (1).
5. D.K. Sharma, M. Chatterjee, G. Kaur, S. Vavilala. Deep learning applications for disease diagnosis. *Deep Learn. Med. Appl. with Unique Data* **2022**, 31–51.
6. M. Field, D.I. Thwaites, M. Carolan, et al. Infrastructure platform for privacy-preserving distributed machine learning development of computer-assisted theragnostics in cancer. *J. Biomed. Inform.* **2022**, 134, 104181.
7. J. Zhou, S. Chen, Y. Wu, et al. PPML-Omics: a Privacy-Preserving federated Machine Learning system protects patients' privacy from omic data. *bioRxiv*. 2022.
8. F. Zerka, S. Barakat, S. Walsh, et al. Systematic Review of Privacy-Preserving Distributed Machine Learning From Federated Databases in Health Care. *JCO Clin. Cancer Informatics* **2020**, 4 (4), 184–200.
9. Y.S. Can, C. Ersoy. Privacy-preserving Federated Deep Learning for Wearable IoT-based Biomedical Monitoring. *ACM Trans. Internet Technol.* **2021**, 21 (1), 1–17.
10. H.J. Yoon, C. Stanley, J.B. Christian, et al. Optimal vocabulary selection approaches for privacy-preserving deep NLP model training for information extraction and cancer epidemiology. *Cancer Biomarkers* **2022**, 33 (2), 185–198.
11. K.K. Chennam, V. Uma Maheshwari, R. Aluvalu. Maintaining IoT Healthcare Records Using Cloud Storage. In *EAI/Springer Innovations in Communication and Computing*; Springer, Cham, **2022**; pp 215–233.
12. Z. Yue, S. DIng, L. Zhao, et al. Privacy-preserving Time-series Medical Images Analysis Using a Hybrid Deep Learning Framework. *ACM Trans. Internet Technol.* **2021**, 21 (3), 1–21.
13. D. Nisha, E. Sivaraman, P.B. Honnavalli. Predicting and Preventing Malware in Machine Learning Model. In *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*; **2019**; pp 1–7.
14. A. Thirumalraj, V.S. Anusuya, B. Manjunatha. Detection of Ephemeral Sand River Flow Using Hybrid Sandpiper Optimization-Based CNN Model. In *Innovations in Machine Learning and IoT for Water Management*; IGI Global, **2023**; pp 195–214.
15. N.S. Divya, V. Bobba, R. Vatambeti. An Adaptive Cluster based Vehicular Routing Protocol for Secure Communication. *Wirel. Pers. Commun.* **2022**, 127 (2), 1717–1736.
16. P. Kumar, R. Kumar, G.P. Gupta, et al. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *J. Parallel Distrib. Comput.* **2023**, 172, 69–83.
17. S. Selvarajan, H. Mouratidis. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Sci. Rep.* **2023**, 13 (1), 7107.
18. A. Lakhan, M.A. Mohammed, J. Nedoma, et al. DRLBTS: deep reinforcement learning-aware blockchain-based healthcare system. *Sci. Rep.* **2023**, 13 (1), 4124.
19. M.A. Mohammed, A. Lakhan, K.H. Abdulkareem, et al. Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks. *Internet of Things (Netherlands)* **2023**, 22, 100815.
20. A.P. Kalapaaking, I. Khalil, X. Yi. Blockchain-Based Federated Learning With SMPC Model Verification Against Poisoning Attack for Healthcare Systems. *IEEE Trans. Emerg. Top. Comput.* **2023**, 1–11.
21. D. Doreen Hephzibah Miriam, D. Dahiya, Nitin, C.R. Rene Robin. Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. *Intell. Autom. Soft Comput.* **2023**, 35 (2), 1889–1906.
22. I. Ahmed, A. Chehri, G. Jeon. Artificial Intelligence and Blockchain Enabled Smart Healthcare System for Monitoring and Detection of COVID-19 in Biomedical Images. *IEEE/ACM Trans. Comput. Biol. Bioinforma.* **2023**.
23. M.U. Rehman, A. Shafique, Y.Y. Ghadi, et al. A Novel Chaos-Based Privacy-Preserving Deep Learning Model for Cancer Diagnosis. *IEEE Trans. Netw. Sci. Eng.* **2022**, 9 (6), 4322–4337.
24. C. Szegedy, S. Ioffe, V. Vanhoucke, A.A. Alemi. Inception-v4, inception-ResNet and the impact of residual connections on learning. In *31st AAAI Conference on Artificial Intelligence, AAAI 2017*; Phoenix, AZ, USA, **2017**; pp 4278–4284.
25. K. He, X. Zhang, S. Ren, J. Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*; IEEE Computer Society, Las Vegas, NV, USA, **2016**; Vol. 2016-December, pp 770–778.
26. C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, Z. Wojna. Rethinking the Inception Architecture for Computer Vision. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*; Honolulu, HI, USA, **2016**; Vol. 2016-December, pp 2818–2826.
27. Y. Yu, M. Liu, H. Feng, Z. Xu, Q. Li. Split-Attention Multiframe Alignment Network for Image Restoration. *IEEE Access* **2020**, 8, 39254–39272.
28. P.-T. de Boer, D.P. Kroese, S. Mannor, R.Y. Rubinstein. A Tutorial on the Cross-Entropy Method. *Ann. Oper. Res.* **2005**, 134 (1), 19–67.