A MINI PROJECT

on

ONLINE TRANSACTION FRAUD DETECTION

Submitted in partial fulfilment of the Requirements for the award of the degree of

Bachelor of Technology

In

Computer Science and Engineering

By

P.V.M. Meghana	**(O180824)**
M. Aparna	**(O180825)**
CH.Vyshnavi	**(O180850)**
A.Sunitha	**(O180855)**

Under the guidance of

Mrs. S. Nagamani M.Tech(Ph.D), Assistant Professor

Department of Computer Science Engineering

RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES

ONGOLE CAMPUS

2023

RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is certify that the project entitled on **'ONLINE TRANSACTION FRAUD DETECTION'**, being submitted by the Team of, P.V.M. Meghana (O180824), M.Aparna(O180825), CH.Vyshnavi(O180850) and A.Sunitha (O180855) in partial fulfillment of the requirements for the award of the degree of the Bachelor Of Technology in computer science and Engineering in Dr. APJ Abdul Kalam ,RGUKT-AP IIIT Ongole is a record of bonafide work carried out by them under my guidance and supervision during the academic year 2022-23.

The results presented in this project have been verified and found to be satisfactory. The results embodied in this project report have not been submitted to any other University for the award of any other degree or diploma.

Mrs. S Nagamani M.Tech(Ph.D)
Assistant Professor,
Department of CSE,
RGUKT Ongole.

Mr. B Sampath BabuM.Tech(Ph.D)
Head of Department,
Department of CSE,
RGUKT Ongole

RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is certify that the project entitled on **'ONLINE TRANSACTION FRAUD DETECTION'**, being submitted by the Team of, P.V.M. Meghana (O180824), M.Aparna(O180825), CH.Vyshnavi(O180850) and A.Sunitha (O180855) in partial fulfillment of the requirements for the award of the degree of the Bachelor Of Technology in computer science and Engineering in Dr. APJ Abdul Kalam ,RGUKT-AP IIIT Ongole is a record of bonafide work carried out by them under my guidance and supervision during the academic year 2022-23.

Mrs. S Nagamani M.Tech(Ph.D)
Assistant Professor,
Department of CSE,
RGUKT Ongole.

Mr. B Sampath Babu M.Tech(Ph.D)
Head of Department,
Department of CSE,
RGUKT Ongole.

APPROVAL SHEET

This report entitled "**ONLINE TRANSACTION FRAUD DETECTION**" submitted by the Team of, P.V.M. Meghana (O180824), M.Aparna(O180825), CH.Vyshnavi(O180850) and A.Sunitha (O180855). **Mrs.S Nagaman**i M.Tech(Ph.D), Assistant Professor,Department of CSE, RGUKT Ongole approved for the degree of **Bachelorof Technology** in **COMPUTER SCIENCE AND ENGINEERING**.

Examiner

_____

_____

_____

_____

Supervisor

_____

_____

_____

_____

Date: _____

Place:

ACKNOWLEDGEMENT

It is our privilege and pleasure to express a profound sense of respect, gratitude and Indebtedness to our guide **Mrs S Nagamani M.Tech(Ph.D), Assistant Professor**, Dept. of Computer Science and Engineering, Rajiv Gandhi University of Knowledge Technologies, for her indefatigable inspiration, guidance, cogent discussion, constructive criticisms and encouragement throughout this dissertation work. We express our sincere gratitude to **B Sampath Babu, Assistant Professor & Head of Department of Computer Science and Engineering**, Rajiv Gandhi University of Knowledge Technologies, for his suggestions, motivations and co-operation for the, successful completion of the work. We extend our sincere thanks to **Prof. B Jayarami Reddy**, **Director**, Rajiv Gandhi University of Knowledge Technologies for his encouragement. And also we thank each individual of the RGUKT, Ongole campus for their impeccable support for our project.

With Sincere Regards,

P.V.M.Meghana- O180824

M. Aparna - O180825

CH. Vyshnavi - O180850

A.Sunitha - O180855

DECLARATION

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in out submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

P.V.M.Meghana – O180824 (signature)

M. Aparna– O180825 (signature)

CH.Vyshnavi – O180850 (signature)

A.Sunitha – O180855 (signature)

Date:

ABSTRACT

With the exponential growth of e-commerce and digital transactions, the need for robust fraud detection systems has become increasingly vital. This project focuses on developing a machine learning-based solution for online payment fraud detection, aiming to mitigate financial losses and protect both consumers and businesses. Leveraging a dataset comprising historical transactional data, the proposed approach employs state-of-the-art machine learning algorithms to identify patterns and anomalies indicative of fraudulent activities. Feature engineering techniques are employed to extract relevant information, while various supervised learning models such as logistic regression, decision trees, and ensemble methods are trained to classify transactions as fraudulent or legitimate. The system also incorporates real-time monitoring capabilities to adapt and respond to emerging fraud techniques. Through extensive evaluation and performance metrics analysis, the effectiveness and efficiency of the proposed solution are measured, demonstrating its potential to significantly enhance the security of online payment systems. This research contributes to the advancement of fraud detection techniques, helping businesses and financial institutions detect and prevent fraudulent activities, safeguarding user trust and financial integrity in the ever-evolving digital landscape.

CONTENTS

1. INTRODUCTION

1.1 MOTIVATION:

Machine Learning has become one of the most interesting and opted fields of computer science. But apart from learning the techniques, usage of the prediction techniques requires a lot of programming knowledge and familiarity with their respective statistical approaches and mathematical calculations. Which makes building a prediction model difficult for people new to the domain and even for experts in building models of various strategies for a single scenario or just one dataset, takes a lot of time, effort and knowledge requirement. This motivated the idea of online transaction fraud detection together.

1.2 PROBLEM DEFINITION:

Traditional rule-based fraud detection systems often struggle to keep pace with the evolving strategies employed by fraudsters. These systems rely on pre-defined rules and thresholds, which may fail to adapt to emerging fraud patterns and may generate high rates of false positives, inconveniencing legitimate users. Therefore, there is a pressing need for an advanced fraud detection system that harnesses the power of machine learning to accurately and efficiently detect fraudulent transactions in real-time.

1.3 OBJECTIVE OF THE PROJECT:

Develop and implement an effective machine learning-based fraud detection system for online payment transactions, leveraging diverse datasets, exploring multiple algorithms, conducting feature engineering, optimizing model performance, enabling real-time monitoring, and ensuring scalability and adaptability to detect and prevent fraudulent activities while maintaining a high level of accuracy and minimizing false positives.

2. LITERATURE SURVEY

Abstract:-

Conducting transactions online is a general user behaviour nowadays with an alarming increase rate. It completely hassle-free and becoming a habit of the users. With such a large network of online transactions, it is expected to get big mistakes like frauds and glitches. In this paper we will be discussing a fraud detection and verification system targeting online transactions mainly e-commerce. This paper says certain techniques that can be used to verify any online transaction. If found any fraud, it is followed by verification mechanism that more or less helps to validate the authenticity of the transaction. The aspects laid down in this paper can no doubt be further scrutinised to build a robust fraud detection system, but certainly, they form a basis towards building a viable fraud detection system.

PUBLICATION:

- Published On April 22, 2021. By Nidhika Chauhan and Prikshit Tekta on international journel of Electronic Banking 2 (4), 267-274,2020.

ABSTRACT:-

The covid-19 pandemic has reduced people's mobility to a certain extent, making it difficult to purchase goods and service offline, which has led the people to be dependent on online services. By this so many people are using credit cards and so many are facing problems like frauds. Consequently, there is more need to develop the best approach using machine learning. All K-nearest neighbours (ALLKNN) under sampling technique along with cat Boost (ALLKNN-Cat Boost) is considered to be best proposed model. The results indicates best features which detect the frauds accurately.

PUBLICATION:

Published by Noor Saleh Alfaiz and Suliman Mohamed Fati in college of computer and information sciences, prince sultan university, Piyadh 11586, Saudi arabia

Received:19 December 2021 and

Revised:13 February 2022 and

Accepted:14 February 2022 and

Published:21 February 2022.

ABSTRACT:-

Naturally, there has also been a problem in online transaction frauds which is having a major impact on banks, persons who issues online transaction permissions to users. Consequently there is a urgent need to implement a system which is used to decrease frauds by using machine learning models, in the second experiment performed for the purpose of this research, the data set has been expended by utilizing the synthetic

Minority over-sampling approach. The experimental findings clearly demonstrate that the models tunded by the proposed algorithm obtained superior results in comparison to other models hybridized with competitor meta heuristics.

PUBLICATION:

Published by Dijana Jovanovic and Milos Antonijevic, Milos Stankovic, Miodrag Zivkovic, Marko Tanaskovic and Nebojsa Bacanin in college of Academic Studies Dositej,11000 Belgrade, Serbia

Faculty of informatics and Computing, Singidunum University, Danijelova 32, 11010 Belgrade,Serbia

Received: 5 June 2022

Revised: 21 June 2022

Accepted: 23 June 2022

Published: 29 June 2022

3. METHODOLOGIES AND ANALYSIS

3.1 EXISTING SYSTEM:

In case of credit card fraud detection, the existing system is detecting the fraud after fraud has been happen. Existing system maintain the data when customer comes to know about inconsistency in transaction, he/she made complaint and then fraud detection system start it working. It first tries to detect that fraud has actually occur after that it starts to track fraud location and so on. In case of existing system there is no confirmation of recovery of fraud and customers satisfaction.

3.2 PROPOSED SYSTEM:

The aim of the proposed system is to develop a website which has capability to restrict and block the transaction performing by attacker from genuine user's credit card details. The system here is developed for the transactions higher than the customers current transaction limit. As we seen the existing system detects the fraud after fraud has been occurred i.e. based on customers complained . The proposed system tries to detect fraudulent transaction . In proposed system, while registration we take required information which is efficient to detect fraudulent user activity .

- It detects the fraud transactions with high accuracy.
- Because we maintain large amount of real world dataset.
- Here we implement speech recognition for detecting the fraud transaction.
- It tries to find any anomaly in the transaction based on the spending profile of the cardholder,shipping address, and billing address, etc.

3.3 REQUIREMENTS SPECIFICATION :

Programming Languages : PYTHON
Modules : Numpy, Pandas, Matplotlib, Seaborn, Tkinter, Sklearn
Operating system : WINDOWS 10 PRO, UBUNTU 20.04 LTS and any OS that runs python
IDE editor : VISUAL STUDIO CODE
Tools : Anaconda, Jupyter Notebook
RAM required: 4GB and above

3.4 INTRODUCTION TO TECHNOLOGIES USED:

PYTHON

Python is a versatile, high-level programming language widely used in machine learning due to its simplicity and the availability of numerous libraries. Libraries like Scikit-learn, TensorFlow, and PyTorch make Python a preferred choice for machine learning. Scikit-learn supports various machine learning algorithms for classification, regression, and clustering. Tkinter, on the other hand, is Python's standard GUI (Graphical User Interface) package. It's a lightweight and user-friendly tool for creating desktop applications.

NUMPY

NumPy is a powerful Python library that stands for "Numerical Python." It provides efficient and versatile tools for performing mathematical and scientific computations. With NumPy, users can create multidimensional arrays, manipulate them, and apply various mathematical operations efficiently. NumPy's core functionality lies in its nd array (n-dimensional array) object, which allows for efficient storage and manipulation of large datasets.

The library offers a wide range of mathematical functions, including linear algebra, Fourier transform, random number generation, and more. These functions are optimized for speed and memory usage, making NumPy an essential tool for numerical computations. NumPy also provides convenient and intuitive indexing and slicing mechanisms, enabling users to extract and modify specific elements or subarrays of arrays. It integrates seamlessly with other Python libraries, such as SciPy, Matplotlib, and Pandas, creating a powerful ecosystem for scientific computing and data analysis. Overall, NumPy's performance, versatility, and extensive mathematical functionality make it a fundamental library for numerical computing in Python, serving as the backbone for many scientific and data-related applications.

PANDAS

Pandas is a powerful and versatile Python library that is widely used for data manipulation and analysis. It provides easy-to-use data structures and data analysis tools, making it ideal for working with structured data. Pandas introduces two primary data structures: Series, which represents a one-dimensional labeled array, and DataFrame, which

is a two-dimensional labeled data structure resembling a table. With Pandas, users can effortlessly load, manipulate, and filter data, handle missing values, merge and join datasets, and perform various statistical computations. It offers a rich set of functions for data exploration, transformation, and visualization. Pandas integrates well with other Python libraries, such as NumPy and Matplotlib, further enhancing its capabilities for data analysis and visualization. Pandas is widely adopted in domains like data science, finance, economics, and social sciences, where data preprocessing and analysis are fundamental. Its intuitive syntax and extensive functionality make it a go-to tool for data wrangling and analysis tasks in Python.

MATPLOTLIB

Matplotlib is a comprehensive Python library for creating static, animated, and interactive visualizations. It provides a wide range of high-quality plots, charts, and graphs, allowing users to effectively communicate and present their data. With Matplotlib, users can generate line plots, scatter plots, bar plots, histograms, pie charts, and much more. It offers extensive customization options, enabling users to control every aspect of their visualizations, including colors, fonts, labels, and annotations.

Matplotlib integrates seamlessly with NumPy, making it easy to visualize data stored in NumPy arrays. It also works well with other libraries in the scientific Python ecosystem, such as Pandas, SciPy, and Seaborn. Whether you need to explore data, communicate insights, or create publication-quality figures, Matplotlib provides a powerful and flexible solution. Its versatility and intuitive interface make it a popular choice for data visualization tasks in various domains, including scientific research, data analysis, and machine learning.

SEABORN

Seaborn is a Python data visualization library built on top of Matplotlib. It provides a high-level interface for creating attractive and informative statistical graphics. Seaborn simplifies the process of creating complex visualizations by offering a range of pre-defined plot types and color palettes. With Seaborn, users can create visually appealing plots such as scatter plots, bar plots, box plots, heatmaps, and more. It offers several built-in themes and customization options to enhance the aesthetics of the plots.

Seaborn also provides statistical functionalities like visualizing linear regression models and plotting distributions. One of Seaborn's key advantages is its integration with Pandas, allowing for easy manipulation and visualization of data stored in data frames. It

enables users to quickly explore and communicate insights from their datasets. Whether you're a data scientist, analyst, or researcher, Seaborn is a valuable tool for creating professional and insightful visualizations in Python.

SKLEARN

Scikit-learn, also known as sklearn , is a popular machine learning library in Python. It provides a wide range of tools for data preprocessing, feature extraction, model selection, and evaluation. With sklearn , users can effortlessly implement various machine learning algorithms, including classification, regression, clustering, and dimensionality reduction. One of the key advantages of sklearn is its easy-to-use and consistent API, which allows for seamless integration with other Python libraries. It offers a comprehensive set of functionalities for tasks such as data splitting, cross-validation, hyperparameter tuning, and model evaluation. Additionally, sklearn supports a vast collection of metrics for assessing the performance of machine learning models. Sklearn is widely adopted in both academia and industry due to its simplicity, scalability, and robustness. It enables practitioners to efficiently build and deploy machine learning solutions, making it a valuable tool for data scientists and researchers alike.

LINEAR REGRESSION

Linear regression is a statistical modeling technique used to establish the relationship between a dependent variable and one or more independent variables. Its goal is to find a linear equation that best describes the relationship between these variables by minimizing the difference between the observed data points and the predicted values. The equation for a simple linear regression model is y = mx + b, where “y” is the dependent variable, “x” is the independent variable, “m” is the slope or coefficient, and “b” is the y-intercept. The slope represents the change in the dependent variable for every unit change in the independent variable, while the y-intercept is the predicted value of the dependent variable when the independent variable is zero.

In linear regression, the model is built by estimating the values of the coefficients (slope and y-intercept) using a method called ordinary least squares (OLS). The OLS method calculates the best-fit line by minimizing the sum of the squared differences between the

observed and predicted values. This approach allows us to make predictions and understand the relationship between variables. Linear regression is commonly used for forecasting, understanding correlations, and identifying trends in data. Additionally, it provides valuable insights into the strength and direction of the relationship between variables, helping researchers and analysts make informed decisions based on the model's coefficients and statistical significance.

DECISION TREE REGRESSION

Decision tree regression is a machine learning algorithm that uses a decision tree to predict continuous numeric values. It works by recursively splitting the data based on features, creating a tree-like structure where each internal node represents a test on a feature, and each leaf node represents a predicted value. In decision tree regression, the tree is built by minimizing the variance of the target variable within each leaf node. This allows the algorithm to find optimal splits that maximize the reduction in variance, leading to accurate predictions. Decision tree regression is widely used in various domains, including finance, healthcare, and retail. Its simplicity, interpretability, and ability to capture non-linear relationships make it a popular choice. However, it can be prone to overfitting and may require techniques such as pruning or ensemble methods like random forests to improve its performance.

3.5 OVERALL DESCRIPTION

The current world is inconspicuously run and affected by Machine Learning in several daily events of our lives. This computer science field is first named by Arthur Samuel, an IBM employee and an expert in Computer gaming and Artificial Intelligence. ML grants computers the ability to train from the data given to them and generate similar outputs mentioned in the data by observing the patterns in them. As the subspace of Artificial Intelligence, Machine Learning makes the computer learn through mathematical and logical calculations and yield knowledge similar to that of humans in predicting outcomes or generate possible values. And the other fascinating field of Data Science utilizes the accurate Machine Learning models to predict missing or future data to draw insights from them.

As the relative fields of Data Science and Machine Learning becoming more popular and being used in vast fields of real life applications, the key part of identifying the most

accurate machine learning models for each individual scenario hassles the domain workers. Prior to exploring the in-depth concepts of models, novice students or professionals on the way to transition their careers need a more facade approach to the basics of the models about their working functionalities and practical experience about predicting models. The project Multi Regressor hides all the complex programs and implements exactly what we need and shows a full fledged regression based prediction model. As multiple algorithms are being clumped together, the working efficiency of the program is directly proportional to the clarity, versatility and precision of the datasets.

As built purely based on the python packages, one good python interpreter is only needed for the project implementation. And the single platform based tool accepts the datasets of test values through the direct csv files. The analyzer displays the columns available for the user to choose for training the model. Then the independent and dependent features are selected.

Once the features are selected, finalized and cleaned for the selected regression models from both supervised and unsupervised methods, like Simple Linear Regression,, DecisionTreeModel etc., the prediction models are trained and made available for prediction, as they accept the similar inputs of the features and predict the outputs. Each regression models will be validated based on their R2 value. Thus the project is useful for both professionals to quickly compare between several methods and new programmers to learn from live examples.

4. DESIGN

4.1 UML DIAGRAMS:

UML is the short form of 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 important goal for UML is to create a common modelling language for the sake of Object Oriented Software engineering. In its current form UML consists 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 artifacts of software systems, as well as for business modelling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems. The 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.

Activity Diagram:

An activity diagram provides a view of the behaviour of a system by describing the sequence of actions in a process.

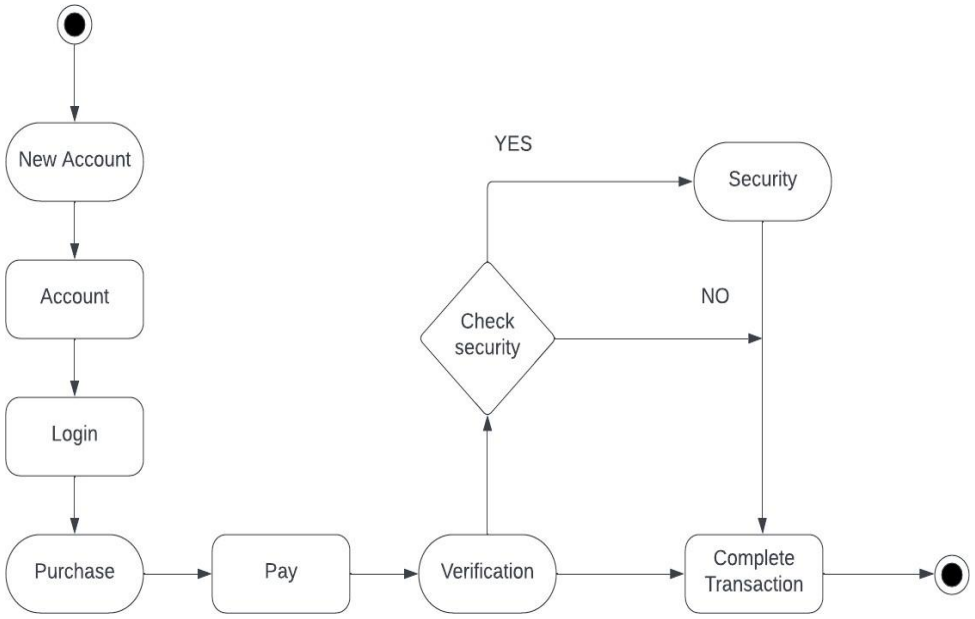

Fig 1: Activity Diagram

Use case Diagram:

A use case diagram is used to represent the dynamic behavior of a system. It encapsulates the system's functionality by incorporating use cases, actors, and their relationships. It models the tasks, services, and functions required by a system/subsystem of an application.

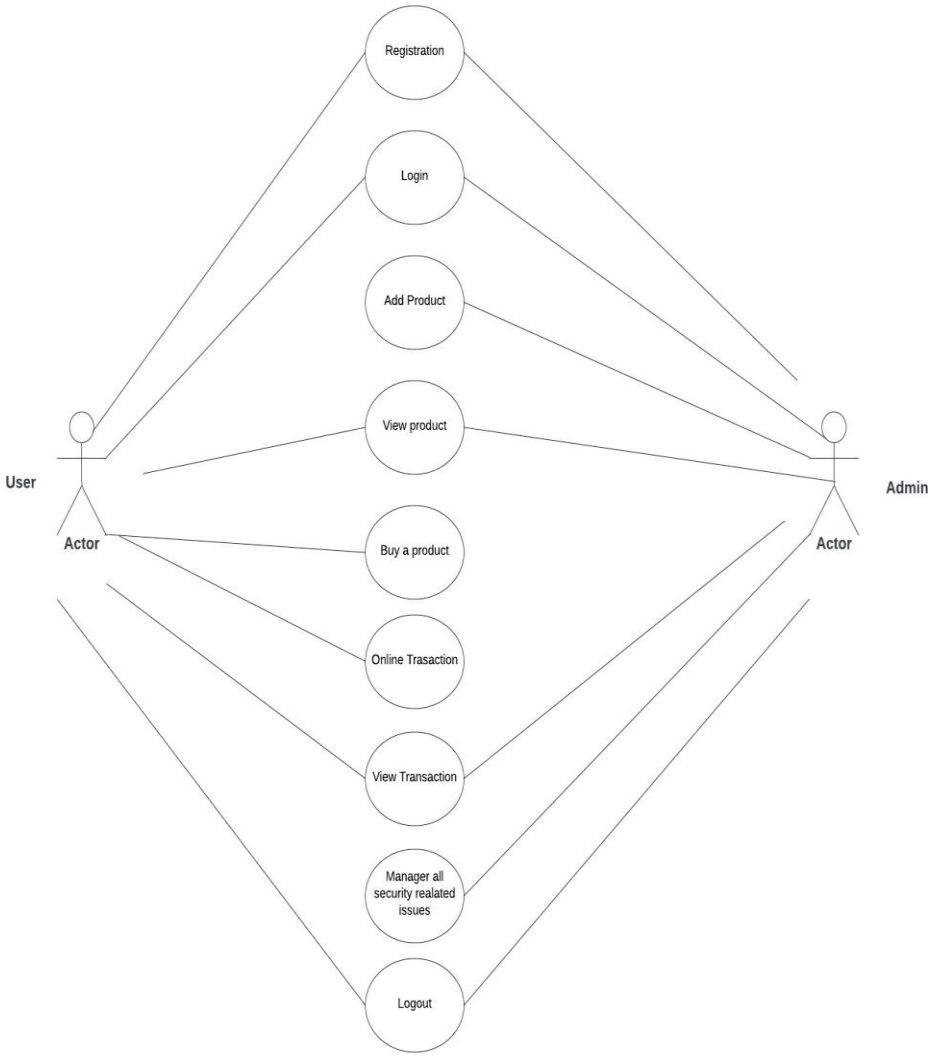

Fig 2: Use case Diagram

Component Diagram:

The component diagram is to show the relationship between different components in a system.

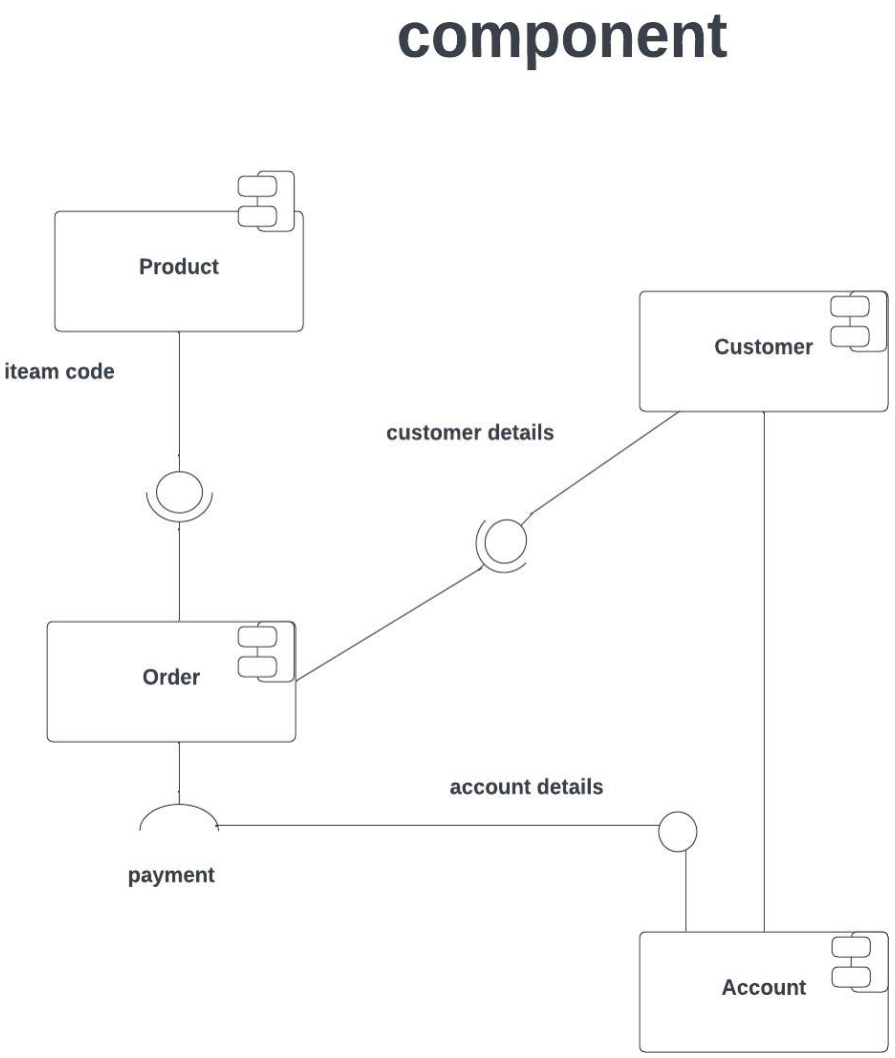

Fig 3: Component Diagram

5. IMPLEMENTATION

5.1 SAMPLE CODE

```
 <!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Online Transaction Fraud Detection</title>
    <link
      href="https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.css"
      rel="stylesheet"
    />
    <script>
      function redirectToResultPage() {
        // Perform fraud detection logic and determine the result
        const isFraud = true;

        // Redirect to the result page with the result as a query parameter
        window.location.href = "result.html?isFraud=" + isFraud;
      }
    </script>
    <style>
      .h-screen{
      background-color:#009FBD;
      }
      .container{
      background-color:#210062;
      width:500px;
      height:500px;
      border-radius:5%;
      }
      .inside{
```

```
    margin-top:20%;
    width:400px;
    padding-left:100px;;

    }
  </style>
</head>
<body>
  <div class="h-screen">

    <h1
      class="text-4xl font-bold text-center py-4 text-blue-800 bg-blue-100"
    >
      Online Transaction Fraud Detection
    </h1>

    <div class="flex flex-col items-center justify-center h-screen bg-blue-200">
      <div class="container">
      <form action='/predict' method="POST" class="inside">
        <div class="flex flex-col gap-4">
          <select
            class="border border-green-300 rounded px-4 py-2 bg-green-100" name="type"
            placeholder="Payment Type" required>
            <option value=1>CASH_OUT</option>
            <option value=2>PAYMENT</option>
            <option value=3>DEBIT</option>
            <option value=4>TRANSFER</option>
            <option value=5>CASH_IN</option>

          </select>
          <input
            class="border border-green-300 rounded px-4 py-2 bg-green-100"
            type="text"
```

```
            name="amount"
            placeholder="Transaction Amount" required
          />
          <input
            class="border border-green-300 rounded px-4 py-2 bg-green-100"
            type="text"
            name="OldBalance"
            placeholder="Old Balance" required
          />
          <input
            class="border border-green-300 rounded px-4 py-2 bg-green-100"
            type="text"
            name="NewBalance"
            placeholder="New Balance" required
          />
          <button
            class="border border-green-300 rounded px-4 py-2 bg-green-100 hover:border-2
p-4"
            type="submit">
            Submit
          </button>
        </div>
      </form>
      </div>
    </div>
  </div>
    </div>
  </div>
</body>
</html>
```

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Online Transaction Fraud Detection - Result</title>
    <link
      href="https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.css"
      rel="stylesheet"
    />
    <style>
    .container{
    margin-top:30px;
    border-radius:5%;
    margin-left:300px;
    width:60%;
    background-color:#9DB2BF;
    }
    .container1{
    margin-top:30px;
    border-radius:5%;
    margin-left:300px;
    width:60%;
    background-color:#9DB2BF;
    }
      .result-container {
        display: flex;
        flex-direction: column;
        align-items: center;
        justify-content: flex-start;
        min-height: 100vh;
      }
```

```
.result-title {
  font-weight: bold;
  color: #1a202c;
  padding: 2rem;
  /* background-color: #ebf8ff; */
  margin-bottom: 2rem;
}

.result-message {
  font-size: 25px;
  font-weight: bold;
  color: #1a202c;
  height: 100%;
  width: 100%;
  text-align: center;
}

.fraud {
  background-color: #ffcccc;
}

.valid {
  background-color: #ccffcc;
}
body{
background-color:#ACBCFF;
}
.again{
margin-top:30px;
padding-left:2%;
padding-bottom:20%;
}
.submit{
```

```
    border:2px solid green;
    color:red;
    backgroun-dolor:#E6FFFD;
    border-radius:10%;
    }
  </style>
  <script>
    document.addEventListener("DOMContentLoaded", function () {});
  </script>
</head>
<body>
  <div class="result-container w-full h-screen" id="result-container-id">
    <h1
      class="text-4xl w-full font-bold py-4 text-center text-blue-800 bg-blue-100"
    >
      Online Transaction Fraud Detection
    </h1>
    <div class="result-message h-screen pt-16" id="result">
      {% if pred %} {% if pred == 'Fraud' %}
      <p class="fraud">This is a fraud transaction.</p>
      <div class="container">
      <p>
        We regret to inform you that your recent transaction has been deemed
        invalid. After careful analysis and evaluation, our system has
        determined that the transaction does not meet the necessary criteria
        for validation. This decision is based on various factors, including
        but not limited to transaction details, security protocols, and
        established patterns of fraudulent or suspicious activities.
      </p>
        </div>

      {% else %}
      <p class="valid">This is not a fraud transaction.</p>
```

```
        <div class="container1">
        <p>We are happy to inform you that your transaction is not having fraudulent
          behaviour. You can continue with your payment.
        </p>
        {% endif %} {% endif %}
           <div class="again">
    <button class="submit" ><a href="/" action="/">Predict Again</a></button>
   </div>
        </div>
      </div>

    </div>

  </body>
</html>
```

5.2 SCREENSHOTS

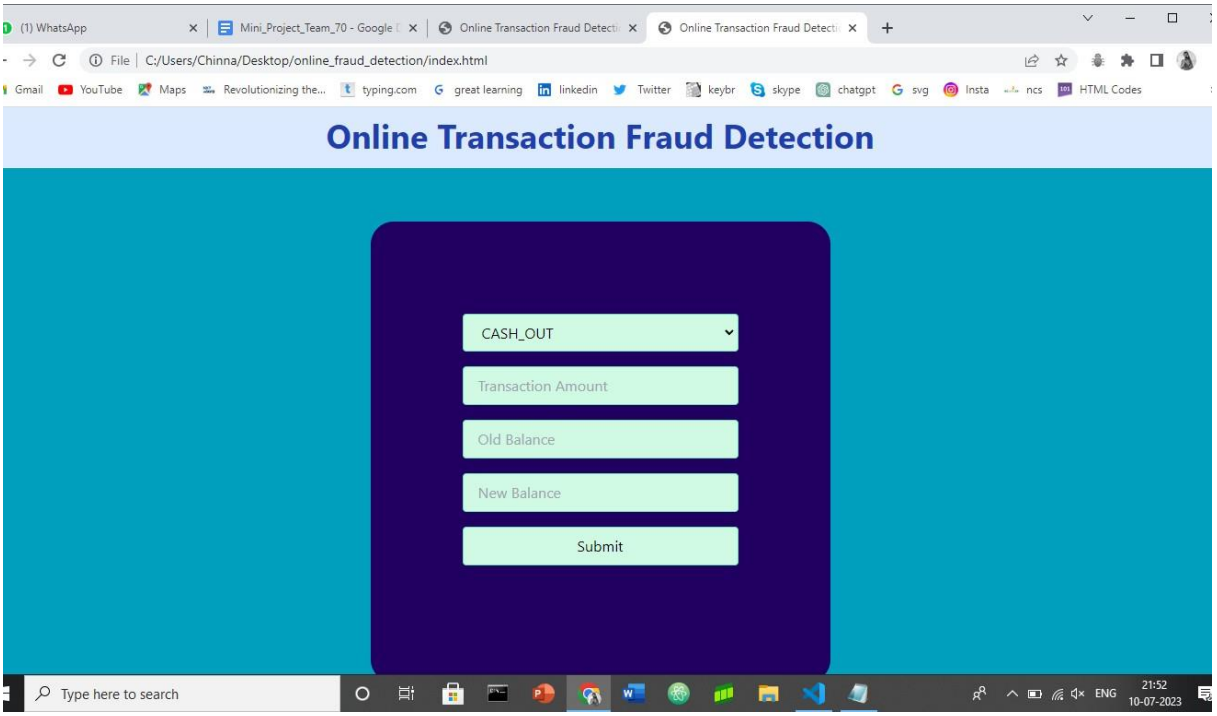

Fig 1: Online Transaction Fraud Detection UI

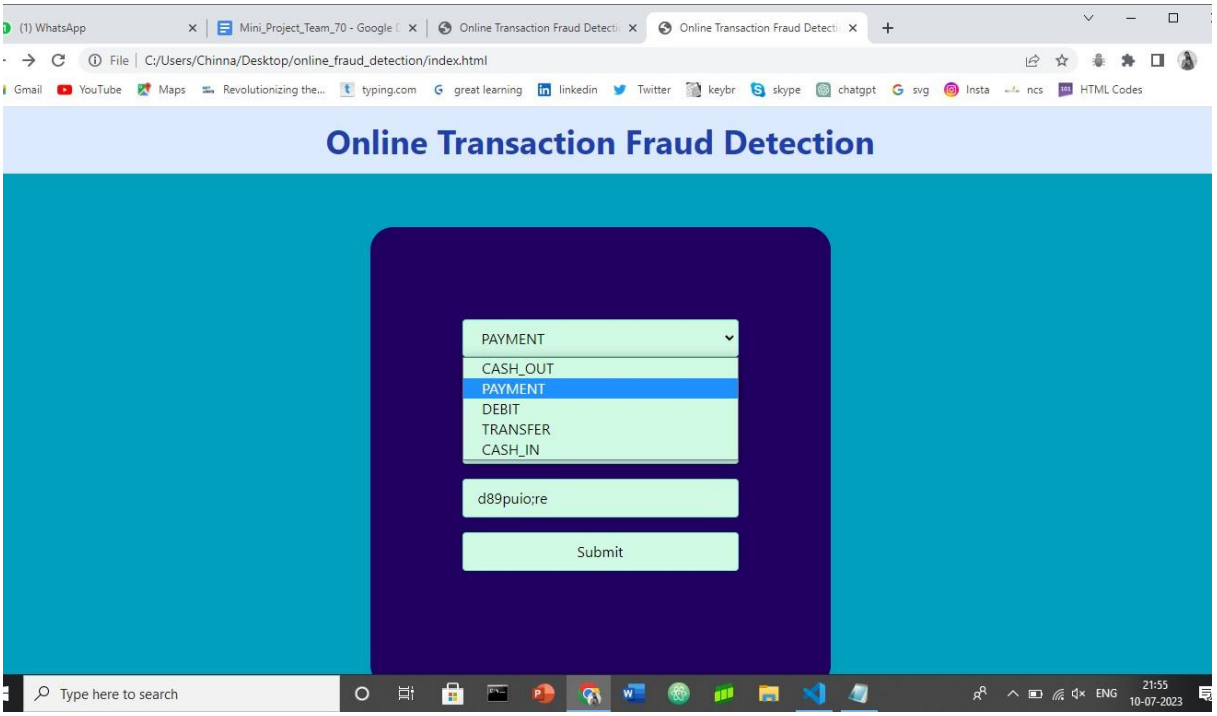

Fig 2: Payment Selection

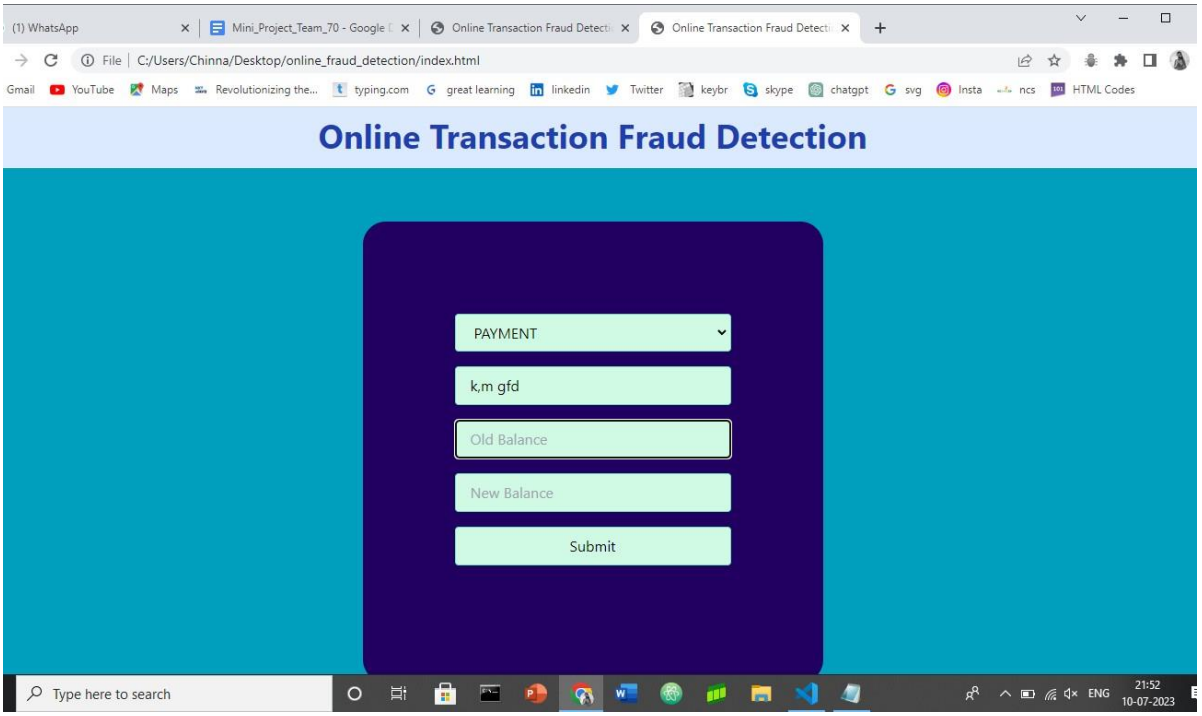

Fig 3: Entering Payment Details

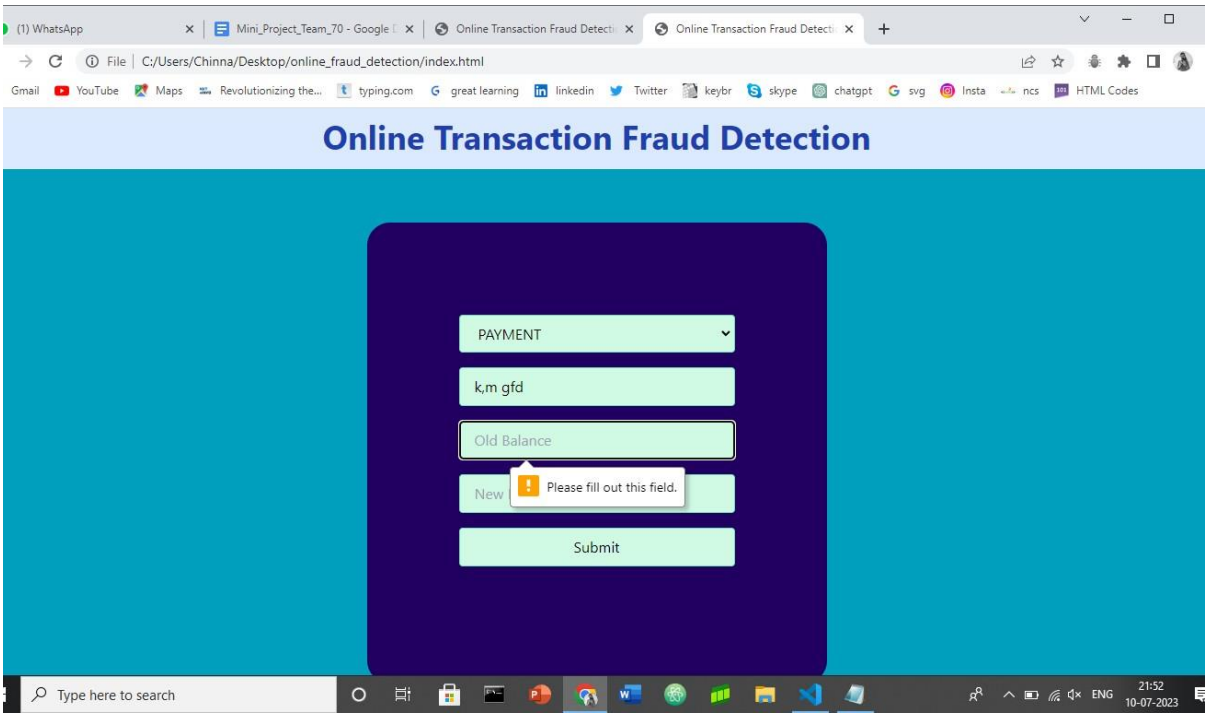

Fig 4:Running Test Cases

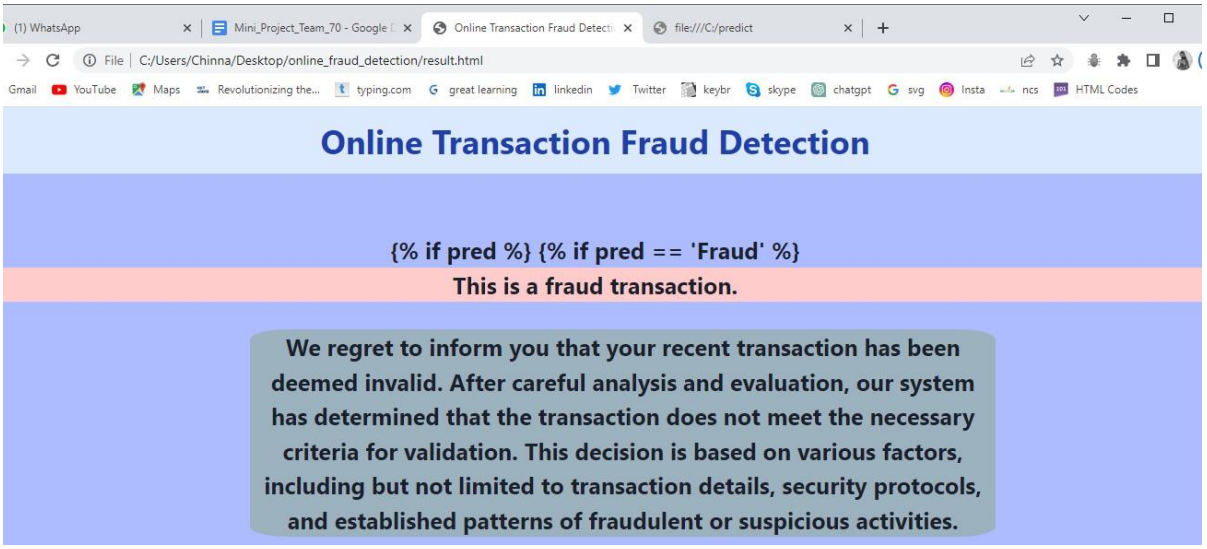

Fig 5: This is Fraud Transaction

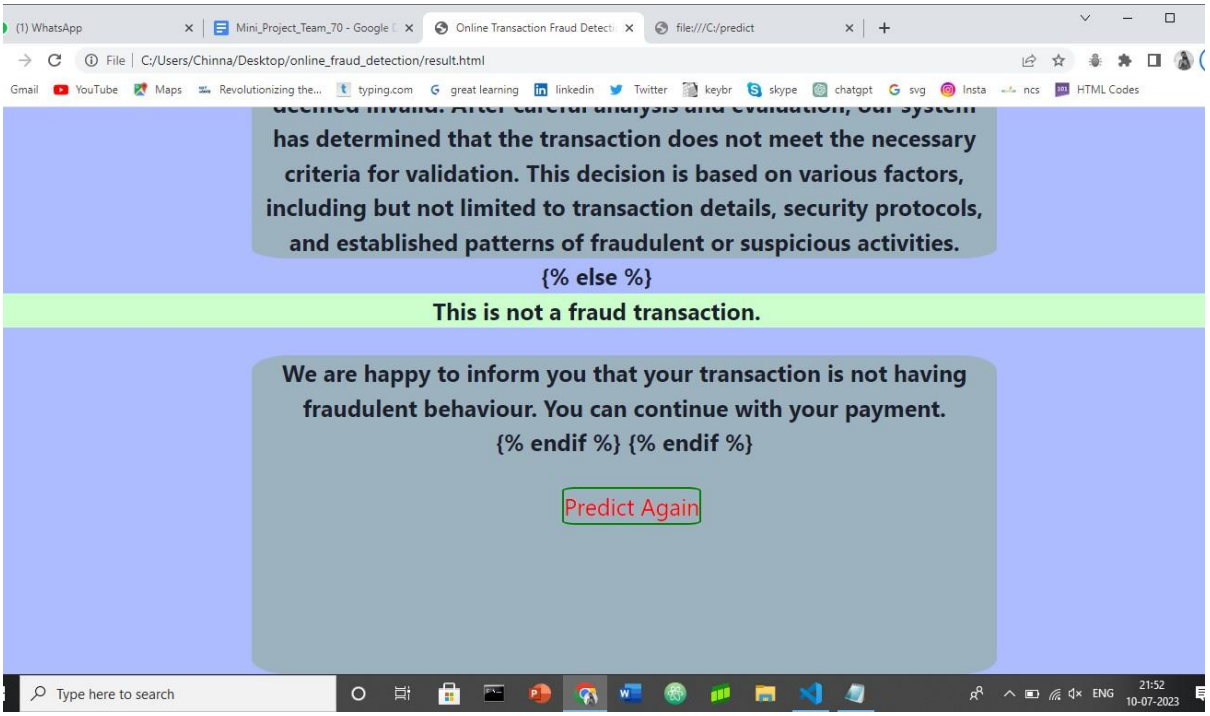

Fig 6: This is Not a Fraud Transaction

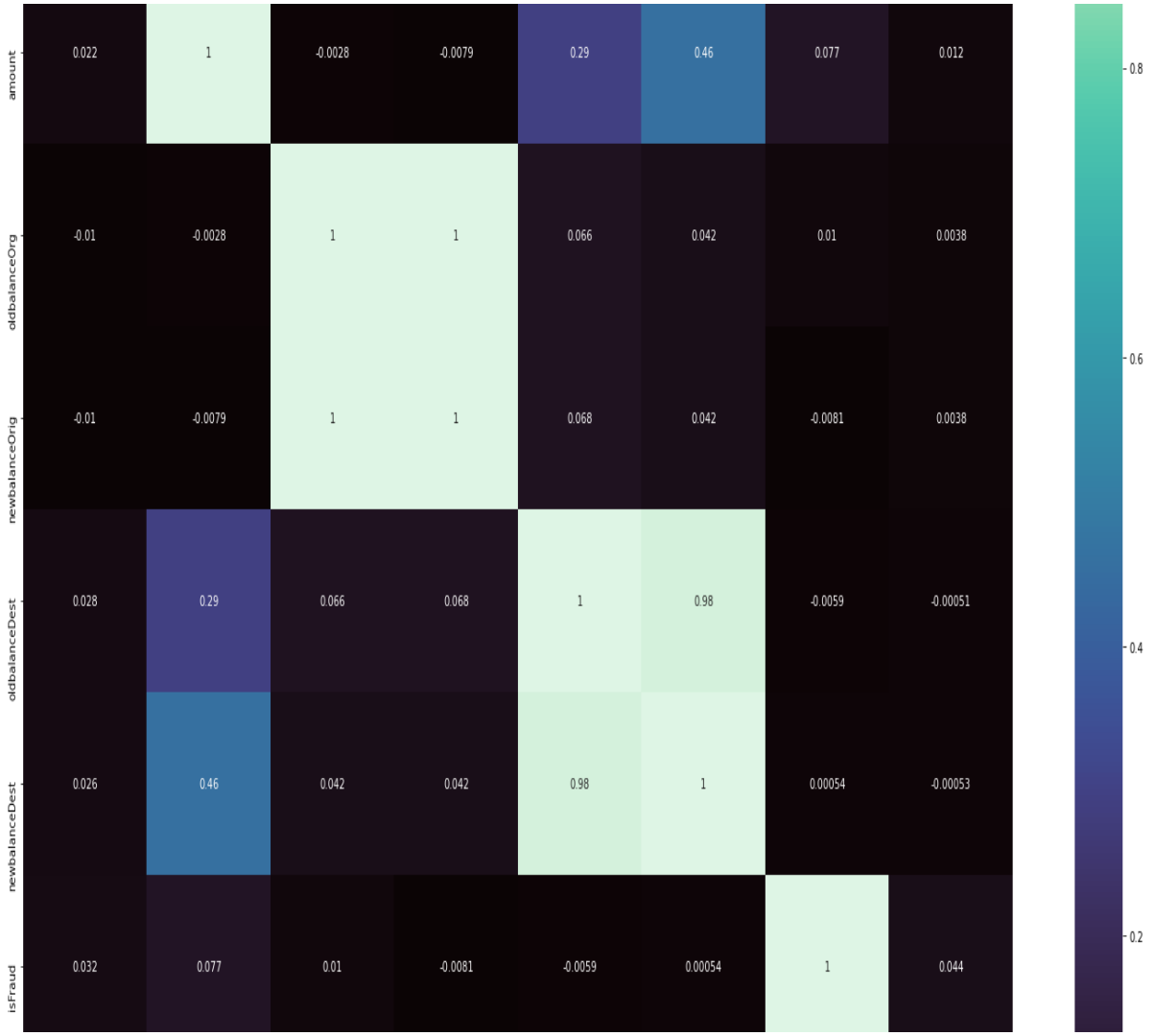

Fig 7: Prediction using Random Forest Regression

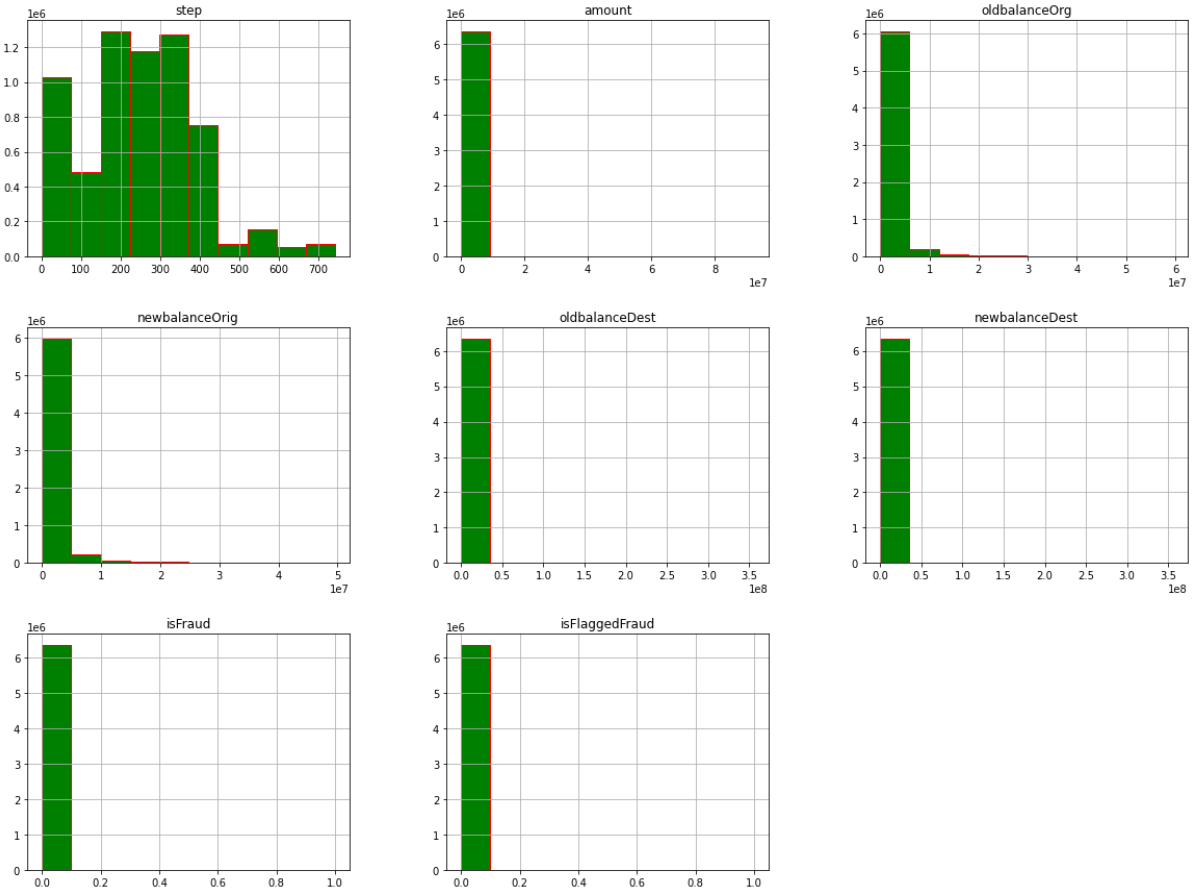

Fig 9: Prediction using Histograms

6. CONCLUSION

6.1 RESULTS

In conclusion, this project aimed to develop an online payment fraud detection system using machine learning techniques. The project successfully demonstrated the effectiveness of the developed model in detecting and preventing fraudulent transactions in real-time. By leveraging advanced algorithms and data analysis, the system showed promising results in accurately
identifying fraudulent activities, protecting users, and maintaining the integrity of online payment systems.The implementation of this fraud detection system has significant implications for various industries, including e-commerce, financial institutions, mobile payment applications, and government agencies. By integrating this system into their platforms, organizations can enhance
security measures, minimize financial losses, and foster trust among users.

6.2 FUTURE SCOPE

The future scope tries to detect fraudulent transaction before transaction succeed . In future scope , while registration we take required information which is efficient to detect fraudulent user activity .

•In proposed system, I present a Behavior and Location Analysis (BLA).
•Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder’s spending habit.
• Card transaction processing sequence by the stochastic process of a BLA.
• The details of items purchased in Individual transactions are usually not known to any Fraud Detection System (FDS) running at the bank that issues credit cards to the cardholders. Hence, I feel that BLA is an ideal choice for addressing this problem.
•Another important advantage of the BLA - based approach is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine.

• FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or not.
• The types of goods that are bought in that transaction are not known to the FDS.
• It tries to find any anomaly in the transaction based on the spending profile of the cardholder,shipping address, and billing address, etc.

• If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

• An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification.
• FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or not.
• The types of goods that are bought in that transaction are not known to the FDS.
• It tries to find any anomaly in the transaction based on the spending profile of the cardholder,shipping address, and billing address, etc.

• If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

7. REFERENCES AND CITATIONS

7.1 PAPERS REFERRED

1. Zhang, Z., Zhang, H., Guo, X., & Cheng, X. (2020). Online Payment Fraud Detection with a Novel Deep Belief Network Model. IEEE Access, 8, 151225-151236.
2. Yaseen, Z. M., & Al-Radaideh, Q. A. (2021). A Review of Machine Learning Techniques for Online Payment Fraud Detection. Computers, Materials & Continua, 68(3), 4053-4073.
3. Saleh, R. M., & Ahmed, A. M. (2019). Online Payment Fraud Detection Techniques: A Review. International Journal of Advanced Computer Science and Applications, 10(8), 312-317.
4. Al-Samarraie, H., & Al-Jumeily, D. (2021). Detecting Online Payment Fraud Using Machine Learning Approaches: A Systematic Review. Applied Sciences, 11(12), 5431.
5. Sharma, V., & Srivastava, S. (2020). A Comprehensive Survey on Online Payment Fraud Detection Techniques. International Journal of Information Technology, 12(2), 319-332.
6. Academic databases: Utilize academic databases such as IEEE Xplore, ACM Digital Library, Google Scholar, or PubMed. These platforms provide access to a wide range of research papers and publications.
7. Keywords: Use relevant keywords or phrases when searching for papers, such as "online fraud detection," "payment fraud detection," "machine learning for fraud detection," or "fraud detection techniques."
8. Citations and references: Once you find a relevant paper or article on the topic, review its citations and references section. This can lead you to additional papers that are related to online fraud detection.
9. ResearchGate and Academia.edu: Explore research community platforms like ResearchGate and Academia.edu, where researchers often share their published papers and articles.
10. Collaboration with experts: Connect with researchers, professors, or industry professionals who specialize in fraud detection or related fields. They may be able to provide you with specific papers or suggest relevant sources.

7.2 WEBSITES

These are the websites that we referred to while doing this project.

https://www.geeksforgeeks.org/

https://stackoverflow.com/

https://www.analyticsvidhya.com/

https://www.javatpoint.com/

https://scikit-learn.org/stable/

https://www.youtube.com/

https://www.mygreatlearning.com/

https://machinelearningmastery.com/