TRANSACTION GUARD

SUBMITTED BY : JITHIN T

November 7, 2024

COLLEGE OF ENGINEERING CHERTHALA

GUIDE: **Ms.ATHIRA MURALI**

OVERVIEW

- ABSTRACT
- EXISTING SYSTEM
- PROPOSED SYSTEM
- LITERATURE REVIEW
- METHODOLOGY
- SOFTWARE REQUIREMENTS
- ANALYSIS AND DESIGN
- SAMPLE CODE
- RESULT
- APPLICATIONS
- LIMITATIONS
- FUTURE SCOPE
- CONCLUSION
- REFERENCES

ABSTRACT

The Transaction Guard Project is designed to enhance fraud detection in bank payments by leveraging machine learning. This project explores the use of the Random Forest Classifier algorithm. Machine learning models are continuously retrained on new data to adapt to emerging fraud patterns.

EXISTING SYSTEM

- Device fingerprinting uniquely identifies devices based on their attributes to detect suspicious activity.
- Biometric authentication verifies a user's identity through unique biological traits, like fingerprints or facial recognition.
- Multifactor authentication enhances security by requiring users to verify their identity through multiple methods, such as a password, device, or biometric factor.

PROPOSED SYSTEM

- High system scalability ensures that a system can efficiently handle increasing workloads or expand in capacity without compromising performance.
- Real-time processing enables immediate data analysis and response, allowing systems to handle and react to events as they happen.
- Reduce false positive rates:Implement stricter validation criteria and advanced anomaly detection techniques to reduce false positive rates."

LITERATURE REVIEW

Reference	Methodologies	Pros	Cons
1.Machine Learning-Based Real-Time Fraud Detection in Financial Transactions published in (2020), Author: J.Smith , A. Johnson.	Supervised Learning Models , Unsupervised Anomaly Detection	Real-Time Detection, Adaptability	Data imbalance, High computational costs, False positives
2.Financial Fraud Detection Based on MachineLearning Authors:Abdulalem Ali,Shukor Abd Razak,ORCID,Siti Hajar Othman 1ORCID,Arafat Al-Dhaqm(2022)	Analysis of Techniques and Metrics,Identification of Gaps and Future Research Directions	Improved Accuracy, Adaptability, Automation,	Data Dependency, complexity, overfitting,

LITERATURE REVIEW

Reference	Methodologies	Pros	Cons
3.European Centre for Research Training and Development.Author:European Centre for Research Training and Development published(2023)	supervised learning,unsupervised learning,deeplearning	Increased Detection Rates, Data-Driven Decision Making,	Dependence on Quality Data, Maintenance and Retraining Costs
4.Machine Learning Algorithms for Real-Time Fraud, Author:Khaire, Waghmare Detection in Digital Payments. published (2024)	Data Preprocessing,Feature Engineering	Real-Time Processing, Reduced False Positives	Data Quality Requirements, High Initial Investment

LITERATURE REVIEW

Reference	Methodologies	Pros	Cons
5.Fraud Detection using Machine Learning and Deep Learning, author:Pradheepan Raghavan,Gayar,(2024)	Feature Engineering,Model Evaluation	Real-time Detection,accuracy	False Positives,Data Dependency

METHODOLOGY

1. **Random forest classifier(Algorithm):**Random Forest Classifier for fraud detection in financial transactions is a popular approach, as it handles large datasets well and can capture complex patterns indicative of fraudulent behavior.
    - Bagging
    - Feature Selection for Splitting
    - Grow Decision Trees
    - Aggregate Predictions

SOFTWARE REQUIREMENTS

- **Programming languages:**Python 3.x(for backend)and Html,css(for frontend functionality)
- **Library Needed :**
    - Numpy
    - Pandas
    - Scikit-learn
- **Framework:**Django(web framework for backend)

ANALYSIS AND DESIGN

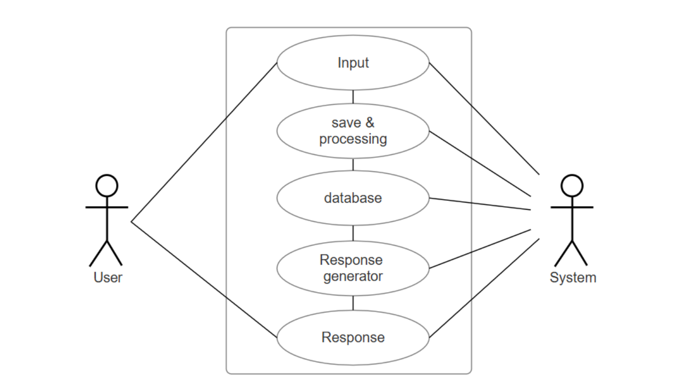

Figure: Usecase Diagram

ANALYSIS AND DESIGN

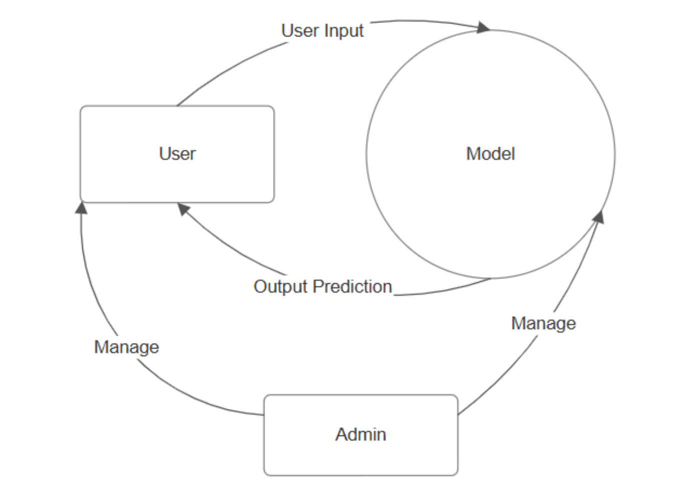

Figure: DFD Level 0

ANALYSIS AND DESIGN

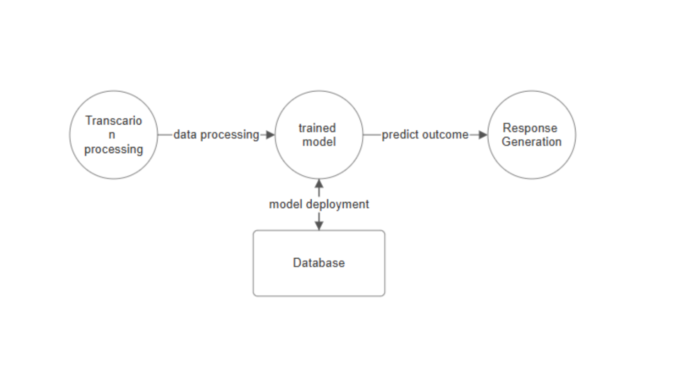

Figure: DFD Level 1

SAMPLE CODE

```html
<body class="index-page">

  <header id="header" class="header d-flex align-items-center fixed-top">
    <div class="container-fluid container-xl position-relative d-flex align-items-center">

      <a href="index.html" class="logo d-flex align-items-center me-auto">
        <!-- Uncomment the line below if you also wish to use an image logo -->
        <!-- <img src="{%static '/assets/img/logo.png'%}" alt=""> -->
        <h1 class="sitename">TRAN$ACTIONGUARD</h1>
      </a>

      <nav id="navmenu" class="navmenu">
        <ul>
          <li><a href="/" class="active">HOME</a></li>
          <li><a href="#about">ABOUT</a></li>
          <li><a href="/adm_usr_login">SIGN IN</a></li>
          <li><a href="/thrreg">SIGNUP</a></li>
```

Figure: Frontend

SAMPLE CODE

```python
        new_transaction = pd.DataFrame({
            'Amount': [amount],
            'Transaction Date': [transaction_date],
            'Transaction Type': [transaction_type_encoded]
        })

        prediction = model.predict(new_transaction)[0]
        result = "Fraud" if prediction == 1 else "Genuine"

        Transaction.objects.create(
            transaction_id=f"T{random.randint(100000, 999999)}",
            account_number=account_no,
            ifsc_code=ifsc_code,
            amount=amount,
            transaction_date=datetime.fromtimestamp(transaction_date),
            transaction_type=transaction_type,
            fraud_label=prediction
        )

        return render(request, 'result.html', {'result': result})

    return render(request, 'predict.html')


def index_page(request):
    return render(request, 'index1.html')
```

Figure: Backend

SAMPLE CODE

```python
def load_data(num_records=1000):
    data = []
    for _ in range(num_records):
        account_no = f"ACC{random.randint(10000000, 99999999)}"
        ifsc_code = f"IFSC{random.randint(100000, 999999)}"
        amount = round(random.uniform(10, 10000), 2)
        transaction_date = datetime.now() - timedelta(days=random.randint(0, 30))
        transaction_type = random.choice(['credit', 'debit'])
        is_fraud = random.choices([0, 1], weights=[0.5, 0.5])[0]

        data.append({
            'Transaction ID': f"T{random.randint(100000, 999999)}",
            'Account Number': account_no,
            'IFSC Code': ifsc_code,
            'Amount': amount,
            'Transaction Date': transaction_date,
            'Transaction Type': transaction_type,
            'Fraud Label': is_fraud
        })

    return pd.DataFrame(data)


def train_model():
    df = load_data()
    df['Transaction Date'] = pd.to_datetime(df['Transaction Date']).astype('int64') / 10**9
    label_encoder = LabelEncoder()
    df['Transaction Type'] = label_encoder.fit_transform(df['Transaction Type'])

    X = df.drop(['Transaction ID', 'Account Number', 'IFSC Code', 'Fraud Label'], axis=1)
    y = df['Fraud Label']
```

Figure: Training Model

SAMPLE CODE

```python
class login(models.Model):
    login_id=models.AutoField(primary_key=True)
    username=models.CharField(max_length=200)
    password=models.CharField(max_length=200)
    usertype=models.CharField(max_length=200)

class register(models.Model):
    user_id=models.AutoField(primary_key=True)
    firstname=models.CharField(max_length=200)
    lastname=models.CharField(max_length=200)
    # place=models.CharField(max_length=200)
    phone=models.CharField(max_length=200)
    email=models.CharField(max_length=200)
    loginss=models.ForeignKey(login,on_delete=models.CASCADE)


class Transaction(models.Model):
    transaction_id = models.CharField(max_length=20, unique=True)
    account_number = models.CharField(max_length=12)
    ifsc_code = models.CharField(max_length=12)
    amount = models.FloatField()
    transaction_date = models.DateTimeField()
    transaction_type = models.CharField(max_length=6)  # Either 'credit' or 'debit'
    fraud_label = models.IntegerField()  # 0 for genuine, 1 for fraud
```

Figure: Models(database)

RESULT

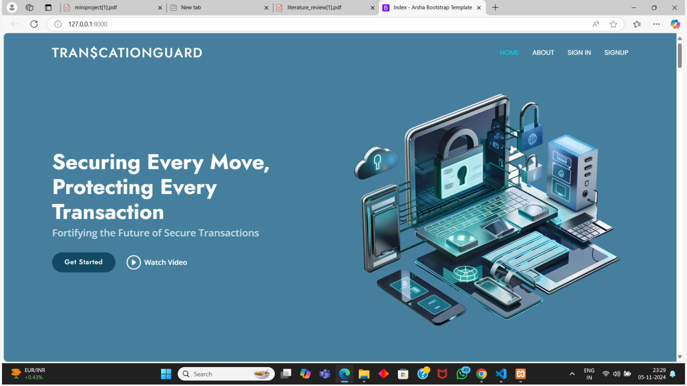

Figure: User Interface

RESULT

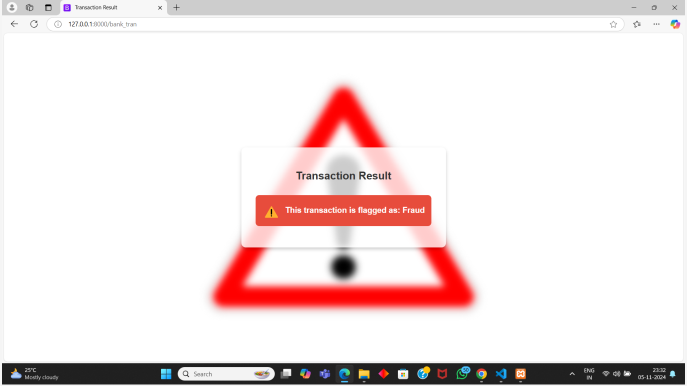

Figure: OUTPUT-FRAUD

RESULT

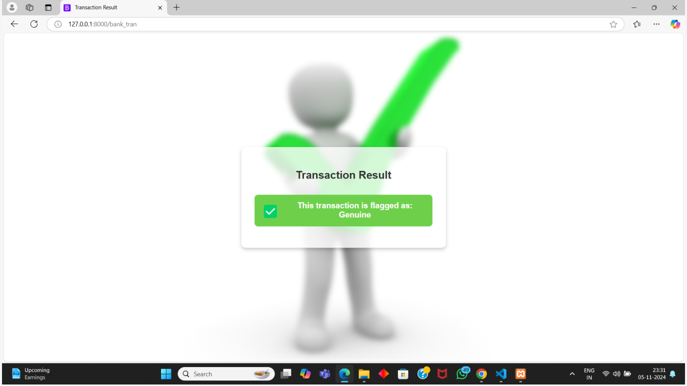

Figure: OUTPUT-GENUINE

APPLICATIONS

- **Transaction Risk Scoring:** Assign a risk score to each transaction based on features such as transaction amount, frequency, location, device, and user behavior.
- **Behavioral Profiling:**Track and update customer behavior profiles to detect any shifts that may indicate fraud.
- **Chargeback Reduction:** Predict and prevent potential chargeback fraud by identifying high-risk transactions,

LIMITATIONS

- **Data Quality and Availability:**Fraud detection relies on accurate, detailed transaction data.incorrect data can negatively impact model performance.
- **Evolving Fraud Patterns:** Fraudsters constantly adapt to new detection methods, which can make models trained on historical data less effective over time.
- **Data Privacy Concerns:** Fraud detection models need access to sensitive personal and transaction data, which must be managed carefully to comply with privacy regulations.

FUTURE SCOPE

- **Model Collaboration with Financial Institutions:**Collaborating with banks and financial institutions to share data on fraudulent activities can improve the training datasets and enhance detection capabilities.
- **Advanced Machine Learning Techniques:**Implementing deep learning algorithms, such as neural networks, can enhance the accuracy of fraud detection by capturing complex patterns in large datasets.
- **Enhanced User Authentication:** Integrating behavioral biometrics, such as analyzing user interaction patterns (e.g., typing speed, mouse movements), can provide an additional layer of security.

CONCLUSION

The Transaction Guard project represents a significant advancement in the fight against fraud in banking transactions through the application of machine learning techniques. By leveraging real-time data analysis, anomaly detection, and user behavior insights, this system enhances security and minimizes the risk of fraudulent activities. Its potential for integration with big data technologies, advanced user authentication methods, and continuous learning capabilities positions it as a vital tool for financial institutions.

REFERENCES

- A Survey of Machine Learning Techniques for Fraud Detection,Khaire, P., Waghmare, L. (2020). International Journal of Engineering and Computer Science, 6(1), 20372-20377.
- Fraud Detection in Financial Transactions Using Machine Learning Techniques,P. A., H. R. (2022). International Journal of Computer Applications, 182(23), 13-20.
- Fraud Detection in Banking and Financial Services using Machine Learning,H. A., A. S. (2023). Journal of Theoretical and Applied Information Technology, 98(18), 3683-3705.
- Financial Fraud Detection Based on Machine Learning Authors: Abdulalem Ali,Shukor Abd Razak,ORCID,Siti Hajar Othman,published in 2024
- Fraud Detection using Machine Learning and Deep Learning ,au- thor:Pradheepan Ragha- van,NeamatGayar, published(2024)