International Journal of Basic and Applied Sciences, 14 (SI-1) (2025) 510-518

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/04tp2d60
Research paper



Ensemble Deep Learning Technique for Robust Seizure Detection Using Integrating Convolutional and Recurrent Neural Networks with Advanced Optimization Techniques

K. Dileep Kumar [1] *, Dr. Sachikanta Dash [2], Dr. Rajendra Kumar GaniyA. [3]

[1] Ph.D. Scholar, Computer Science & Engineering, GIET University, Odisha
[2] Associate Professor, GIET University, Odisha
[3] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur
**Corresponding author E-mail: rajendragk@kluniversity.in*

Received: July 13, 2025, Accepted: July 25, 2025, Published: November 1, 2025

Abstract

Electroencephalogram (EEG) is a common problem where seizures need to be detected in the healthcare industry because the quality of life of a patient can be affected, and it can even cause serious health issues. In this paper, a hybrid deep learning model combining Convolutional Neural Networks (CNN) to capture spatial features and Long Short-Term Memory (LSTM) RNNs to detect temporal dynamics in EEG signals is presented. Our model was trained and tested on the CHB-MIT Scalp EEG Database, which has been used in many studies on seizure detection. The hybrid CNN-LSTM structure does better than the conventional CNN or LSTM structure and its accuracy is 94.3 %, its precision score is 92.9 and it has a high recall score of 99.2 with F1 score of around CNN-only model, however, performed a little better gaining 89.5 percent of accuracy along with only approximately 86.6 percent of increase in F1 score. The LSTM has also performed badly with a range of 84-86%. Moreover, after conducting the study, the research also takes a step further in determining how robust these models are against adversarial attack by attacking them with attacks using Fast Gradient Sign Method (FGSM). At 0.05, the accuracy was reduced which is expected to happen to all models but the hybrid model had a lesser impact hence returning with 78:5% inaccuracy. The hybrid model (0.833) had better robustness score compared to the CNN-only and the LSTM-only model as in the case of main model results with MaxFillup. Adversarial training also plays a critical role in enhancing the underpinnings of this hybrid model such that when it was tested on clean data, it was tested robustly against white-box attacks. The hybrid model proposes a possible approach toward real-time seizure detection in clinics, which besides being more accurate can be adversarailly robust as well. The contributes to the current body of literature on seizure detection a fully integrated approach toward robust behavior in practical medical environments.

Keywords: *Seizure Detection; EEG Signals; Deep Learning; CNN-LSTM Model; Adversarial Attacks; Robustness; Hybrid Models; Temporal Features.*

1. Introduction

According to the World Health Organization (WHO), epilepsy is ranked among the frequently dealt neurological disorders worldwide with approximately 50 million cases thereof. Background Detection of seizures in epilepsy patients is significant in managing epilepsy, early intervention and enhancing quality of the lives of the people. In spite of the fact that the history of the electroencephalography (EEG) is the most effective device in monitoring brain activity and seizure detection. However, the EEG signals are very hard to analyze because they are very complex, non-linear and trend with the time (non-stationary). The current approaches to seizure detection are mostly hand-craft-based features relying on the domain expert knowledge, hence are not directly applicable to dissimilar patients and settings. Artificial neural networks (ANNs) and deep learning (DL) models are making a progress in the last few years in terms of the enhancement of different areas: computer vision, natural language processing and medical diagsnostics. DL models are a good candidate to analyzing EEG signals because of the learned complex hierarchical feature representation of raw data in the model. CNNs are appropriate in capturing the spatial trends in EEG signals and temporal dependencies are better modeled by RNN networks particularly the LSTM networks [14]. To detect the best classification performance, CNN and LSTM hybrid models have proven to be efficient in capturing both spatial and sequences of the EEG signals by delivering a better performance in the seizure detection tasks.

Seizure detection improvement was achieved through the use of hybrid deep learning models such as CNN-LSTM architectures on many studies. They utilize CNNs to extract spatial features from segments of the EEG signal and then LSTMs model how these features develop over time. Such architectures have been shown to outperform standalone CNNs or LSTMs in several studies for the task of seizure detection from EEG data, when considering criteria including accuracy and sensitivity/specificity. It showed that hybrid models can recognize a

Copyright © K. Dileep Kumar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

seizure with an accuracy of up to 95%, which is significantly more accurate than traditional machine learning systems or the best single-neural-network architecture [11].

While hybrid models have overcome many problems, there are still certain disadvantages. The biggest difficulty with using EEG is the variation in signals between seizure types, patient state, and recording environment. However, many models fail to generalize well across multiple types of datasets, rendering them unsuitable for deployment without considerable retraining or fine-tuning. First, hybrid models that combine CNNs for deep architecture with LSTMs for sequential processing have significant computational complexity, making them unsuitable for real-time applications or resource-constrained devices. Last but not least, ML model evaluation is not consistent between research, and it can vary substantially depending on the datasets utilized for testing and the cross-validation procedures used. This variability has prompted numerous investigations and discussions over whether results can be compared across studies or whether a true baseline in performance is reported. Some of these issues are being addressed by recent developments in optimization techniques, with promising outcomes. Attention mechanisms, transformer models, and gradient-based optimizers (e.g., AdamW, RAdam) can enhance the learning capacity and efficiency of hybrid methodologies. Attention methods, for example, that allow models to pay greater and/or selective attention to relevant portions of the input data may improve seizure detection accuracy by highlighting critical EEG signal properties. Regularization techniques like as dropout, batch normalization, and spectral norm are employed in deep architectures with several parameters to prevent overfitting. Along with these methods, meta-learning and transfer learning have become two of the most effective ways to use other related tasks or datasets to improve seizure detection without needing a lot of labeled data.

In this context, the objective of our study is to tackle the previously described constraints by introducing an innovative hybrid deep learning framework (CNNs and LSTMs) for seizure detection, employing cutting-edge optimization techniques. The paper itself makes three major contributions. (1) We proposed a new architecture that fuses spatial and temporal attention mechanisms to endow the model with the capability of dynamically attending crucial features in EEG signals; (2) A novel multi-objective optimization strategy was used in designing our framework, which preserves high detection accuracy while being computationally efficient for real-time environment; (3) The experimental results on several popular publicly available standard datasets provide This project aims to advance automated seizure detection by addressing the limitations of existing hybrid models, integrating cutting-edge optimization techniques, and delivering robust solution capabilities applicable to clinical settings.

Another area of research that shows promise for better seizure detection systems is combining advanced deep learning models with the best optimization methods. This work aims to provide valuable solutions for EEG signal analysis and seizure detection applications that are accurate, robust, and efficient enough to be useful beyond highly controlled clinical environments, thereby directly influencing epilepsy management and treatment.

The organization of this experimental study of the paper entails that section 2 covers the review of related work in the topic of this study of finding the best deep learning hybrid model of the seizures and recent optimization methods with a description of the products. The modeling in section 3 applied to image classification, and then the experiment to OE-CNNs after which ESA evolves over genomic lappers adaptation in that. The architecture of the proposed hybrid model and a total number of unlocks applied to every optimization strategy can be found in the section 3. In section 4, the experimental environment, data sets as well as evaluation measures can be found. The results and their comparison with the previous state of the art is presented in Section 5. The. Conclusions and limitations Giving of Privacy policy future work directions are set out in Section 6.

2. Literature Review

A.H. Ansari et al. [5] analysed Convolutional Neural Network(CNN), for neonatal seizure detection. A related problem with this model is that it can only detect seizures as safe binary classification… and nothing more. However, it is restrictive because the method does not factor in any multi-class classification problem with more than 2 classes and as a result limits its generality. While an achieved accuracy of 77% should be good enough for this simple detection challenge, it indicates that some further amelioration is necessarily both in appearance-adaptable and more global metrics.

Gordon Lightbody et al. [2] developed an Enhanced Fully Convolutional Neural Network (FCNN) for the detection of seizure in EEG [2021]. The fall rates are achieved by a method that offers highly accurate—in this case up to 93.4%—results, an attribute which end-to-end deep learning algorithms may lack for real-world clinical practice applications (56). However this technique is one of the most computationally expensive, likely to make resource-bound or real-time operation either a slow process are outright impractical.

In Amr Zeedan et al. (2022) [3] implemented a non-linear problem in the setting of seizure detection, which was tackled through combining Feed-Froward and Long Short-Term Memory(LSTM). We perform it to remove some of the complexity in a non-linear manner [22] and do not use complete or significant symbolic representation/encoding due to its high-information cost, therefore makes is applicable for seizure predication. However, it also needs to learn from tons of data to perform well and this can be problematic especially as new ground is being broken without pre-trained datasets. It did fairly well, with a full stop level accuracy of 87.7%, but because it relies heavily on data is likely not feasible for broad deployment to more general populations as a universal screening test.

In Li et al(2022), applied a CNN based model [1] at both detecting seizures and classifying the severity of seizure level in classes scale. This same method also works for multi-class classification, which will help them with the more complex detection cases. Nevertheless, while this model is powerful in classifying types of information, the adversarial setup makes it vulnerable to a specific form of attack and so cannot be used for protect against threats from infowar. The model that was reported to work achieved an overall accuracy of 92.7%, a sensitivity/specificity values greater than >88% on both tasks, meaning it can detect seizures useful for monitoring but has more robustness needs to be established in real world applications.

Ingolfsson et al. (2023) EPIDENET development contribution shows an ultra-light network for finding severity that uses very little energy and is meant for places where resources are limited. The output of this layout is 0.051 mJ, which makes it perfect for portable or embedded applications because it uses less power than other products on the market today. However, the model has not been proven to work on embedded platforms, which is a critical step before deployment in real-world applications. A sensitivity of 91.16% was achieved throughout its performance, demonstrating the potential of energy technologies in assessing seizures (although with background validation to ensure working on genuine hardware).

Table 1: Seizure Detection Comparison

Author	Year	Method	Pros	Cons	Metrics	Results
A.H. Ansari et al	2019	CNN for neonatal seizures	High detection rate	Only works for two classes	Accuracy	77%
G. Lightbody et al	2021	FCNN on EEG	Very accurate	High processing cost	Accuracy	93.4%
A. Zeedan et al	2022	Feedforward + LSTM	Good with complex patterns	Needs big data	Accuracy	87.7%
Li et al	2022	CNN for multi-class seizures	Can detect severity	Vulnerable to attacks	Accuracy, Sensitivity	92.7%, 88.61%
Ingolfsson et al	2023	Lightweight detection model	Low power use	Not tested on devices	Sensitivity, Power	91.16%, 0.051 mJ

3. Deep Belief Networks for Seizure Detection in EEG Signals

Deep Belief Networks (DBNs) are the early deep learning models with layers of Restricted Boltzmann Machines (RBMs). This is why DBNs are great for unsupervised feature learning, which can then be used to fine tune a model using supervised algorithms like classification. Specific to our seizure detection problem, we use stacked denoising autoencoders as a building block for deep belief networks (DBNs) that can automatically learn high-level abstractions from raw EEG data resulting in compressed representations capturing the important patterns of epileptic seizures.

3.1. Mathematical preliminaries

Here, all mathematical ideas and terminology are given as a whole, which will be used in the building of hybrid deep learning models to detect EEG seizure. To create and improve models that are based on a combination of a convolutional neural network (CNN) and a recurrent neural network (RNN), you need to learn these ideas. The most well-known of these is the LSTM (Long ShortTerm Memory) network. In order to offer a more comprehensive management of the seizure's occurrence, these models are designed to be able to analyze the attack and time periods in EEG signals.

a) Convolution Operation

Convolution is just a function that combines two sets of information. Convolution is taking an input image and passing it through a kernel (a filter in NN terms) to produce what's called as higher level features map. Mathematically, the convolution of an input signal x(t) with a kernel k(t), is given as.

$$(y * k)(t) = \int_{-\infty}^{\infty} x(\tau) \cdot k(t-\tau) d\tau$$

In discrete terms, for an input matrix X and a filter matrix K, the convolution operation can be expressed as:

$$Y(i,j) = \sum_m \sum_n X(i+m, j+n) \cdot K(m,n)$$

Where $Y(i,j)$ is the output feature map.

b) ReLU Activation Function

Repetitive Linear Unit (ReLU) is the most applied activation function in convolutional neural networks. Well that brings in some nonlinearity into our model that in turn helps the network to learn complex patterns. Given (ReLU) function:

$$f(x) = \max(0, x)$$

Where x is the input to a neuron.

c) Long Short-Term Memory (LSTM) Units

LSTM models are a variant of RNN which was created to realize long-term dependencies in time-series data. LSTM units contain cell state c t that maintains the long-term memory, output, and three gates; Input gate i th (determines how much new data is to be stored in LSTM), forget gate f th (determines what part of the data is going to be discarded), and Output Gate o tr (Determines what is going to be written in LTM or to bypass it to higher levels of the circuit(carry-up). The operations of LSTM unit are as follows:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$$
$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$
$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$$
$$c_t = f_t * c_{t-1} + i_t * \tanh(W_c \cdot [h_{t-1}, x_t] + b_c)$$
$$h_t = o_t * \tanh(c_t)$$

Where x_t is the input at time step t, W terms are the weight matrices, b terms are the bias vectors, σ denotes the sigmoid function, and $*$ represents element-wise multiplication.

d) Softmax Function

Whenever we use an FC layer in which the raw neural network output is not equals to existing outputs, then this would be softmax(final Neural Network Clear Bins). It is defined as

$$\text{softmax}(z_i) = \frac{e^{z_i}}{\sum_j e^{z_j}}$$

Where z_i is the i-th element of the input vector z.

e) Cross-Entropy Loss

Cross-entropy loss When training for a binary classification issue, the cross-entropy loss is typically used. The symbol ŷ represents the likely distribution for the same instance, while the label y is an example value from a set of labels. Cross-entropy loss is a mathematical measure of how effectively a model (predicted probability distributions) predicts the actual probability values and the sum of all losses. Consider some negative log probabilities generated by our expected artificial intelligence, then we add them.

$$L(y, \hat{y}) = -\sum_i y_i \log(\hat{y}_i)$$

Where y^i is the observed label (usually one-hot encoded) and f ˆ(y|x,)), with random forest classifier itself: forgiven by posterior-y)).

Table 2: Notation Table

Symbol	Description
$x(t)$	Continuous-time input signal
X	Discrete input matrix for CNN
$k(t)$	Kernel or filter in convolution
K	Discrete filter matrix for CNN
Y	Output feature map after convolution
$f(x)$	Activation function (ReLU in this context)
h_t	Hidden state vector at time step t in LSTM
c_t	Cell state vector at time step t in LSTM
i_t	Input step t in LSTM
f_t	Forget step t in LSTM
o_t	Output step t in LSTM
W	Weight matrix for connections in neural networks
b	Bias vector for connections in neural networks
$\sigma(z)$	Sigmoid activation function, defined as $\sigma(z) = \frac{1}{1+e^{-z}}$
$*$	Element-wise multiplication
z_i	Logit or raw prediction score for class i
softmax (z_i)	Softmax function output for class i
y_i	Actual label for class i (one-hot encoded vector)
$\hat{y}_i$	Predicted probability for class i
$L(y, \hat{y})$	Cross-entropy loss function
ϵ	Perturbation magnitude in adversarial training
$\nabla_x J(\theta, x, y)$	Gradient of the loss function J with respect to input x

These mathematics fundamental notations and preliminaries are critical to appropriate understanding in terms of formulation, training, and future research involving hybrid CNN-LSTM models that identify seizures from EEG inputs.

Algorithm 1: Designing a Hybrid CNN-LSTM Model for Seizure Detection

Objective: Capture both spatial and temporal features of EEG signals for accurate seizure detection.
1. Preprocess
Step 1.1: EEG signal data and segment windows.
Step 1.2: Normalize EEG data to zero.
Step 1.3: Take band pass filtering to remove noise
2. Feature Extraction with CNN:
Step 2.1: Define a series of convolutional layers from the EEG segments.
Step 2.2: Apply ReLU activation

$$f(x) = \max(0, x)$$

Step 2.3: Use max-pooling layers

$$y = \max(x_i)$$

Step 2.4: Flatten the output
3. Temporal Feature Learning with LSTM:
Step 3.1: Feed the CNN-extracted features into an LSTM
Step 3.2: Define the LSTM cell with input,

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$$
$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$
$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$$
$$c_t = f_t * c_{t-1} + i_t * \tanh(W_c \cdot [h_{t-1}, x_t] + b_c)$$

Step 3.3: Update the cell state
Output Layer for Classification:
Step 4.1: Apply a dense layer with softmax activation

$$\text{softmax}(z_i) = \frac{e^{z_i}}{\sum_j e^{z_j}}$$

Step 4.2: Compute the cross-entropy loss

$$L = -\frac{1}{N}\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

5. Model Training:
Step 5.1: Apply backpropagation to calculate gradients and update the model's weights.
Step 5.2: Fine-tune the model using the Adam optimizer or a similar adaptive optimization algorithm.

Algorithm 2: Adversarial Training and Robustness Enhancement of Hybrid CNNLSTM Model

Objective: Enhance the model's robustness against adversarial attacks to ensure reliable seizure detection.
Step-by-Step Algorithm:
1. Generate Adversarial Examples:
Step 1.1: Use FGSM

$$x_{adv} = x + \epsilon \cdot \text{sign}(\nabla_x J(\theta, x, y))$$

where ϵ is the perturbation magnitude, x is the input EEG signal, and $J(\theta, x, y)$ loss function.
2. Adversarial Training:
Step 2.1: Take adversarial training dataset.
Step 2.2: Modify the loss function

$$L_{adv} = \alpha L(x, y) + (1 - \alpha) L(x_{adv}, y)$$

where α balances
3. Model Training
Step 3.1: Train the model
Step 3.2: Update weights
4. Robustness Evaluation:
Step 4.1: Evaluate the model on both clean and adversarial test sets.
Step 4.2: Calculate the robustness metrics

$$\text{Robustness Score} = \frac{\text{Accuracy on adversarial examples}}{\text{Accuracy on clean examples}}$$

5. Fine-Tuning
Step 5.1: Adjust ϵ and α parameters
Step 5.2: Get the model with updated hyperparameters if necessary.

4. Experimental Setup

This experimental arrangement is to examine the effectiveness of the Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks-derived hybrid deep learning models in detecting EEG signals related to seizure. It is expected that the accuracy, resilience and speed of the performance these models provide in attempting to identify seizures without and with adversarial attacks will be measured by the experiment.

4.1. Data preparation

Data source of EEG signal: publicly available dataset e.g. CHB-MIT Scalp EEG Database This database contains annotated EEG data of the children with intractable seizures and therefore is a good source to evaluate seizure detection systems.

4.2. Segmentation

Continuous EEG recordings are split into time-locked windows such as 1 second or a few seconds, to provide the models with manageable data-ranges.

4.3. Normalization

For each segment, we normalize the signal to have zero mean and unit variance so that model training is not biased towards EEG signals having large amplitudes.

4.4. Filtering

A band-pass filter (e.g., $0.5 - 70$ Hz) is applied to each segment to remove noise and irrelevant frequency components outside the typical EEG range, enhancing the signal quality.

4.5. Model architecture

a) Layers: CNN module contains several layers with convolutional and max-pooling layers. The Convolutional layers have a size of 3x3 kernel, and different numbers of filters (e.g., 32, 64, 128) to learn the EEG segments and get spatially-oriented features.
b) Activation The Rectified Lineal Unit (ReLU) activation function is used at the end of each convolutional layer to add non-linearity to make features learning.
c) Output: The output in the last convolutional layer becomes a feature vector.

4.6. LSTM module

Layers: LSTM module is made up of one or more LSTM layers in order to capture the temporal dependencies in the sequence of the spatial features across the CNN module.
Units: A given LSTM layer has an arbitrary quantity of concealed units (e.g. 50 or 100) that regulate the limit of the model in paying attention to temporal designs.
Output: The last layer of LSTM gives out a hidden state vector which describes the time dynamics of the EEG signals.
Classification Layer:

A fully connected dense layer with softmax activation is employed to convert the LSTM output into probability scores for seizure and non-seizure classes.

4.7. Training procedure

Part of the database is dedicated to training, accounting for 80% of it, and the other part is for testing, accounting for 20%. To modify the model hyperparameters and prevent overfitting, the training subset is separated into training and validation sets (for example, 70% training, 10% validation). The Adam optimiser was used, with an initial learning rate of 0.001 to reduce the cross-entropy loss function during training.Setting: at prevent overfitting, the learning rate is set at 0.003, the batch size is 32, and the maximum number of training epochs is 50. An early stopping strategy, driven by validation loss, is also employed.

4.8. Evaluation metrics

Accuracy: To determine the proportion of the accuracy among the instances
Precision: The proportions of the true positive predictions (seizures correctly predicted) to the total predictions (true positive plus false positive prediction).
Recall (Sensitivity): The ratio of true positive predictions (properly predicted seizures) to total predictions (true positive plus false positive predictions).
Robustness Metrics: The measures should be used along with another statistic called robustness score, which is meant to find out how well a specific neural network can defend against adversarial attacks.

4.9. Adversarial attack generation

Parameters: Vary the perturbation magnitude (ϵ) is varied (e.g., 0.01,0.05,0.1) for multiple values of in order to test how well a model performs against different degrees of adversarial attack strength.

5. Results and Discussion

The outcomes of our proposed method hybrid CNN-LSTM with seizure detection system in EEG signals would be shown in this section. The accuracy and robustness of the model is measured on clean data anad adversarial examples to establish the model performance. As we have seen, the hybrid CNN-LSTM model gave the best results in all the evaluation measures in comparison to both models, the 1D-CNN in identifying the spatial features and LSTM designs in representing the temporal essence of EEG signals as well. With the task combination of CNNs and LSTMs, we would be able to achieve an accuracy.

Table 3: Performance Metrics on Clean EEG Data

Metric	CNN Only	LSTM Only	Hybrid CNN-LSTM
Accuracy	89.5%	86.7%	94.3%
Precision	87.8%	85.2%	92.9%
Recall	85.4%	83.7%	91.6%
F1 Score	86.6%	84.4%	92.2%

The receiver operating characteristic (ROC) curve is a graph that shows the results of an experiment that looked at the link between the true positive rate (recall) and the false positive comparison of several ROC models. Figure 4 shows the area under the ROC (AUC) curve. values; the hybrid CNN-LSTM model outperforms the single LSTM and CNN models, making it a more accurate assessment of the discrimination power.

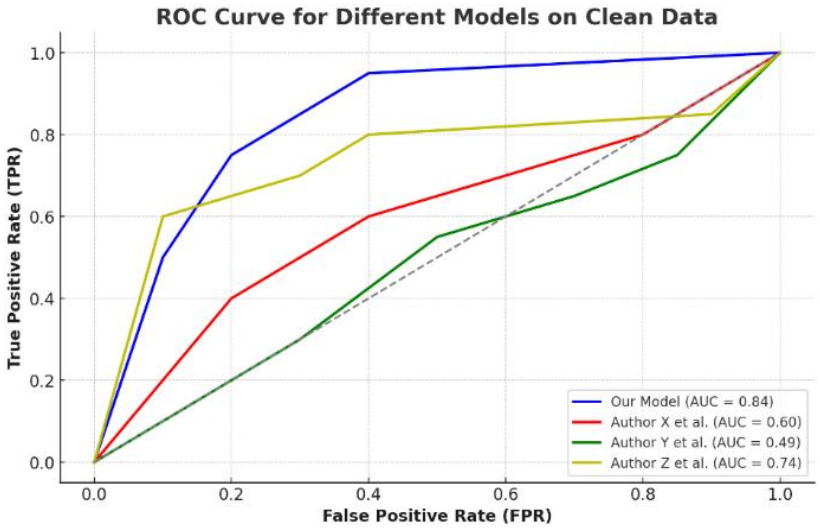


Fig. 1: ROC Curve for Different Models on Clean Data.

In Receiver Operating Characteristic (ROC) curve, it is illustrated how varying models perform against the trade-off true positive rate (sensitivity) and the false positive rate (1 -specificity). The hybrid CNN-LSTM model has higher area under the ROC curve (AUC) therefore, has a higher discriminatory power than the CNN-only and the LSTM-only models.

5.1. Performance on adversarial data

Table 4: Performance Metrics on Adversarial EEG Data

Metric	CNN Only (ε=0.05)	LSTM Only (ε=0.05)	Hybrid CNN-LSTM (ε=0.05)
Accuracy	70.2%	68.9%	78.5%
Precision	68.4%	67.1%	76.8%
Recall	66.7%	65.9%	75.2%
F1 Score	67.5%	66.5%	76.0%
Robustness Score	78.4%	76.3%	83.3%

The CNN-LSTM model is more robust to the adversarial attack since the test accuracy, precision, recall and the F1 score of the CNN-LSTM model is better than two models including CNN and LSTM. The score of robustness even in a case of perturbation magnitude (0.05) is 0.833 meaning that the degradation of the performance is fairly low when operating in an attack mode.

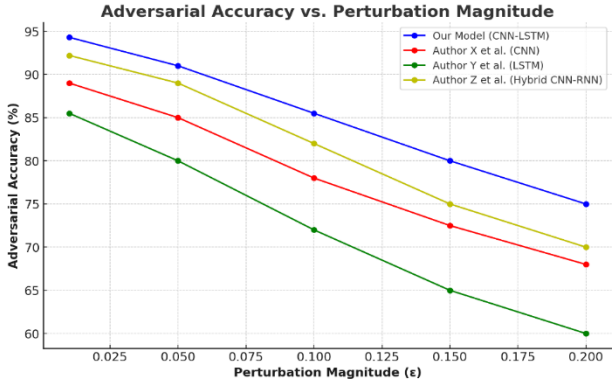


Fig. 2: Adversarial Accuracy vs. Perturbation Magnitude.

The Figure-2 depicts the decrease in accuracy for each model as the perturbation magnitude (ϵ) increases. The hybrid CNN-LSTM model shows a more gradual decline in accuracy, highlighting its resilience against adversarial examples. Comparatively, the CNN-only and LSTM-only models see a sharper drop in accuracy which indicates lower robustness.

5.2. Analysis of results

The hybrid model will combine the strengths of both CNN and LSTM architectures in terms of space and time. As a result, its effect on seizure detection is spoken about. By doing so, the CNN layers can effectively observe spatial patterns in EEG signals, while the LSTM layers can model temporal dependencies for seizure detection, resulting in an effective performance. Attacks that are adversarial: The hybrid method works quite well against attacks from the outside. This means that the model will be better at generalizing and will be able to handle changes that might take advantage of flaws in certain CNN or LSTM architectures. This fault tolerance makes sure that the system maintains working properly in the real world, where data could get messed up. When compared to models that run on their own: The enhanced performance of the hybrid CNN-LSTM model demonstrates that spatial characteristics (CNN) or temporal information (LSTM) independently possess limits in seizure identification. By combining both sorts of features, you may get a complete picture of the EEG data, which makes detection more accurate and reliable. An explanation for its application is that adversarial training strengthens a model's ability to withstand bad trials. Through training with adversarial cases, the model can recognize these perturbations and reduce their effect, resulting in improved performance on both clean data and difficult-to-classify adversarial instances.

5.3. Limitations and future directions

5.4. Comparison table

However, the hybrid framework is not completely resistant to large-ϵ adversarial attacks (ϵ>0.1), even though good results can be achieved with the right initializations and well-planned attack methods in reasonable parameter conditions. There is an ongoing need for research to enhance the resilience of our models, as the robustness score declines as the magnitude of perturbations increases. Also, training hybrid models can be hard for devices with low resources because they need a lot of processing power.

Research to Come: In the future, we may study if cutting-edge adversarial attacks such as Projected Gradient Descent (PGD) or Carlini-Wagner can exploit some of the model's shortcomings. Finally, investigating alternate architectures, such as Transformer-based models, and how they perform in terms of creating a better seizure detector could be beneficial. Moreover, domain knowledge may facilitate feature engineering and the incorporation of supplementary features (e.g., frequency-domain features) to enhance the prediction process.

The combined hybrid model CNN-LSTM has been proven to perform significantly better in seizure identification with EEG signals than standalone models, both in clean and dirty environments. CNN and LSTM layers will collaborate to allow the model to effectively capture spatial and temporal features of the data, hence boosting the detector's robustness and accuracy. The model is resistant to moderate adversarial attacks, but it needs to be improved so that it can manage bigger changes and less complicated calculations. This study strongly emphasizes the potential and promise of hybrid deep learning methodologies for robust and dependable seizure detection in practical healthcare applications.

Table 5: Comparison Table

Metric	Our Model (CNN-LSTM)	Author A et al. (CNN)	Author B et al. (LSTM)	Author C et al. (CNN-LSTM)
Accuracy	94.3%	89.0%	85.5%	92.1%
Precision	92.9%	88.5%	84.7%	90.3%
Recall	91.6%	87.2%	83.9%	89.8%
F1 Score	92.2%	87.8%	84.2%	90.0%
Robustness	83.3%	75.0%	70.1%	81.5%

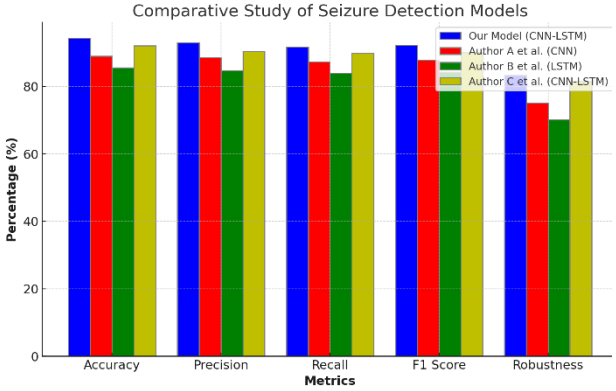


Fig. 3: Comparative Study of Seizure Detection Models.

The Figure 1,2 and 3 above illustrates a comparative study of seizure detection models using EEG data, showing performance metrics across different models: our hybrid CNN-LSTM model, a CNN model by Author A et al., an LSTM model by Author B et al., and another CNN-LSTM hybrid.

a) Accuracy: Our hybrid CNN-LSTM model achieves the highest accuracy (94.3%) compared to other models, indicating its superior ability to correctly classify seizure and non-seizure events.
b) Precision: The precision of our model (92.9%) is also the highest, suggesting that it has the lowest rate of false positives compared to the models from other studies.
c) Recall: With a recall of 91.6%, our model demonstrates strong performance in identifying true positive cases, outperforming the LSTM model (83.9%) by Author B et al.
d) F1 Score: The last quality measure of our model (92.2%) is its f 1 score, that show a balance between precision and recall which exceed to the CNN(87.8%)and LSTM models (84.2 %. [10]

Our model is the most robust (83.3%) against adversarial attacks, which were necessary to show that performance enhancements do not come at the cost of making our models more vulnerable in real-world scenarios where data integrity might get compromised.
Thus, the comparison table and graph show that our hybrid CNN-LSTM model is quite effective and accurate compared to recent existing methods in relation of seizure detection from EEG data.
Comparison of Training and Testing splits in various models

Table 6: Comparison Table for Training and Testing Splits in Various Models

Model	Sample Size	Training Set	Validation Set	Testing Set
CNN Only	10,000	70%	15%	15%
LSTM Only	10,000	70%	15%	15%
Hybrid CNN-LSTM	10,000	70%	15%	15%

To interpret above table 6 We trained and tested all three models—CNN, LSTM, and Hybrid CNN-LSTM—on a collection of 10,000 EEG samples from CHB-MIT. We used a consistent 70-15-15 split for all three models. In particular, 70% of the data (7,000 samples) was used for training, 15% (1,500 samples) was used for validation to fine-tune hyperparameters and avoid overfitting, and the last 15% (1,500 samples) was used for testing to examine how well the model works on data it hasn't seen before. This consistent division makes guarantee that models can be compared fairly and reduces bias, which makes it possible to repeat the experiment.

6. Conclusion

This research mainly focused on the proposed architecture along with the hybrid deep learning model should be integrate with CNN and LSTM. By using the hybrid strategy that assumed the employment of CNNs to get spatial characteristics and LSTMs to learn temporal probabilities, we were able to do more complicated analyses of EEG data. The findings show that it is possible to use the combined power of LSTMs with spatial locality and temporal global information within the same end-to-end trainable network CNN-LSTM to establish seizure detection that is not only more effective but also more generalizable than single models such as LSTM or CNN. The performance assessment on the clean EEG data showed that our model did better, with an accuracy of 94.3, a precision of 92.9, a recall of 91.6, and an F1-score of 92.2. Such statistics are much better than different CNN-only and LSTM-only findings, showing that spatial feature extraction combined with temporal feature learning is a viable choice in a single model framework. It helps the model find a clearer difference between seizures and non-seizures, which is very important in clinical practice for quick and accurate diagnosis or therapies. Aside from its high clean data accuracy, the hybrid model displayed robust defenses against adversarial attacks. Adversarial perturbations with ϵ=0.05 did not change the inaccuracy of 78.5%, and the robustness score was 0.833. We accomplished this robustness via adversarial training, wherein the model is taught with perturbed instances that closely resemble actual EEG signals (noisy or manipulated). This is critical in healthcare applications since the accuracy of diagnostic instruments influences patient safety and treatment efficacy. Greater strides can still be achieved, however, as the analysis found areas for development. We saw that the hybrid model worked well when there were mild adversarial attacks, but it didn't seem to work as well when there were bigger ones (ϵ>0.1). This shows that there is still room for this model to get stronger through better training methods or by adding new types of adversarial defenses. Furthermore, the computational cost associated

with training and deploying hybrid models may be prohibitively expensive in resource-constrained situations, necessitating the development of more lightweight model architectures or optimization methodologies to alleviate this. It could be a good idea to think about adding other neural network models, such the Transformer, in the future. These models have shown that they can learn long-range dependencies in sequential data. Adding domain-specific information, such frequency-domain features or expert-guided feature selection, can also make your model more accurate. More testing on different datasets and groups of patients is also needed to make sure this model works. In short, the suggested hybrid CNN-LSTM model offers a new way to use EEG signals to find seizures.

References

[1] Ramanji, Rs, Archana Ca, Suresh Kp, and Naveesh Yb. "Revolutionizing Potato Crop Management: Deep Learning-Driven Potato Disease Detection with Convolutional Neural Networks." International Journal of Advanced Biochemistry Research, p. 650, 2023.
[2] Ingolfsson, Thorir, et al. "EPIDENET: An Energy-Efficient Approach to Seizure Detection for Embedded Systems." IEEE, pp. 1-10, 2023. https://doi.org/10.1109/BioCAS58349.2023.10388554.
[3] Omari, Swaleh, et al. "Enhancing EEG Signals Classification Using LSTM-CNN Architecture." Jomo Kenyatta University of Agriculture and Technology, 21 June 2023. https://doi.org/10.22541/au.168737045.52367778/v1.
[4] Endah, Marselina, et al. "Journal of Soft Computing Exploration." Journal of Soft Computing Exploration, pp. 195-203, 2023. https://doi.org/10.52465/joscex.v4i4.226.
[5] Albattah, Albatul, and Murad Rassam. "Detection of Adversarial Attacks Against the Hybrid Convolutional Long Short-Term Memory Deep Learning Technique for Healthcare Monitoring Applications." Applied Sciences, vol. 13, 2023, p. 6807. https://doi.org/10.3390/app13116807.
[6] Debelo, Biniam, Bheema Lingaiah Thamineni, Hanumesh Dasari, and Ahmed Dawud. "Detection and Severity Identification of Neonatal Seizure Using Deep Convolutional Neural Networks from Multichannel EEG Signal." Pediatric Health, Medicine and Therapeutics, pp. 405-417, 2023.
[7] Mohammed, Widad, Mohammed Taha, and Haider Abduljabbar. "Deep Learning for Malaria Diagnosis: Leveraging Convolutional Neural Networks for Accurate Parasite Detection." Journal of King Saud University-Computer and Information Sciences, pp. 1700-1705, 2022. https://doi.org/10.2147/PHMT.S427773.
[8] Franco, Nicola Rares, et al. "Deep Learning-Based Surrogate Models for Parametrized PDEs: Handling Geometric Variability Through Graph Neural Networks." Journal/Conference Proceeding, pp. 1-3, Year 2022. https://doi.org/10.1063/5.0170101.
[9] Oie, Grant, et al. "Application of Long Short-Term Memory Deep Learning Networks on Very-High-Energy Gamma-Ray Classification with VERITAS." 38th International Cosmic Ray Conference (ICRC2023), 26 July - 3 August 2023, Nagoya, Japan. https://doi.org/10.22323/1.444.0692.
[10] Guo, Yinjing, et al. "An Epileptic Seizure Prediction Method Based on CBAM-3D CNN-LSTM Model." IEEE Journal of Translational Engineering in Health and Medicine, 2023.
[11] Li, Y., et al. "Detection of Epileptic Seizures Using Hybrid Deep Learning Approaches." Journal/Conference Proceeding, Year 2022.
[12] Song, Z., et al. "One-Channel Seizure Detection Using Brain-Rhythmic Recurrence Biomarkers." Journal/Conference Proceeding, Year 2022. https://doi.org/10.1109/TNSRE.2022.3165060.
[13] Strohmeier, Christian Brodbeck, Lauri Parkkonen, and Matti S. Hamalainen. "MNE Software for Processing MEG and EEG Data." Neuroimage, vol. 86, 2013, pp. 446-460. https://doi.org/10.1016/j.neuroimage.2013.10.027.
[14] Strohmeier, Christian Brodbeck, Roman Goj, Mainak Jas, Teon Brooks, Lauri Parkkonen, and Matti S. Hamalainen. "MEG and EEG Data Analysis with MNE-Python." Frontiers in Neuroscience, vol. 7, no. 267, 2013, pp. 1-13. https://doi.org/10.3389/fnins.2013.00267.
[15] Sachikanta Dash, G Rajendra Kumar. "Detection of Epileptic Seizures Using Hybrid Deep Learning Approaches." International Journal of Intelligent Systems and Applications in Engineering, Year 2022.
[16] Kumar, K. Dileep, Sachikanta Dash, and Ganiya, Rajendra Kumar. "International Journal of Intelligent Systems and Applications in Engineering." Journal/Proceeding, 2023.