Online Payment Fraud Detection

Developing an Online Payment Fraud Detection Model

This project will be focused on making an Online Payment Fraud Detection Model to overcome the increasing rate of online frauds.

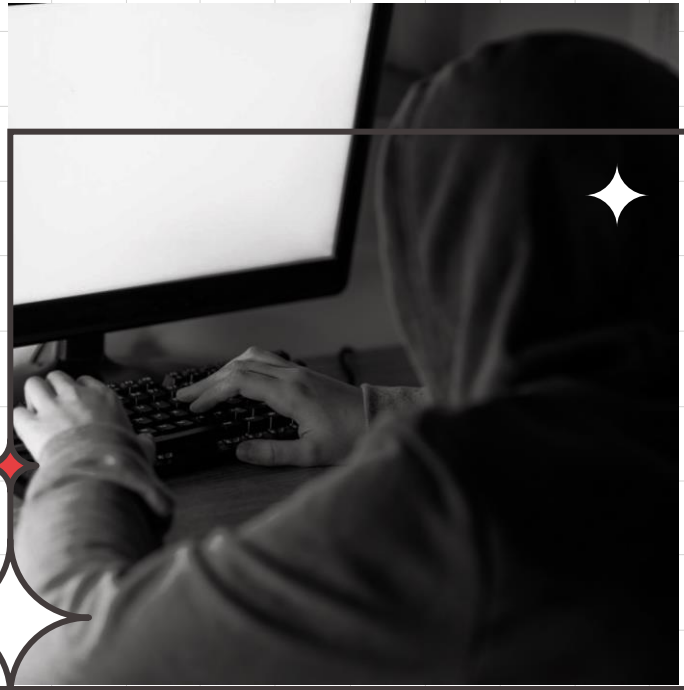
Project Guide: Prof. S.R.Kasture
(H.O.D. Artificial Intelligence & Machine Learning)
Project Cordinator: Mr. Aman Gupta

Industry: Customer Service
Presenter: Aditya Jha
Enrollment No: FS23AI005
Year: 1st Year

Centre for Artificial Intelligence and Machine Learning

What are Online Payment Frauds?

- Phishing scams steal personal and financial data.
- Hackers exploit system vulnerabilities.
- Malware secretly gathers sensitive information.
- Fraudsters misuse stolen data for unauthorized transactions.
- Stolen information can lead to identity theft.
- Results in losses for consumers, merchants, and banks.
- Stay informed on cybercrime trends and latest threats.



Example of an Online Scam

Some key things to know about online payment fraud:

Here's the lowdown:

- **Criminals use sneaky tricks:** Phishing, hacking, malware – they'll try it all to steal your credit card details, passwords, and more.
- **Your info, their playground:** Online stores, apps, e-wallets, even your bank account – nowhere is safe.
- **They pretend to be you:** Fake emails, websites, even your friends – they'll trick you into giving them your info.
- **What they want:** Your money, your identity, anything valuable they can get.
- **Who loses?** You, the merchants, the banks – everyone's at risk.

Stay vigilant! Protect yourself from online payment fraud.

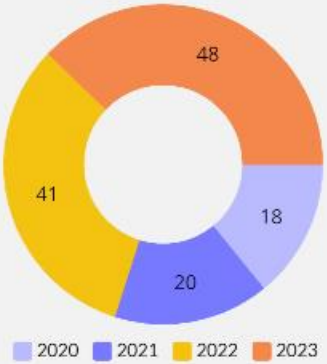
Digital scam worldwide

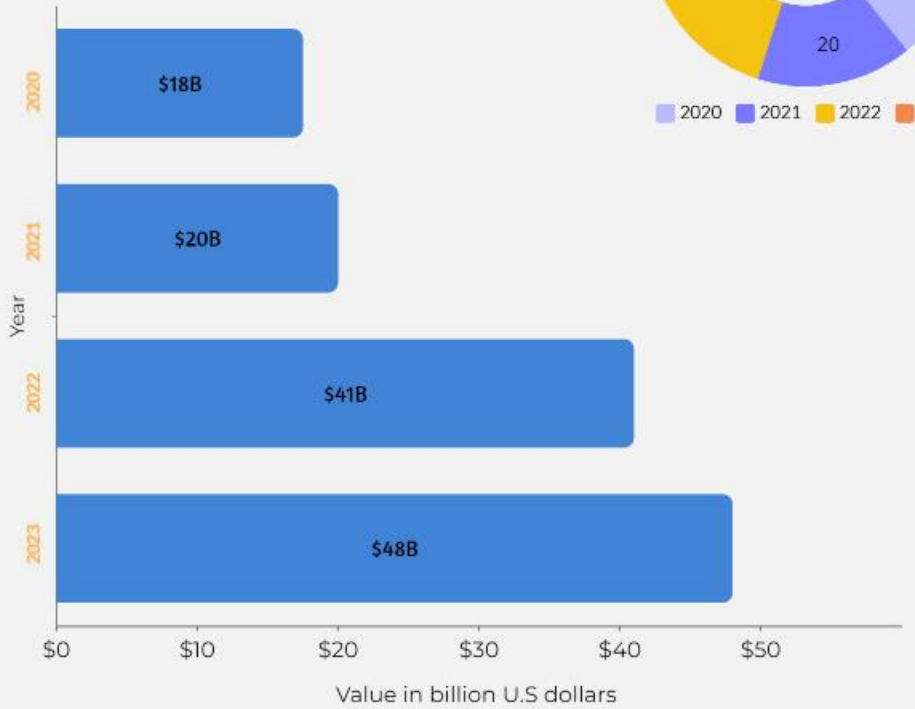
The rate of scams and frauds worldwide has been increasing on a worrisome rate and we have to take measures to prevent them from happening and secure our digital banks.

Increase in Online Payment Fraud Rate

AN BRIEF OVERVIEW ON THE INCREASE IN THE ONLINE PAYMENT FRAUD RATE IN THE CURRENT YEARS

Graphical Data



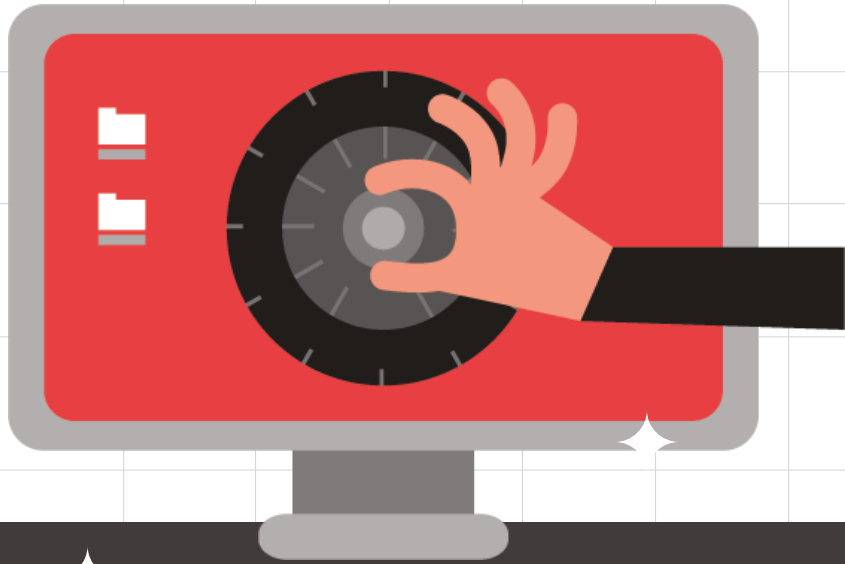


Source- https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/

How do we tackle this problem?

In order to be safe from getting ourselves scammed with such tricks, I will be making this Online Payment Fraud Detection Model. Which would help us detect the fraud callers and we can take strict measures against this crime in our defense.

This would keep us safe from such scammers.



What will the model do?

- Analyze transactional data to identify suspicious activity patterns
- Assign risk scores to transactions using algorithms
- Detect outlier transactions with machine learning
- Use rules to check for known fraud markers
- Generate alerts for risky transactions
- Provide recommended actions for flagged transactions
- Produce reports on fraud rates, detection & prevention

Market Analysis

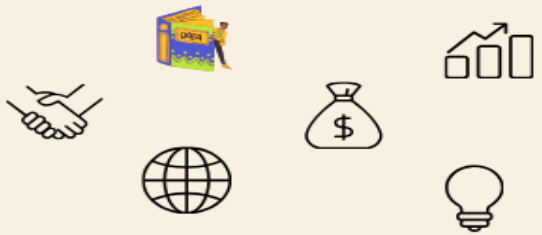
60-80%

Studies say that the demand for such online fraud detections models have increased a lot recently and is about 60-80% worldwide.

100M+

Over 100M+ individuals have shown interest in this model. Over 1 million business merchants in US have been looking for developers and even numerous companies worldwide have been hiring many such developers.

https://www.persistencemarketresearch.com/market-research/online-payment-fraud-detection-market.asp



The Formula for Fraud Detection

Data Collection

- Obtain labeled transaction data including key attributes like customer, transaction, merchant info, timestamps etc.

Model Development

- Build models using techniques like logistic regression, random forests, neural networks trained on labeled data to predict fraud risk.

Model Deployment

- Integrate top performing model into live systems to score transactions in real-time and flag high risk ones.

Additionally:

- Ensure security, privacy, compliance and continuous updates to the model.

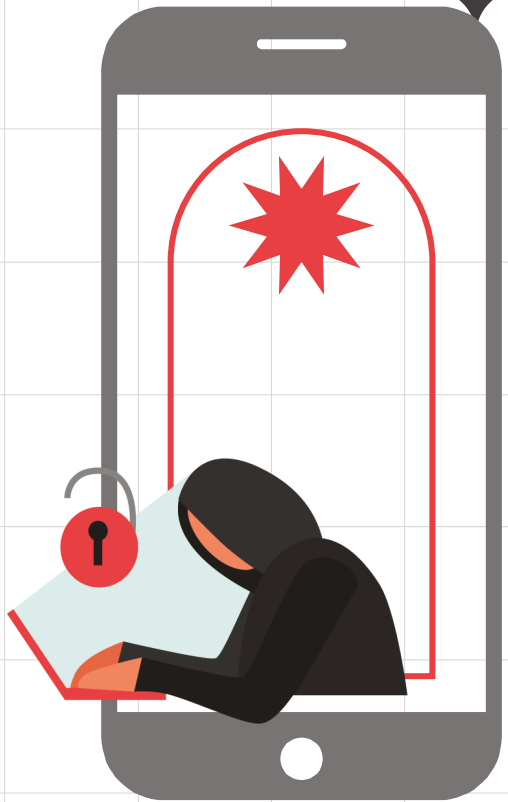
- Focus on accuracy, transparency, and usability for operational success.

project.py

```python
import streamlit as st
from PIL import Image
import pytesseract

# Set the path to the Tesseract OCR executable
pytesseract.pytesseract.tesseract_cmd = r'C:\Users\Aditya\PycharmProjects\pythonProject2\Tesseract\tesseract.exe'  # Replace with the correct path for your system

# Function to read text from an image
1 usage
def read_text_from_image(image):
    text = pytesseract.image_to_string(image)
    return text

def main():
    st.title("Fraudulent Text Detector")

    # Upload image
    uploaded_file = st.file_uploader("Choose an image", type=["jpg", "png", "jpeg"])

    if uploaded_file is not None:
        image = Image.open(uploaded_file)
        st.image(image, caption='Image Uploaded', use_column_width=True)

        # Read text from the image
        text = read_text_from_image(image)

        # Display the extracted text
        st.subheader("Text Extracted From Image:- ")
        st.write(text)

if __name__ == "__main__":
    main()
```

How will I train the Machine Learning Model

1. Curate labeled transactional data and preprocess for modeling.
2. Stratically split data to ensure model integrity during training, validation and testing.
3. Handcraft relevant features and trial superior algorithms like logistic regression and random forest.
4. Tune hyperparameters to optimize model performance and prevent overfitting.
5. Continual retraining on new data for sustained accuracy over time.



Algorithms in use

NLP

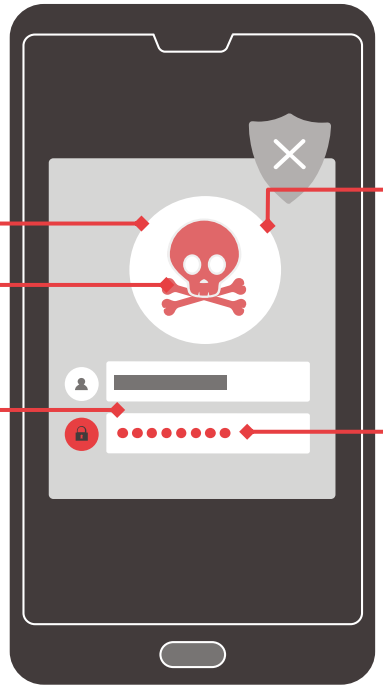
Fraudulent Text Recognition

Logistic Regression

Fast binary classification algorithm providing fraud probability predictions.

Random Forest

Ensemble technique using many decision trees to model fraud's non-linear patterns.



XGBoost

Boosted tree algorithm regularizing models to prevent overfitting on imbalanced classes.

Neural Networks (like FFN)

Multilayer algorithm learning complex feature representations needed to uncover fraud.

Alternate Algorithms like:

SVM,
KNN,
Naive Bayes

could also be used for deeper implementation.

Stay Safe From Such Threats

Thanks!

Do you have any questions?

adityajhagpm1819@gmail.com

Thankyou for giving your time to my presentation.
Hope you liked it!!