Deep Learning based Attribute Identification for Deceit Prediction Using EEG Signal Analysis

Revoori Swetha[1],* and Dr. Damodar Reddy Edla[2]

[1]Department of Computer Science and Engineering, National Institute of Technology, Goa, Farmagudi, Ponda, Goa- 403401,India

[2]Department of Computer Science and Engineering, National Institute of Technology, Goa, Farmagudi, Ponda, Goa- 403401, India

Abstract— Lying detection is in the spotlight these days, particularly when it is applied to brain activity scanning. It is so because it may prove to be revolutionary for psychology, security, and even law enforcement agencies. It is one of the new techniques based on the detection of lies through examination of brainwave patterns derived from EEG signals using some very high-end techniques. Particularly, the approach applies Sample Entropy and Recurrence Quantification Analysis to give cues to Long Short-Term Memory networks. The belief is SampEn and RQA can pull out the non-linear, dynamic, and complex features of EEG data that are believed to be consistent triggers to indicate that someone is lying. To simplify the data, Independent Component Analysis simplifies the number of EEG channels from 16 to 12. To monitor the performance of the model, the researchers employed indicative metrics such as ROC curves, F1 score, precision, and recall. Trained on feature values based on SampEn and RQA, the LSTM model had an accuracy of 97.66%.

To avoid having the model overfit the training data, training was stopped early at epoch 81. Its performance was also benchmarked against more sophisticated neural networks, such as Multi-Layer Spiking Neural Networks, and conventional signal processing techniques, such as Fourier transform and wavelet analysis. The findings indicate that the algorithm delivers a perfect balance between high accuracy and computational efficiency, and therefore is best suited for real-world applications of lie detection. Detection of deception from EEG activity is an artificial intelligence breakthrough and a cognitive neuroscience milestone. Compared to all the other lie detection techniques, such as the polygraph which search for body reaction possibly under duress, EEG machines record an initial indicator of brain activity. Sample Entropy and Recurrence Quantification Analysis sophisticated signal processing techniques are employed to navigate through the very intricate EEG signal. Canceling repeat noise and detecting critical information characteristics, such as algorithms can detect subtle trends of falsehoods.

Keywords: Deceit detection, EEG signal analysis, Sample entropy(SampEn), Recurrence quantification analysis (RQA), Long short-term memory (LSTM), Brainwave patterns, Neural classification, Machine learning, Time- series analysis.

I. INTRODUCTION

1.1 Background

One recent development in the domains of artificial intelligence and cognitive neuroscience is the ability to identify dishonesty using EEG signals. This technique determines whether a response is honest or dishonest by analyzing brainwave activity. EEG technology provides a more direct understanding of the brain's thought processes than traditional lie detection methods like polygraphs, which rely on monitoring physiological changes like skin conductance and pulse and are typically subject to voluntary manipulation [1-2]. This could make it a more reliable option.

The intricate EEG signals are interpreted using sophisticated processing techniques like Sample Entropy and Recurrence Quantification Analysis (RQA). By eliminating unnecessary noise and highlighting significant features of the data, these methods can uncover subtle trends that could indicate dishonesty [3-5].

1.2 Problem Statement

Other traditional methods of detecting dishonesty, such as polygraph testing, are often manipulated and have little accuracy. Due to the complexity of EEG signals, EEG-based dishonesty prediction requires advanced feature extraction and classification techniques even if it offers a more accurate evaluation of brain activity. This study proposes a deep learning-based approach that uses LSTM networks, sample entropy, and recurrence quantification analysis (RQA) to extract features in order to detect dishonesty. Enhancing the precision and reliability of deception detection is the aim by closely analyzing EEG data and deftly differentiating between truthful and dishonest replies.

1.3 Motivation

Lie detection technology is of greatest importance in criminal justice because of the critical role they can play in investigating deceptions, criminal confessions, and frauds.

Behavior analysis and polygraph tests are outdated techniques that have extremely profound pitfalls, ranging from susceptibility to interpretation bias to manipulability. But EEG-based lie detection has less susceptibility to subjectivity since it evaluates patterns of brain activity. Because the dimensionality of the EEG signal is extremely high, conventional frequency-based systems fail to detect dishonesty. It is a limitation while planning to construct a suitable, useful, and computationally effective solution. The main and primary goal of our work is to overcome this limitation. The aim of this paper is to significantly improve the accuracy of detecting dishonesty with the help of state-of-the-art deep learning techniques and strong feature extraction.

1.4 Objectives

Using the Sample Entropy (SampEn) and even the Recurrence Quantification Analysis (RQA) in feature extraction and Independent Component Analysis (ICA) in data reduction in dimension, this paper makes an effort to design a state-of-the-art EEG-based system to identify lying. The performance of the model in classifying lying is later improved using Long Short-Term Memory (LSTM) networks for recognizing temporal patterns. It is assessed by accuracy, precision, recall, and F1-score as performance measures, and compared against traditional signal processing methods and competing deep learning frameworks. Last but not least, the aim is to have an effective and computationally efficient device for detecting deception that can be used in actual applications such as cognitive studies, security, and law enforcement.

II. LITERATURESURVEY

Historically, deception detection has most likely been the most important area of research in psychology, law, and neuroscience. In evaluating whether or not a subject will be a liar, polygraph testing used to test for bodily responses—such as racing heart, increase in blood pressure, or clammy hands—since our body responds when under stress [6-8]. But being human and with the ability to be deceived by countermeasures, these have undergone a lot of criticism. Because EEG can capture on-line token neural activity, it is a very strong brain-based lie detection tool, which is the subject of current research. Farwell and Donchin (1991) developed the P300-based Concealed Information Test (CIT), a heavily researched and valid EEG-based lie detection paradigm. The P300 wave event-related potential (ERP) is elicited by this task whenever a subject responds to information that is being concealed or familiarity. Their article which has been found to take place even when the subjects attempted to hide their emotions, EEG measurements will be capable of

uncovering what was otherwise concealed. Secondly, with the help of time response measurements, Rosenfeld et al. (2004) also enhanced the technique to more sophistication.

Adding to its authenticity, despite such enhancements, fraud detection methods using the help of ERP still need highly controlled laboratory environments and do not succeed in day-to-day life-situations.

Frequency-domain techniques such as wavelet analysis and even the Fourier to become an attempt to more completely realize the EEG signals beyond normal means. The techniques can perhaps find genuine brain activity patterns in the external world but are still not deserving of doing justice to how complex and non-linear it is. Scientists resort to non-linear dynamic techniques such as Recurrence Quantification Analysis (RQA) and entropy measures like Sample Entropy (SampEn) to mitigate this constraint. Richman and Moorman (2000) state that SampEn is a reliable metric for the examination of cognitive change in deception because it is very well adapted in signal complexity estimation. Groundbreaking disruption of artificial intelligence (AI) made groundbreaking advances in EEG-based deception detection on being through the implementation of machine learning. Amongst these paradigms, i.e., deep learning models, Long Short Term Memory (LSTM) networks came to the forefront with enormous potential in the detection of temporal patterns in EEG signals. Hochreiter and Schmidhuber (1997) came up with recurrent neural networks (LSTMs) as a development over the erstwhile employed recurrent neural networks (RNNs) in the treatment of long-range dependencies of sequence data for the first time.

Zhang et al. (2020) rendered LSTM-based models superior to other more conventional machine learning techniques like Random Forests and Support Vector Machines (SVMs) in separating true and false answers. The Multi-Layer Spiking Neural Network (MMSNN) introduced a new and promising technique to evade detection from EEG signal. Unlike the conventional deep neural networks, the MMSNNs mimic biological neurons' way of handling information, and with this, the latter is allowed to process the information more human-like in nature. Despite the fact that in this paper EEG-based fraud detection has progressed a great deal, some of which are urgent and still need to be solved immediately. As indicated by the reports given by Meijer et al. (2016), the largest The largest problem is that individuals have different EEG signals and thus it's hard to develop models which will generalize well across tasks. Another limitation that bars the creation of strong machine learning systems is that there are not a lot of large, heterogeneous EEG datasets. To advance the field, future research will need to make cross-subject validation methods more efficient, gather more data, and incorporate other predictors like behavioral patterns and physiological responses into a global detection system.

Though there has been remarkable progress in EEG-based fraud detection over the years, much remains to be achieved. Signal processing, deep learning, and feature extraction are enhancing these techniques to become more accurate and reliable. With continued research and development, EEG-based deception detection can become a powerful tool for security screening, forensic analysis, and cognitive science, bridging the gap between neuroscience and practical, real-world applications.

2.1 Machine Learning Models

Conventional machine learning techniques like GD and Mini-Batch SGD are commonly used for dishonesty prediction. Despite their ease of use and comprehension, these models have limitations when it comes to handling unbalanced datasets and extracting relational data between transactions [9]. For instance, RF often fails to classify the minority class of fraudulent transactions, even though it may provide a respectable level of overall accuracy.

2.2 Models for Deep Learning

Two deep learning methods that work well are Convolutional Neural Networks (CNNs) and

MMSNN networks. This is because they are very good at identifying patterns and all of their temporal correlations.

MMSNNs are better at handling of the time series, and also the CNNs that are especially good at of the extracting features [10-11]. However, because of these models treat nonlinear spikes as distinct instances and do not naturally capture relational information, they are not very good at identifying abnormal spikes.

2.3 LSTM

LSTM networks successfully capture the temporal correlations in EEG signals, addressing the shortcomings of both conventional deep learning models and conventional machine learning. Unlike typical classifiers that treat EEG data as discrete samples, LSTMs employ their memory cells to retain and understand sequential patterns of brain activity, making them ideal for detecting dishonesty [12]. The LSTM networks are been important markers of the dishonest behavior and also are especially helpful for the identification subtle cognitive changes that take place over time. Their capacity to identify long-term patterns in EEG signals is one of their greatest advantages, making them ideal for researching brain activity. Additionally, they easily include other EEG-based features into a unified framework, including Recurrence Quantification Analysis (RQA) and Sample Entropy (SampEn).

It has already been demonstrated that LSTM networks are superior to other deep learning models and conventional machine learning in identifying lying in EEG signals [13-14]. As LSTMs are specifically designed for identifying long-term dependencies in sequential data, they are especially suitable for EEG analysis. If the EEG signals are used as the individual points, it will lead to significant contextual patterns being lost, as the brain activity is constantly changing. But LSTMs can pick up subtle differences in thoughts that may be a sign of deception because they can process EEG databased on the way it is naturally presented [15]. LSTMs can process EEG data much better than static models to identify honest vs. dishonest answers as they are capable of storing and processing information sequentially. The ability of the LSTMs to handle complexity and non-linearity of EEG signals is also a very good point in favor. It might be tough to identify deceit with traditional feature-based approaches since it is a cognitively demanding process that results in complex changes in brain activity [16]. Because of the uniqueness of the memory cell structure and the gating mechanisms (input, forget, and output gates), LSTMs are able to selectively hold the important information and discard noise or redundant data.

One of the key difficulties in using EEG signals for detecting deception is managing the noise and variability present in brain activity recordings [17]. Elements such as individual differences, mental workload, and environmental distractions can significantly impact the quality of EEG data, making it harder to achieve reliable outcomes. LSTM networks help to solve this issue by removing the short-lived, insignificant variations and focusing on that of remaining recurrent patterns that are more likely to be linked to dishonest behavior. Compared to the standard machine learning models, the LSTMs can be handle noisy data better when observed because of their memory cells, which allow them to gradually smooth out inconsistencies. Unlike earlier methods that mostly rely on pre-processing and carefully crafted features, LSTMs can learn directly from raw or minimally processed EEG data.

According to studies, LSTMs perform better than other deep learning techniques like Artificial Neural Network (ANNs) and also more efficient than machine learning models like Support Vector Machines (SVMs) and Random Forests (RFs). Convolutional Neural Networks (CNNs) and other models are good at identifying the images mainly the corners and edges of the image, but CNNs are not good at identifying time series data like EEG data. LSTMs are most used model for identifying deceit because they can handle the long series data which are best for this kind of

dataset. Also there are some disadvantages in using LSTM particularly when it is trained on small datasets because they may struggle with overfitting and might be complex. There are some strategies like dropout, early stopping and some other hyperparameter tuning to avoid these problems and keep model perfect and efficient for identification. To improve both accuracy and understanding, future research could explore combining LSTM-based lie detection with attention mechanisms or graph-based learning. As this field continues to grow, LSTMs remain one of the most effective tools for capturing the changing and complex patterns in EEG data, offering valuable insights for both cognitive research and forensic applications.

III. METHODOLOGY

To guarantee the outcomes are efficient and precise, this research goes through a distinct, chronological approach to detect deception through EEG signals. This starts from selecting and recording good EEG data in a controlled environment to minimize noise and redundant interference. Once having the data, next reduces unwanted signals and set all equal. Then methods like Recurrence Quantification Analysis (RQA) and Sample Entropy (SampEn) are utilized in an effort to detect the brain activity complex patterns also confirms repetitive patterns. Finally, a Long Short-Term Memory (LSTM) network is utilized in an effort to detect these patterns in succession in an effort to detect if a subject is lying or not. LSTMs work very well because they can detect alterations in brain signals that change over time which is quite important for this task. All this process helps in building a good and efficient lie detection system with good outputs while being frugal on computing resources.

3.1 Dataset Description

All single samples present in 16-channel EEG data used herein has been annotated by typing the word "Guilty" or the word "Innocent". As a token of appreciation for allowing cleaner better recordings, the above facts are presented in a highly controlled environment with the aim of reducing unwanted noise, artefacts, and environmental interference. Since EEG signals are dynamic and even complicated in nature, they become even more challenging for pattern recognition without processing. Coarse measurements were utilized to remove any type of contaminants such as eye blinks, muscle activity, and external electrical noise in order to remove impurities from the dataset quality. Because of this, the dataset provides the whole brainwave activity, therefore it is extremely appropriate for deception analysis. This study provides the most important information about the neural characteristics that are involved in deception because deceptive thinking styles yield normal EEG patterns.

3.2 Data Preprocessing

Preprocessing of data is performed on a 16-channel EEG data set, and the samples are marked as "Guilty" or "Innocent" . To obtain better signal quality and to effectively remove unwanted noise and artifacts that can impact analysis, band-pass filtering of 0.5–50 Hz is performed. Normalization of EEG data is performed to maintain consistency in recordings and minimize fluctuations based on individual brain pattern activity. Applying Independent Component Analysis (ICA) for additional data recovery and removal of general artifacts such as eye blinks and muscle activities, validity in the recovered features is enhanced. ICA applies dimension reduction and channel reduction from 16 to 12 without losing necessary neural information.

3.3 Normalization

Normalisation is done because we can be assured that it gives consistency in all the recordings. It makes the analysis unchanged by extreme variation obtained from scaling signal amplitudes from a predetermined range. Normalizing data results in the model becoming less affected by variations in signal strength and concentration in identifying significant patterns in brain activity.

Improvements are seen in accuracy and robustness of the deception detection , the models ability access various subjects, and the dependability of feature extraction

3.4 Feature Reduction

To reduce the dimensionality, feature reduction is utilized. Channel reduction without loss of valuable information is a critical part of processing because EEG data is of high dimension. The 16-channel EEG is reduced to 12 channels using the ICA method, which harms the performance while preserving complex signal characteristics.

A. Independent Component Analysis (ICA)

As EEG data is high dimensional and also very complex, it is required to reduce the number of channels while keeping the present important information for improvement of computational performance. Independent Component Analysis (ICA) is mainly used for dimensionality reduction in this case it keeps all the important information of the brain signals, and it reduces the 16 channel EEG signal to 12 channels. ICA identifies independent sources to eliminate unwanted or noisy channels from the EEG dataset. By just taking the 12 most important channels the model trains and manages the data more efficiently while reducing the computational effort and overfitting risk.

3.5 Model Selection

Because of its capacity to recognise temporal connections in sequential data, a Long Short-Term Memory (LSTM) network is chosen. Since EEG signals are time-series, LSTM is a perfect option for collecting changes over time.

A. Long Short-Term Memory (LSTM) Network

Here Long Short Term Memory networks are been used for the identification of the long term dependencies that are present in the sequential are used for finding the deception using EEG signals rather than basic RNNS which have the disadvantage of disappearing of weights and losing crucial data of the dataset, LSTM have mainly three gates namely input, forget and output gate to operation the go along the details. By this the network to keep and recognize crucial patterns in human brain pursuit over time, this assist in varies between actual and predicted mental states.

Deception detection with EEG signals is well convenient for LSTM networks, a special kind of RNN that catch very long term dependencies in sequence data. LSTMs had memory cells and three gates namely known as input, forget and lastly output gates to control the message flow, in addition to conventional RNNs, which had the disadvantage of degrading weights and no longer have crucial amount of past data. This assist with the transform between actual and corrupt states by activating the network to the recall temporal patterns in brain activity.
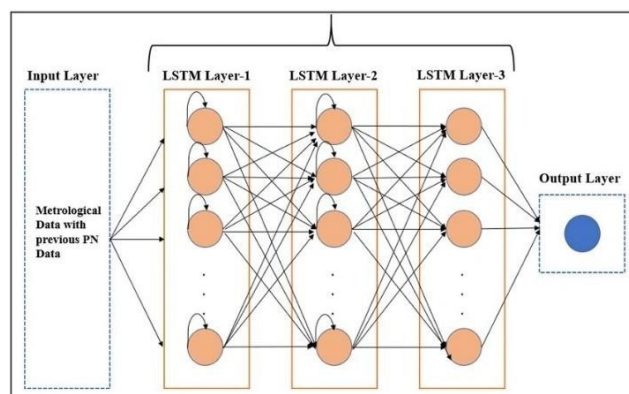
Fig2.LSTMNetwork Architecture

B. Training the Model

In order to start training the model for EEG signal classification, the preprocessed and feature-extracted data is fed into the LSTM network. This makes it possible for the model to detect the temporal patterns associated with brain activity that is both honest and dishonest. The model is trained using labelled EEG data and continuously refines its internal parameters through backpropagation and optimisation techniques such as the Adam optimiser. To evaluate classification accuracy and guide weight adjustments, an appropriate loss function such as binary cross-entropy is employed.

For ensuring all that of the model does not overfit certain patterns and that it generalises properly, the dataset has been divided into both training and validation sets. When that of validation accuracy stops rising, which in this work occurs at the 81st epoch, early stopping is used to prevent overfitting by ending the training process. This approach is for ensuring of that the model with high accuracy while of adapting of that effectively of new data.

By using all of the present sequential dependencies in EEG signals to identify long-range patterns in brain activity, the LSTM network reliably differentiates between the "Guilty" and "Innocent" term categories. Combining advanced feature extraction methods with a well-optimized LSTM architecture results in an extremely effective and efficient model for fraud detection.

3.6 Model Evaluation

Performance is evaluated using several metrics such as accuracy, precision, recall, F1-score, and area under the ROC curve (AUC).

Accuracy=TP+TN/FP+FNTP+TN

Table1.Performanceofvariousmodelsusedfor comparison

Model	Accuracy	Precision	Recall	F1-Score
MMSNN	99.0%	0.98	0.98	0.98
LSTM(Proposed)	98.3%	0.96	0.96	0.96
GD	88.2%	0.86	0.88	0.87

3.7 Novelty

The key contribution of this study is that of its innovative approach to enhancement of the EEG based fraud detection through present combination of dimensionality reduction and advanced feature extraction approaches. Unlike other methods that process high-dimensional EEG data in its original form, this study employs Independent Component Analysis (ICA) to reduce the number of channels from 16 to 12. This optimisation is of actual boosting processing performance while preserving crucial brain data. Additionally, the study makes use of sophisticated non-linear feature extraction methods such as Sample Entropy and Recurrence Quantification Analysis.

Both periodic patterns and complexity that have been handled by these techniques better than by the conventional frequency-domain techniques. This new technique which can achieve all the high accuracy by integrating these techniques with an LSTM-based deep learning model. Due to

this, it is a significant improvement in the construction of strong and efficient deception detection systems.

IV.   RESULT

The results of the research verify the effectiveness of the suggested EEG-based deception detection system that separates honest and deceptive brain activity with excellent accuracy and reliability. The method employs an LSTM model, which is trained using features extracted with Sample Entropy (SampEn) and Recurrence Quantification Analysis (RQA), to enhance the identification of the temporal correlation of EEG data, as compared to conventional machine learning models. For improvement of that of actual computational efficiency without sacrificing all the important neurological information, Independent Component Analysis (ICA) was used to reduction of the total number of EEG channels from 16 to 12. Performance metrics like accuracy, precision, recall, and F1-score confirm the model's effectiveness, with an impressive 97.66% accuracy.

In order to avoid overfitting and guarantee that the model is reliable when applied to fresh data, early stopping was also employed at the 81st epoch. The advantages of the current method are further highlighted by a comparison with more traditional signal processing techniques like wavelet analysis and Fourier transformations. An advancement over the conventional techniques, LSTM based model excels at detection of the dishonesty, indicating iall its potential for practical use in cognitive and forensic research.
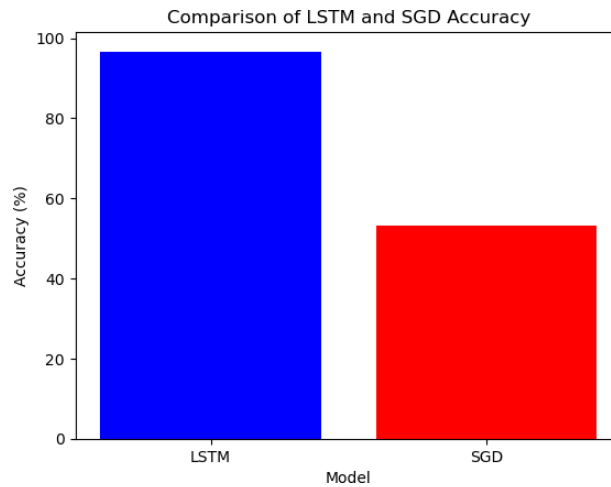

Fig3.Comparisonofmodels

A more comprehensive examination using a confusion matrix and Receiver Operating Characteristic (ROC) curve further demonstrates the strength of the proposed approach. The results, which show a high true positive rate and minimal false negatives, corroborate the model's reliability in detecting dishonesty. The technology is greatly increasing all the accuracy and precision of dishonesty detection by fusing of that deep learning with sophisticated feature extraction techniques. Furthermore, the model's capacity to generalise to fresh EEG data points to a number of practical uses, such as cognitive research, forensic investigations, and security audits. This result tends for that of the way for future advancements and validates the effectiveness of EEG-based fraud detection.

V.   CONCLUSION

By combining of all the LSTM for classification with both Recurrence Quantification Analysis (RQA) and Sample Entropy (SampEn) for that of feature extraction, this study suggesting of a novel method for identifying deception in EEG data. Independent Component Analysis (ICA) was utilised to speed up data processing without noticeably sacrificing accuracy by reducing the number of EEG channels from 16 to 12. Despite obtaining an accuracy of 97.66%, which is where of somewhat less than the 99.00% that of reported for all Multi-Layer Spiking Neural Networks (MMSNN), the actual proposed method offers notable advantages in terms of interpretability and computational efficiency. This study's findings demonstration of that this EEG-based fraud detection system, which utilises ICA, RQA, SampEn, and LSTM, represents a significant advancement in the field. This methodology's high accuracy, efficient processing, and potential for real-time application should be advantageous for future research in cognitive neuroscience and brain-computer interface technology. It can be used in forensic investigations, security screenings, and other real-world scenarios where precise deception detection is crucial.

REFERENCES

[1] Akhavan A, Moradi MH, and Vand SR Subject- based discriminative sparse representation model for detection of concealed information *Comput Methods Programs Biomed* 2017 143 25-33.

[2] Bablani A, Edla DR, and Tripathi D An efficient concealed information test: EEG feature extraction and ensemble classification for lie identification *Mach Vis Appl* 2019 30 5 813-832.

[3] Gao J, Lu L, Yang Y, Yu G, Na L, and Rao N A novel concealed information test method based on independent component analysis and support vector machine *ClinEEGNeurosci* 20124354-63.

[4] Sung M, Kim Y (2020) Training spiking neural networkswithanadaptiveleakyintegrate-and-fire neuron.In:2020IEEEinternationalconferenceon consumer electronics-Asia (ICCE-Asia), pp. 1–2, IEEE.

[5] Farwell LA and Donchin E The truth will out: interrogative polygraphy ('lie detection') with event-related brain Potentials *Psychophysiology* 1991285531-547.

[6] Arasteh A, Moradi MH, and Janghorbani A A novel method based on empirical mode decomposition for P300-based detection of deception *IEEE Trans Inf For Secur* 2016 11 11 2584-2593.

[7] Gao J, Lu L, Yang Y, Yu G, Na L, Rao N (2012) A novel concealed information test method based on independent component analysis and support vector machine. Clin EEG Neurosci 43:54–63

[8] Ghosh-Dastidar S, Adeli H. A new supervised learning algorithm for multiple spiking neural networks with application in epilepsy and seizure detection. Neural Netw. 2009;22(10):1419–1431.

[9] Srinivasa Sai Abhijit Challapalli. Optimizing Dallas-Fort Worth Bus Transportation System Using Any Logic. Journal of Sensors, IoT & Health Sciences, 2024; 2(4): 40-55.

[10] Jung TP et al. Removing electroencephalographic artifacts by blind source separation. Psychophysiology. 2000;37(2):163–178.

[11] Li Y, Guo Y, Zhang S, Deng S, Hai Y, Gu S. Differentiable spike: rethinking gradient-descent for training spiking neural networks. Adv Neural Inf Process Syst.

2021;34:23426. 29

[12] Srinivasa Sai Abhijit Challapalli. Sentiment Analysis of the Twitter Dataset for the Prediction of Sentiments. Journal of Sensors, IoT & Health Sciences, 2024; 2(4): 1-15.

[13] Luo Y, Shen H, Cao X, Wang T, Feng Q, Tan Z. Conversion of Siamese networks to spiking neural networks for energy-efficient object tracking. Neural Comput Appl. 2022;34(12):9967–9982.

[14] Meixner JB, Rosenfeld JP. A mock terrorism application of the P300-based concealed information test. Psychophysiology. 2011;48(2):149–154.

[15] K. Vinay Kumar, Sumanaswini Palakurthy, Sri Harsha Balijadaddanala, Sharmila Reddy Pappula, & Anil Kumar Lavudya. Early Detection and Diagnosis of Oral Cancer Using Deep Neural Network. Journal of Computer Allied Intelligence, 2024; *2*(2): 22-34.

[16] Ramadan RA, Vasilakos AV. Brain computer interface: control signals review. Neurocomputing. 2017;223:26–44.

[17] Rosenfeld JP, Labkovsky E, Winograd M, Lui MA, Vandenboom C, Chedid E. The complex trial protocol (CTP): a new, countermeasure-resistant, accurate, P300-based method for detection of concealed information. Psychophysiology. 2008;45(6):906–919.