A Project report on

UPI FRAUD DETECTION USING MACHINE LEARNING

Submitted in partial fulfillment of the requirements

for the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

(DATA SCIENCE)

By

S. JAHEDA	**214G1A3229**
G. AFRA TAHASEEN	**214G1A3202**
K. DIVYA MADHURI	**214G1A3219**
P. MOHAMMAD ARSHAD	**214G1A3253**

Under the Guidance of

Ms. P. SIRISHA **M. Tech**
Assistant Professor

Department of Computer Science & Engineering
(Data Science)

SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY
(AUTONOMOUS)
Rotarypuram Village, B K Samudram Mandal, Ananthapuramu - 515701

2024-2025

SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY

(AUTONOMOUS)

(Affiliated to JNTUA, Accredited by NAAC with 'A' Grade, Approved by AICTE, New Delhi &
Accredited by NBA (EEE, ECE & CSE)
Rotarypuram Village, BK Samudram Mandal, Ananthapuramu-515701

COMPUTER SCIENCE & ENGINEERING

(DATA SCIENCE)

Certificate

This is to certify that the project report entitled UPI Fraud Detection Using Machine Learning is the bonafide work carried out by **S. Jaheda, G. Afra Tahaseen, K. Divya Madhuri, P.Mohammad Arshad** bearing Roll Number **214G1A3229, 214G1A3202, 214G1A3219, 214G1A3253** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering(Data Science)** during the academic year 2024-2025.

Project Guide	**Head of the Department**
Ms.P. Sirisha, M.Tech	Dr. P. Chitralingappa, M.Tech., Ph.D
Assistant Professor	Associate professor & Head

Date:	**External Examiner**
Place: Rotarypuram	

DECLARATION CERTIFICATE

We students of **Computer Science and Engineering(Data Science)** , **SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY(AUTONOMOUS)**, Rotarypuram, hereby declare that the dissertation entitled **"UPI FRAUD DETECTION USING MACHINE LEARNING"** embodies the report of our project work carried out by us during IV year under the guidance of Ms.P.Sirisha,M.Tech, Assistant Professor ,Department of Computer Science and Engineering(Data Science), Srinivasa Ramanujan Institute of Technology, and this work has been submitted for the partial fulfillment of the requirements for the award of degree of Bachelor of Technology.

The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree or Diploma.

Date:

Place:

S.No.	Name of the Student	Roll Number	Signature
1	S. Jaheda	214G1A3229	
2	G. Afra Tahaseen	214G1A3202	
3	K. Divya Madhuri	214G1A3219	
4	P. Mohammad Arshad	214G1A3253	

Vision & Mission of the SRIT

Vision:

To become a premier Educational Institution in India offering the best teaching and learning environment for our students that will enable them to become complete individuals with professional competency, human touch, ethical values, service motto, and a strong sense of responsibility towards environment and society at large.

Mission:

- Continually enhance the quality of physical infrastructure and human resources to evolve in to a center of excellence in engineering education.
- Provide comprehensive learning experiences that are conducive for the students to acquire professional competences, ethical values, life-long learning abilities and understanding of the technology, environment and society.
- Strengthen industry institute interactions to enable the students work on realistic problems and acquire the ability to face the ever changing requirements of the industry.
- Continually enhance the quality of the relationship between students and faculty which is a key to the development of an exciting and rewarding learning environment in the college.

Vision & Mission of the Department of CSE (Data Science)

Vision:

To evolve as a leading department by offering best comprehensive teaching and learning practices for students to be self-competent technocrats with professional ethics and social responsibilities.

Mission:

DM 1: Continuous enhancement of the teaching-learning practices to gain profound knowledge in theoretical & practical aspects of computer science applications.

DM 2: Administer training on emerging technologies and motivate the students to inculcate self-learning abilities, ethical values and social consciousness to become competent professionals.

DM 3: Perpetual elevation of Industry-Institute interactions to facilitate the students to work on real-time problems to serve the needs of the society.

Program Educational Objectives (PEOs)

An SRIT graduate in Computer Science & Engineering (Data Science), after three to four years of graduation will:

PEO 1: Lead a successful professional career in IT / ITES industry / Government organizations with ethical values.

PEO 2: Become competent and responsible computer science professional with good communication skills and leadership qualities to respond and contribute significantly for the benefit of society at large.

PEO 3: Engage in life-long learning, acquiring new and relevant professional competencies / higher academic qualifications.

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible, whose constant guidance and encouragement crowned our efforts with success. It is a pleasant aspect that I have now the opportunity to express my gratitude for all of them.

It is with immense pleasure that I would like to express my indebted gratitude to my Guide **Ms.P.Sirisha, Assistant Professor ,Computer Science and Engineering (Data Science)**, who has guided me a lot and encouraged me in every step of the project work. we thank her for the stimulating guidance, constant encouragement and constructive criticism which have made possible to bring out this project work.

we are very much thankful to **Dr. P. Chitralingappa, Associate Professor & Head of the Department, Computer Science and Engineering (Data Science),** for his kind support and for providing necessary facilities to carry out the work.

I wish to convey my special thanks to **Dr. G. Balakrishna, Principal** of **Srinivasa Ramanujan Institute of Technology** for giving the required information in doing my project work. Not to forget, I thank all other faculty and non-teaching staff, and my friends who had directly or indirectly helped and supported me in completing my project in time.

I also express our sincere thanks to the Management for providing excellent facilities**.**

Finally, I wish to convey my gratitude to my family who fostered all the requirements and facilities that I need.

Project Associates
214G1A3229
214G1A3202
214G1A3219
214G1A3253

ABSTRACT

The rapid adoption of Unified Payments Interface (UPI) has heightened the risk of fraudulent activities in digital transactions. To mitigate this, we propose a robust fraud detection system utilizing four machine learning algorithms: Decision Tree, Random Forest, Gradient Boosting Machines (GBMs), and XGBClassifier.Decision Tree offers clear, rule-based classification, enhancing interpretability. Random Forest improves accuracy and resilience by reducing overfitting. GBMs iteratively refine weak models to detect evolving fraud patterns effectively.

XGBClassifier, a high-performance gradient boosting algorithm, ensures fast computation, handles missing values efficiently, and prevents overfitting, making it ideal for large-scale fraud detection.By integrating these techniques, our approach enhances fraud detection accuracy, reliability, and adaptability in UPI transactions. The system efficiently differentiates fraudulent transactions, strengthening financial security and fostering trust in digital payments, making it suitable for real-world financial deployment.

Keywords: UPI, Fraud Detection, Decision Tree, Random Forest, GBMs, XGBClassifier, Machine Learning, Financial Security.

Contents

List of Figures

List of Tables

LIST OF ABBREVIATIONS

UPI	Unified Payments Interface
GBM	Gradient Boosting Machine
XAI	Explainable Artificial Intelligence
FL	Federated Learning
CNN	Convolutional Neural Network
SMOTE	Synthetic Minority Over-sampling Technique
PCA	Principal Component Analysis
DFD	Data Flow Diagram
ER Diagram	Entity Relationship Diagram
UML	Unified Modeling Language
XGBoost	Extreme Gradient Boosting
ROC Curve	Receiver Operating Characteristic Curve

CHAPTER - 1

INTRODUCTION

1.1 Motivation:

The rapid growth of Unified Payments Interface (UPI) has revolutionized digital transactions, making them faster and more convenient. However, this convenience has also led to an alarming increase in fraudulent activities, posing significant risks to users and financial institutions. The motivation behind this project is to develop an effective fraud detection system that safeguards UPI transactions. By leveraging machine learning algorithms like Decision Tree, Random Forest, Gradient Boosting Machines (GBMs), XGBClassifier, we aim to analyze transaction details such as transaction type,amount, initialBalanceSender, finalBalanceSender, initialBalanceReceiver, finalBalanceReceiver.

The Random Forest classifier’s resilience to overfitting enhances accuracy, while GBMs iteratively refine predictions. Strengthen the model’s predictive power by recognizing complex and sequential patterns. This multi-algorithm approach seeks to ensure secure UPI transactions, providing users with peace of mind and fostering trust in digital payment systems.

1.2 Problem Statement:

- The rise in UPI transactions has led to an increase in fraudulent activities, making it essential to develop a robust fraud detection system to safeguard users and financial institutions.

- Existing fraud detection methods often suffer from high false positives, incorrectly flagging legitimate transactions, which affects user experience and trust in digital payment systems.
- Traditional rule-based fraud detection approaches struggle to adapt to evolving fraud patterns, necessitating the use of machine learning algorithms for more accurate and dynamic fraud detection.

1.3 Objective of the Project:

- **Development of Fraud Detection System**: The project focuses on creating a robust fraud detection system specifically for Unified Payments Interface (UPI) transactions, analyzing critical details like bank book name, transaction ID, and transaction amount.
- **Machine Learning Algorithms**: We aim to implement a framework using machine learning algorithms, including Random Forest, XGBClassifier, Gradient Boosting and Decision Tree, to effectively classify transactions as either fraudulent or successful.
- **Accuracy and Minimized False Positives**: The goal is to enhance the accuracy of fraud detection while minimizing false positives, ensuring that legitimate transactions are not incorrectly flagged.
- **Integration into Financial Systems**: Ultimately, the proposed model will be integrated into real-world financial systems, providing users with increased protection against unauthorized transactions and fostering confidence in digital payment processes.

1.4 Scope:

The scope of this project is to develop a robust system for detecting fraudulent activities in Unified Payments Interface (UPI) transactions by analyzing various transaction details, such type,amount, initialBalanceSender, finalBalanceSender, initialBalanceReceiver, finalBalanceReceiver. We will implement four machine learning algorithms: Decision Tree, Random Forest, Gradient Boosting Machines (GBMs), XGBClassifier. Each algorithm will be evaluated for its effectiveness in classifying transactions as either "Transaction Failed: Incorrect Details Entered" or "Transaction Successful: Details Verified and Processed."

The integration of these models aims to enhance the security of UPI transactions, providing users with a reliable mechanism to prevent fraud while ensuring legitimate transactions are processed smoothly. By comparing the performance of these classifiers, the project will identify the most effective approach for real-world application in financial systems, contributing to increased user trust and safety in digital payments.

1.5 Introduction:

With the rapid adoption of the Unified Payments Interface (UPI) for digital transactions, the associated risk of fraudulent activities has surged significantly. To combat this challenge, we propose a robust approach to detect UPI fraud by analyzing critical transaction details, including the bank book name, transaction ID, and transaction amount. Our method employs four machine learning algorithms: Decision Tree, Random Forest, Gradient Boosting Machines (GBMs), XGBClassifier.

The Random Forest classifier is renowned for its accuracy and resistance to overfitting, making it a strong candidate for distinguishing between legitimate and fraudulent transactions. GBMs refine predictions iteratively, while strengthen the model's overall predictive power by recognizing complex and sequential patterns in transaction data. XGBClassifier is a powerful gradient boosting algorithm for classification tasks.

It is fast, handles missing values, prevents overfitting. This ensemble of techniques classifies transaction outcomes as either "Transaction Failed: Incorrect Details Entered" or "Transaction Successful: Details Verified and Processed." By integrating these methods, our model aims to enhance the security of UPI transactions, ensuring smoother processing of legitimate activities while mitigating the threat of fraud.

CHAPTER – 2

LITERATURE SURVEY

2.1 Related Work:

1. Boutaher N, Elomri A, Abghour N, Moussaid K, Rida M (2020) – A Review of Credit Card Fraud Detection Using Machine Learning Techniques. In 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), pp. 1–8, IEEE, Casablanca, Morocco.

This paper explores the role of big data and machine learning in credit card fraud detection. The study examines anomaly detection and classification techniques, comparing machine learning methods such as Random Forest and Convolutional Neural Networks (CNNs) for fraud prevention. The research highlights challenges in digital transactions and suggests solutions to improve fraud detection accuracy while reducing false positives

2. Valavan M, Rita S (2022) – Predictive Analysis-Based Machine Learning Model for Fraud Detection with Boosting Classifiers. In Computer Systems Science & Engineering, vol. 45, no. 1, pp. 231–245, Tech Science Press.

This paper investigates the use of boosting classifiers in financial fraud detection, comparing Decision Tree, Random Forest, Linear Regression, and Gradient Boosting models. The study evaluates models using accurate metrics such as precision, recall, F1-score, and ROC curves. Results indicate that ensemble learning, particularly Gradient Boosting, improves fraud detection accuracy, especially in imbalanced datasets

3. Rupa Rani, Alam A, Javed A (2024) – Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions. In 2nd International Conference on Disruptive Technologies (ICDT), pp. 924–932, IEEE, Bangalore, India.

This study presents a fraud detection system for UPI transactions using the XGBoost algorithm. The system preprocesses UPI transaction data, applying feature selection techniques such as SMOTE and PCA. The trained model achieves 98.2% accuracy and is integrated into a real-time fraud monitoring system. The research highlights the importance of hyperparameter tuning and feature selection for fraud prevention

4. Gupta Y, Saxena N, Kumar K (2024) – UPI Fraud Detection Using Machine Learning. In International Journal of Advances in Engineering and Management (IJAEM), vol. 6, issue 10, pp. 29–34, ISO 9001:2008 Certified Journal.

This paper proposes a hybrid fraud detection approach combining rule-based strategies with anomaly detection for secure UPI transactions. The system monitors transaction patterns and user behavior to detect fraud in real-time. By integrating traditional fraud detection rules with machine learning models, the approach enhances transaction security and continuously adapts to new fraud tactics

5. Nagaraju M, Reddy YC, Babu PN, Ravipati VSP, Chaitanya V (2024) – UPI Fraud Detection Using Convolutional Neural Networks (CNNs). In Research Square Preprint, pp. 1–16.

This research applies to CNNs to detect fraudulent UPI transactions, focusing on feature extraction and real-time fraud prevention. CNNs effectively capture complex fraud patterns in transactional sequences, offering superior accuracy compared to conventional fraud detection techniques.

CHAPTER – 3

SYSTEM ANALYSIS

3.1 Existing System:

The existing systems for fraud detection in digital transactions often rely on traditional machine learning algorithms. However, many of these systems suffer from scalability issues and poor generalization due to their reliance on models that are sensitive to noisy or irrelevant features. Additionally, algorithms such as Decision Trees, k-Nearest Neighbors (KNN), and other simpler models can become computationally expensive with large datasets, resulting in inefficiencies, especially in real-time applications.KNN, in particular, faces challenges in fraud detection due to its high computational cost during inference, as it requires calculating distances to all training samples. Furthermore, KNN is sensitive to irrelevant or redundant features, making it less effective when dealing with high-dimensional or noisy data.

3.2 Disadvantages of Existing Systems:

- **Data Sensitivity:** Existing systems may struggle with noisy or irrelevant features, which can lead to inaccurate predictions and decreased performance.
- **Scalability Issues:** Simpler methods can be computationally expensive, leading to slower response times with large datasets.
- **Overfitting Risk:** Simpler algorithms like decision trees can easily overfit to training data, impacting generalization to unseen transactions.

- **Limited Interpretability:** While Decision Trees provide some level of transparency, more complex algorithms can be less interpretable, making it harder to understand decision-making processes.
- **Imbalanced Data:** Fraud detection systems often deal with imbalanced datasets, leading to biased predictions favoring legitimate transactions over fraudulent ones.

3.3 Proposed System

The proposed system enhances UPI fraud detection by using a combination of Random Forest, Decision Tree, Gradient Boosting Machines (GBMs), XGBClassifier.

- Random Forest is an ensemble method that builds multiple decision trees and aggregates their predictions, improving both accuracy and robustness against overfitting. It is well-suited to detecting fraud in noisy, imbalanced, and complex data, capturing intricate relationships between features .
- Decision Tree is a simple and interpretable model that splits data based on feature importance. While effective for small datasets, it tends to overfit on complex data. However, it provides a solid foundation for more advanced ensemble methods.
- Gradient Boosting Machines (GBMs) enhance performance by iteratively refining predictions, improving precision and recall for fraud detection. They are particularly adept at capturing complex, non-linear patterns within vast amounts of data, improving detection accuracy by learning intricate relationships that simpler models might miss. This model is well-suited for large datasets.

- XGBClassifier (Extreme Gradient Boosting) is an optimized version of GBMs, offering higher speed and scalability. It effectively handles missing values and noisy data, making it ideal for real-time fraud detection. Its regularization techniques prevent overfitting, and its parallel processing capabilities enable efficient learning from large datasets.

3.4 Advantages of the Proposed System:

- **Enhanced Accuracy:** By leveraging a combination of Random Forest, Decision Tree, Gradient Boosting Machines (GBMs), and XGBClassifier, the system benefits from the strengths of each model, improving classification accuracy and minimizing false positives and negatives.
- **Robustness Against Overfitting**: Random Forest and GBMs mitigate overfitting by using ensemble learning techniques, ensuring the system generalizes well to unseen data, even in the presence of noisy or imbalanced data.
- **Interpretability:** While boosting methods like GBMs and XGBClassifier focus on accuracy, Decision Trees and Random Forest provide a level of interpretability, allowing users to understand classification outcomes and feature importance in fraud detection.
- **Real-time Detection:** The system can efficiently process transactions in real-time, utilizing the fast computational capabilities of XGBClassifier and GBMs to quickly identify and prevent fraudulent activities.
- **User Protection:** By accurately distinguishing between legitimate and fraudulent transactions, the system enhances user confidence and security, ensuring safer UPI transactions.

CHAPTER – 4
REQUIREMENT ANALYSIS

4.1 Functional and non-functional requirements

Requirement analysis is very critical process that enables the success of a system or software project to be assessed. Requirements are generally split into two types: Functional and non-functional requirements.

4.1.1 Functional Requirements:

These are the requirements that the end user specifically demands as basic facilities that the system should offer. All these functionalities need to be necessarily incorporated into the system as a part of the contract. These are represented or stated in the form of input to be given to the system, the operation performed, and the output expected. They are basically the requirements stated by the user which one can see directly in the final product, unlike the non-functional requirements.

Examples of functional requirements:

1) Authentication of user whenever he/she logs into the system
2) System shutdown in Solar prediction.
3) A verification email is sent to a user whenever he/she register for the first time on some software system.

4.1.2 Non-functional requirements:

These are basically the quality constraints that the system must satisfy according to the project contract. The priority or extent to which these factors are implemented varies from one project to another. They are also called non-behavioral requirements.

They basically deal with issues like:

- Portability
- Security
- Maintainability
- Reliability
- Scalability
- Performance
- Reusability
- Flexibility

Examples of non-functional requirements:

1) Emails should be sent with a latency of no greater than 12 hours from such an activity.
2) The processing of each request should be done within 10 seconds
3) The site should be loaded in 3 seconds whenever of simultaneous users are > 10000

4.2 Hardware Requirements

Operating system	: Windows 7 or 7+
RAM	: 8 GB
Hard disc or SSD	: More than 500 GB
Processor	: Intel 3rd generation or high or Ryzen with 8 GB Ram

4.3 Software Requirements:

Software’s	: Python 3.10 or high version
IDE	: Visual Studio Code.
Framework	: Flask
IDE/Workbench	: PyCharm
Technology	: Python 3.6+
Server Deployment	: Xampp Server
Database	: MySQL

4.4 Architecture

The diagram represents a fraud detection system that authenticates users through login credentials. Upon successful authentication, the system processes input data for fraud detection. The system follows key steps, including data collection, preprocessing, and splitting. It then builds predictive models using machine learning algorithms such as Decision Tree, Random Forest, Gradient Boosting Machines (GBMs), and XGBClassifier. The model analyzes the input data and classifies transactions as either "Fraud" or "No Fraud," providing the final classification result to the user.

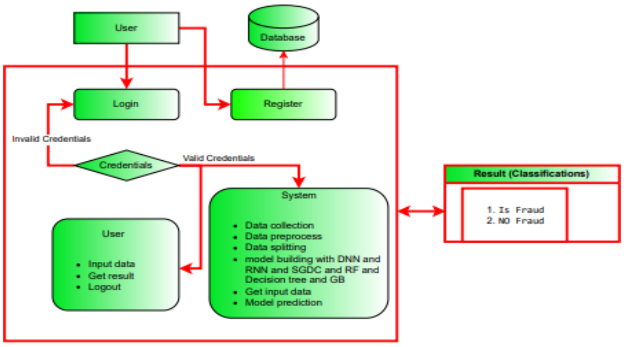


Figure 4.1 : Fraud Detection System Architecture

CHAPTER – 5
SYSTEM DESIGN

5.1 Introduction of Input Design:

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider input devices such as PC, MICR, OMR, etc. Therefore, the quality of system input determines the quality of system output. Well-designed input forms and screens have following properties −

- It should serve specific purpose effectively such as storing, recording, and retrieving the information.
- It ensures proper completion with accuracy.
- It should be easy to fill and straightforward.
- It should focus on user’s attention, consistency, and simplicity.
- All these objectives are obtained using the knowledge of basic design principles regarding −
    - What are the inputs needed for the system?
    - How end users respond to different elements of forms and screens.

5.1.1 Objectives for Input Design:

The objectives of input design are −

- To design data entry and input procedures
- To reduce input volume

- To design source documents for data capture or devise other data capture methods
- To design input data records, data entry screens, user interface screens, etc.
- To use validation checks and develop effective input controls.

5.1.2 Output Design:

The design of output is the most important task of any system. During output design, developers identify the type of outputs needed and consider the necessary output controls and prototype report layouts.

The objectives of input design are:

- Developing output design that serves the intended purpose and eliminates the production of unwanted output.
- To develop the output design that meets the end user’s requirements.
- To deliver the appropriate quantity of output.
- To form the output in appropriate format and direct it to the right person.
- To make the output available on time for making good decisions.

5.2 UML Diagrams:

UML stands for Unified Modelling Language. UML is a standardized general-purpose modelling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.The Unified Modelling Language is a standard language for specifying, Visualization, Constructing and documenting the artefacts of software system, as well as for business modelling and other non-software systems. The UML represents a collection of the best engineering practices that have proven successful in the modelling of large and complex systems.UML is a very important part of developing object-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users with a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of programming languages and development process.
4. Provide a formal basis for understanding the modelling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.

7. Integrate best practices.

5.3 Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis.

- Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.

- The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

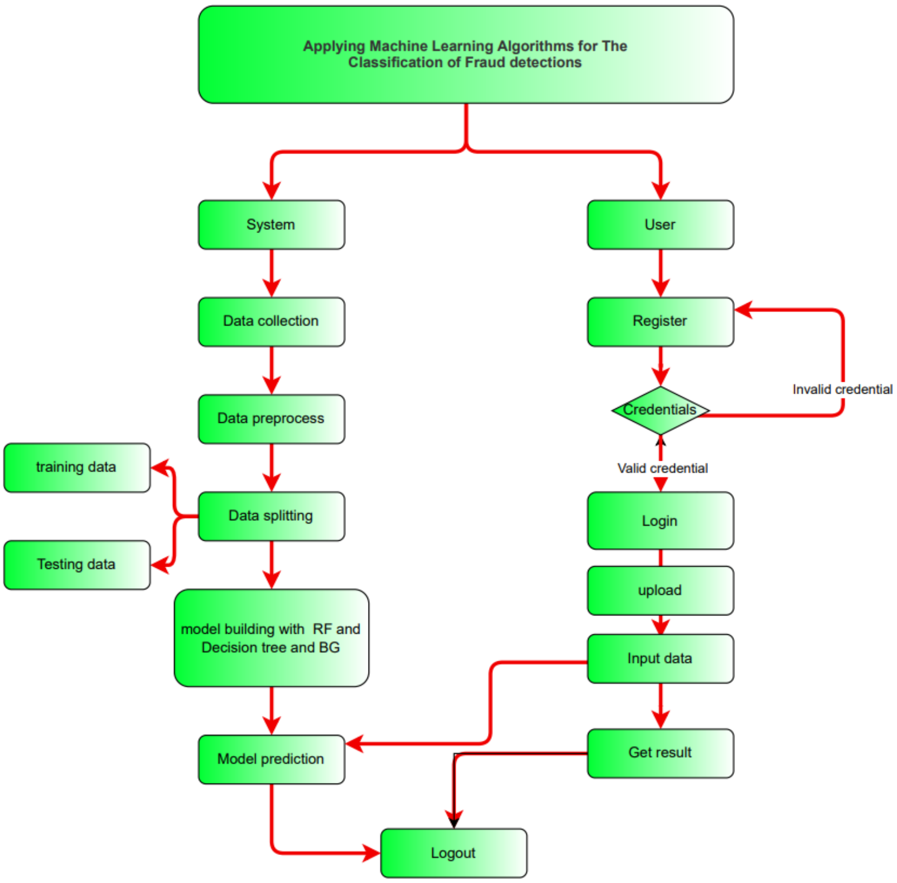


Figure 5.1: Fraud Detection System Flow

5.4 Class Diagram

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

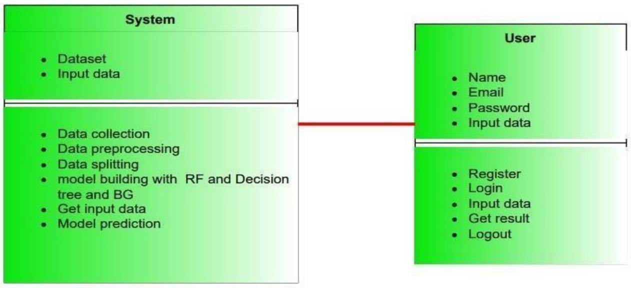


Figure 5.2: Class Diagram

5.5 Sequence Diagram

- A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order.

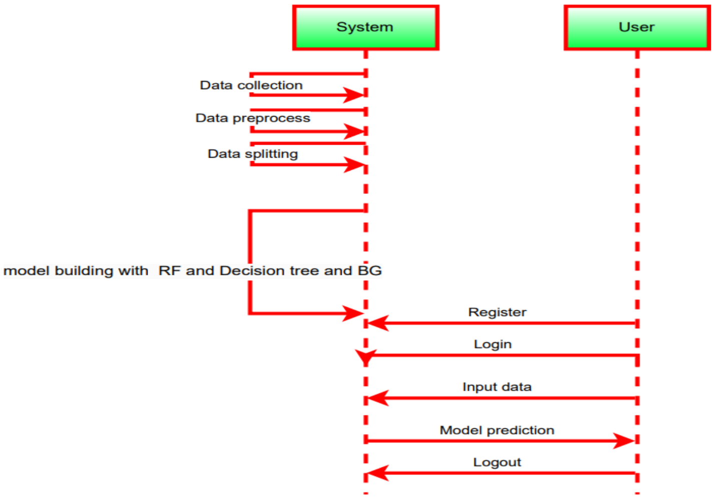


Figure 5.3: Sequence Diagram

5.6 Deployment Diagram

Deployment diagram represents the deployment view of a system. It is related to the component diagram. Because the components are deployed using the deployment diagrams. A deployment diagram consists of nodes. Nodes are nothing but physical hardware's used to deploy the application.

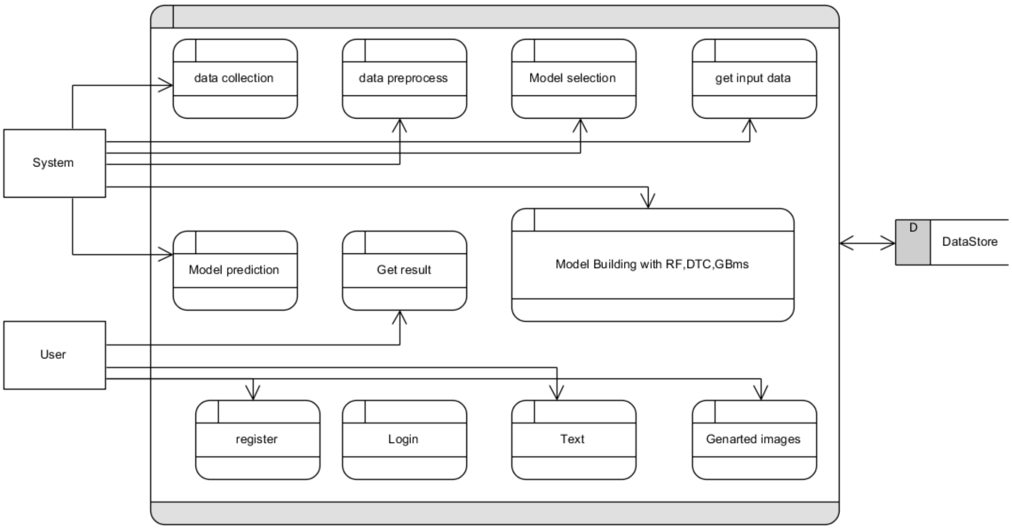


Figure 5.4: Deployment Diagram

5.7 Activity Diagrams:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

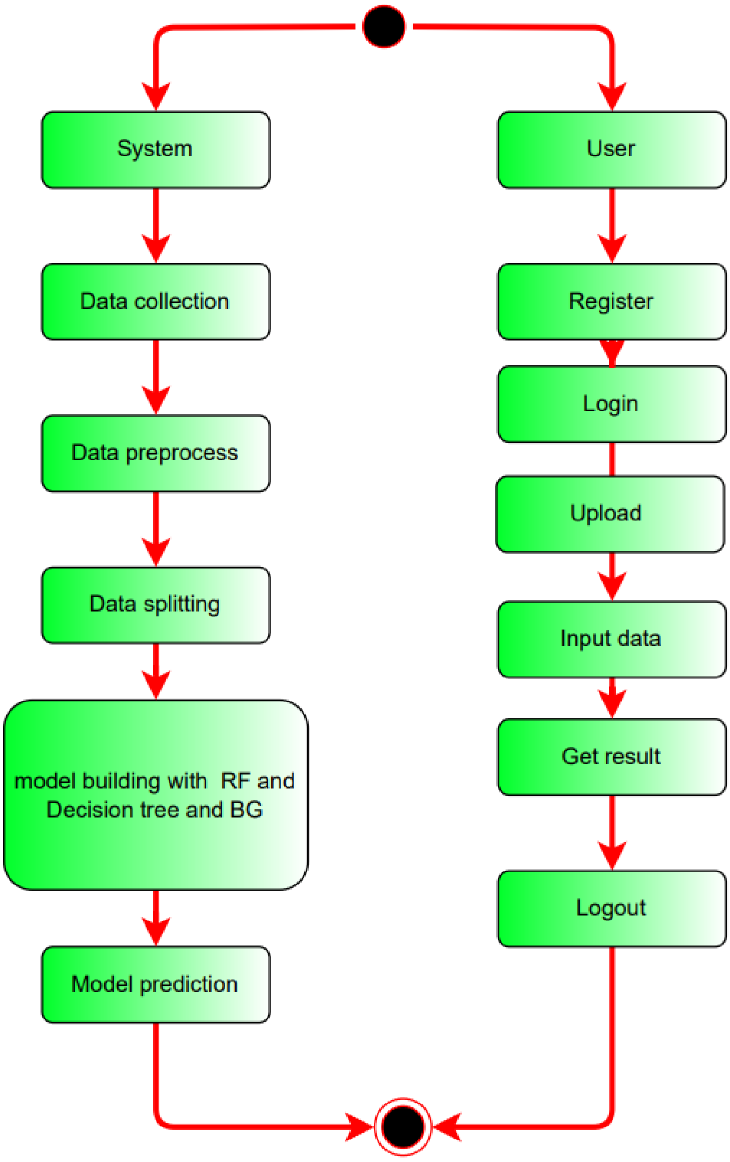


Figure 5.5: Activity Diagram

5.8 Component Diagram:

A component diagram, also known as a UML component diagram, describes the organization and wiring of the physical components in a system. Component diagrams are often drawn to help model implementation details and double-check that every aspect of the system's required function is covered by planned development.

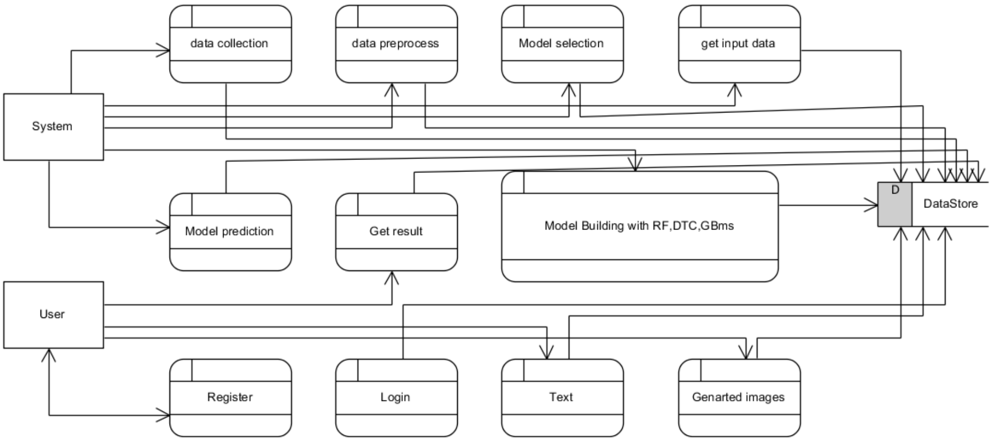


Figure 5.6: Component Diagram

5.9 ER Diagram:

An Entity–relationship model (ER model) describes the structure of a database with the help of a diagram, which is known as Entity Relationship Diagram (ER Diagram). An ER model is a design or blueprint of a database that can later be implemented as a database. The main components of E-R model are: entity set and relationship set.An ER diagram shows the relationship among entity sets. An entity set is a group of similar entities and these entities can have attributes. In terms of DBMS, an entity is a table or attribute of a table in database, so by showing relationship among tables and their attributes, ER diagram shows the complete logical structure of a database. Let’s have a look at a simple ER diagram to understand this concept.

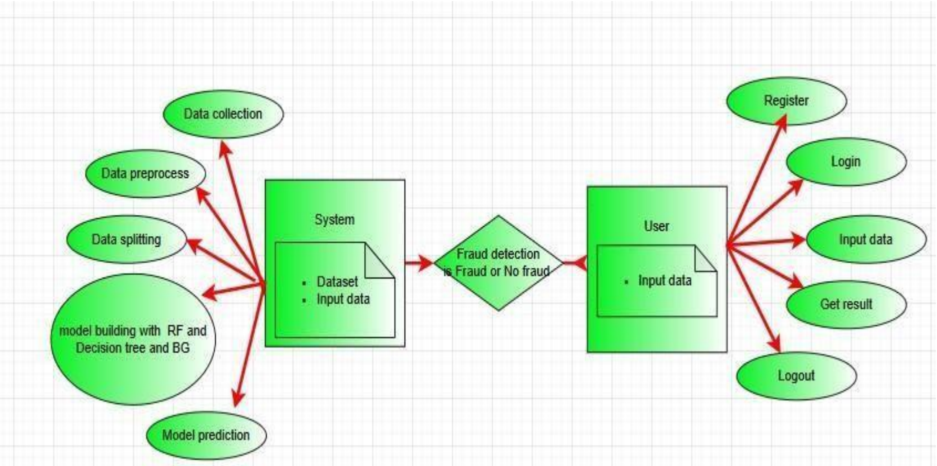


Figure 5.7: ER Diagram

5.10 DFD Diagram:

A Data Flow Diagram (DFD) is a traditional way to visualize the information flows within a system. A neat and clear DFD can depict a good amount of the system requirements graphically. It can be manual, automated, or a combination of both. It shows how information enters and leaves the system, what changes the information and where information is stored. The purpose of a DFD is to show the scope and boundaries of a system. It may be used as a communications tool between a systems analyst and any person who plays a part in the system that acts as the starting point for redesigning a system.

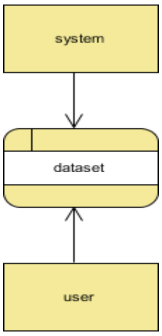


Figure 5.8: DFD Diagram

CHAPTER – 6

IMPLEMENTATION AND RESULTS

6.1 Modules

- Users can upload a dataset, which is a crucial initial step for the system to work with relevant data. This dataset likely contains historical information or examples that the system will use for its predictions.
- Users have the capability to view the dataset they've uploaded. This feature helps users confirm the data they've provided and ensures transparency in the process.
- Users need to input specific values or parameters into the system to request predictions or results. These input values likely correspond to the variables or features in the dataset.

6.2 System

- **Take the Dataset:** The system accepts and processes the dataset provided by the user. This dataset forms the foundation for building the predictive model.
- **Preprocessing:** Before training a predictive model, the system preprocesses the dataset. This includes handling missing data, data cleaning, and feature extraction. Preprocessing ensures that the data is in a suitable format for modeling.
- **Training:** The system uses machine learning techniques and Python modules to train a model based on the preprocessed dataset. The model learns patterns and relationships within the data, allowing it to make predictions.

- **Generate Results:** Once the model is trained, the system can generate results based on user input values. These results typically indicate whether the input data corresponds to a specific condition, event, or prediction, such as Medical Insurance Cost.

6.3 Algorithms:

Random Forest

A random forest is a machine learning technique that’s used to solve regression and classification problems. It utilizes ensemble learning, which is a technique that combines many classifiers to provide solutions to complex problems.

A random forest algorithm consists of many decision trees. The ‘forest’ generated by the random forest algorithm is trained through bagging or bootstrap aggregating. Bagging is an ensemble meta-algorithm that improves the accuracy of machine learning algorithms.

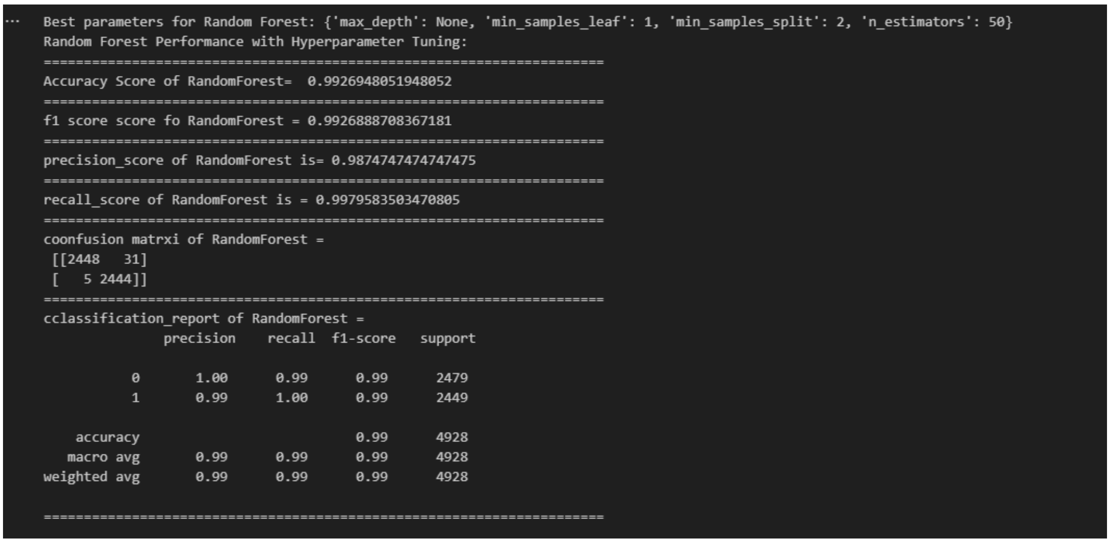
The (random forest) algorithm establishes the outcome based on the predictions of the decision trees. It predicts by taking the average or mean of the output from various trees. Increasing the number of trees increases the precision of the outcome.

A random forest eradicates the limitations of a decision tree algorithm. It reduces the over fitting of datasets and increases precision. It generates predictions without requiring many configurations in packages (like Scikit-learn).

Features of a Random Forest Algorithm:

- It’s more accurate than the decision tree algorithm.
- It provides an effective way of handling missing data.

- It can produce a reasonable prediction without hyper-parameter tuning.
- It solves the issue of over fitting in decision trees.
- In every random forest tree, a subset of features is selected randomly at the node's splitting point.



```
...  Best parameters for Random Forest: {'max_depth': None, 'min_samples_leaf': 1, 'min_samples_split': 2, 'n_estimators': 50}
     Random Forest Performance with Hyperparameter Tuning:
     ======================================================================
     Accuracy Score of RandomForest=  0.9926948051948052
     ======================================================================
     f1 score score fo RandomForest = 0.9926888708367181
     ======================================================================
     precision_score of RandomForest is= 0.9874747474747475
     ======================================================================
     recall_score of RandomForest is = 0.9979583503470805
     ======================================================================
     coonfusion matrxi of RandomForest =
      [[2448   31]
      [   5 2444]]
     ======================================================================
     cclassification_report of RandomForest =
                    precision    recall  f1-score   support

                0       1.00      0.99      0.99      2479
                1       0.99      1.00      0.99      2449

         accuracy                           0.99      4928
        macro avg       0.99      0.99      0.99      4928
     weighted avg       0.99      0.99      0.99      4928

     ======================================================================
```

Figure 6.1: Random Forest Performance Metrics

Decision trees

Decision trees are the building blocks of a random forest algorithm. A decision tree is a decision support technique that forms a tree-like structure. An overview of decision trees will help us understand how random forest algorithms work.

A decision tree consists of three components: decision nodes, leaf nodes, and a root node. A decision tree algorithm divides a training dataset into branches, which further segregate into other branches.

This sequence continues until a leaf node is attained. The leaf node cannot be segregated further.The nodes in the decision tree represent attributes that are used for predicting the outcome. Decision nodes provide a link to the leaves. The following diagram shows the three types of nodes in a decision tree.

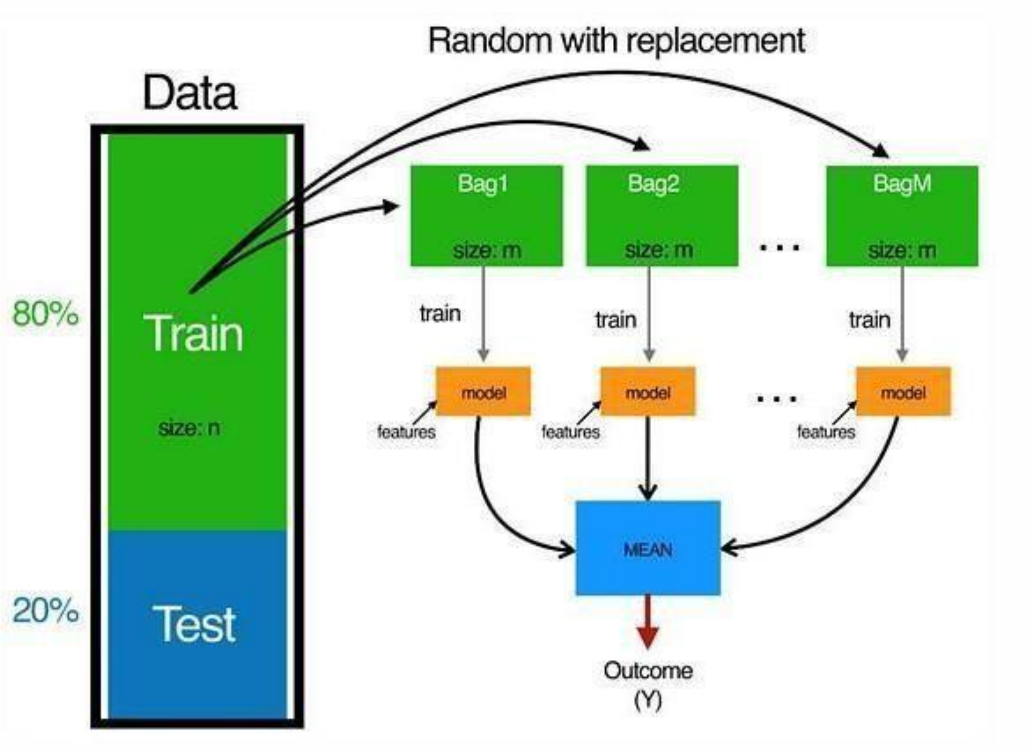
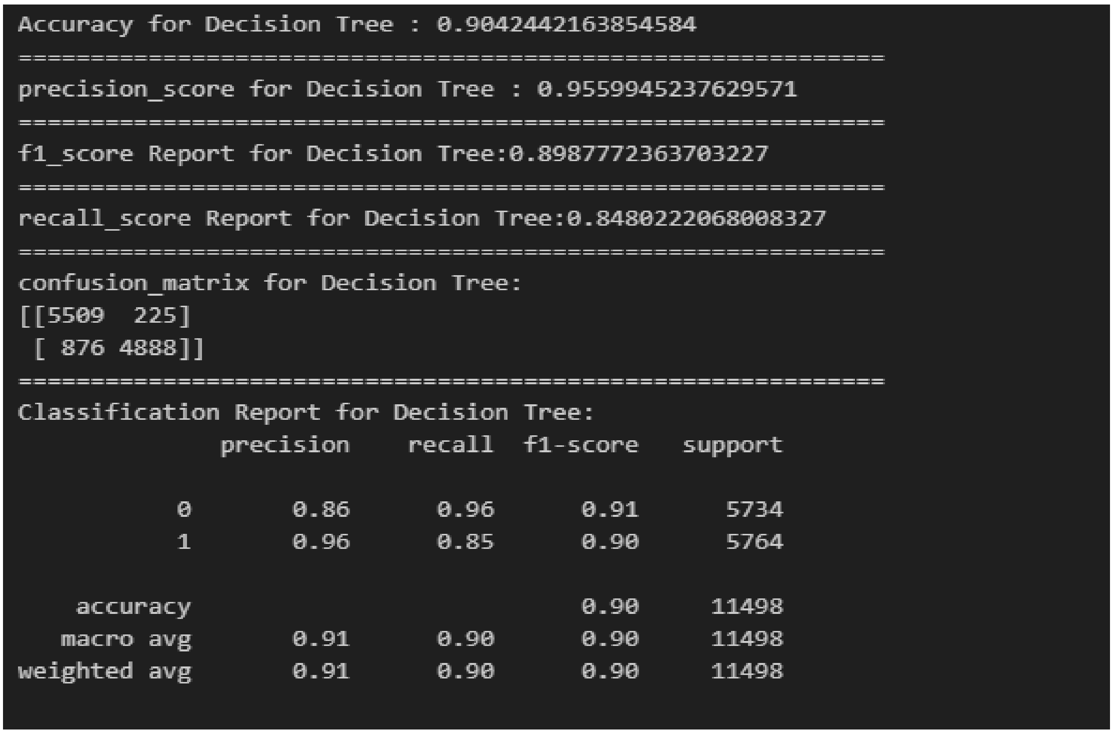


Figure 6.2: Bagging Process in Ensemble Learning

The information theory can provide more information on how decision trees work. Entropy and information gain are the building blocks of decision trees. An overview of these fundamental concepts will improve our understanding of how decision trees are built.

Entropy is a metric for calculating uncertainty. Information gain is a measure of how uncertainty in the target variable is reduced, given a set of independent variables. The information gain concept involves using independent variables (features) to gain information about a target variable (class). The entropy of the target variable (Y) and the conditional entropy of Y (given X) are used to estimate the information gain. In this case, the conditional entropy is subtracted from the entropy of Y.Information gain is used in the training of decision trees. It helps in reducing uncertainty in these trees. A high information gain means that a high degree of uncertainty (information entropy) has been removed. Entropy and information gain are important in splitting branches, which is an important activity in the construction of decision trees.

Let’s take a simple example of how a decision tree works. Suppose we want to predict if a customer will purchase a mobile phone or not. The features of the phone form the basis of his decision. This analysis can be presented in a decision tree diagram.



```
Accuracy for Decision Tree : 0.9042442163854584
============================================================
precision_score for Decision Tree : 0.9559945237629571
============================================================
f1_score Report for Decision Tree:0.8987772363703227
============================================================
recall_score Report for Decision Tree:0.8480222068008327
============================================================
confusion_matrix for Decision Tree:
[[5509  225]
 [ 876 4888]]
============================================================
Classification Report for Decision Tree:
              precision    recall  f1-score   support

           0       0.86      0.96      0.91      5734
           1       0.96      0.85      0.90      5764

    accuracy                           0.90     11498
   macro avg       0.91      0.90      0.90     11498
weighted avg       0.91      0.90      0.90     11498
```

Figure 6.3: Decision trees Performance Metrics

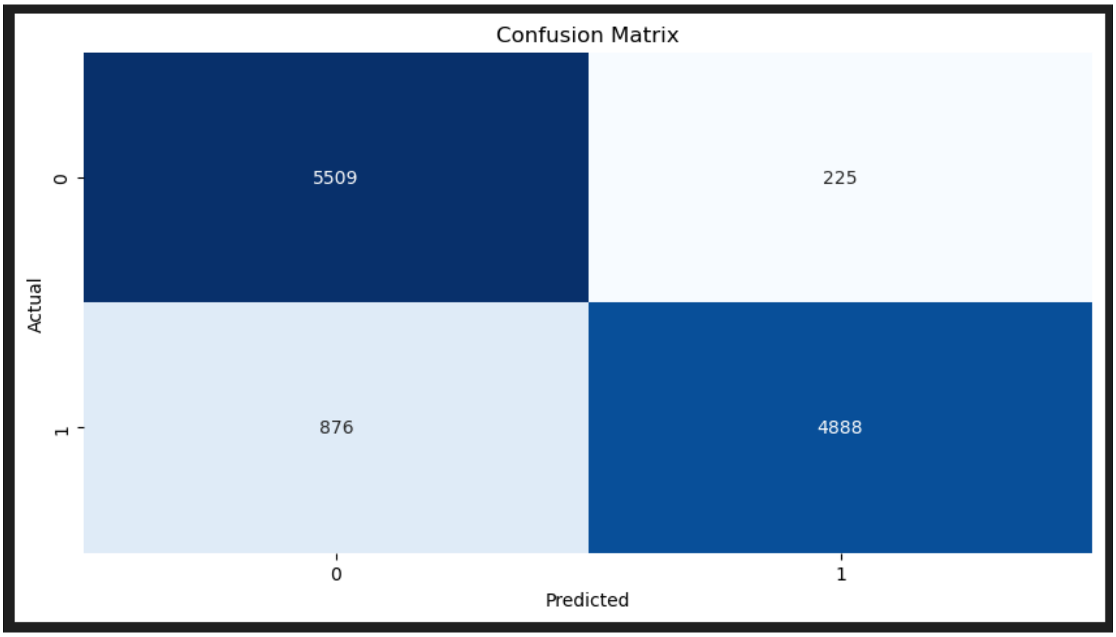


Figure 6.4: Decision trees Confusion Matrix

XGBoost

XGBoost, which stands for Extreme Gradient Boosting, is a scalable, distributed gradient-boosted decision tree (GBDT) machine learning library. It provides parallel tree boosting and is the leading machine learning library for regression, classification, and ranking problems.

It's vital to an understanding of XGBoost to first grasp the machine learning concepts and algorithms that XGBoost builds upon: supervised machine learning, decision trees, ensemble learning, and gradient boosting. Supervised machine learning uses algorithms to train a model to find patterns in a dataset with labels and features and then uses the trained model to predict the labels on a new dataset's features.

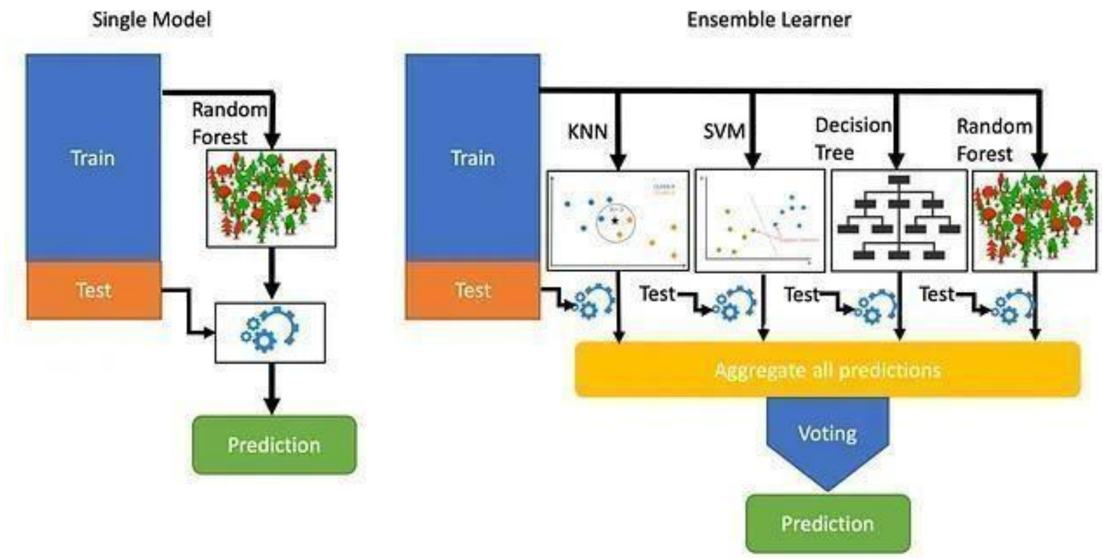
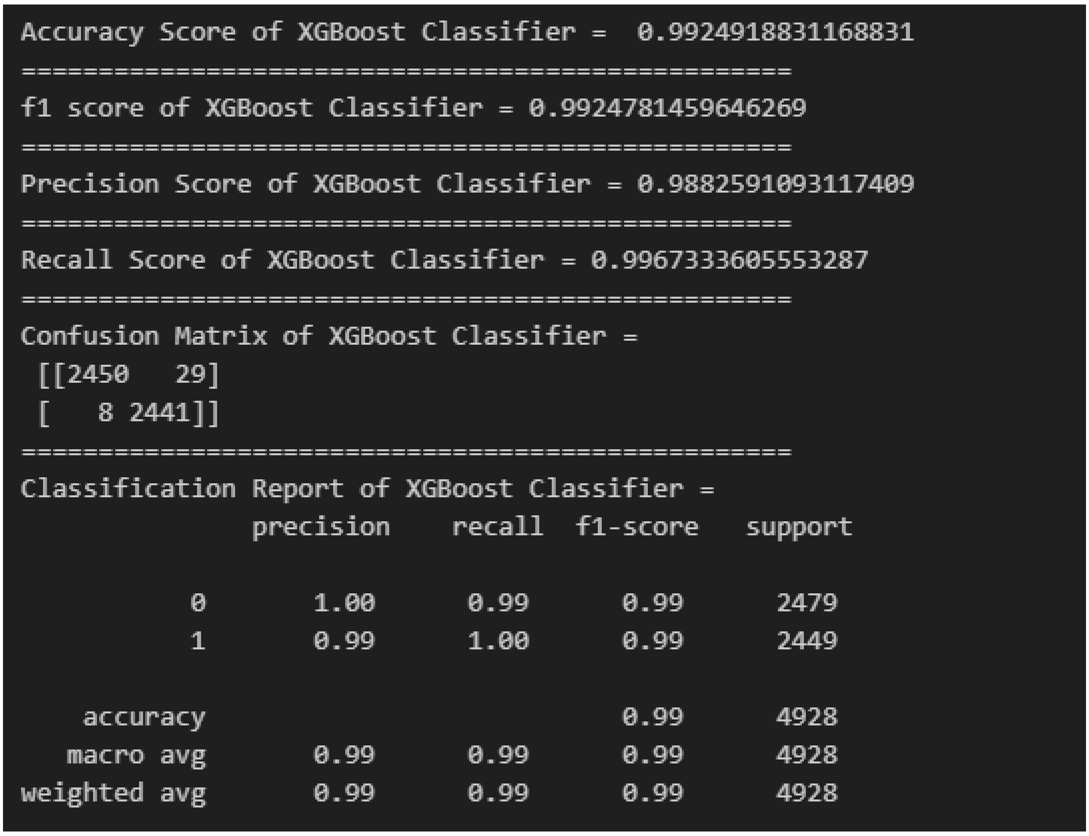


Figure 6.5: Single vs. Ensemble Learning Approaches



```
Accuracy Score of XGBoost Classifier =  0.9924918831168831
==================================================
f1 score of XGBoost Classifier = 0.9924781459646269
==================================================
Precision Score of XGBoost Classifier = 0.9882591093117409
==================================================
Recall Score of XGBoost Classifier = 0.9967333605553287
==================================================
Confusion Matrix of XGBoost Classifier =
 [[2450   29]
 [   8 2441]]
==================================================
Classification Report of XGBoost Classifier =
               precision    recall  f1-score   support

           0       1.00      0.99      0.99      2479
           1       0.99      1.00      0.99      2449

    accuracy                           0.99      4928
   macro avg       0.99      0.99      0.99      4928
weighted avg       0.99      0.99      0.99      4928
```

Figure 6.6: XGBoost Classifier Performance Report

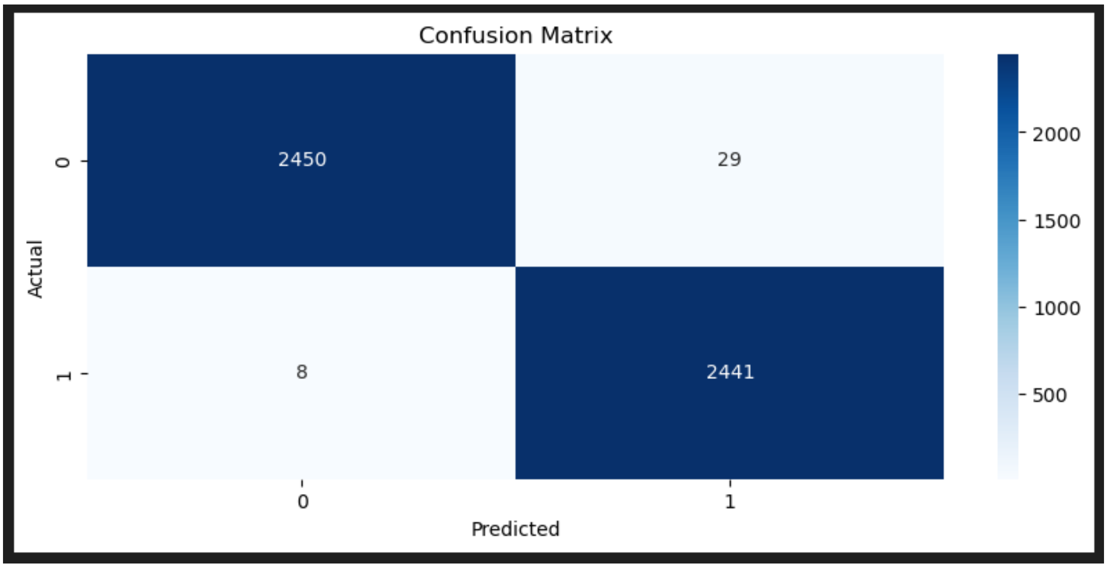


Figure 6.7: XGBoost Confusion Matrix

Gradient Boosting Classifier

The Boosting Algorithm is one of the most powerful learning ideas introduced in the last twenty years. Gradient Boosting is a supervised machine learning algorithm used for classification and regression problems. It is an ensemble technique which uses multiple weak learners to produce a strong model for regression and classification.

Gradient Boosting relies on the intuition that the best possible next model, when combined with the previous models, minimizes the overall prediction errors. The key idea is to set the target outcomes from the previous models to the next model to minimize the errors.

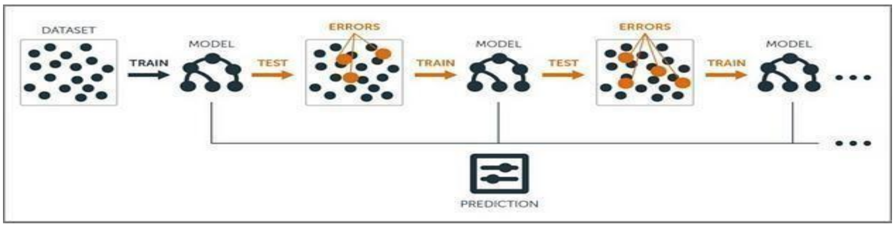
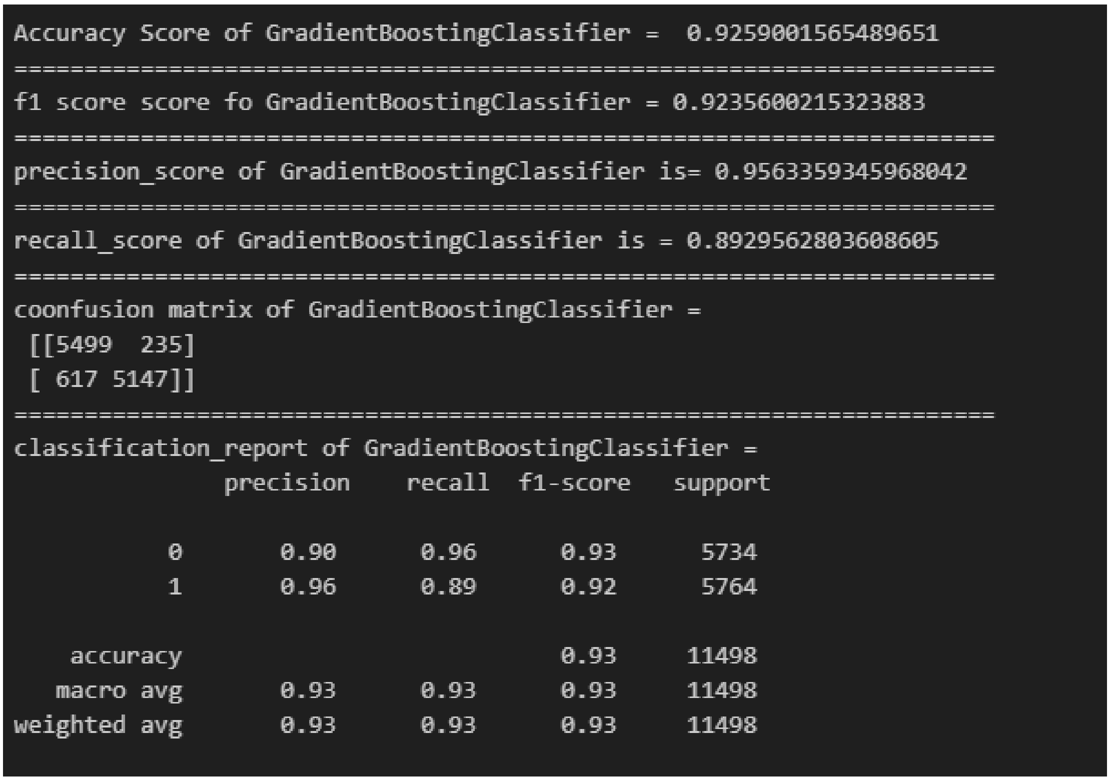


Figure 6.8: Gradient Boosting Algorithm Workflow



```
Accuracy Score of GradientBoostingClassifier =  0.9259001565489651
======================================================================
f1 score score fo GradientBoostingClassifier = 0.9235600215323883
======================================================================
precision_score of GradientBoostingClassifier is= 0.9563359345968042
======================================================================
recall_score of GradientBoostingClassifier is = 0.8929562803608605
======================================================================
coonfusion matrix of GradientBoostingClassifier =
 [[5499  235]
 [ 617 5147]]
======================================================================
classification_report of GradientBoostingClassifier =
               precision    recall  f1-score   support

           0       0.90      0.96      0.93      5734
           1       0.96      0.89      0.92      5764

    accuracy                           0.93     11498
   macro avg       0.93      0.93      0.93     11498
weighted avg       0.93      0.93      0.93     11498
```

Figure 6.9: Gradient Boosting Classifier Performance Report

CHAPTER – 7
SYSTEM STUDY AND TESTING

7.1 System Testing

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

7.2.1 Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application. it is done after the completion of an individual unit before integration.

This is structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

7.2.2 Integration testing

Integration tests are designed to test integrated software components to determine if they run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

7.2.3 Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

7.2.4 Functional testing

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

7.2.5 White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

7.2.6 Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box. you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

Test cases Model building:

S.NO	Test cases	I/O	Expected O/T	Actual O/T	P/F
1	Read the datasets	Dataset's path.	Datasets need to read successfully.	Datasets fetched successfully.	It produced P. If this not F will come
2	Registration	Valid username, email, password.	Verify that the registration form accepts valid user inputs and successfully creates a new account.	User is successfully registered, and an account is created	It produced P. If this is not, it will undergo F.
3	Login	Valid username and password	Verify that users can log in with valid credentials	User is successfully logged in and redirected to the dashboard	It produced P. If this is not, it will undergo F.
4	Find out Fraud or Not	Inputs old balance and new balance and type of transaction	Output as predicted classification of fraud or Not	Output as predicted classification of Fraud or Not	It produced 0 is No Fraud and 1 Fraud

Table 7.1: Test cases Model building

CHAPTER – 8

RESULT

COMPARISON OF ALL MODELS

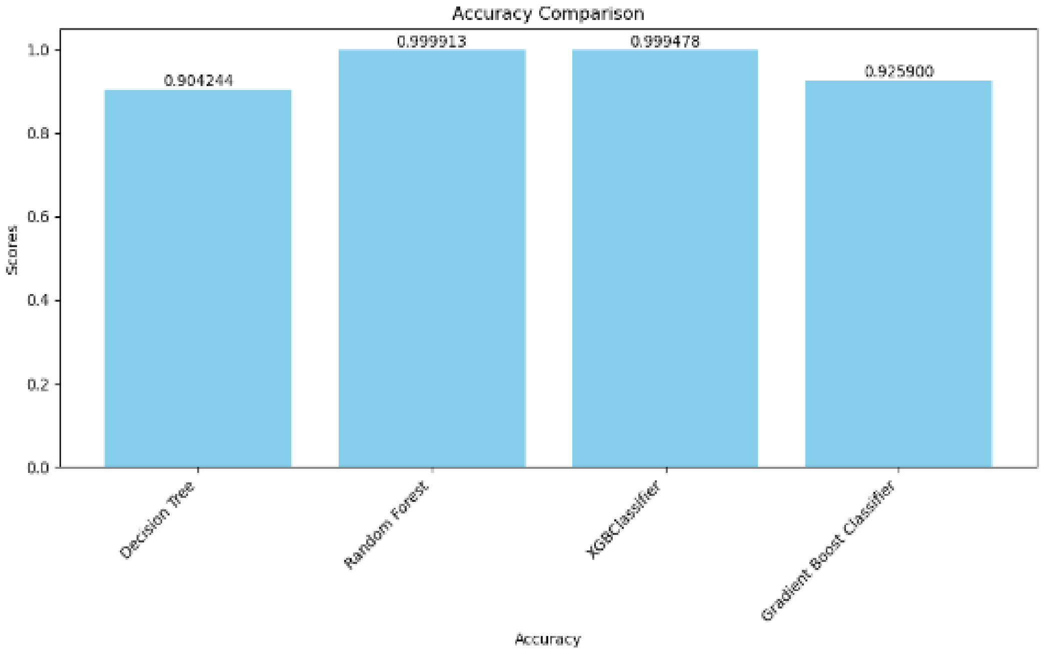


Figure 6.10: Accuracy Comparison of Different Models

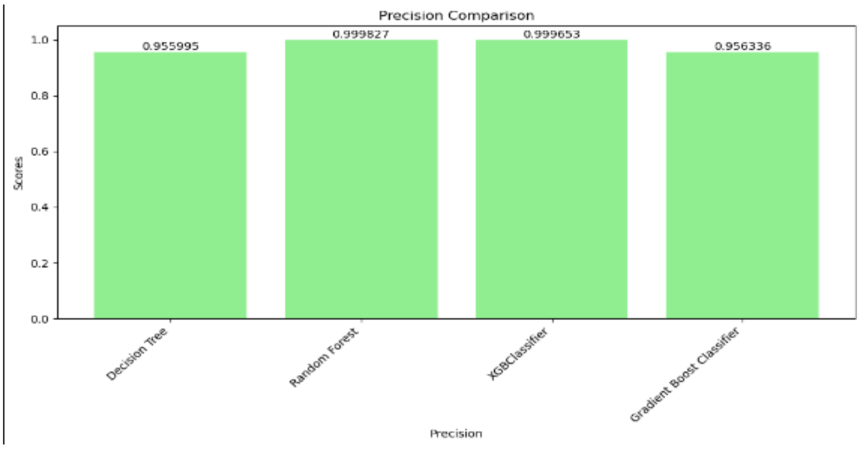


Figure 6.11: Precision Comparison of Different Models

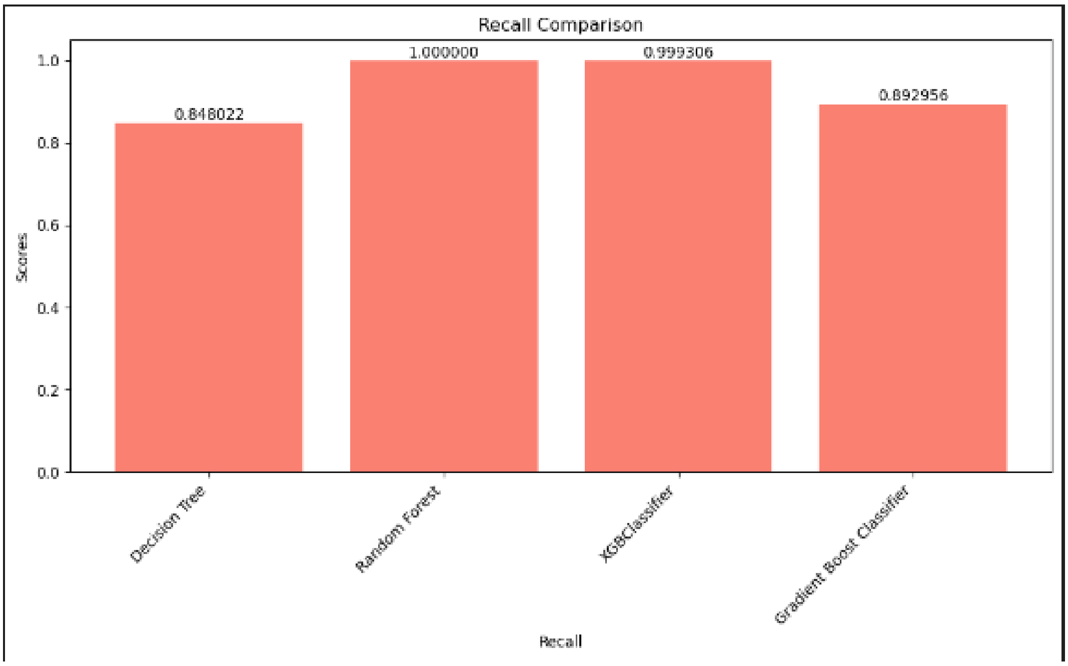


Figure 6.12: Recall Comparison of Different Models

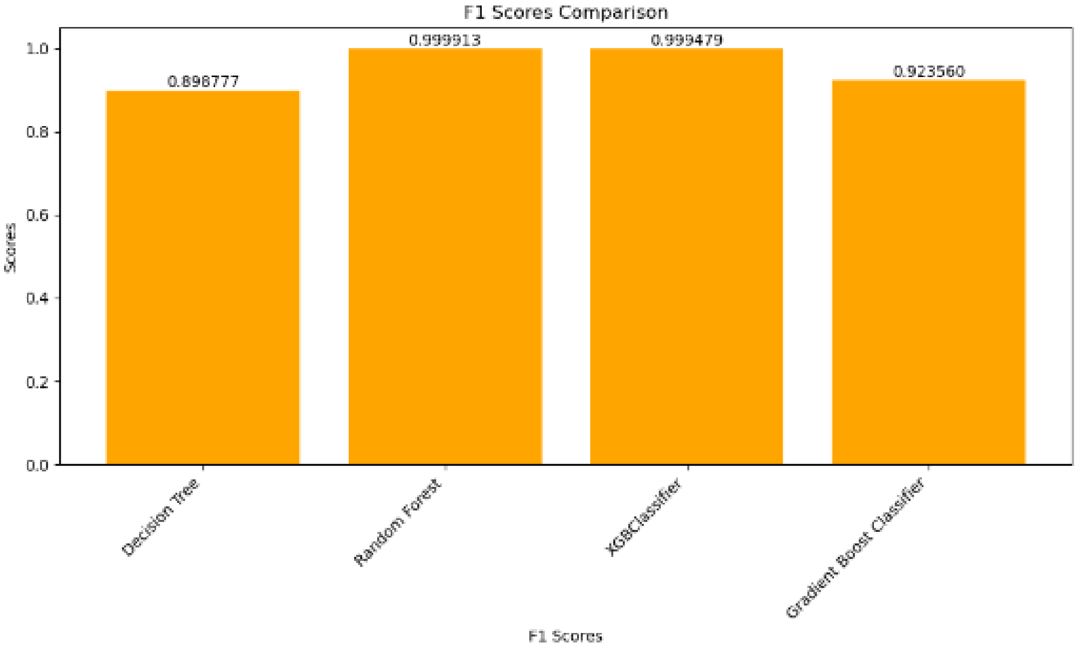
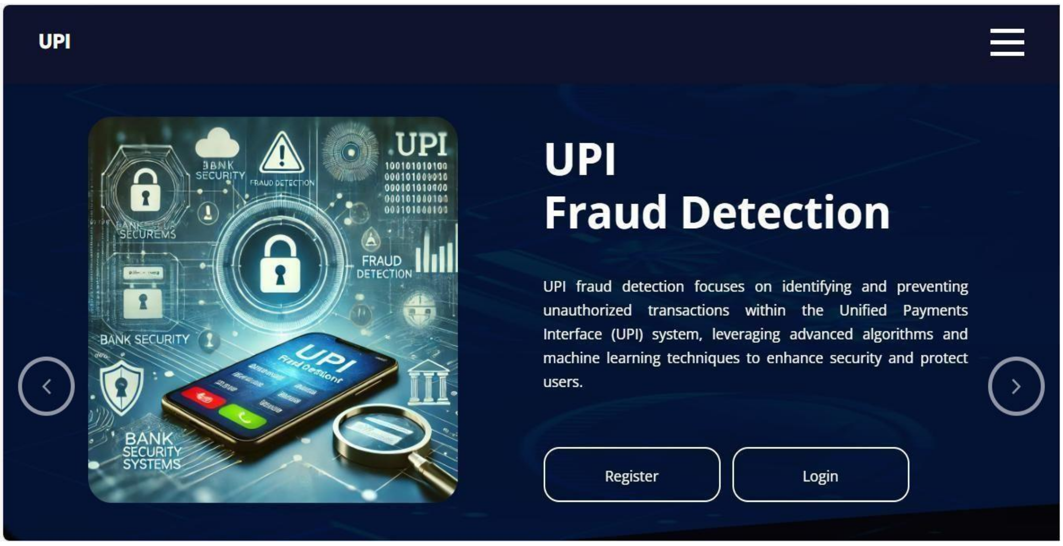


Figure 6.13: F1 Scores Comparison of Different Models

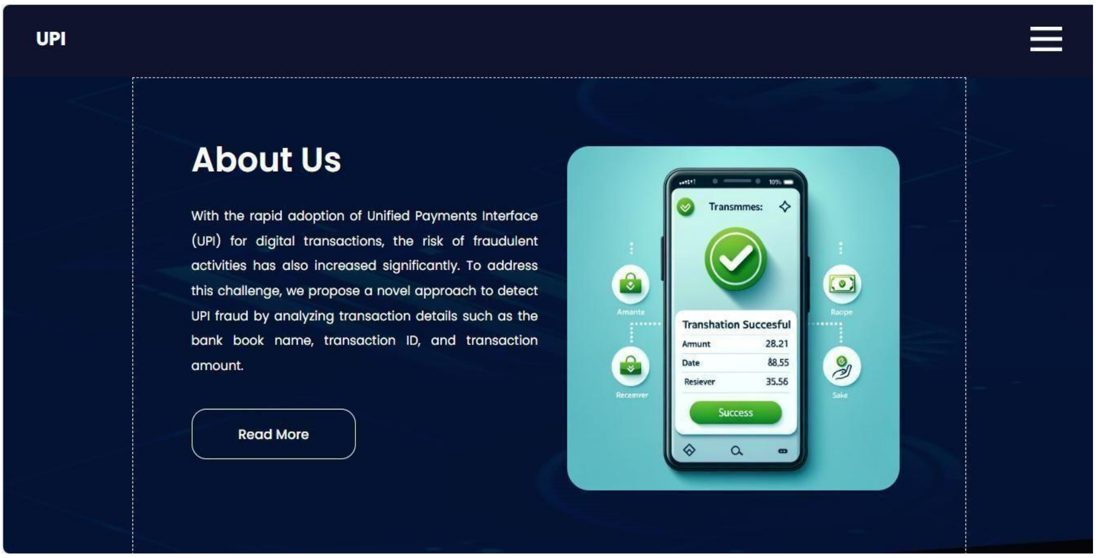


UPI
Fraud Detection

UPI fraud detection focuses on identifying and preventing unauthorized transactions within the Unified Payments Interface (UPI) system, leveraging advanced algorithms and machine learning techniques to enhance security and protect users.

Figure 6.14: Home Page

- This interface enables users to, facilitating Register and login to model home page and prediction and training page



About Us

With the rapid adoption of Unified Payments Interface (UPI) for digital transactions, the risk of fraudulent activities has also increased significantly. To address this challenge, we propose a novel approach to detect UPI fraud by analyzing transaction details such as the bank book name, transaction ID, and transaction amount.

Figure 6.15: About Page

- The project predicts using machine learning models, emphasizing interpretability and superior accuracy with ensemble methods.

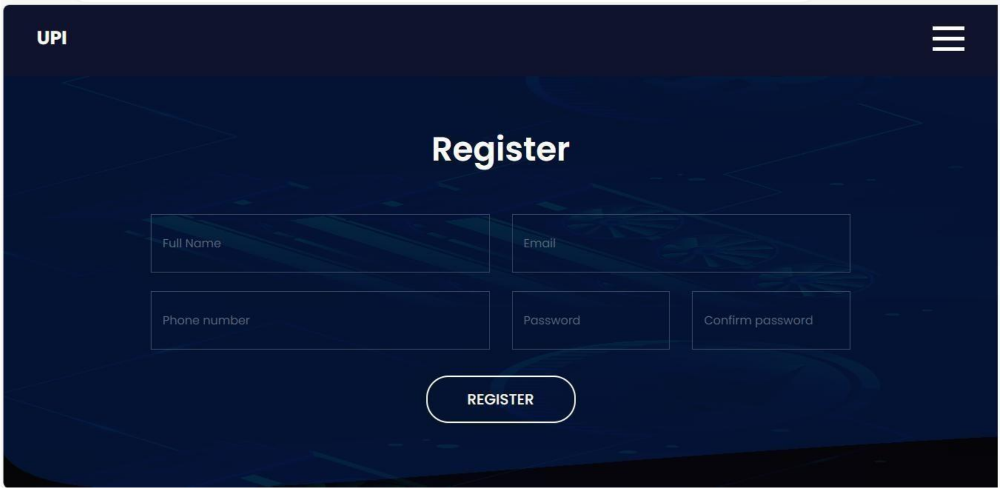


Figure 6.16: Registration Page

- This page allows users to register for services, ensuring secure access by requiring personal details and password confirmation. It provides a user-friendly interface for creating a secure account.

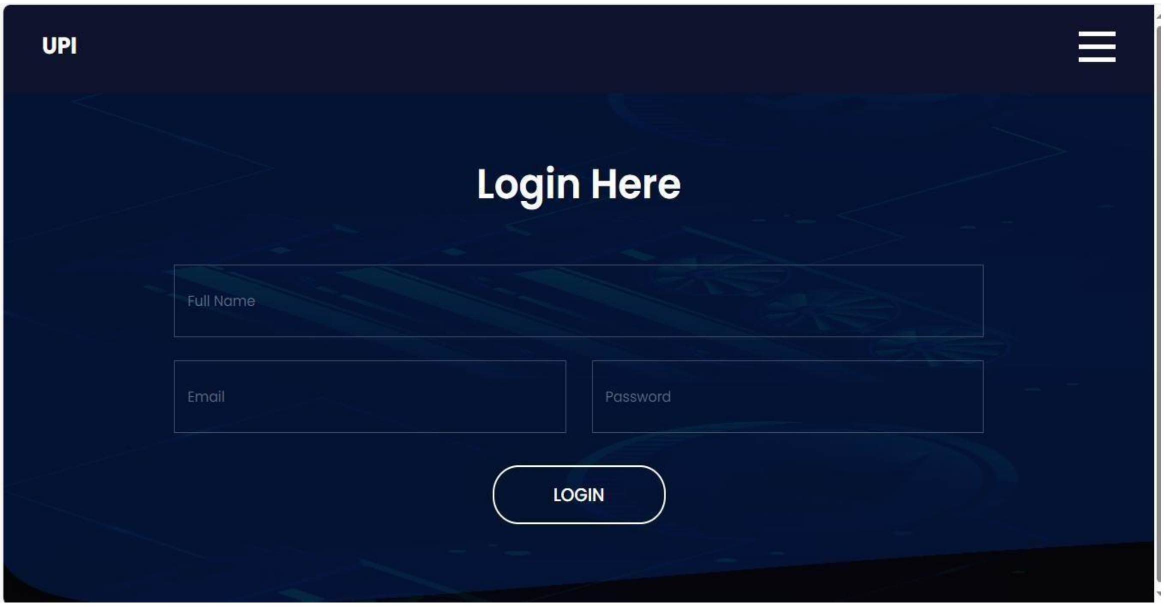
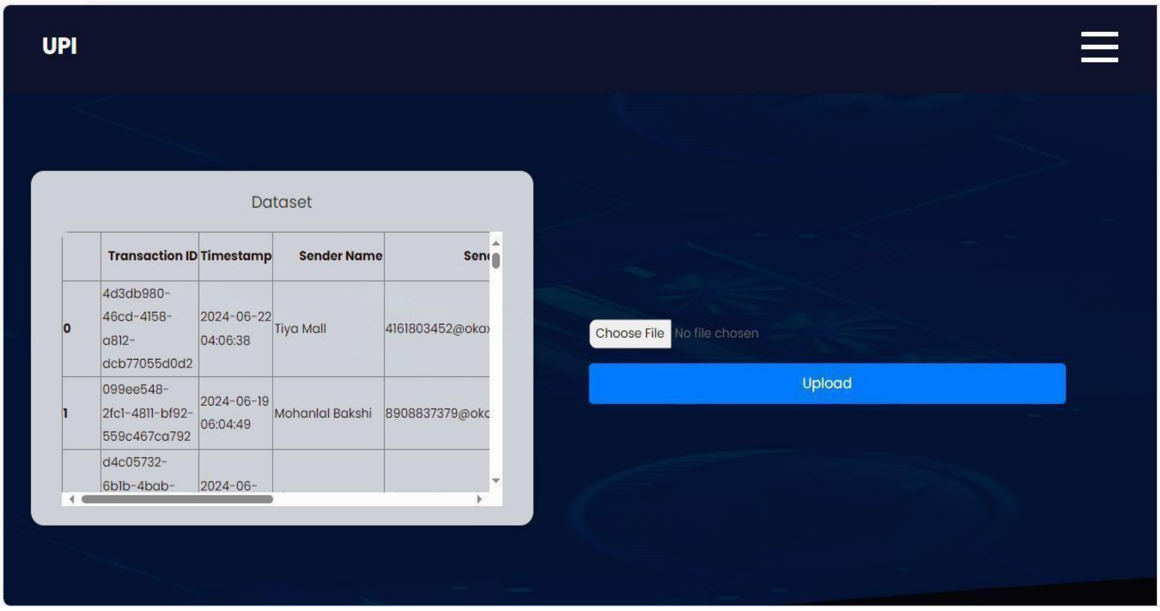


Figure 6.17: Login Page

- This page provides a secure login interface for users to access the prediction account using their email and password.



Dataset

	Transaction ID	Timestamp	Sender Name	Sen
0	4d3db980-46cd-4158-a812-dcb77055d0d2	2024-06-22 04:06:38	Tiya Mall	4161803452@oka
1	099ee548-2fc1-4811-bf92-559c467ca792	2024-06-19 06:04:49	Mohanlal Bakshi	8908837379@okc
	d4c05732-6b1b-4bab-	2024-06-		

Figure 6.18: Upload Page

- This interface enables users facilitating Selection the dataset uploads and model training and prediction and evaluation to achieve precise predictive outcomes.
- This page allows users to upload datasets for prediction, enabling model training and evaluation for accurate results.

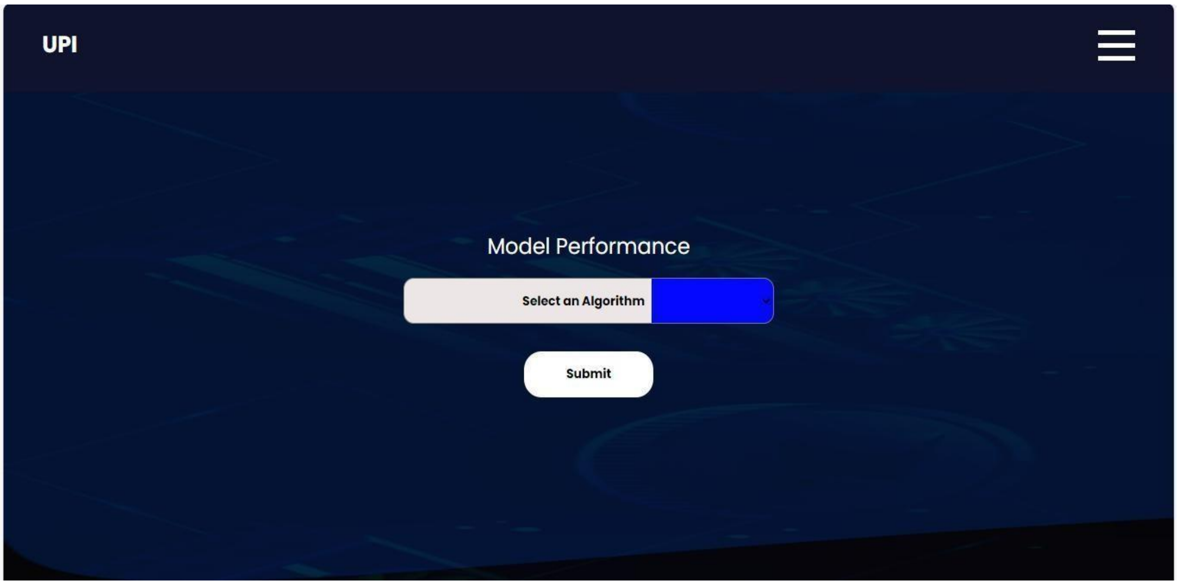
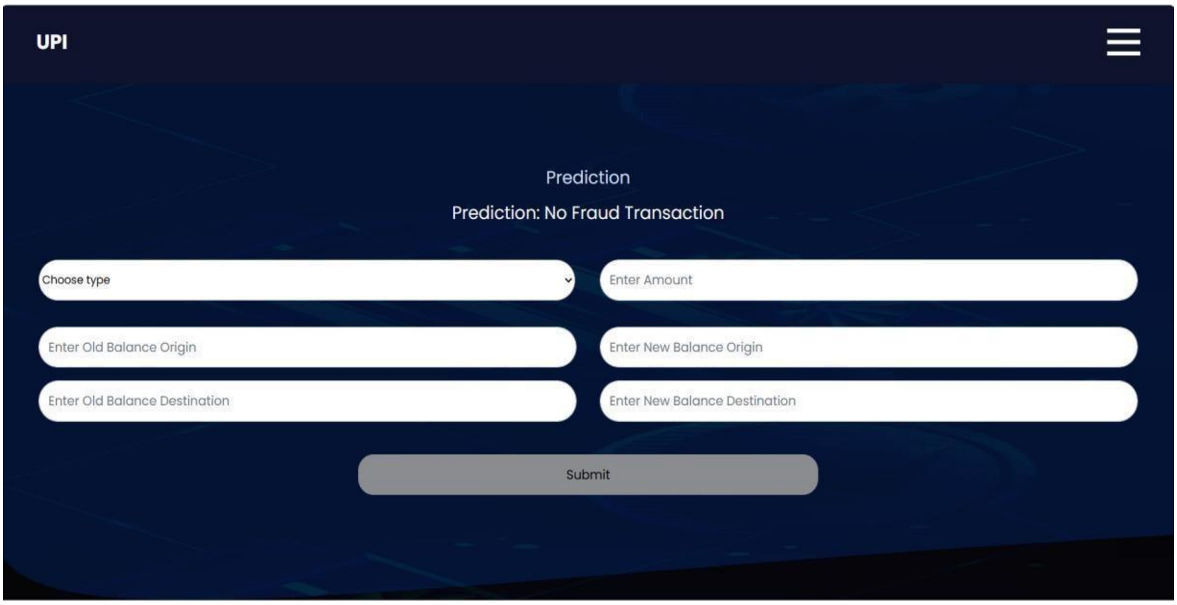


Figure 6.19: Model selection Page

- This page allows users to select an algorithm analysis, enhancing decision-making through machine learning models.



Prediction: No Fraud Transaction

Figure 6.20: Prediction Page

- This page collects user input for various detection parameters to predict the Fraud Detection

CONCLUSION

The integration of **Explainable AI (XAI)** and **Federated Learning (FL)** offers a transformative approach to financial fraud detection by addressing key challenges of transparency and privacy. By employing **Decision Trees, Random Forest, Gradient Boosting Machines (GBMs), and XGBClassifier**, this project enhances model interpretability and performance over traditional approaches.**XGBClassifier and GBMs** improve fraud detection accuracy by capturing complex patterns, while **Random Forest and Decision Trees** provide transparency, allowing financial institutions to understand classification outcomes. Additionally, **Federated Learning (FL)** strengthens privacy by enabling decentralized model training, preserving the confidentiality of sensitive financial data without requiring direct data sharing.

This dual approach not only enhances fraud detection precision but also fosters a more transparent and privacy-preserving framework. The results underscore the potential of combining **XAI and FL** to advance financial fraud detection systems, ensuring both **robust performance and compliance with privacy standards**. This paradigm shift holds promise for **more secure and accountable financial systems** in the future.

FUTURE ENHANCEMENTS

Future advancements in fraud detection can focus on integrating advanced techniques for even greater **precision, interpretability, and privacy**.

- **Hybrid Model Integration:** Combining the interpretability of Decision Trees and Random Forests with the predictive power of Gradient Boosting Machines (GBMs) and XGBClassifier can enhance fraud detection accuracy. Incorporating deep learning architectures like Transformer models can further capture complex fraud patterns.
- **Improved Cross-Device Communication:** Enhancing federated learning (FL) frameworks with optimized communication strategies can improve model accuracy and efficiency across multiple financial institutions while maintaining data privacy.
- **Differential Privacy for Security:** Implementing differential privacy technique**s** within FL ensures that sensitive financial data remains protected, reducing the risk of data leakage while still allowing effective fraud detection.
- **Real-Time Fraud Detection:** Leveraging streaming data and adaptive learning algorithms can enable immediate fraud detection and prevention, reducing response time and minimizing financial losses. XGBClassifier and GBMs, known for their speed and scalability, can be optimized for real-time applications.

REFERENCES

[1] N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, "A Review of Credit Card Fraud Detection Using Machine Learning Techniques," in *5th* International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications *(*CloudTech*)*, IEEE, Casablanca, Morocco, 2020

[2] M. Valavan and S. Rita, "Predictive Analysis-Based Machine Learning Model for Fraud Detection with Boosting Classifiers," Comput. Syst. *Sci.* Eng., vol. 45, no. 1, pp. 231–245, 2022.

[3] R. Rani, A. Alam, and A. Javed, "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions," in 2nd International Conference on Disruptive Technologies *(*ICDT*)*, IEEE, Bangalore, India, 2024, pp. 924–932.

[4] Y. Gupta, N. Saxena, and K. Kumar, "UPI Fraud Detection Using Machine Learning," Int. J. Adv. Eng. Manag. (IJAEM), vol. 6, no. 10, pp. 29–34, Oct. 2024.

[5] M. Nagaraju, Y. C. Reddy, P. N. Babu, V. S. P. Ravipati, and V. Chaitanya, "UPI Fraud Detection Using Convolutional Neural Networks (CNNs)," Res. Square Preprint, pp. 1–16, 2024.

[6] S. Vyas, A. N. Patra, and R. M. Shukla, Histopathological image classification and vulnerability analysis using,' 2023, arXiv:2306.05980.

[7] A. Abdallah, M. A. Maarof, and A. Zainal, Fraud detection system: A survey,'' J. Netw. Comput. Appl., vol. 68, pp. 90–113, Jun. 2016.

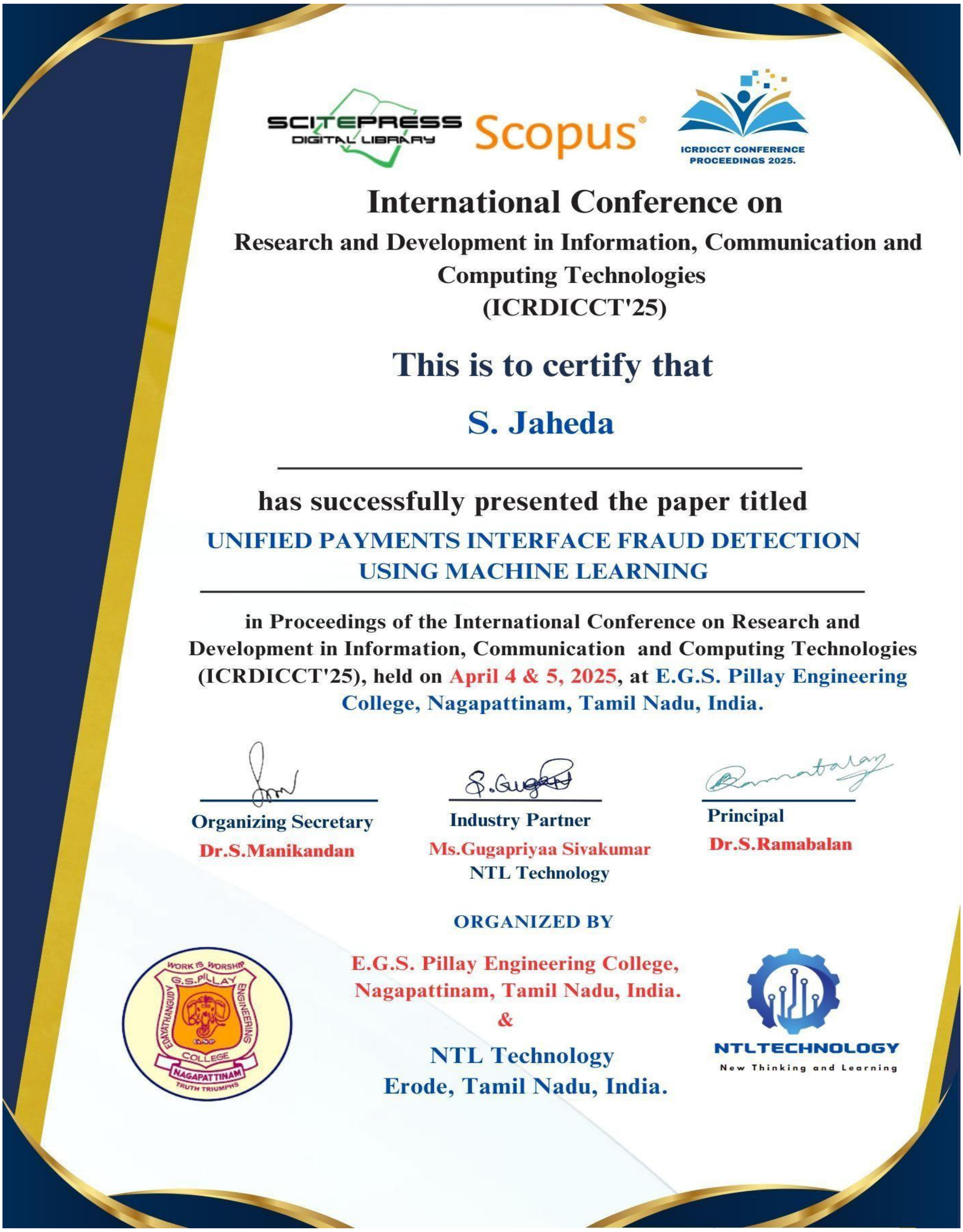
[8] A. Pascual, K. Marchini, and S. Miller. (2017). 2017 Identity Fraud: Securing the Connected Life. Javelin. [Online]. Available: http://www. javelinstrategy.com/coverage-area/2017-identity-fraud

[9] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, Data mining for credit card fraud: A comparative study,'' Decis. Support Syst., vol. 50, no. 3, pp. 602–613, Feb. 2011

[10] L. T. Rajesh, T. Das, R. M. Shukla, and S. Sengupta, Give and take: Federated transfer learning for industrial IoT network intrusion detection,'' 2023, arXiv:2310.07354.

[11] H. van Driel, Financial fraud, scandals, and regulation: A conceptual framework and literature review,' Bus. Hist., vol. 61, no. 8, pp. 1259–1299, Nov. 2019.

PUBLICATION



SCITEPRESS DIGITAL LIBRARY

Scopus®

ICRDICCT CONFERENCE PROCEEDINGS 2025.

International Conference on

Research and Development in Information, Communication and Computing Technologies (ICRDICCT'25)

This is to certify that

S. Jaheda

has successfully presented the paper titled

UNIFIED PAYMENTS INTERFACE FRAUD DETECTION USING MACHINE LEARNING

in Proceedings of the International Conference on Research and Development in Information, Communication and Computing Technologies (ICRDICCT'25), held on April 4 & 5, 2025, at E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

Organizing Secretary
Dr.S.Manikandan

Industry Partner
Ms.Gugapriyaa Sivakumar
NTL Technology

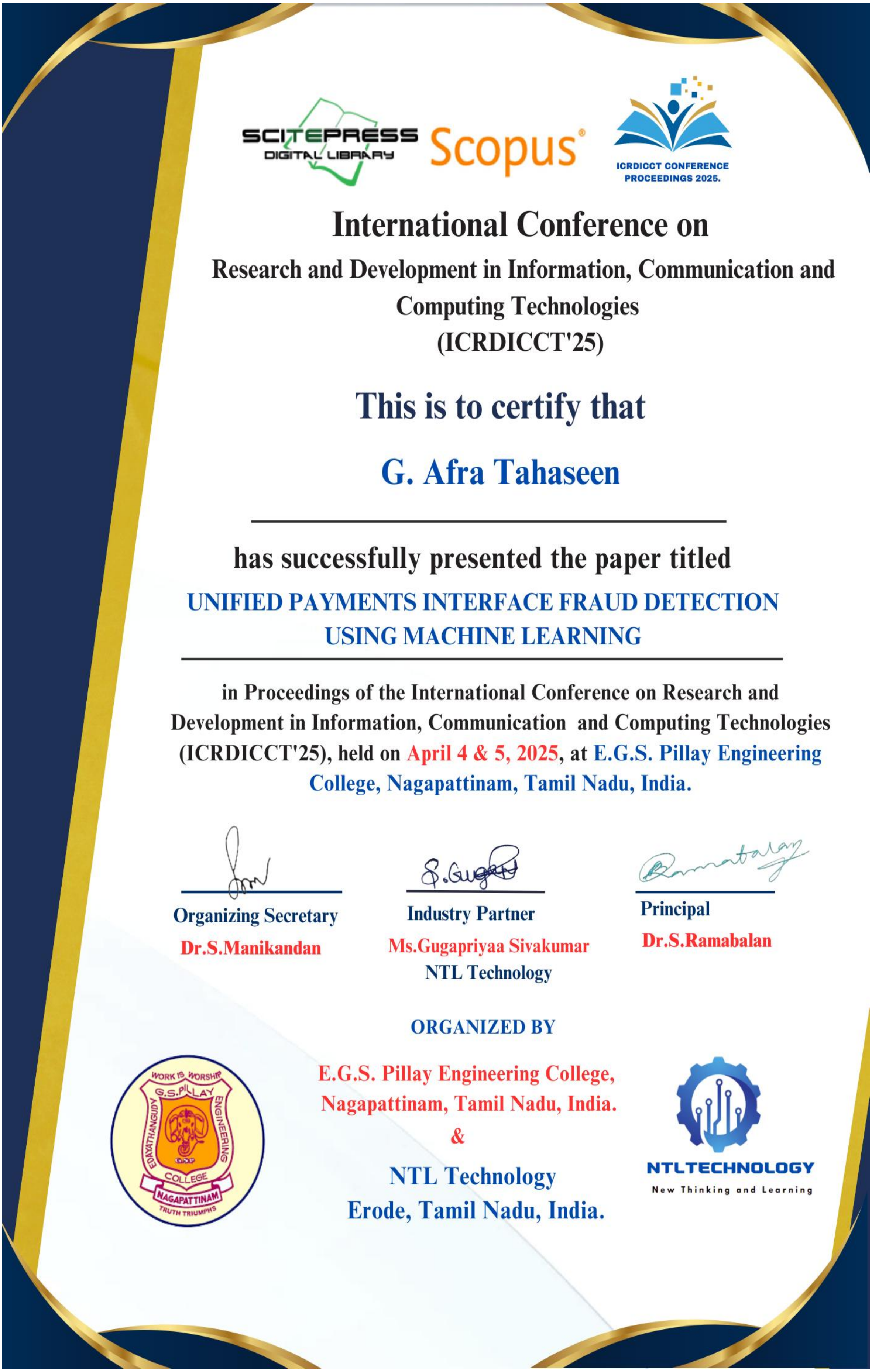
Principal
Dr.S.Ramabalan

ORGANIZED BY

WORK IS WORSHIP
E.G.S.PILLAY ENGINEERING COLLEGE
NAGAPATTINAM
TRUTH TRIUMPHS

E.G.S. Pillay Engineering College,
Nagapattinam, Tamil Nadu, India.
&
NTL Technology
Erode, Tamil Nadu, India.

NTLTECHNOLOGY
New Thinking and Learning



SCITEPRESS DIGITAL LIBRARY

Scopus

ICRDICCT CONFERENCE PROCEEDINGS 2025.

International Conference on

Research and Development in Information, Communication and Computing Technologies
(ICRDICCT'25)

This is to certify that

G. Afra Tahaseen

has successfully presented the paper titled

UNIFIED PAYMENTS INTERFACE FRAUD DETECTION USING MACHINE LEARNING

in Proceedings of the International Conference on Research and Development in Information, Communication and Computing Technologies (ICRDICCT'25), held on April 4 & 5, 2025, at E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

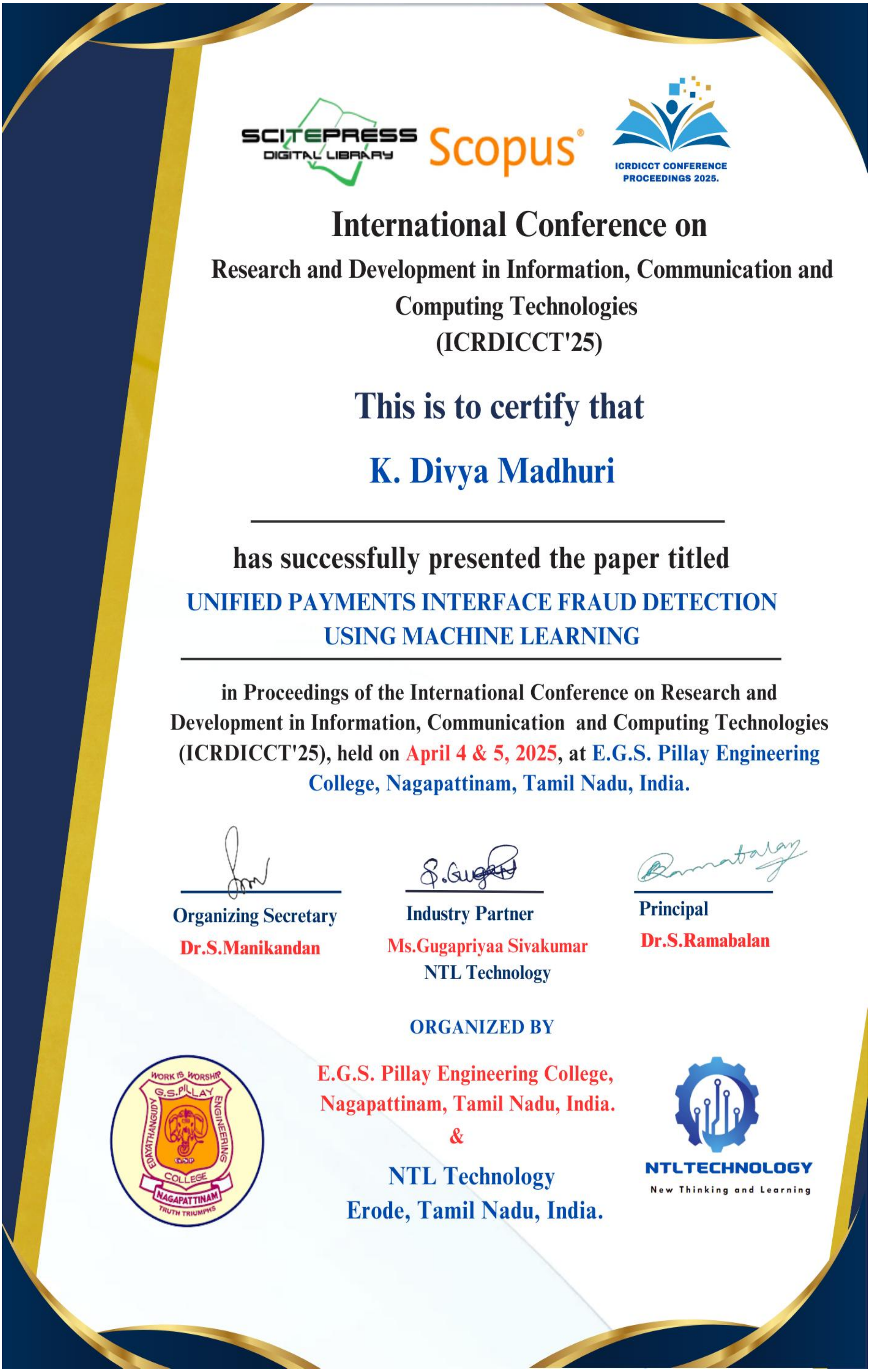
Organizing Secretary	Industry Partner	Principal
Dr.S.Manikandan	Ms.Gugapriyaa Sivakumar NTL Technology	Dr.S.Ramabalan

ORGANIZED BY

WORK IS WORSHIP
G.S.PILLAY ENGINEERING COLLEGE
EDAYATHANGUDY
NAGAPATTINAM
TRUTH TRIUMPHS

E.G.S. Pillay Engineering College,
Nagapattinam, Tamil Nadu, India.
&
NTL Technology
Erode, Tamil Nadu, India.

NTLTECHNOLOGY
New Thinking and Learning



SCITEPRESS DIGITAL LIBRARY Scopus® ICRDICCT CONFERENCE PROCEEDINGS 2025.

International Conference on

Research and Development in Information, Communication and Computing Technologies (ICRDICCT'25)

This is to certify that

K. Divya Madhuri

has successfully presented the paper titled

UNIFIED PAYMENTS INTERFACE FRAUD DETECTION USING MACHINE LEARNING

in Proceedings of the International Conference on Research and Development in Information, Communication and Computing Technologies (ICRDICCT'25), held on April 4 & 5, 2025, at E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

Organizing Secretary
Dr.S.Manikandan

Industry Partner
Ms.Gugapriyaa Sivakumar
NTL Technology

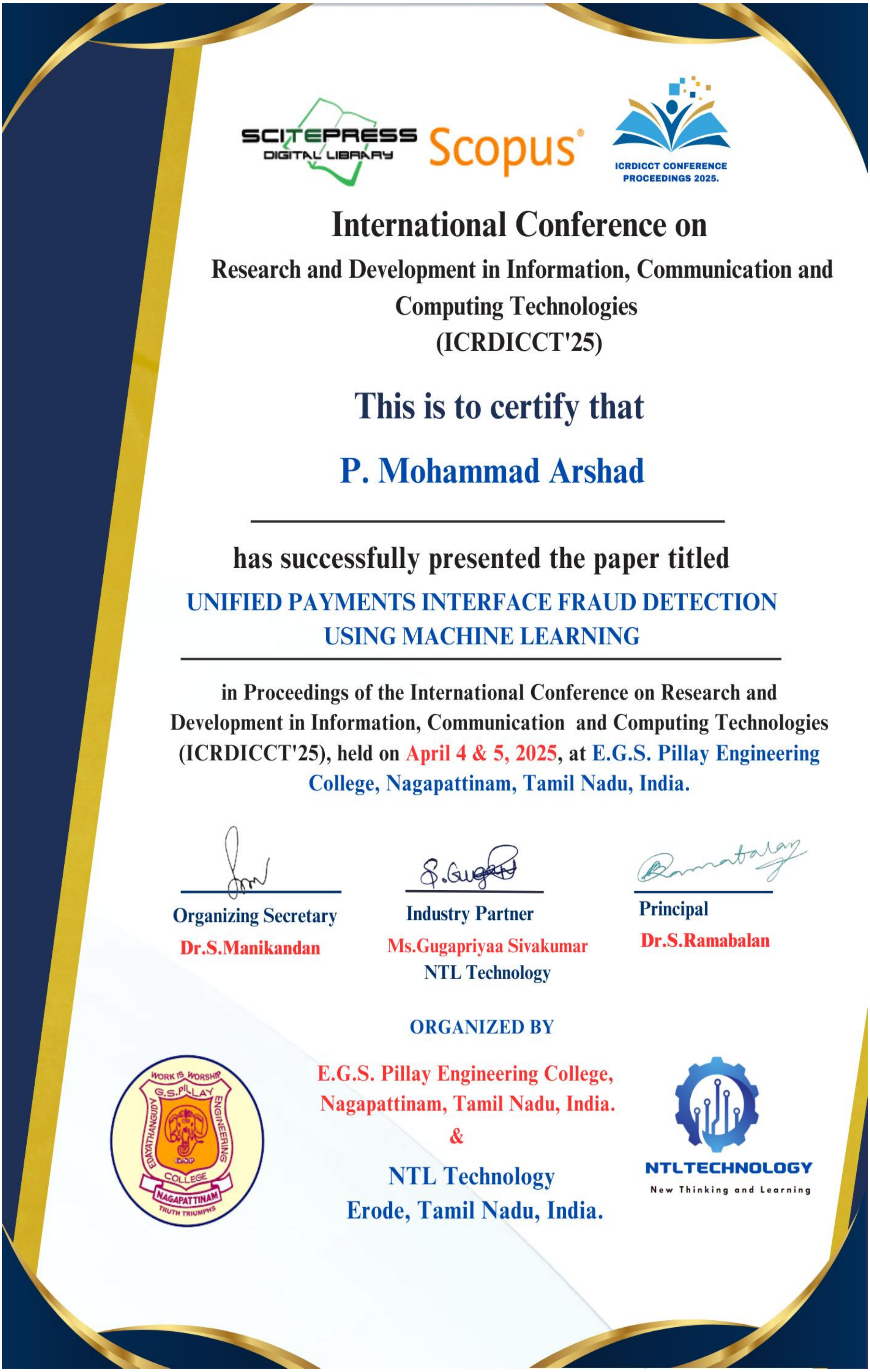
Principal
Dr.S.Ramabalan

ORGANIZED BY

E.G.S. Pillay Engineering College,
Nagapattinam, Tamil Nadu, India.
&
NTL Technology
Erode, Tamil Nadu, India.

WORK IS WORSHIP G.S.PILLAY ENGINEERING COLLEGE EDAYATHANGUDY NAGAPATTINAM TRUTH TRIUMPHS

NTLTECHNOLOGY
New Thinking and Learning



SCITEPRESS DIGITAL LIBRARY Scopus® ICRDICCT CONFERENCE PROCEEDINGS 2025.

International Conference on

Research and Development in Information, Communication and Computing Technologies
(ICRDICCT'25)

This is to certify that

P. Mohammad Arshad

has successfully presented the paper titled

UNIFIED PAYMENTS INTERFACE FRAUD DETECTION USING MACHINE LEARNING

in Proceedings of the International Conference on Research and Development in Information, Communication and Computing Technologies (ICRDICCT'25), held on April 4 & 5, 2025, at E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

Organizing Secretary	Industry Partner	Principal
Dr.S.Manikandan	Ms.Gugapriyaa Sivakumar NTL Technology	Dr.S.Ramabalan

ORGANIZED BY

E.G.S. Pillay Engineering College,
Nagapattinam, Tamil Nadu, India.
&
NTL Technology
Erode, Tamil Nadu, India.

WORK IS WORSHIP E.G.S.PILLAY ENGINEERING COLLEGE EDAYATHANGUDY NAGAPATTINAM TRUTH TRIUMPHS

NTLTECHNOLOGY
New Thinking and Learning