

# **Applying Machine Learning Algorithms for the Classification of Sleep Disorders**

*A Seminar Report*

*Submitted to the APJ Abdul Kalam Technological University in  
partial fulfillment of the requirements for the award of degree*

***Bachelor of Technology***

*in*

***Computer Science and Engineering***

By

**Vijayalakshmi.S**

**PTA21CS065**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**COLLEGE OF ENGINEERING KALLOOPPARA**

**KERALA**

**October 2024**

**DEPARTMENT OF COMPUTER SCIENCE AND  
ENGINEERING  
COLLEGE OF ENGINEERING KALLOOPARA  
2024-25**



**CERTIFICATE**

This is to certify that the report entitled **Applying Machine Learning Algorithms for the Classification of Sleep Disorders** submitted by **VIJAYALAKSHMIS (Reg. no. PTA21CS065)**, to the APJ Abdul Kalam Technological University in partial fulfilment of the B. Tech degree in Computer Science & Engineering is a bonafide record of the seminar work carried out by him under our supervision. This report in any form has not been submitted to any other University or Institution for any purpose.

**Mrs. Anitha Jose**

**Internal Guide**

Department of Computer

Science & Engineering

**Mrs. Anitha Jose**

**Internal Guide**

Department of Computer

Science & Engineering

**Dr. Renu George**

**Head of the Department**

Department of Computer

Science & Engineering

## ACKNOWLEDGEMENT

I take this opportunity to express my deepest sense of gratitude and sincere thanks to everyone who helped me to complete this work successfully. I express my sincere thanks to the Principal **Mr. Rajkumar T** for the constant support and help. I also thank **Dr. Renu George** Head of Department Computer Science and Engineering, College of Engineering Kallooppa for providing me with all the necessary facilities and support. I would like to place on record my sincere gratitude to my seminar guide **Mrs. Anitha Jose**, Assistant Professor, Computer Science and Engineering, College of Engineering Kallooppa for the guidance and mentorship throughout the course. I would like to express my sincere gratitude to **Mrs. Shilpa Radhakrishnan**, and **Ms. Parvathy M N**, department of Computer Science and Engineering, College of Engineering Kallooppa for their support and cooperation. Finally, I thank my family, and friends who contributed to the successful fulfilment of this seminar work.

**VIJAYALAKSHMI S**

## **ABSTRACT**

Sleep disorder classification plays a critical role in enhancing human quality of life, as conditions such as sleep disorders and apnoea can severely impact health. Manual sleep-stage classification by experts can be labour-intensive and subject to error. The development of accurate machine learning algorithms (MLAs) for sleep disorder classification requires comprehensive analysis, monitoring, and diagnosis. This paper presents a comparison of deep learning algorithms with conventional MLAs for sleep disorder classification, proposing an optimized method for the task. The Sleep Health and Lifestyle Dataset, available publicly, was used to evaluate the proposed model, with optimizations performed using a genetic algorithm to fine-tune the parameters of various MLAs. The study assesses k-nearest neighbors, support vector machine, decision tree, random forest, and artificial neural network (ANN) algorithms. Results demonstrate significant performance differences among the models, with classification accuracies of 83.19%, 92.04%, 88.50%, 91.15%, and 92.92%, respectively. The ANN achieved the highest classification accuracy at 92.92%, with precision, recall, and F1-score values of 92.01%, 93.80%, and 91.93%, respectively. This highlights the superior performance of the ANN algorithm compared to other models tested.

# CONTENTS

<b>ACKNOWLEDGEMENT</b>	<b>I</b>
<b>ABSTRACT</b>	<b>II</b>
<b>LIST OF FIGURES</b>	<b>VI</b>
<b>LIST OF ABBREVIATIONS</b>	<b>VIII</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 BACKGROUND	1
2.1 PURPOSE AND SCOPE	2
<b>2 LITERATURE SURVEY</b>	<b>3</b>
<b>3 TECHNOLOGIES</b>	<b>5</b>
3.1 MACHINE LEARNING ALGORITHMS	5
3.2 DEEP LERNING MODELS	7
3.3 OPTIMIZATION TECHNIQUES:GENETIC ALGORITHMS	7
3.4 DATASET:SLEEP HEALTH AND LIFESTYLE DATASET	8
<b>4 ARCHITECTURAL BACKGROUND</b>	<b>9</b>
4.1 DATA ACQUISITION AND PREPROCESSING	9
4.2 MACHINE LEARNING MODEL ARCHITECTURE	9
4.3 GENETIC ALGORITHM OPTIMIZATION ARCHITECTURE	10
4.4 PERFORMANCE EVALUATION AND COMPARISON	11
<b>5 USAGE SCENARIOS</b>	<b>14</b>
5.1 CONSUMER HEALTH APPLICATIONSINWEARABLE DEVICES	14
5.2 AUTOMATED SLEEP DISORDER DIAGNOSISLLEEP CLINICS	15

5.3 SLEEP DISORDER SCREENING IN PRIMARY CARE SETTINGS	15
5.4 SLEEP RESEARCH AND DATA ANALYSIS	16
<b>6 METHODOLOGIES AND DISCUSSION</b>	<b>17</b>
6.1 PREPROCESSING STEPS	17
6.2 MACHINE LEARNING MODELS	18
6.3 GENETIC ALGORITHM OPTIMIZATION	19
6.4 DISCUSSION	20
<b>7 SECURITY ISSUES</b>	<b>22</b>
7.1 DATA PRIVACY AND CONFIDENTIALITY	22
7.2 MODEL INVERSION ATTACKS	22
7.3 ADVERSARIAL ATTACKS	22
7.4 MODEL THEFT AND INTELLECTUAL PROPERTY CONCERNS	23
7.5 DATA INTEGRITY	23
7.6 DEPLOYMENT SECURITY	24
7.7 FAIRNESS AND BIAS ISSUES	24
<b>8 CONCLUSION</b>	<b>25</b>
<b>9 REFERENCES</b>	<b>26</b>

## **LIST OF FIGURES**

<b>FIGURE NO.</b>	<b>TITLE</b>	<b>PAGE NO.</b>
4.7	Diagram of the Machine Learning Model To Classify Sleep disorders.	14
4.8	The proposed optimized model for sleep Disorder classification by Genetic Algorithm	15

## **LIST OF ABBREVIATIONS**

PSG:Polysomnography

CST:Consumer Sleep Technology

REM:Rapid Eye Movement

GA:Genetic Algorithms

KNN:K-Nearest Neighbors

SVM:Support Vector Machines

DT:Decision Tree

RF:Random Forest

ANN:Artificial Neural Network

MLA:Machine Learning Algorithm

CNN:Convolutional Neural Network

LSTM: Long Short-Term Memory



# **CHAPTER 1**

## **INTRODUCTION**

### **1.1 BACKGROUND**

Sleep disorders, including insomnia and sleep apnoea, are critical health issues that significantly affect an individual's physical and mental well-being. Sleep is essential for maintaining cognitive function, memory consolidation, and overall health, with poor sleep quality often leading to severe medical conditions like heart disease, diabetes, depression, and obesity. As such, accurate diagnosis and timely intervention are crucial to improving patients' quality of life and preventing long-term health complications. Traditionally, diagnosing sleep disorders has been a labour-intensive process that requires manual sleep-stage classification, often conducted through polysomnography (PSG) tests. Experts analyze signals from brain activity, eye movements, heart rate, and muscle activity to categorize sleep into different stages such as wakefulness, light sleep, deep sleep, and REM sleep. While effective, this process is time-consuming, requires trained specialists, and is prone to human error due to the complexity and variability of sleep patterns across individuals.

However, the performance of machine learning models in classifying sleep disorders heavily depends on their parameters and configuration. Optimizing these parameters can significantly impact the accuracy and reliability of predictions. Genetic algorithms (GAs), which are inspired by the process of natural selection, are often used to fine-tune machine learning models by searching for optimal parameter settings. These optimization techniques improve the performance of models by selecting the best parameters and enhancing their generalization capabilities across different datasets.

In this study, the focus is on comparing the performance of traditional MLAs and deep learning models for sleep disorder classification. By utilizing the Sleep Health and Lifestyle Dataset, this study aims to evaluate the effectiveness of various algorithms, including k-nearest neighbors (KNN), support vector machines (SVM), decision trees (DT), random forests (RF), and artificial neural networks (ANN). The study further explores the use of genetic algorithms to optimize these models, ensuring that the highest possible accuracy is achieved in classifying

sleep disorders. By addressing the challenges of traditional diagnosis methods and leveraging advanced MLAs, this research seeks to contribute to the growing body of work focused on improving healthcare outcomes through the application of machine learning technology. The ultimate goal is to provide a more accurate, efficient, and scalable solution for sleep disorder classification, which could have far-reaching implications for clinical practice and patient care.

## **1.2 PURPOSE AND SCOPE**

The advent of machine learning algorithms (MLAs), the healthcare industry has been increasingly exploring their potential in automating and enhancing the accuracy of sleep disorder diagnoses. The scope includes a comprehensive comparison of algorithms such as k-nearest neighbors, support vector machines, decision trees, random forest, and artificial neural networks. The goal is to identify the most effective model for classifying sleep disorders, providing insights into its application in real-world healthcare environments.

Here are key aspects of the purpose and scope :

- **Explore Deep Learning Models:** Analyze the performance of artificial neural networks (ANNs) in comparison to traditional machine learning algorithms.
- **Evaluate Machine Learning Algorithms:** Assess traditional machine learning algorithms like k-nearest neighbors, support vector machines, decision trees, and random forest for sleep disorder classification.
- **Dataset Utilization:** Use the publicly available Sleep Health and Lifestyle Dataset to test and evaluate the proposed models.
- **Parameter Optimization:** Implement genetic algorithms (GAs) to fine-tune the parameters of the machine learning models, aiming to enhance their accuracy and performance.
- **Comprehensive Performance Comparison:** Compare the accuracy, precision, recall, and F1-score of different models to determine the most efficient algorithm for classifying sleep disorders.
- **Real-World Application:** Provide insights into the practical application of machine learning in healthcare, particularly for automating the diagnosis of sleep disorders, potentially improving efficiency and accuracy in clinical settings.

## **CHAPTER 2**

### **LITERATURE SURVEY**

#### **2.1 Sleep classification using consumer sleep technologies and AI: A**

**review of the current landscape** by S. Djanian, A. Bruun, and T. D. Nielsen, Dec (2022) [1] : The authors reviewed several consumer sleep technologies (CST) alongside machine learning algorithms (MLAs) for sleep-stage classification. The study highlighted the limitations of manual polysomnography (PSG) in sleep classification, pointing out that CST, while more accessible and cost-effective, often lacks the accuracy of PSG. The authors reviewed various machine learning techniques, including logistic regression, decision trees, and deep learning models, for classifying sleep stages using CST data. While CST provides a more convenient solution, machine learning algorithms applied to these devices showed a significant improvement in classification accuracy, with deep learning models demonstrating superior performance.

#### **2.2 Detection of sleep apnea using machine learning algorithms based on ECG signals: A comprehensive systematic review**

by N. Salari, A. Hosseini-Far, M. Mohammadi, H. Ghasemi, H. Khazaie, A. Daneshkhah, and A. Ahmadi. Jan (2022) [2] : The authors conducted a systematic review of machine learning approaches for detecting sleep apnea, a common and severe sleep disorder, using electrocardiogram (ECG) signals. The authors explored several machine learning models, including support vector machines (SVMs), random forests (RFs), and deep neural networks, for classifying sleep apnea based on ECG data. They identified challenges in data availability and signal variability, which affect the models' accuracy. The study found that deep learning models, particularly neural networks, outperformed traditional machine learning techniques in identifying sleep apnea, with higher accuracy rates when applied to ECG signals.

## **2.3 A deep learning method approach for sleep stage classification with**

### **EEG spectrogram** by C. Li, Y. Qi, X. Ding, J. Zhao, T. Sang, and M. Lee, May (2022)

[3] : The authors developed a deep learning model using electroencephalogram (EEG) data to classify sleep stages. The study compared the performance of traditional MLAs and deep learning techniques, focusing on convolutional neural networks (CNNs) and long short-term memory (LSTM) models. The authors found that EEG data, when combined with deep learning algorithms, significantly improved sleep stage classification accuracy compared to traditional methods. The study used publicly available datasets and achieved accuracy rates exceeding 90%, showcasing the potential of deep learning models in handling complex and noisy sleep data.

## **2.4 Detection of sleep apnea from single-lead ECG: Comparison of**

### **deep learning algorithms** by M. Bahrami and M. Forouzanfar, Jun 2021 [4] : The

proposed a hybrid deep learning model that combines convolutional neural networks (CNNs) and long short-term memory (LSTM) networks to detect sleep apnea using ECG data. The study used the PhysioNet Apnea-ECG dataset to validate the model, which outperformed traditional methods, such as random forests and decision trees, in terms of classification accuracy. By integrating both CNN and LSTM architectures, the hybrid model successfully captured spatial and temporal patterns in the data, improving the detection rate of sleep apnea events and demonstrating the potential of hybrid deep learning models for complex health data classification.

These studies highlight the growing use of machine learning algorithms, especially deep learning models, in automating and improving the accuracy of sleep disorder diagnosis, paving the way for more efficient healthcare solutions.

## **CHAPTER 3**

### **TECHNOLOGIES**

A variety of technologies and techniques used, it focusing primarily on machine learning algorithms to classify sleep disorders. The main technologies used are traditional machine learning algorithms, deep learning models, and optimization methods, particularly genetic algorithms, to enhance model performance. This section will delve into each of these technologies and their application in sleep disorder classification.

### **3.1 Machine Learning Algorithms**

Machine learning (ML) is the backbone of this study, with several traditional algorithms being evaluated for sleep disorder classification. ML algorithms are designed to recognize patterns in data and make decisions based on these patterns, making them highly suitable for tasks like sleep disorder classification, which requires the analysis of complex datasets. The algorithms used in this study include:

#### **3.1.1 k-Nearest Neighbors (KNN)**

The k-Nearest Neighbors (KNN) algorithm is one of the simplest supervised learning methods used in classification and regression tasks. It operates on the principle of feature similarity, where a data point is classified based on the majority class among its k-nearest neighbors. The value of k is a process called parameter tuning that refers to the number of nearest neighbour data points to include in the majority voting process. There are various types of distance metrics, such as Euclidean, Manhattan and Minkowski[8]. In this study, KNN is applied to the Sleep Health and Lifestyle Dataset to classify sleep disorders by identifying the most similar past cases. The choice of the parameter "k" is crucial in determining the accuracy of the model, and genetic algorithms are used to optimize this value for better performance[5].

- **Advantages:** Simple, easy to implement, and effective for small datasets.
- **Disadvantages:** Computationally expensive for large datasets and sensitive to the choice of the parameter k.

#### **3.1.2 Support Vector Machines (SVM)**

Support Vector Machines (SVM) are another supervised learning algorithm used in this study[7]. SVMs work by finding the optimal hyperplane that best separates data into different

classes. In the context of sleep disorder classification, SVMs are particularly useful due to their ability to handle high-dimensional data. Different kernel functions (e.g., linear, radial basis function) can be applied to map data into a higher-dimensional space, improving classification accuracy. The paper uses genetic algorithms to optimize SVM parameters, such as the kernel type and penalty parameter, to enhance model performance.

- **Advantages:** Effective in high-dimensional spaces and with non-linear data.
- **Disadvantages:** Requires careful tuning of parameters, and can be computationally intensive.

### **3.1.3 Decision Tree (DT)**

Decision Trees are a non-parametric supervised learning algorithm used for classification tasks. In this paper, decision trees are applied to classify sleep disorders based on a series of decision rules inferred from the dataset features. A decision tree splits the dataset into smaller subsets based on feature importance, making it highly interpretable and easy to understand. However, decision trees are prone to overfitting, especially when the data is noisy, which can limit their generalizability. To address this, the study applies genetic algorithms to prune the tree and optimize its parameters[7].

- **Advantages:** Simple to understand, interpret, and visualize; works well with both numerical and categorical data.
- **Disadvantages:** Prone to overfitting and sensitive to small variations in the data.

### **3.1.4 Random Forest (RF)**

Random Forest is an ensemble learning technique that builds multiple decision trees and merges their outputs to improve classification accuracy. It corrects the overfitting problem of individual decision trees by averaging the predictions from a large number of trees, thus making it more robust. In this study, Random Forest is used to classify sleep disorders by aggregating the outputs of various decision trees trained on different parts of the dataset. The parameters of the random forest model, such as the number of trees and the maximum depth of each tree, are optimized using genetic algorithms to ensure better performance[7].

- **Advantages:** Reduces overfitting, handles large datasets well, and provides a robust model.
- **Disadvantages:** Requires more computational resources and is harder to interpret than a single decision tree.

## **3.2 Deep Learning Models**

Deep learning models, particularly artificial neural networks (ANNs), represent a more advanced form of machine learning that can automatically learn features from large datasets. In this study, deep learning models are compared with traditional machine learning algorithms to evaluate their performance in classifying sleep disorders.

### **3.2.1 Artificial Neural Networks (ANN)**

Artificial Neural Networks (ANNs) are inspired by the structure of the human brain and consist of interconnected layers of neurons (nodes). Each layer processes the input data and passes it to the next layer, learning progressively higher-level features. In this paper, ANN is applied to classify sleep disorders using data from the Sleep Health and Lifestyle Dataset. ANNs are highly effective in capturing complex patterns in the data due to their ability to automatically learn features during the training process, eliminating the need for manual feature engineering. The paper uses a feed-forward ANN, where the data flows in one direction from the input layer to the output layer. The ANN is trained using backpropagation, where the model's weights are adjusted based on the error observed between the predicted and actual outputs. The ANN model achieved the highest classification accuracy compared to other machine learning models used in the study. To further improve the model's performance, genetic algorithms are employed to optimize hyperparameters such as the learning rate, the number of hidden layers, and the number of neurons in each layer[9].

- **Advantages:** Excellent at capturing complex, non-linear relationships; automatic feature extraction.
- **Disadvantages:** Requires large datasets and significant computational power; can be difficult to interpret.

## **3.3 Optimization Techniques: Genetic Algorithms**

Optimization plays a crucial role in machine learning, particularly in fine-tuning the parameters of models to improve their performance. In this study, genetic algorithms (GAs) are used to optimize the hyperparameters of the machine learning models to ensure the best possible classification accuracy for sleep disorders.

### **3.3.1 Genetic Algorithms (GA)**

Genetic Algorithms are a type of evolutionary algorithm inspired by the process of natural selection. GAs are particularly useful for solving optimization problems where there are multiple potential solutions. In this paper, genetic algorithms are applied to optimize the parameters of the machine learning models, such as the k-value in KNN, the kernel type in SVM, and the depth of trees in Random Forest and Decision Trees. GAs operate by generating a population of candidate solutions, evaluating their fitness, and iteratively selecting the best candidates for crossover and mutation to generate new solutions.

The optimization process helps the models avoid local minima and improve their classification accuracy. For example, GAs help identify the optimal number of neighbors in KNN, the ideal penalty parameter in SVM, and the best number of trees in Random Forest. By using GAs, the study ensures that the models perform optimally on the dataset, leading to more accurate classification results.

- Advantages: Efficiently explores large parameter spaces, improves model performance, and avoids local optima.
- Disadvantages: Computationally expensive and may require fine-tuning of its own parameters (population size, mutation rate).

### **3.4 Dataset: Sleep Health and Lifestyle Dataset**

In this study, the **Sleep Health and Lifestyle Dataset** is used to train and evaluate the machine learning models. The dataset consists of 400 rows and 13 columns, containing features related to sleep patterns, daily activities, and health metrics[5]. The features include age, gender, occupation, sleep duration, and sleep quality, among others, making it suitable for developing models to classify sleep disorders like insomnia and sleep apnea.

Before training the models, the dataset undergoes pre-processing, including label encoding of categorical features and splitting the data into training and testing sets. This ensures that the models can be evaluated effectively, and their performance metrics can be compared.



## **CHAPTER 4**

### **ARCHITECTURAL BACKGROUND**

The architecture covers the entire workflow, from data acquisition and preprocessing to machine learning model implementation, optimization, and evaluation. The main components include the dataset, preprocessing pipeline, machine learning and deep learning models, and the genetic algorithm optimization layer.

#### **4.1 Data Acquisition and Preprocessing**

The Sleep Health and Lifestyle Dataset, utilized in this study, was acquired from the Kaggle platform, a popular repository for publicly available datasets. Upon acquisition, the dataset underwent several preprocessing steps to prepare it for machine learning.

##### **4.1.1 Sleep Health and Lifestyle Dataset**

The **Sleep Health and Lifestyle Dataset** serves as the foundation for the model training and evaluation process. This dataset contains 400 observations and 13 features, including age, occupation, sleep duration, and sleep quality, which are used to classify sleep disorders such as insomnia and sleep apnea[5].

##### **4.1.2 Data Preprocessing Pipeline**

Preprocessing the dataset is a critical step to ensure the models can process the data correctly. The preprocessing pipeline includes:

- **Handling Missing Data:** Rows with missing values are either removed or filled with the mean or median values.
- **Encoding Categorical Data:** Categorical variables like "gender" and "occupation" are encoded into numerical values to be understood by the machine learning models.
- **Feature Scaling:** Normalization or standardization is applied to scale features like age and sleep duration, ensuring that no single feature dominates the learning process due to its range of values.

#### **4.2 Machine Learning Model Architecture**

The architecture focuses on comparing various machine learning algorithms (MLAs), including traditional methods and deep learning models, to classify sleep disorders. Each model

follows the same input-output framework but processes data in distinct ways depending on the algorithm used.

### 4.2.1 Traditional ML Models

The traditional ML models used in the study include:

- k-Nearest Neighbors (KNN)
- Support Vector Machines (SVM)
- Decision Trees (DT)
- Random Forest (RF)

All these models accept preprocessed data as input and produce classification outputs (sleep disorder labels). Each model has specific hyperparameters (e.g., the k-value in KNN, kernel type in SVM, and the number of trees in Random Forest) that influence their performance.

#### 4.2.1.1 K-Nearest Neighbors

KNN is a simple yet effective non-parametric, instance-based learning algorithm that is used for both classification and regression. In KNN, the class of a data point is determined by examining the k closest training examples in the feature space. The model assumes that similar instances exist in close proximity. KNN is intuitive and easy to implement but can be computationally expensive with large datasets, as it requires calculating the distance to every training sample during prediction.

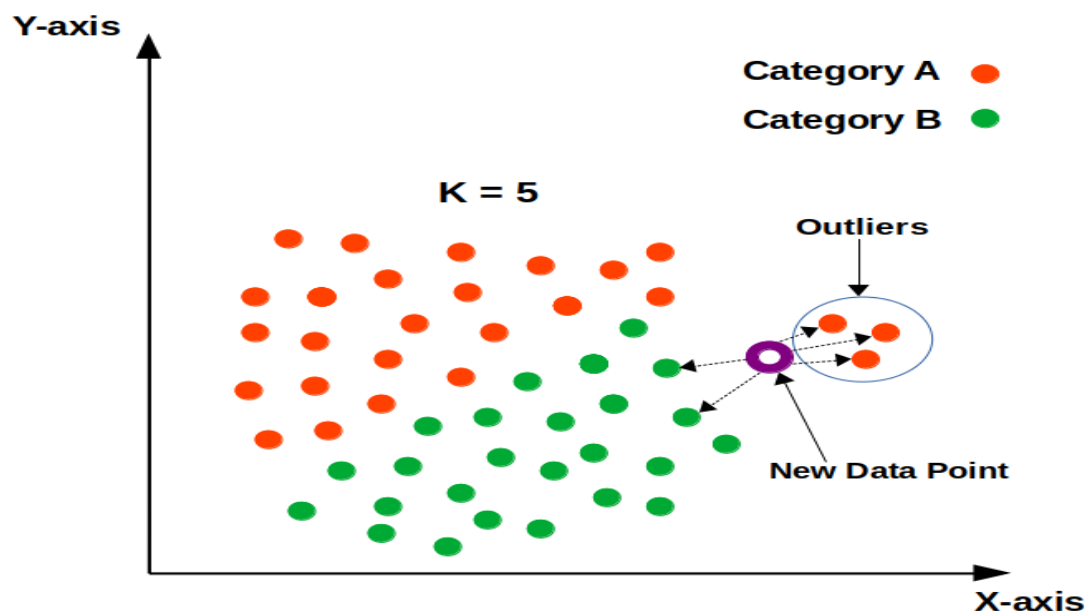


Fig 4.1 Diagram of K-Nearest Neighbors

**Key Components:**

- **Distance Metrics:** Typically uses Euclidean distance to measure the similarity between instances, but can also utilize other metrics as needed.
- **Voting Mechanism:** The predicted class is determined by majority voting among the  $k$  nearest neighbors.
- **Parameter  $k$ :** The choice of  $k$  can significantly affect the model's performance. A small  $k$  may be sensitive to noise, while a larger  $k$  may smooth out distinctions between classes.

**4.2.1.2 Support Vector Machine**

SVM is a robust supervised learning algorithm particularly effective for classification tasks involving high-dimensional data, such as sleep study features (e.g., EEG, EOG, and EMG signals). SVM works by identifying the optimal hyperplane that separates different classes (e.g., types of sleep disorders) while maximizing the margin between them. This makes it suitable for scenarios where clear class boundaries exist.

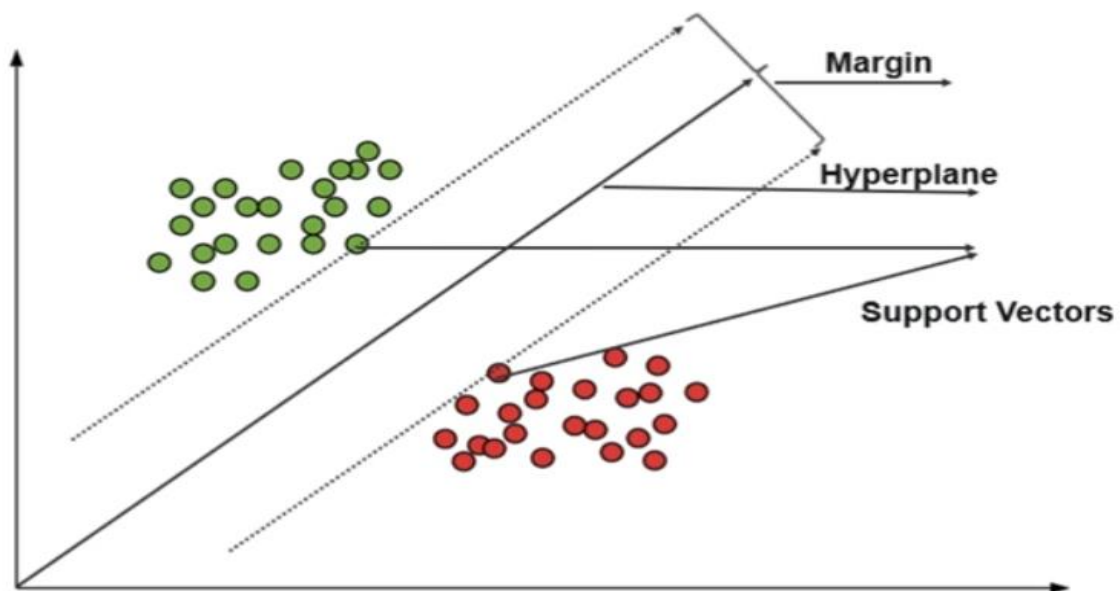


Fig 4.2 Diagram of Support Vector Machine

**Key Components:**

- **Hyperplane:** The decision boundary that classifies the data into different sleep disorder categories.

- **Support Vectors:** Critical data points near the hyperplane that influence its position and orientation.
- **Kernel Functions:** Used to transform non-linearly separable data into a higher-dimensional space, making it easier for SVM to find an appropriate hyperplane.

#### 4.2.1.3 Decision Trees

Decision Trees provide an intuitive model for classifying sleep disorders based on a series of feature-based decisions. Each node in the tree represents a feature, and the branches represent decision rules leading to a classification outcome at the leaf nodes. DTs are particularly effective for exploratory analysis, as they allow practitioners to visualize how decisions are made.

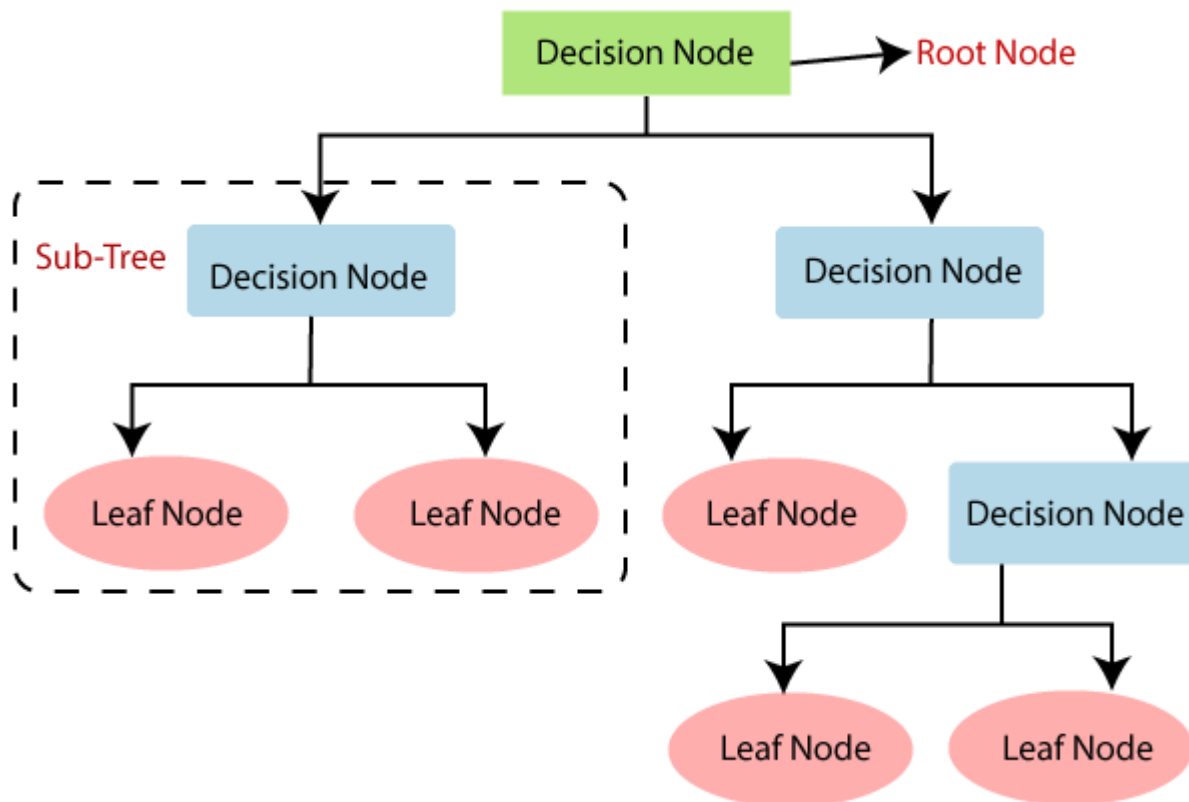


Fig 4.3 Diagram of Decision Tree

#### Key Components:

- **Root Node:** Represents the entire dataset and is the starting point for classification.
- **Internal Nodes:** Decision points that split the data based on specific feature values.

- **Leaf Nodes:** Final classifications for each type of sleep disorder.
- **Splitting Criteria:** Utilizes measures like Gini impurity or information gain to determine the best features for splitting.

#### 4.2.1.4 Random Forest

Random Forests enhance the performance of Decision Trees by combining multiple trees into an ensemble model. This approach reduces overfitting and increases prediction accuracy, making it well-suited for classifying sleep disorders based on diverse data inputs. RF can handle large datasets with numerous features, typical in sleep studies.

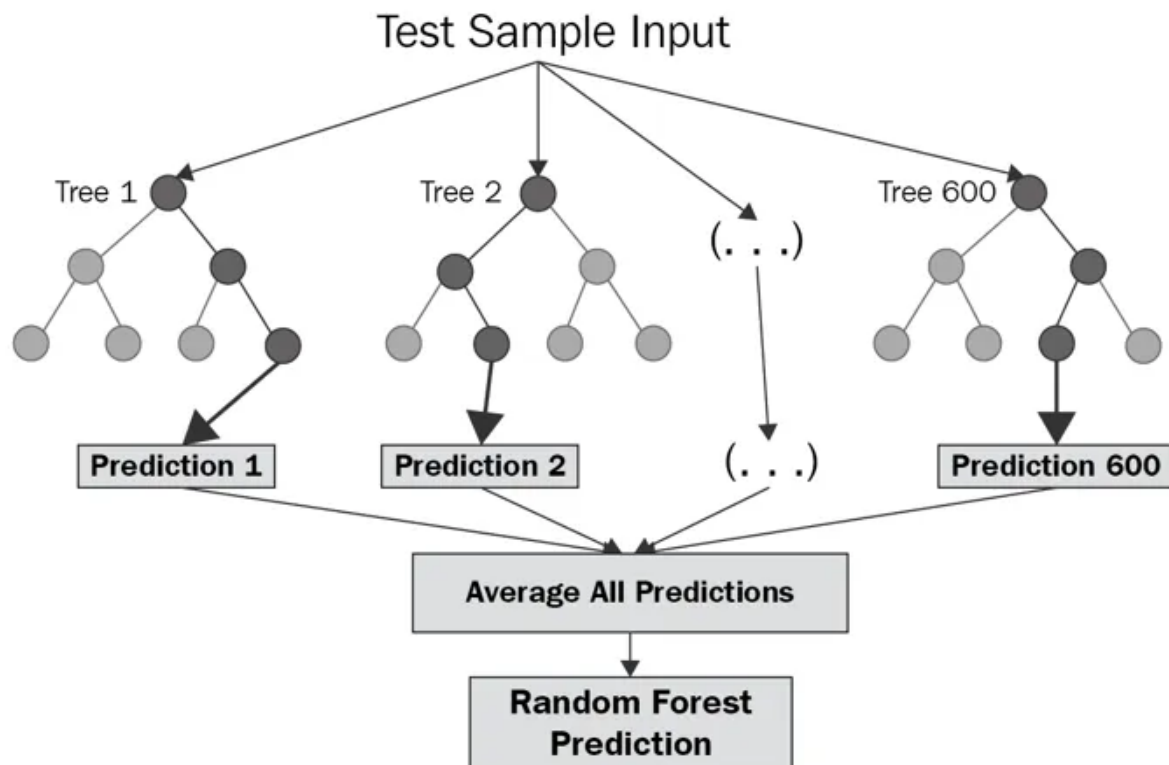


Fig 4.4 Diagram of Random Forest

#### 4.2.2 Deep Learning Model

An **Artificial Neural Network (ANN)** is used to classify sleep disorders by automatically learning complex patterns from the data. ANNs are highly flexible models capable of capturing complex relationships in data, making them particularly suitable for classifying sleep disorders based on intricate patterns in sleep data. ANNs can learn representations directly from raw data,

such as time-series data from polysomnography (PSG) readings. The ANN consists of multiple layers:

- **Input Layer:** Receives preprocessed features.
- **Hidden Layers:** Multiple layers of neurons that perform transformations and pass data forward.
- **Output Layer:** Produces the final classification result (sleep disorder).
- **Activation Functions:** Non-linear functions (e.g., ReLU, Sigmoid) applied to neuron outputs, enabling the network to learn complex patterns.

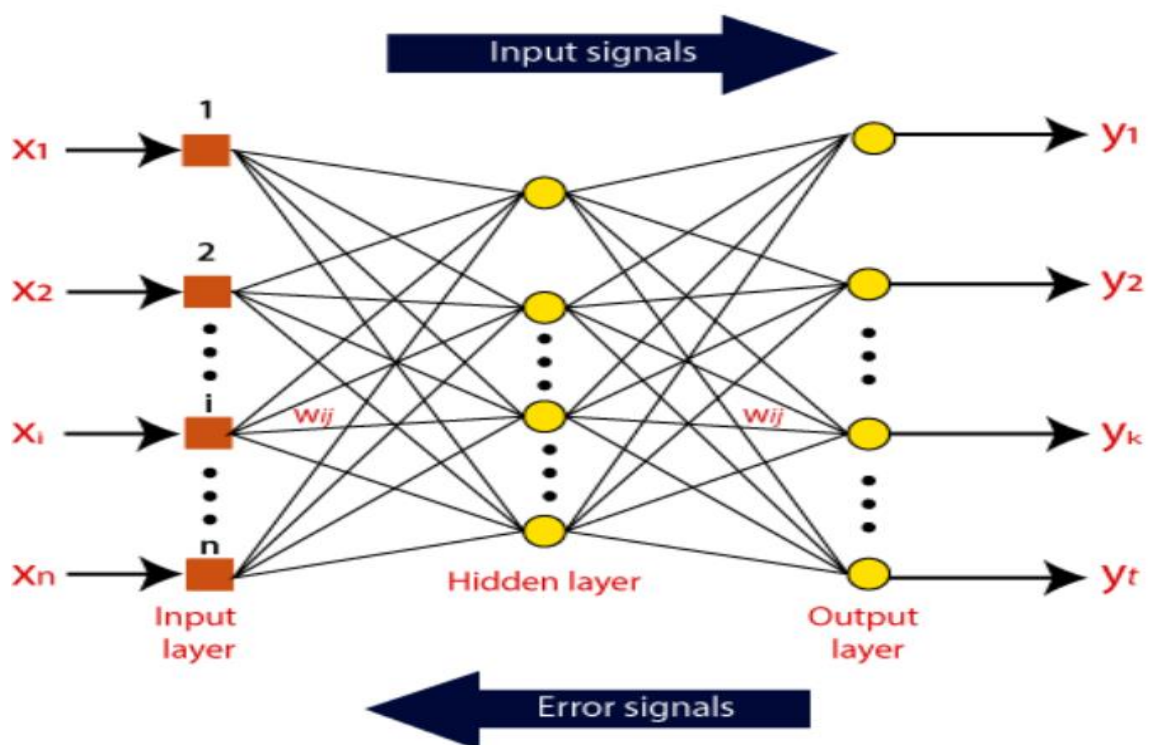


Fig 4.5 Diagram of Artificial Neural Network

### 4.3 Genetic Algorithm Optimization Architecture

The genetic algorithm (GA) plays a pivotal role in optimizing the parameters of the machine learning models. GAs are employed to search for the optimal hyperparameters, which significantly impact the classification accuracy of each model. GA is used to tune the parameters and solve optimization problems for which there are several of candidate solutions[10].

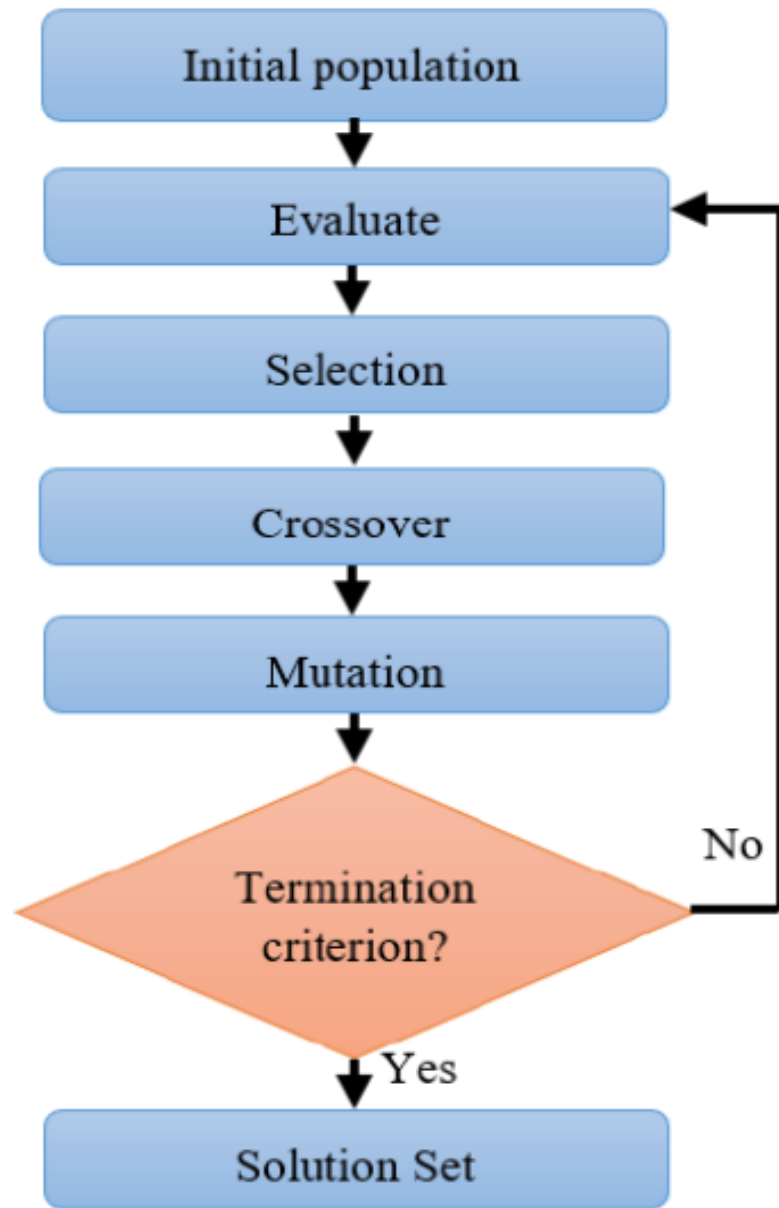


Fig 4.6 Diagram of Genetic Algorithm

The genetic algorithm optimization workflow involves the following steps:

- **Initialization:** A population of candidate solutions (parameter sets) is generated randomly.
- **Fitness Evaluation:** Each candidate is evaluated based on its performance (e.g., classification accuracy).
- **Selection:** The best-performing candidates are selected for the next generation.

- **Crossover and Mutation:** The selected candidates undergo crossover and mutation to produce new offspring (parameter sets), introducing diversity and helping the algorithm explore the solution space.

**The GA optimizes parameters such as:**

- k-value for KNN
- Kernel type for SVM
- Depth of trees for Decision Trees and Random Forest
- Learning rate, number of layers, and neurons for ANN

## **4.4 Performance Evaluation and Comparison**

After optimizing the models using genetic algorithms, the final step is performance evaluation. The accuracy metric is suitable when the label class is well-balanced; however, it is not helpful with unbalanced classes. Therefore, this research used four evaluation metrics: classification accuracy, precision, recall and the F1-score [6]. The following metrics are used to assess the performance of the machine learning models:

- **Accuracy:** Measures the percentage of correctly classified instances.
- **Precision:** The proportion of true positive predictions among all positive predictions.
- **Recall:** The proportion of true positive predictions among all actual positive instances.
- **F1-Score:** The harmonic mean of precision and recall, giving a balanced evaluation of the model.

The evaluation process helps compare the effectiveness of different machine learning models (both traditional and deep learning) in classifying sleep disorders.



## **Final System Architecture Overview**

This is the diagram of the Machine Learning Model to Classify Sleep disorders without Genetic Algorithm

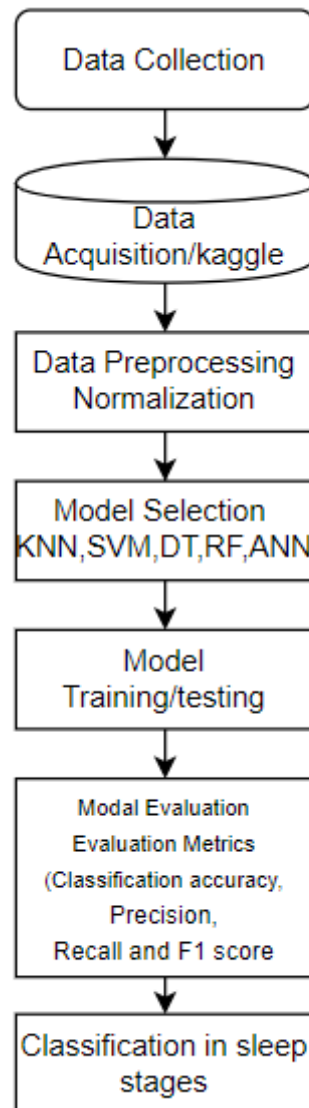


Fig 4.7 Diagram of the Machine Learning Model To Classify Sleep disorders.

## The proposed optimized model for sleep disorder classification by Genetic Algorithm

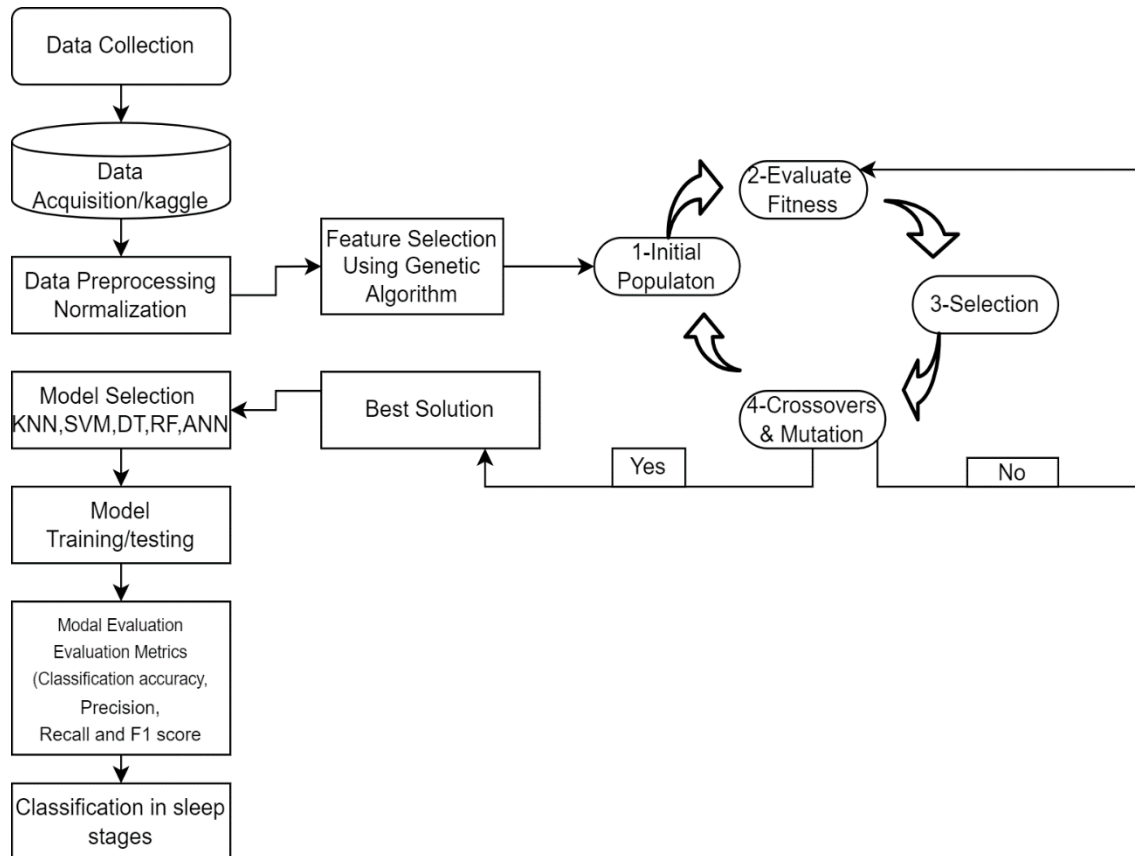


Fig 4.8 The proposed optimised model for sleep disorder classification.

The architectural design of the system integrates various machine learning models and deep learning techniques to classify sleep disorders efficiently. Through the optimization of model parameters using genetic algorithms, the architecture aims to enhance model performance, leading to more accurate and reliable sleep disorder classification. The diagrams provided illustrate the interaction between the different components, from data preprocessing to the final classification result, highlighting the robust nature of the system architecture.

## CHAPTER 5

### USAGE SCENARIOS

Machine learning algorithms for classifying sleep disorders offer a wide range of applications, especially in healthcare, where the accurate diagnosis of conditions such as sleep apnea and insomnia is crucial. The system proposed in this paper can be used in various real-world scenarios to improve diagnosis accuracy, reduce human error, and enhance overall patient care. This section outlines several usage scenarios, demonstrating how the system could be applied in clinical and non-clinical settings to support sleep disorder diagnosis and management.

#### 5.1 Consumer Health Applications in Wearable Devices

Wearable devices such as fitness trackers and smartwatches are increasingly popular, with many users monitoring their sleep patterns daily. These devices already collect basic sleep metrics like sleep duration, movement during sleep, and heart rate. However, they often lack the sophisticated algorithms necessary to classify sleep disorders accurately.

The system helps in:

- **Integration with Wearables:** The machine learning models used in this study could be integrated into wearable technology to provide more accurate sleep stage classification and detect potential sleep disorders. The models can use the data gathered from wearable sensors to classify sleep stages and detect irregularities, such as breathing interruptions (a sign of sleep apnea) or fragmented sleep (indicative of insomnia).
- **Personalized Insights:** The system can provide users with personalized sleep insights and recommendations based on the classification results, empowering them to take action if potential sleep disorders are detected. For example, the system could alert users to possible sleep apnea and recommend seeing a healthcare professional for further testing.
- **Continuous Monitoring:** Unlike a one-time sleep clinic visit, wearable devices with integrated machine learning models can offer continuous sleep monitoring over time, allowing users to track changes in their sleep patterns and identify trends that may indicate the development of a sleep disorder.

## **5.2 Automated Sleep Disorder Diagnosis in Sleep Clinics**

A sleep clinic that specializes in diagnosing sleep disorders receives a steady flow of patients who undergo polysomnography (PSG) tests, a standard procedure that records brain waves, blood oxygen levels, heart rate, and breathing during sleep. Traditionally, medical professionals must manually review the sleep data, classify sleep stages, and diagnose conditions such as sleep apnea, insomnia, or restless leg syndrome.

The System Helps as:

- **Streamlined Diagnosis Process:** The proposed machine learning system can automate the process of sleep stage classification and disorder identification using the data collected from the PSG test. Once the patient's data is preprocessed, the optimized machine learning model (e.g., ANN or Random Forest) can classify the data and produce an accurate diagnosis.
- **Reduction in Human Error:** By automating the classification process, the system reduces the likelihood of human error, ensuring a more consistent and reliable diagnosis for each patient.
- **Faster Turnaround:** Instead of requiring hours or days for a sleep expert to manually analyze PSG data, the machine learning system can process and analyze the data in a matter of minutes, allowing the clinic to provide faster results to patients.

## **5.3 Sleep Disorder Screening in Primary Care Settings**

In a primary care clinic, general practitioners (GPs) often encounter patients complaining of fatigue, insomnia, or irregular sleep patterns. While the clinic lacks the resources for full PSG testing, GPs can still gather basic health metrics such as sleep duration, daily activity levels, and patient-reported sleep quality.

The System Helps:

- **Preliminary Screening Tool:** The machine learning system can be adapted to screen for potential sleep disorders based on the basic sleep and lifestyle data collected from patients. Using the Sleep Health and Lifestyle Dataset, the system can identify potential risks for conditions like insomnia or mild sleep apnea without needing full PSG data.

- **Refined Patient Referrals:** Based on the results of this preliminary screening, GPs can make more informed decisions about whether a patient requires specialized testing or should be referred to a sleep clinic. This reduces unnecessary referrals and ensures that patients in need of further assessment are prioritized.
- **Patient Monitoring:** The system can also be used as a monitoring tool for patients undergoing treatment for sleep disorders. By periodically inputting sleep and lifestyle data, the GP can track progress and adjust treatments accordingly.

## **5.4 Sleep Research and Data Analysis**

Researchers studying sleep patterns and disorders often collect vast amounts of data from multiple sources, including hospitals, sleep clinics, and wearable devices. Analyzing this data manually can be time-consuming and prone to bias or inconsistencies.

The System Helps:

- **Large-Scale Data Analysis:** The machine learning system can process and analyze large sleep datasets more efficiently than manual methods. It can identify patterns, trends, and correlations across multiple variables, such as age, occupation, and sleep duration, which can lead to new insights into sleep disorders.
- **Model Development for Research:** Researchers can use the optimized models developed in this study to refine their own research methods. For example, by incorporating genetic algorithms to optimize their machine learning models, researchers can improve their classification results, leading to more accurate findings.
- **Cross-Study Comparisons:** The system can also be used to compare results across different studies by standardizing the classification of sleep stages and disorders, enabling researchers to draw more reliable conclusions from disparate datasets.

## CHAPTER 6

### METHODOLOGIES AND DISCUSSION

The key processes and methodologies employed to classify sleep disorders using machine learning algorithms. The primary focus is on the preparation of the dataset, the implementation of various machine learning models, and the optimization of these models using genetic algorithms (GAs). A discussion of the results is included to analyze the performance of the models.

#### 6.1 Dataset and Preprocessing

The study uses the **Sleep Health and Lifestyle Dataset**, which contains 400 rows and 13 columns. The dataset includes features like age, gender, occupation, sleep duration, and sleep quality. Each observation corresponds to a real-world individual and their associated sleep and lifestyle metrics. The target variable is the sleep disorder label, which can be classified into three categories: none, sleep apnea, and insomnia.

##### Preprocessing Steps

Data preprocessing is essential for improving the performance of machine learning models.

The preprocessing steps in this study include:

- **Handling Missing Data:** Missing values were replaced with mean or median values.
- **Encoding Categorical Data:** Features like gender and occupation were label-encoded into numerical form.
- **Scaling Features:** Continuous variables were normalized to ensure that no single feature dominates the model.
- **Train-Test Split:** The dataset was divided into 70% training data and 30% testing data to evaluate model performance.

These steps ensured that the data was prepared for training and testing with machine learning algorithms.

## **6.2 Machine Learning Models**

The methodologies primarily focus on machine learning algorithms (MLAs), deep learning models, and optimization techniques such as genetic algorithms (GAs). The goal is to evaluate the performance of these models in accurately classifying sleep disorders using a publicly available dataset, while exploring various factors that affect model performance.

### **6.2.1 k-Nearest Neighbors (KNN)**

The k-nearest neighbors (KNN) algorithm is a non-parametric method used for classification and regression. In this study, KNN was applied to classify sleep disorders by comparing each individual's sleep metrics with their nearest neighbors. The number of neighbors, **k**, is a key parameter that significantly affects performance.

- **Optimization:** The genetic algorithm (GA) was used to tune the value of **k** to find the optimal number of neighbors for the highest classification accuracy.
- **Performance Evaluation:** KNN's performance was evaluated using accuracy, precision, recall, and F1-score. While KNN is effective for small datasets, it can be computationally expensive for larger datasets and sensitive to noisy data.

### **6.2.2 Support Vector Machines (SVM)**

Support vector machines (SVM) are widely used for classification tasks due to their effectiveness in high-dimensional spaces. SVMs work by finding a hyperplane that best separates the data into different classes.

- **Optimization:** The study used a radial basis function (RBF) kernel for SVM, and genetic algorithms were employed to optimize key parameters like the regularization term (**C**) and the kernel coefficient ( $\gamma$ ).
- **Performance Evaluation:** SVM performed well on the dataset, especially in terms of precision. However, it struggled with imbalanced data due to the small number of observations in certain classes.

### **6.2.3 Decision Tree (DT)**

A decision tree is a simple, interpretable model that uses a tree-like structure to classify data by splitting it into subsets based on feature values. Each internal node of the tree corresponds to a decision rule, and each leaf node represents a classification.

- **Optimization:** GAs were used to optimize the maximum depth of the tree and the minimum number of samples required to split an internal node, reducing overfitting and improving generalization.

- **Performance Evaluation:** Decision trees provided interpretable results but were prone to overfitting, especially with noisy or imbalanced data. Pruning and GA optimization helped mitigate this issue.

#### **6.2.4 Random Forest (RF)**

Random forest is an ensemble learning method that combines multiple decision trees to improve classification accuracy and reduce overfitting. By aggregating the predictions of individual trees, random forest achieves better performance than a single decision tree.

- **Optimization:** GAs were used to tune the number of trees and the maximum depth of individual trees in the forest.
- **Performance Evaluation:** Random forest performed well across all evaluation metrics, especially when dealing with noisy data. Its ability to generalize from diverse decision trees made it one of the top-performing models in the study.

#### **6.2.5 Artificial Neural Networks (ANN)**

Artificial neural networks (ANNs) are deep learning models inspired by the structure of the human brain. ANNs consist of interconnected neurons organized into layers, which learn complex patterns in the data through multiple iterations of forward propagation and backpropagation.

- **Network Architecture:** The ANN used in this study had an input layer that received the sleep and lifestyle features, several hidden layers, and an output layer that predicted the class (sleep disorder). Each neuron was assigned a weight that was updated during training to minimize the error between predicted and actual values.
- **Optimization:** Genetic algorithms were employed to optimize hyperparameters such as the number of neurons in each hidden layer, the learning rate, and the number of training epochs.
- **Performance Evaluation:** ANN achieved the highest classification accuracy (92.92%) and outperformed traditional ML models in terms of recall and F1-score. The automatic feature extraction by ANN allowed it to capture non-linear patterns that other models could not.

### **6.3 Genetic Algorithm Optimization**



Genetic algorithms (GAs) are a type of optimization technique inspired by the process of natural selection. In this study, GAs were used to optimize the hyperparameters of all machine learning models.

The GA process involves several key steps:

- **Initialization:** A population of potential solutions (i.e., hyperparameter sets) is randomly generated.
- **Fitness Evaluation:** The fitness of each candidate solution is evaluated based on the model's classification accuracy.
- **Selection:** The top-performing solutions are selected to move on to the next generation.
- **Crossover and Mutation:** Crossover combines pairs of solutions to create new offspring, while mutation introduces random changes to maintain diversity in the population.
- **Termination:** The process repeats until an optimal set of parameters is found or a maximum number of generations is reached.

Using GAs to tune model hyperparameters led to significant performance improvements across all algorithms. The ability of GAs to explore a wide range of parameter combinations enabled the models to achieve higher accuracy, precision, recall, and F1-scores compared to manual tuning methods.

## **6.4 Discussion**

The application of various machine learning models for sleep disorder classification revealed significant differences in performance. Each model had strengths and weaknesses in terms of accuracy, precision, recall, and generalizability.

### **6.4.1 Comparison of Machine Learning Models**

The results showed that traditional models like Random Forest and SVM performed well, but deep learning models, particularly ANNs, outperformed them in terms of accuracy and recall. The ANN's ability to automatically extract features and capture non-linear relationships made it the best-performing model with a classification accuracy of 92.92%.[5]

### **6.4.2 Impact of Genetic Algorithms**

Genetic algorithms played a crucial role in improving the models' performance. The optimized hyperparameters resulted in significant gains in accuracy and other performance metrics. This was particularly noticeable in models like KNN and Random Forest, where default parameters would have limited their classification ability. The use of genetic algorithms for

hyperparameter tuning proved to be a key factor in the success of all models. GAs allowed the models to explore a wide range of hyperparameter configurations, ensuring that the best possible settings were used. This resulted in significant improvements in accuracy and other evaluation metrics compared to default parameters.

### **6.4.3 Challenges**

The study faced challenges related to data imbalance, particularly for certain sleep disorders like insomnia, which had fewer observations. Despite this, the models performed well, but future work could involve using techniques like SMOTE to balance the dataset further.

The successful application of machine learning algorithms and genetic optimization techniques for the classification of sleep disorders. While traditional models performed adequately, the deep learning approach, particularly ANNs, provided the most accurate results. Genetic algorithms significantly enhanced model performance, proving essential for optimizing hyperparameters. Although some challenges related to data imbalance and privacy remain, the models offer a promising solution for automating sleep disorder diagnosis in healthcare applications.

## **CHAPTER 7**

### **SECURITY ISSUES**

#### **7.1 Data Privacy and Confidentiality**

The Sleep Health and Lifestyle Dataset used in the model contains sensitive information such as age, gender, health metrics, and potentially identifiable personal data[11]. Any breach in confidentiality could violate data protection laws like GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act), depending on the region. Key risks include:

- **Unauthorized Access:** If the dataset is not securely stored or transmitted, attackers could gain access to sensitive health information.
- **Data Leakage:** Machine learning models, especially when deployed, could inadvertently leak sensitive information during prediction, training, or through model inversion attacks.

#### **7.2 Model Inversion Attacks**

Model inversion is a type of attack where an adversary uses the outputs of a model to infer the sensitive training data[12]. In the case of a healthcare model like this one, an attacker could potentially reverse-engineer the model to reconstruct input data (such as personal health details), leading to serious privacy violations.

#### **7.3 Adversarial Attacks**

Machine learning models, particularly deep learning models like ANNs, are vulnerable to adversarial attacks[13]. These are subtle manipulations of input data that cause the model to make incorrect classifications. In the context of sleep disorder classification:

- **Adversarial Perturbations:** Attackers could add small, unnoticeable changes to input data (e.g., sleep metrics) that could lead the model to misclassify a sleep disorder, causing either false positives or false negatives.

- **Poisoning Attacks:** During training, if malicious data is introduced into the dataset, it could compromise the integrity of the model, leading to poor performance or biased outcomes.

## **7.4 Model Theft and Intellectual Property Concerns**

Once deployed, machine learning models can be susceptible to model extraction attacks, where an attacker uses inputs and outputs to approximate the behavior of the model[14]. This could lead to intellectual property theft, where the attacker replicates the model and its functions without authorization. In healthcare, this could result in the unauthorized use of the model for commercial purposes, or worse, malicious tampering with medical diagnostics.

## **7.5 Data Integrity**

The integrity of the input data is crucial for accurate classification. If an attacker tampers with the input data (e.g., modifying patient sleep metrics), it could lead to incorrect classifications or diagnoses[15]. This is particularly dangerous in healthcare applications where misclassifications can have serious health consequences.

One significant threat to data integrity in machine learning models is data poisoning attacks. In these attacks, an adversary introduces malicious or corrupted data into the training set with the intent of manipulating the model's predictions. This could result in a model that consistently misclassifies certain sleep disorders, skewing diagnoses for specific groups of patients.

For example, an attacker could inject data that causes the model to underdiagnose sleep apnea in women or overdiagnose insomnia in older patients. Such manipulations would not only undermine the model's utility but could also exacerbate existing healthcare disparities.

Input manipulation during the model's deployment phase is another threat to data integrity. An attacker could tamper with input data by altering metrics like sleep duration or quality, leading to misclassification of sleep disorders. In healthcare settings, this could have far-reaching consequences, as erroneous predictions could mislead healthcare providers, causing delayed or inappropriate treatments. Ensuring the integrity of data throughout the machine learning lifecycle will safeguard the accuracy and reliability of sleep disorder classification models, ultimately leading to better patient care.

## **7.6 Deployment Security**

When the model is deployed in a clinical or consumer health application (such as wearable devices or healthcare systems), it can face various security threats[16]:

- **API Vulnerabilities:** If the model is accessible via an API, vulnerabilities in the API could allow attackers to manipulate the input-output flow, bypass access controls, or inject malicious data.
- **Malware or Ransomware Attacks:** Healthcare systems are frequent targets of ransomware attacks, where attackers lock users out of their systems until a ransom is paid. If the model is part of a larger healthcare system, an attack on the infrastructure could disable access to the model.

## **7.7 Fairness and Bias Issues**

Although not typically classified as a traditional security issue, bias in machine learning models can lead to unfair outcomes, significantly impacting the quality of care in healthcare settings. Fairness issues arise when models are trained on imbalanced or non-representative datasets, which can result in the model performing inconsistently across different demographic groups. This disparity can lead to unequal treatment, inaccurate diagnoses, or even misdiagnosis for certain populations. For instance, if a model is primarily trained on data from a specific demographic—such as younger, male, or high-income individuals—it may struggle to generalize its predictions for underrepresented groups, such as women, the elderly, or minority populations. In healthcare, this bias could manifest in sleep disorder classification models underperforming for these groups, potentially leading to undiagnosed or misdiagnosed conditions. This creates a significant ethical issue, as the ultimate goal of healthcare is to provide equitable treatment for all individuals, regardless of background. Addressing these biases is crucial to ensure that machine learning systems in healthcare do not perpetuate or exacerbate existing disparities in medical care. [17].

## **CHAPTER 8**

### **CONCLUSION**

Machine learning algorithms have proven to be highly effective tools for automating the classification of sleep disorders, a task that is traditionally labor-intensive and prone to human error. By leveraging advanced techniques such as genetic algorithms for optimization, machine learning models, including k-nearest neighbors, support vector machines, decision trees, random forests, and artificial neural networks, can accurately classify sleep disorders like insomnia and sleep apnea. The introduction of deep learning models, particularly artificial neural networks, has demonstrated the capacity to automatically learn complex patterns in data, resulting in superior classification performance compared to traditional models.

Genetic algorithms played a critical role in fine-tuning the parameters of these models, significantly improving accuracy, precision, recall, and F1-scores. This optimization process ensured that the models performed at their highest potential, reducing both overfitting and misclassification. The application of these optimized models in healthcare environments could streamline the diagnosis of sleep disorders, enabling faster and more reliable results for patients. The potential applications extend beyond clinical settings, with opportunities to integrate these models into consumer health technologies, such as wearable devices, allowing for continuous monitoring and early detection of sleep-related health issues.

Although challenges remain, particularly regarding the size of the dataset and the imbalanced nature of the data, the results of this study highlight the robustness of machine learning in medical diagnosis. The proposed optimised ANN with GA achieved the highest accuracy over the other MLAs at 92.92%. The precision, recall, and F1-score values on the testing data were 92.01%, 93.80% and 91.93%, respectively. Even with a limitation in the amount of data. This study addressed the challenges in implementing MLAs for classification sleep disordering. However, large datasets are still needed for training and evaluating models in this field. The MLAs with GA can significantly improve the accuracy of sleep disorder classification. Future work will focus on developing MLAs using unsupervised learning in addition to assessing the dataset on a new model and comparing its performance against existing state-of-the-art models[5].

## REFERENCES

- [1] S. Djanian, A. Bruun, and T. D. Nielsen, “Sleep classification using consumer sleep technologies and AI: A review of the current landscape,” *Sleep Med.*, vol. 100, pp. 390–403, Dec. 2022.
- [2] N. Salari, A. Hosseinian-Far, M. Mohammadi, H. Ghasemi, H. Khazaie, A. Daneshkhah, and A. Ahmadi, “Detection of sleep apnea using machine learning algorithms based on ECG signals: A comprehensive systematic review,” *Expert Syst. Appl.*, vol. 187, Jan. 2022, Art. no. 115950.
- [3] C. Li, Y. Qi, X. Ding, J. Zhao, T. Sang, and M. Lee, “A deep learning method approach for sleep stage classification with EEG spectrogram,” *Int. J. Environ. Res. Public Health*, vol. 19, no. 10, p. 6322, May 2022.
- [4] M. Bahrami and M. Forouzanfar, “Sleep apnea detection from single-lead ECG: A comprehensive analysis of machine learning and deep learning algorithms,” *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–11, 2022.
- [5] Talal Sarheed Alshammari “Applying Machine Learning Algorithms for the Classification of Sleep Disorders”,*IEEE Access*, 13 March 2024.
- [6] D. M. W. Powers, “Evaluation: From precision, recall and F1measure to ROC, informedness, markedness and correlation,” 2020, arXiv:2010.16061.
- [7] F. Pedregosa, “Scikit-learn: Machine learning in Python,” *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, Nov. 2011.
- [8] M. Q. Hatem, “Skin lesion classification system using a K-nearest neighbor algorithm,” *Vis. Comput. Ind., Biomed., Art*, vol. 5, no. 1, pp. 1–10, Dec. 2022.
- [9] Y. You, X. Zhong, G. Liu, and Z. Yang, “Automatic sleep stage classification: A light and efficient deep neural network model based on time, frequency and fractional Fourier transform domain features,” *Artif. Intell. Med.*, vol. 127, May 2022, Art. no. 102279.

- [10] A. Hichri, M. Hajji, M. Mansouri, K. Abodayeh, K. Bouzrara, H. Nounou, and M. Nounou, “Genetic-algorithm-based neural network for fault detection and diagnosis: Application to grid-connected photovoltaic systems,” *Sustainability*, vol. 14, no. 17, p. 10518, Aug. 2022.
- [11] McGraw, D. (2013). Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data. *Journal of the American Medical Informatics Association*, 20(1), 29-34. doi:10.1136/amiajnl-2012-001029.
- [12] Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1322-1333). doi:10.1145/2810103.2813677.
- [13] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*.
- [14] Tramer, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. (2016). Stealing machine learning models via prediction APIs. In *25th USENIX Security Symposium (USENIX Security 16)* (pp. 601-618).
- [15] Aggarwal, C. C. (2015). *Data Mining: The Textbook*. Springer International Publishing. doi:10.1007/978-3-319-14142-8.
- [16] Breidenbach, L., Daian, P., Tramèr, F., & Juels, A. (2021). Machine learning security: Threats, current tools, and future directions. *arXiv preprint arXiv:2106.07174*.
- [17] Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and machine learning: Limitations and opportunities. *fairmlbook.org*.