Enhancing Security of Neurological Health Information Using Cryptography in Wireless Sensor Network

Dr.R. Anurekha[1*], N. Thirugnanasambandan[2], Dr.A. Rajivkannan[3]

Abstract

Alzheimer's disease affects irreversible brain damage cells that control memory and reasoning. Owing to comparable brain patterns and pixel intensities, diagnosing Alzheimer's disease in elderly persons is challenging and necessitates a highly discriminative feature representation for classification. These representations can be learned from data using deep learning algorithms. To address these issues, previous research looks into the usefulness of rs-fMRI for multi-class classification of Alzheimer's disease and its phases, such as CN, SMC, EMCI, MCI, LMCI, and AD. To improve the image quality, some pre-processing procedures were used, including brain extraction, motion correction, intensity, normalization, spatial smoothing, high pass filtering, spatial normalizing, image registration, and 4D to 2D conversion. And then Alzheimer's disease multi stage classification was done by using Alex net and Resnet convolutional neural network. Existing research, on the other hand, hasn't concentrated on texture feature extraction. ResNet has proven to be successful in a wide range of applications, but one major drawback is that training a deeper network takes several days, making it unsuitable for real-world applications. Medical records, whether housed in health information systems, the cloud, etc. are critical. For such records, privacy and security must be ensured using encryption and authentication techniques that are not currently in use. To prevent these issues, this study used pre-processing techniques as brain extraction, motion correction, intensity, normalization, spatial smoothing, high pass filtering, spatial normalizing, image registration, and 4D to 2D conversion to improve image quality. And then texture feature extraction will be done by utilizing gray level co occurrence matrix (GLCM). Alzheimer's disease multi stage classification will be computed based on Alexnet and Googlenet models for Neuroimaging data is attained from Alzheimer's disease Neuroimaging Initiative (ADNI) dataset. And then all Medical records will be encrypted using Modified Advanced Encryption Standard (MAES) to provide security and then stored in cloud. Experiments show that the suggested model is effective with respect to encryption time, precision, recall, and accuracy.

Key Words: Alzheimer's Disease, Motion Correction, Normalization, Multi Stage Classification, Security and Modified Advanced Encryption Standard.

DOI Number: 10.14704/nq.2022.20.2.NQ22031 **NeuroQuantology 2022; 20(2):96-106**

Introduction

AD is perhaps is most frequent type of dementia and a degenerative brain disease. Dementia symptoms include memory loss and struggle in thinking, problem-solving, and language, all of which have a significant impact on the patient's everyday life. Mild cognitive impairment is a phase of Alzheimer's disease that is characterized by considerable cognitive impairment without dementia.

Corresponding author: Dr.R. Anurekha

Address: [1*]Assistant Professor, Department of Information Technology, Government College of Engineering, Erode, Tamilnadu, India; [2]Assistant Professor (Senior), Department of Computer Science & Engineering, Government College of Engineering, Erode, Tamilnadu, India; [3]Professor & Head, Department of Computer Science & Engineering, K.S.R. College of Engineering (Autonomous), Tiruchengode, Namakkal District, Tamilnadu, India.

E-mail: [1*]drranurekha@gmail.com; [2]thirugnanam.irtt@gmail.com; [3]rajiv5757@yahoo.co.in

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Received: 23 December 2021 **Accepted:** 19 January 2022

In 2020, there will be more than 5.2 million people in U.S with Alzheimer's disease, with the number rising to 13.8 million by 2050 (Thakare, P. and Pawar, V.R., (2016), Xia, Z. et al (2020)). Precise prediction and identification of Alzheimer's disease, particularly at an early warning stage like MCI, becomes a critical step in delaying or even preventing dementia. Clinicians can evaluate the anatomical and functional changes in brain linked with illness development in vivo using neuroimaging techniques. Magnetic resonance imaging (MRI), fMRI, PET, SPECT, DTI are some of the most frequently utilized modalities (Cui, R, et al (2018), Sweety, M.E. et, al., (2014)).

FMRI is an excellent imaging technique for examining interconnectedness of physically divided and functionally varied brain networks, notably in resting-state fMRI, due to its ease of use in healthcare situations. During phases of neural degeneration, the NN that is the foundation of interactive pathogenesis can hence be created. fMRI data is utilized to identify Alzheimer's disease. A network centred on every resting-state operation might well be formed by assessing the connectivity of brain network in particular brain areas, and loss of brain function among AD and healthy patients can be evaluated (Lee, Y.S., et al (2014), Chenthara, S., et al., 2019).

Recent research examines the utility of rs-fMRI for multi-class classification of Alzheimer's disease and its phases, namely CN, SMC, EMCI, MCI, LMCI, and AD. In which first performed some pre-processing methods such as brain extraction, motion correction, intensity, normalization, spatial smoothing, high pass filtering, spatial normalization, image registration, 4D to 2D conversion to enhance the image quality. And then Alzheimer's disease multi stage classification was done by using Alex net and Resnet convolutional neural network. Current studies, on the other hand, hasn't concentrated on texture feature extraction. ResNet has proven to be successful in a wide range of applications, but one major drawback is that training a deeper network takes several days, making it unsuitable for real-world applications. Medical records, whether housed in health information systems, the cloud, etc are critical. For such records, privacy and security must be ensured using encryption and authentication techniques that are not currently in use (Al Hamid, H.A., et, al., (2017), Li, H., et, al., (2017)).

To avoid these problems in this work first performed some pre-processing methods such as brain extraction, motion correction, intensity, normalization, spatial smoothing, high pass filtering, spatial normalization, image registration, 4D to 2D conversion to enhance the image quality. And then texture feature extraction will be done by utilizing gray level co occurrence matrix (GLCM). Alzheimer's disease multi stage classification will be computed based on Alex net and Google net models for Neuroimaging data is obtained from Alzheimer's disease Neuroimaging Initiative (ADNI) dataset. And then all Medical records will be encrypted using Modified Advanced Encryption Standard (MAES) to provide security and then stored in cloud.

Related Works

For learning numerous features from MR brain pictures, (Li, et al 2017) suggested a classification approach depending on a mixture of multimodel 3D convolutional networks. To begin, a deep 3D CNN is used to translate the MR image to highly compact high-level features in a hierarchical manner. T1-weighted MR brain images from ADNI collection were used to test our approach on 428 participants, including 199 AD patients and 229 normal controls (NC). The suggested technique obtains an accuracy 88.31% and an AUC 92.73 % in experiments, exhibiting good classification outcomes.

(Farooq et al 2017) suggested a DCNN-based pipeline for exploiting MRI data to diagnose Alzheimer's disease and its stages. A four-way classifier is used to distinguish between AD, MCI, LMCI, and healthy people in this study. Experimental tests were carried out on a high-performance graphics processing unit-based system utilising the ADNI database, and new state-of-the-art findings for illness multiclass classification are acquired. The suggested scheme achieves a prediction accuracy of 98.8%, which is a significant improvement over prior experiments and clearly demonstrates the efficiency of the suggested approach.

Ebrahimi-Ghahnavieh et al (2019) used deep learning approaches to identify Alzheimer's disease on MRI scans. A fundamental issue in this line of research is obtaining enough data to train a deep model. To comprehend relationship among sequences of images for every subject, propose using a RNN after CNN and making a decision depending on all input slices rather than every one of the slices. The findings indicate that using features extracted from CNN to train a RNN can increase model's overall accuracy.

Zhang et al (2017) suggested a landmark-based feature extraction technique for AD diagnosis based on longitudinal structural MR images that would not require nonlinear registration or tissue segmentation at the implementation stage and is immune to longitudinal scan differences. First, discriminative landmarks are instantaneously found from entire brain utilizing training images, and afterwards successfully localized using a fast landmark detection approach to evaluate images, all without using nonlinear registration or tissue segmentation; then, high-level statistical spatial features and contextual longitudinal features are extracted depending on those detected landmarks, which can characterize spatial structural abnormalities and longitudinal changes; and third, high-level statistical spatial features and contextual longitudinal features are extracted depending on those detected landmarks, which can characterize spatial. Lastly, employing such geographical and longitudinal data, a linear support vector machine is employed to distinguish AD or MCI participants from HCs. Studies have shown that the Alzheimer's Disease Neuroimaging Initiative dataset has improved performance and efficiency.

To describe every participant, (Liu, et al 2016) used WBHN. Depending on Automated Anatomical Labeling (AAL) atlas, every subject's entire brain is classified into 90, 54, 14, and 1 areas. The Pearson's correlation coefficient is utilized to compute the connection between every pair of regions, which is then utilized as a classification feature. Choose the features with high F- scores to decrease features' dimensionality. Lastly, then do classification using the multiple kernel boosting (MKBoost) approach. On MRI scans from ADNI database, researchers tested our suggested technique on 710 participants (200 AD, 120 MCIc, 160 MCInc, and 230 HC). experimental findings demonstrate that the suggested strategy obtains a 94.65% accuracy rate.

To handle patients' data, (Fan et al 2018) introduced MB, a blockchain-based information management system. The MedBlock distributed ledger enables for quick EMR access and retrieval in this architecture. The new consensus scheme yields EMR consensus without consuming a lot of energy or causing network congestion. In particular, MedBlock combines tailored access control techniques with symmetric cryptography to provide strong information security. MedBlock is likely to play a significant role in sharing sensitive medical information.

Garg and Sharma (2014) presented a technique that employs the RSA algorithm, the Hash function, and a variety of cryptographic tools to enhance data security in the mobile cloud. suggested framework generates superior outcomes than other current techniques, according on test findings.

Proposed Methodology

Here discusses suggested Alzheimer's disease multi stage classification in detail. Which consist of four stages first one is pre processing such as brain extraction, motion correction, intensity, normalization, spatial smoothing, high pass filtering, spatial normalization, image registration, 4D to 2D conversion, Second one is texture feature extraction utilizing GLCM, third one is Alzheimer's disease multi stage classification depending on Alexnet and Googlenet models and the fourth one is neurological medical information encryption using Modified Advanced Encryption Standard (MAES) to provide security and then this encrypted medical data will be stored in cloud. Figure 1 depicts the suggested model's architectural framework.

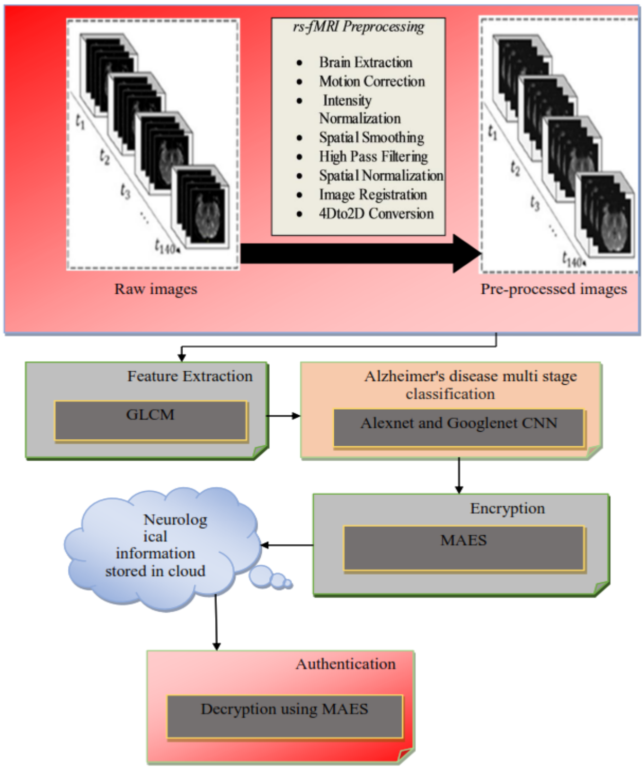

Figure 1. Overall architecture of suggested model

1. Pre-processing

This process removes noise and artefacts from data, which improves image quality and allows for improved feature extraction. The typical pipeline, which consists of several phases, is utilized to pre-process rsfMRI.

To begin, the database is transformed from DICOM to NIFTI format via Chris Rorden's conversion tools. The data is pre-processed through Functional Magnetic Resonance Imaging of the Brain (FMRIB) Software Library (FSL).

On scans, brain extraction is used to eliminate non-brain structures such neck tissues and the skull. The FSL-BET toolbox is utilised for this, that estimates intensity histogram-based threshold, centre of gravity, radius of the sphere of brain's surface to execute brain extraction. tessellated surface is started inside the brain, that gradually modifies one vertex at a time till a complete surface is produced.

After which, throughout data gathering sessions, motion correction is used to eliminate and rectify effect of participants' head movements. FSL-MCFLIRT toolbox was used to do motion correction.

The FEAT module of the FSL library is also used to fix slice timing. To perform the temporal adjustment, the slice timing correction process utilizes interpolation to convert voxel time-series forward or backward in time. For this investigation, sinc interpolation depending on Hanning windowed technique was utilized to convert voxel time series by a portion of the scanner's TR (Repetition Time) regarding middle of TR.

Data is subjected to intensity normalization to assure that every volume contains similar mean intensity. To decrease noise while preserving the underlying signal, spatial smoothing is used. Its goal is to improve signal-to-noise ratio. The magnitude of underlying signal determines level of spatial smoothing.

5 mm FWHM Gaussian kernel was used to do spatial smoothing. For this database, the kernel size selection matches to what was proposed in the literature.

rs-fMRI time series is then subjected to temporal high-pass filtering to eliminate low-frequency noise signals caused by psychological aberrations like breathing, heartbeat, or scanner drift. A temporal filter with cut-off frequency of 0.01 HZ is utilized for producing high pass filtering.

In addition, images were spatially normalised by putting them in T1 weighted space through a 7-degree-of-freedom linear transformation. pictures are registered to an MNI152 template standard space, that is a brain reference template created from the average of 152 MRI scans. A linear transformation with 12 DOF (like translation, scaling, shear, and rotation) is used to register images to MNI152 space. The FSL-FLIRT toolkit is used to accomplish spatial normalization in this work.

Pre-processed 64 64 48x 140 4D fMRI scans are acquired after using pre-processing techniques to fMRI data, with every scan containing 64 64 48 3D volumes per time course (140 s).

The image height and time axis are then translated from the 4D scans to 2D images. Per fMRI scan, this results in 6720 images of 64x64 pixels. Because initial and last three slices contains no useful information, they are eliminated. As a result, 44 slices of data from every scan are employed.

As a result, every fMRI scan yields 6160 2D images, which are stored in PNG format. Using abovementioned pre-processing techniques, data obtained from ADNI is handled and turned to 2D images, resulting in creation of a database.

2. Texture Feature Extraction Using GLCM

After pre-processing it needs to extract the features to classify the Alzheimer's disease subject from the normal one. This work uses GLCM which is helpful in estimating image characteristics associated with second-order statistics are calculated as (Mathew, A.R., et al 2017):

Energy: The uniformity shown in the mammographic image is represented by energy. The value of the mean squared signal is usually used to calculate energy (Maurya, R., et al 2014). It is calculated as follows:

$$\text{Energy} = \sum_{i,j=0}^{n-1} p(i,j)2 \qquad (1)$$

Contrast: The contrast is a measurement of the difference between lowest and highest values of a group of pixels in close vicinity. It calculates the magnitude of the image's local variations.

$$\text{Contrast} = \sum_{i,j=0}^{n-1} (i-j)^2 p(i,j) \qquad (2)$$

Correlation: Over entire image, the correlation provides an assessment of the correlation of a pixel with its neighbour.

$$\text{Correlation} = \sum_{i,j=0}^{n-I} \frac{(i \times j)p(i,j) - u_i u_j}{\sigma_i \sigma_j} \qquad (3)$$

σ2 = the difference in brightness of all reference pixels in the associations that contributed to the GLCM, calculated as follows:

$$\theta^2 = \sum_{i,j=0}^{N-1} p_{i,,j}(i-u) \qquad (4)$$

Homogeneity, Angular Second Moment (ASM): ASM utilized for measuring the homogeneity of the image

$$\text{Homogeneit} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \{p(i,j)\}^2 \qquad (5)$$

Entropy: Entropy specifies measure of irregularity or complexity existing in the image. Entropy achieves the highest value if the values of P (i, j) are assigned quite evenly throughout the entire matrix. Entropy has ahigh but inverse correlation with Energy.

$$\text{Entropy}= -\sum_{i,j=0}^{n-1} p(i,j)\log p(i,j) \quad (6)$$

Wherein 'i' specifies GLCM matrix's row, 'j' refers GLCM matrix's column, 'n' indicates number of gray levels and P(i, j) refers to cell represented by row and column of GLCM matrix. Based on these evaluations, extractions of texture features are acquired (Kumar, C., et, al., (2015), Imani, M. et, al., (2017)).

3. Alzheimer's Disease Multi Stage Classification Using Alex net and Google net based CNN

After feature extraction it might classify multi stages of Alzheimer's disease. This work uses Alex Net and Google Net based CNN for classification.

Alex Net CNN

Alex Net is a CNN which was created. Alex Net CNN was chosen because it is the most researched CNN and has a good balance of speed and accuracy. The Alex Net structure is depicted in Figure 2. Eight learnt layers, five convolutional layers, 3 fully connected layers form this model. The network's final fully linked layer connects to 1000 classes, and the remaining network is a feature extractor. For every image, Alex Net can generate a 4096-dimensional feature vector, that includes activations of hidden layer just before the output layer (Agarwal, A., et, at., (2021), Shaha, M., et, al., (2018)).

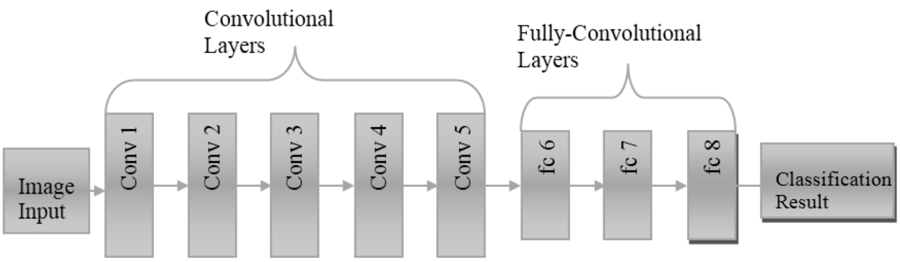

Figure 2. Alexnet Architecture

Google Net CNN: All prior CNN designs pale in comparison to the Google Net approach. Most crucially, it offers "Inception," a new module that combines filters of various sizes and dimensions to a single new filter (see Fig. 3). GoogLeNet contains nine "Inception" layers, 2 convolution layers, and 2 pooling layers. Six convolution layers with one pooling layer make up every "Inception" layer. Figure 3 is an example of a GoogLeNet "Inception" layer. GoogLeNet is the current modern CNN architecture for ILSVRC task, with a top-5 classification error of 2.4% on ImageNet challenge, contrasted to 15.3% for AlexNet (Shaha, M., et al., (2018), Khan, R.U., et, al., (2019)).

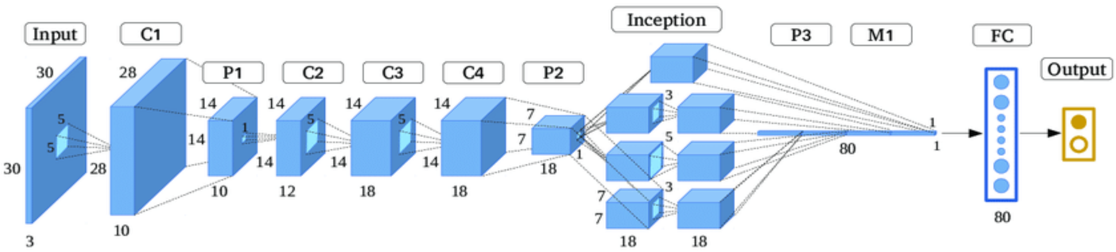

Figure 3. Googlenet Architecture

4. Key Generation Using MAES

After classification it needs to be encrypt and stored in cloud to provide security. In this work medical records like diagnostic reports, FMRI, patient name and doctor detail for which this work uses Modified Advanced Encrypted Standard (M AES).

The AES algorithm is symmetric. Based on the cypher employed, this cryptographic approach use a secret key of any size. Because it is a symmetric method, it employs similar key for encryption and decryption, keys are kept secret, making them difficult to guess by hackers. Three key sizes used by AES are 128, 192, and 256 bits, respectively. The AES

settings have been discovered to be dependent on the key size employed. Data is encrypted using different rounds, such as 10 rounds for 128 bits, 12 rounds for 192 bits, and 14 rounds for 256 bits.
Total iterations used throughout the encryption and decryption process is referred to as rounds. The optimum technique to system security has been determined to be AES.
It's crucial to note that secret key could be of any size, and in the suggested AES method, a 320-bit key is employed rather than the three other key sizes of 128, 192, and 256 bits. AES characteristics are discovered to be dependent on the key size, according to the research. To improve security, bigger key sizes are required, but AES only employs key sizes of 128, 192, and 256 bits. Figure 4 depicts the AES decryption procedure.

Drawbacks of basic AES

Basic AES uses Pseudo random number generator for key generation. But it has Lack of uniformity of distribution for large quantities of generated numbers. And Pseudo random number generators cannot be used for data encryption as the random numbers generated by them are predictable. For data encryption the numbers should be absolutely unpredictable.

Modified AES

Polybius Square is utilized to generate the key in this work to prevent these difficulties.
The number of rounds in this proposed algorithm is improved to 16, since it requires 10 rounds for a 128 bit key size. Model's safety is improved by increasing the number of rounds, which provides privacy to unauthorized users suggested table has a higher number of rounds, which aids to offer the system with increased security and good performance. Hackers will find it more difficult to penetrate the system as the number of rounds increases. It is claimed that no transformation simplification will permit the AES algorithm to be broken. As a consequence, a key size of 320 bits was utilized to achieve better outcomes.

Key Generation Process

With a 6 X 6 matrix, Polybius Square is utilized to produce the key. The Polybius square contains alphabets and digits filled with no repetition from left to right, assisting in secure transmission of data. numerals are organized from 0 to 9 in ascending order.

Table 1. Polybius square utilized for generating key

0	1	2	3	4	5	
0	A	B	C	D	Y	4
1	E	F	G	H	Z	5
2	I	J	K	L	0	6
3	M	N	O	P	1	7
4	Q	R	S	T	2	8
5	U	V	W	X	3	9

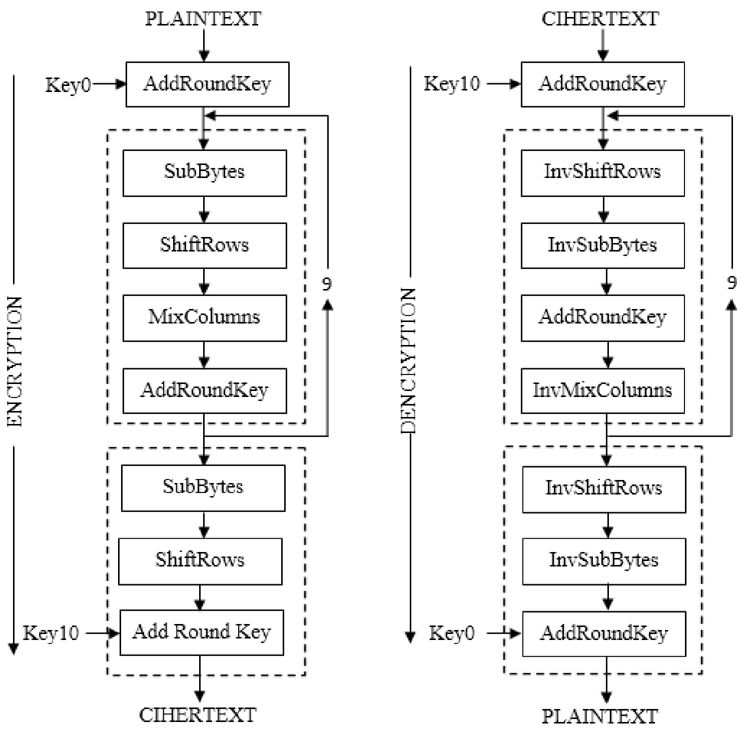

Figure 4. AES Encryption and Decryption

Modified AES Decryption Process

The technique of transforming cypher text to plain text is known as decryption. The decryption procedure occurs through transformations that correlate to the encryption transformations.

1. InvSubBytes
2. InvShiftRows
3. InvMix-Columns
4. AddRoundKey

Consider any row and column intersection (with the row first and column number second) as a depiction of alphabet or numbers to encrypt data. The encryption process involves replacing every letter with its grid coordinates (line, column). The decryption procedure is also followed. As a consequence, a key is generated for encryption and decryption process.

Algorithm Steps: give procedure were employed to encrypt a 320-bit block of data

1. From the cypher key, a set of round keys.
2. Append initial round key to beginning state array and initialize the state array.
3. Do round = 1 to 16: Perform Normal Round.
4. Carry out the last round.
5. Last Round Step's associated encryption message chunk output.

Encryption at the Patient Side

The encryption process is mentioned below steps. The four steps that make up every round are as follows:

i. Sub Bytes: The encryption site employs the first transformation, Sub Bytes. Interpret a byte as two hexadecimal digits to replace it.
ii. Shift Rows: Shift Rows is name of encryption transformation.
iii. Mix Columns: Mix Columns transformation works at column level, converting every state column to new column.
iv. Add Round Key: One column at a time, Add Round Key progresses. Add Round Key combines every state column matrix with a round key word; the action in Add Round Key is matrix addition.

Result of preceding 3 phases is XORed with 4 words from key schedule in final stage. Also, the "Mix columns" step is skipped in the last round of encryption.
By the above procedure input neurological records will get encrypted and then it will be stored in cloud.

Decryption at the Physician/ Specialist Side

Whenever the doctors need to see the medical records stored in cloud they cloud decrypts the data into plain records by using its key.

This AES decoding is refined by turning around all means of AES encryption with inversing capacities; Decryption entails applying inverse functions to reverse all of the procedures involved in encryption. a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key, d) Inverse mix columns.

Outcome of prior 2 phases is XORed with 4 words from key schedule in third stage. The "Inversemix columns" phase is not used in the final round of decryption. Then the decrypted packets are used for treatment. The designed system provide authentication between patient and doctor in health care system.

Results and Discussion

The test data of the suggested model are discussed in this section. MATLAB is used to implement a comprehensive model. In terms of encryption time, precision, recall, and accuracy, the suggested C-MAES model is contrasted with existing RSA and CALRS models for neuroimaging data acquired from ADNI dataset. Table 2 shows the rs-fMRI dataset's characteristics.

Table 2. rs-fMRI database Characteristics

Characteristic	Description
Acquisition Scanner	Philips Medical systems
EPI	140 scans/volume
Field strength	3.0
Flip angle	80 degree
TE = 30.001	30.0001
Width, Height	64,64
Number of slices	6720
Pixel spacing	3.3125
Slice thickness	3.313
Format	DICOM

Experimental Metrics

1) Precision

Precision refers to the proportion of outcomes which are appropriate and described as

$$\text{Precision}=\frac{\text{Truepositive}}{\text{truepositive+falsepositive}} \quad (7)$$

2) Recall

The suggested system's recall is described as the proportion of total relevant results properly classified by the suggested method.

$$\text{Recall}=\frac{\text{Truepositive}}{\text{truepositive+FalseNegative}} \quad (8)$$

3) Accuracy

The measure utilized to evaluate classification models is accuracy. Unofficially, accuracy refers to the percentage of correct predictions made by this model. The below is the proper statement of accuracy:

$$\text{Accuracy}=\frac{\text{Truepositive+TrueNegative}}{\text{Total}} \quad (9)$$

4) Encryption Time

The throughput of any encryption operation is computed by dividing Total Encrypted Plaintext (TEP) (in bytes) by the Execution Time (ET) (in ms).

$$\text{ET}= \frac{TEP}{ET} \quad (10)$$

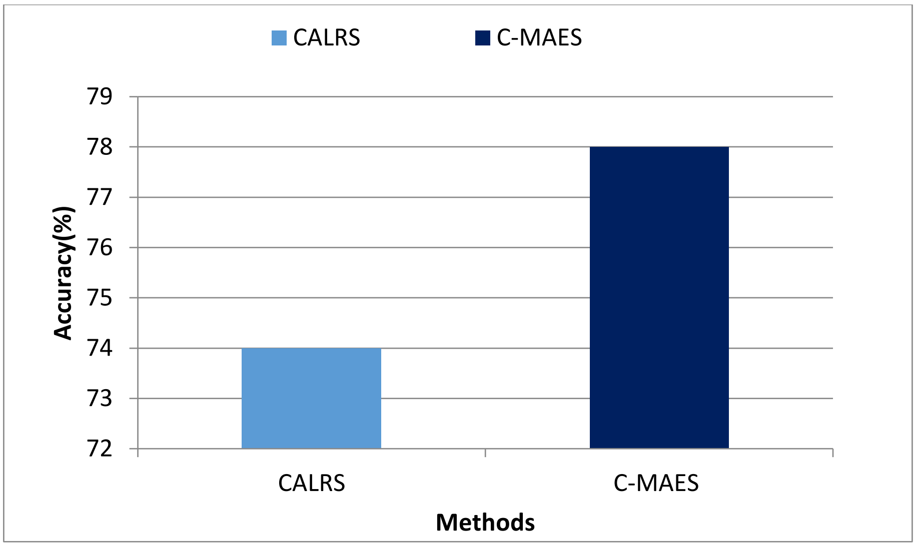

Figure 5. Accuracy vs. classification Algorithms

The above graph compares the performance of Accuracy metrics using the present CALRS and the new C-MAES technique. Various techniques are depicted in the X-axis, while accuracy levels are indicated in the Y-axis. As can be seen from the data, the newly proposed C-MAES model yielded higher accuracy results of 78 %, whereas the existing CALRS technique yielded just 74 %.

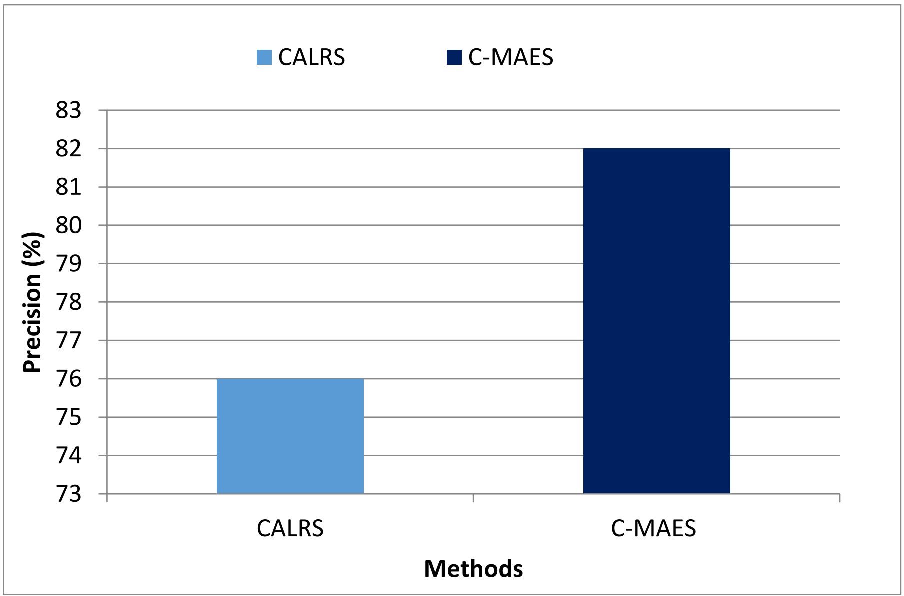

Figure 6. Precision results Comparison of Various Classifiers

From the above figure, the efficiency of the suggested C-MAES is demonstrated by comparing it to the existing CALRS approach with respect to precision. In the graph above, various techniques are depicted along X-axis, while precision are indicated along Y-axis. As can be seen from the findings, the newly introduced C-MAES model achieved precision outcomes of 82 %, while the existing CALRS technique yielded just 76%.

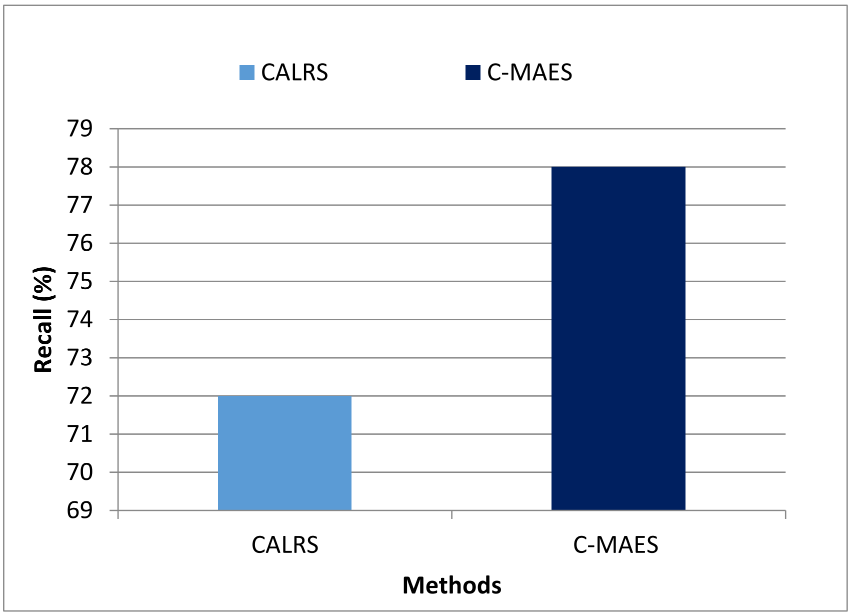

Figure 7. Recall vs. classification approaches

Figure:7. Shows Performance comparison for existing C-MAES classifier and proposed CALRS scheme with respect to recall. In the graph above, different approaches are depicted along X-axis, while recall are represented along Y-axis. As can be seen from the data, the newly presented C-MAES model has a greater memory rate of 78 %, whereas existing CALRS techniques only have a recall rate of 72 %.

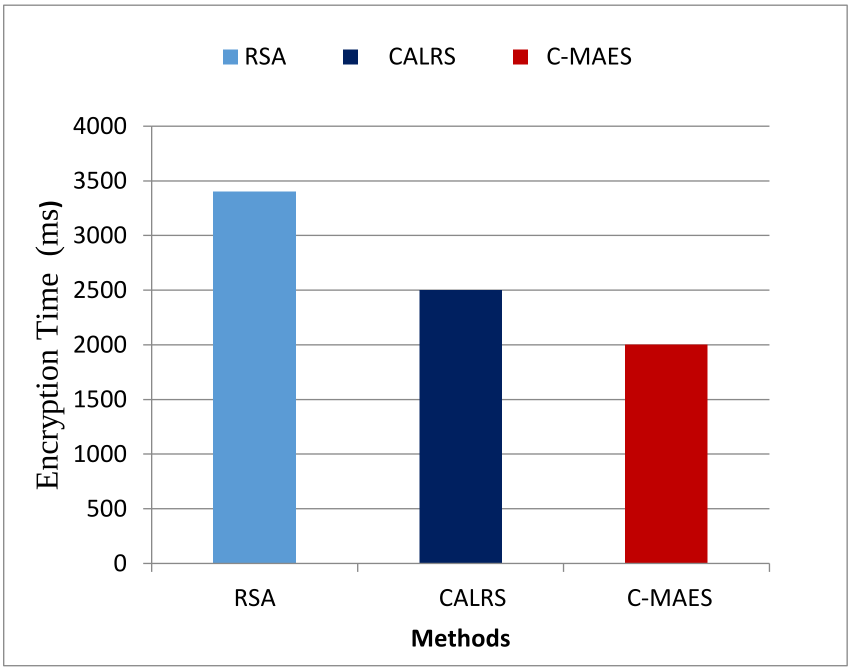

Figure 8. Encryption time (ms)

Efficiency of the proposed C-MAES method is shown via comparing this with the existing RSA and CALRS methods in terms of encryption time (ms) from the figures approaches are plotted against X-Axis and encryption times are taken as Y. Through outcomes it is indicated that suggested C-MAES method consumes 2000(ms) lower encryption time whereas existing RSA and CALRS methods consumes 3400(ms) and 2500(ms) respectively.

Conclusion and Future Work

Electronic Medical Record (EMR) systems are replacing paper-based records in the health-care industry. Health services can be delivered more quickly using EMR, however privacy, security, and data storage will be issues. In this work image quality is improved by pre-processing based on brain extraction, motion correction, intensity, normalization, spatial smoothing, high pass filtering, spatial normalization, image registration, 4D to 2D conversion. Grey level co occurrence matrix is employed for texture feature extraction. Alexnet, Googlenet based CNN models is used for Alzheimer's disease multi stage classification through resting state FMRI data. Then all Medical records will be encrypted using Modified Advanced Encryption Standard (MAES) to provide security and then stored in cloud. The same key is employed for decryption. The suggested approach minimizes the encryption time compared to other current models, according to empirical observations. However, FMRI data which is used for this work has more dimensions and it reduces the classifier performance so future work could use feature selection models.

References

Thakare P, Pawar VR. Alzheimer disease detection and tracking of Alzheimer patient. *In International Conference on Inventive Computation Technologies (ICICT)* 2016; 1: 1-4.

Xia Z, Yue G, Xu Y, Feng C, Yang M, Wang T, Lei B. A novel end-to-end hybrid network for Alzheimer's disease detection using 3D CNN and 3D CLSTM. *In IEEE 17th International Symposium on Biomedical Imaging (ISBI)* 2020: 1-4.

Cui R, Liu M, Li G. Longitudinal analysis for Alzheimer's disease diagnosis using RNN. *In IEEE 15th International Symposium on Biomedical Imaging (ISBI 2018)* 2018: 1398-1401.

Sweety ME, Jiji, GW. Detection of Alzheimer disease in brain images using PSO and Decision Tree Approach. *In IEEE International Conference on Advanced Communications, Control and Computing Technologies* 2014: 1305-1309.

Lee, YS, Alasaarela E, Lee, H. Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system. *In The International Conference on Information Networking 2014 (ICOIN2014)* 2014: 453-457.

Chenthara S, Ahmed K, Wang H, Whittaker F. Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access* 2019; 7: 74361-74382.

Al Hamid HA, Rahman SMM, Hossain MS, Almogren A, Alamri A. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access* 2017; 5: 22313-22328.

Li H, Yang Y, Dai Y, Yu S, Xiang Y. Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data. *IEEE Transactions on Cloud Computing* 2017; 8(2): 484-494.

Li F, Cheng D, Liu M. Alzheimer's disease classification based on combination of multi-model convolutional networks. *In IEEE international conference on imaging systems and techniques (IST)* 2017: 1-5.

Farooq A, Anwar S, Awais M, Rehman S. A deep CNN based multi-class classification of Alzheimer's disease using MRI. *In IEEE International Conference on Imaging systems and techniques (IST)* 2017: 1-6.

Ebrahimi-Ghahnavieh A, Luo S, Chiong R. Transfer learning for Alzheimer's disease detection on MRI images. *In IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)* 2019: 133-138.

Zhang J, Liu M, An L, Gao Y, Shen D. Alzheimer's disease diagnosis using landmark-based features from longitudinal structural MR images. *IEEE journal of biomedical and health informatics* 2017; 21(6): 1607-1616.

Liu J, Li M, Lan W, Wu FX, Pan Y, Wang J. Classification of Alzheimer's disease using whole brain hierarchical network. *IEEE/ACM transactions on computational biology and bioinformatics* 2016; 15(2): 624-632.

Fan K, Wang S, Ren Y, Li H, Yang Y. Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems* 2018; 42(8): 1-11.

Garg P, Sharma V. An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function. *In International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)* 2014: 334-339.

Mathew AR, Anto PB, Thara NK. Brain tumor segmentation and classification using DWT, Gabour wavelet and GLCM. *In International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* 2017: 1744-1750.

Maurya R, Singh SK, Maurya AK, Kumar A. GLCM and Multi Class Support vector machine based automated skin cancer classification. *In International Conference on Computing for Sustainable Global Development (INDIACom)* 2014: 444-447.

Kumar C, Chauhan S, Alla RN. Classifications of citrus fruit using image processing-GLCM parameters. *In International Conference on Communications and Signal Processing (ICCSP)* 2015: 1743-1747.

Imani M, Montazer GA. GLCM features and fuzzy nearest neighbor classifier for emotion recognition from face. *In 7th International Conference on Computer and Knowledge Engineering (ICCKE)* 2017: 8-13.

Agarwal A, Patni K, Rajeswari D. Lung cancer detection and classification based on alexnet CNN. *In 6th International*

Conference on Communication and Electronics Systems (ICCES) 2021: 1390-1397.

Shaha M, Pawar M. Transfer learning for image classification. *In second international conference on electronics, communication and aerospace technology (ICECA)* 2018: 656-660.

Khan RU, Zhang X, Kumar R. Analysis of ResNet and GoogleNet models for malware detection. *Journal of Computer Virology and Hacking Techniques* 2019: 15(1): 29-37.

Ibrahim, Y, Wang, H, Adam, K. Analyzing the Reliability of Convolutional Neural Networks on GPUs: GoogLeNet as a Case Study. *In International Conference on Computing and Information Technology (ICCIT-1441)* 2020: 1-6.