ONLINE PAYMENTS FRAUD DETECTION USING WITH MACHINE LEARNING:

To build an application that can detect the legitimacy of the transaction in real-time and increase the security to prevent fraud.

By

(Marri yashmitha)

(Manthina raja rishika)

(Kutagulla safa)

Guided by

Prof. Ms swetha raj

A Dissertation Submitted to
SRI VENKATESWARA COLLEGE OF ENGINEERING AND TECHNOLOGY, An Autonomous Institution affiliated to 'JNTU Ananthapur' in Partial Fulfilment of the Bachelor of Technology branch of ***Computer science and Engineering***

May 2024

SRI VENKATESWARA COLLEGE OF ENGINEERING AND TECHNOLOGY

R.V.S. Nagar Tirupathi Road, Andhra Pradesh– 517127

Model selection for online fraud detection:

Machine learning models can be deployed in a variety of ways, depending on the infrastructure and needs:

• On-Premises Deployment: Setting up the models on the organization's own local servers or infrastructure.

• Cloud Deployment: Hosting the models on cloud infrastructure like AWS, Azure, or Google Cloud.

• Containerization: Packing the models into containers for scalability and simple deployment (like Docker).

• Serverless Deployment: This method involves deploying the models as functions using serverless platforms (such as AWS Lambda and Google Cloud Functions).

API Development :

To expose the deployed models, a microservice or an API endpoint was created. This made it possible for other programs or systems to communicate with fraud detection models and make predictions. Transaction data are accepted as input by the API, which should then output estimated fraud probability or binary labels

Scalability and effectiveness:

The solution was developed to allow increasing transaction volumes in real-time. To increase performance and scalability, strategies like load balancing, caching, and parallel processing are suggested.

Monitoring and logging systems :

Implementing monitoring and logging systems to keep tabs on the operation and behaviour of the deployed models. This entailed logging all input

information, forecasts, and runtime faults or exceptions. Continuous improvement is made possible via monitoring, which helps find any drift in model performance over time.

Security Consideration:

Applying the proper security precautions to safeguard the deployed models and the data they analyse. Access controls, encryption of sensitive data, and frequent security audits may all be necessary for this.

Versioning and Updates :

Versioning mechanism for the deployed models was created to keep track of changes and simplify future updates. To adapt to changing fraud tendencies, automated pipelines are suggested for model updates and retraining.

A/B Testing and Evaluation:

A/B testing were performed to compare the performance of the deployed models against a baseline or alternative approaches. Continuous evaluation of the effectiveness of the deployed models using relevant metrics including precision, recall, and F1-score.

Continuous Improvement:

Feedback loops were incorporated to collect labelled data on detected fraud cases and use it to improve the models. This iterative process helps enhanced the accuracy and effectiveness of the fraud detection system over time