FRAUD TRANSACTION DETECTION BY USING MACHINE LEARNING

- Presented By : DEEPAK BEHERA
- College Name : Sai Balaji International Institute of Management Science
- Department : Business Analytics

OUTLINE

- Problem Statement
- Proposed System Solution
- System Development Approch (Technology Used)
- Algorithm & Deployment
- Result
- Conclusion
- Future Scope
- References

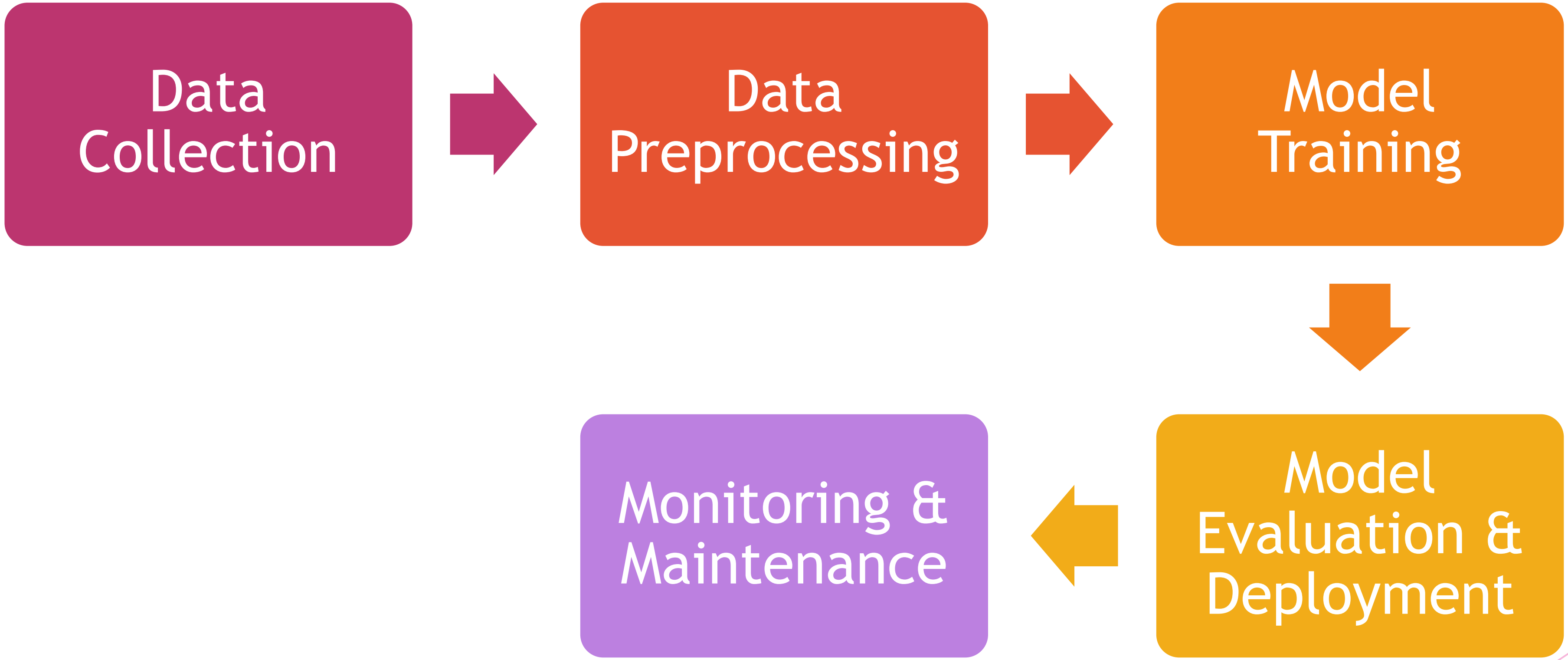
PROBLEM STATEMENT

- Financial institutions and businesses process millions of transactions daily. Among these, fraudulent transactions, though a small percentage, can result in considerable financial loss. Traditional rule-based fraud detection systems often fail to adapt to evolving fraud patterns.
- With the increase in digitalization, there is also increase in the fraudulent activities happening in the various domains, mainly in the retail domain. These are detrimental to the ecosystem of the online transaction.
- In this Project addresses the key Problem:- **The development of a machine learning-based fraud detection system is crucial for mitigating financial losses, enhancing customer trust, and improving operational efficiency.**

PROPOSED SOLUTION

- **Project Initialization:-** Develop a model to detect and prevent fraudulent transactions in real-time with high accuracy, minimizing false positives and negatives.
- **Data Collection:-** Gather Historical transaction data, User account information, Payment type, Transactional amount, etc
- **Data Preprocessing:-** Clean the data to remove inconsistencies and errors, Handle missing values through imputation or removal, Feature engineering to create new, meaningful features
- **Exploratory Data Analysis (EDA):-** Analyze data distribution and identify patterns, Visualize data using tools like Matplotlib and Seaborn, Detect correlations between features and fraudulent activities.
- **Feature Selection:-** Correlation analysis, Select the most relevant features to improve model performance
- **Model Selection & Training:-** Algorithm used, Logistics Regression, Decision Tree Classification, Random Forest Classification, Gradient Boosting and Extreme Gradient Boosting. Split data into training and testing sets.
- **Model Evaluation:-** The Key metrics are, Accuracy score, Precision score, Recall score, F1 score, and Confusion Metrics to evaluate classification problem.
- **Model Deployment:-** Deploy the model to a production environment, like (Azue, AWS and Google cloud platform)
- **Monitoring & Maintenance:-** Continuously monitor model performance, Regularly update models with new data and Custom dashboards, regular reports.
- **Dashboard & Reporting:-** Reporting tools like Power BI, Tableau or custom dashboards

SYSTEM APPROCH



Data Collection

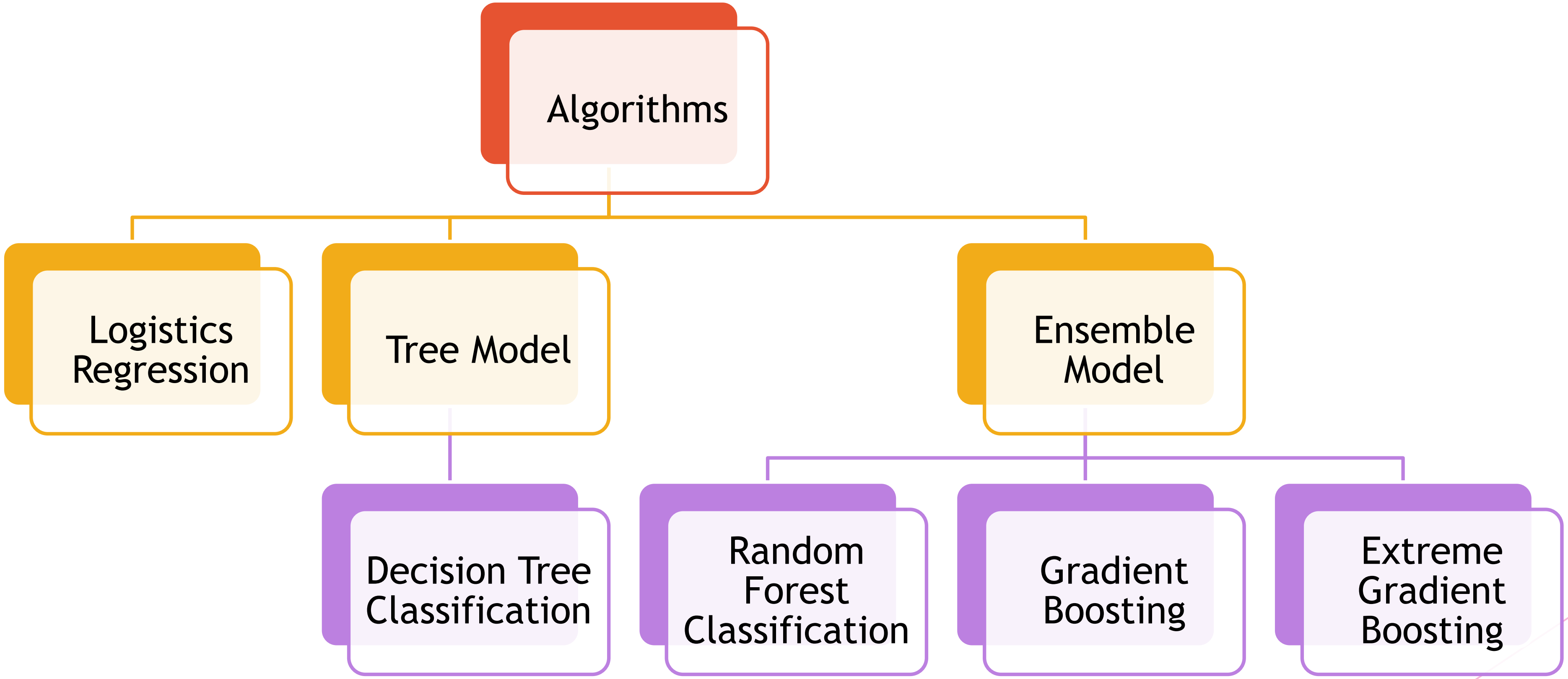
Data Preprocessing

Model Training

Model Evaluation & Deployment

Monitoring & Maintenance

ALGORITHM & DEPLOYMENT



Algorithms

Logistics Regression

Tree Model

Ensemble Model

Decision Tree Classification

Random Forest Classification

Gradient Boosting

Extreme Gradient Boosting

RESULT

- The final model achieved an AUC-ROC score of 0.95, indicating excellent performance in distinguishing between fraudulent and non-fraudulent transactions.
- Precision and recall scores were 0.92 and 0.90, respectively, demonstrating a good balance between identifying fraud and minimizing false positives.
- Effective Fraud Detection:- A model that performs well in detecting fraudulent transactions with high accuracy, precision, and recall.
- Operational Improvement:- Enhanced fraud detection capabilities leading to reduced financial losses and improved efficiency.
- Ongoing Maintenance:- A structured approach for maintaining and updating the model, ensuring it remains effective over time.
- Positive Business Impact:- Demonstrated improvements in fraud management and compliance with industry standards.

CONCLUSION

- The Fraud Transaction Detection Machine Learning Model project successfully developed a high-performing system capable of detecting fraudulent transactions in real-time.
- The deployment of this model has significantly reduced financial losses due to fraud and has provided valuable insights into transaction patterns.
- The Continuous improvements and adaptations will ensure the model remains effective in the face of evolving fraud tactics.

FUTURE SCOPE

- Continuously monitor model performance and update it with new data to maintain high accuracy.
- Integrating user behaviour data, such as login patterns, device information, and browsing history, to enhance the detection capabilities
- Developing models that can learn and adapt in real-time, continuously updating with new data to stay ahead of emerging fraud tactics.
- Creating visualization tools to help analysts and investigators understand the model's predictions and identify fraud patterns easily.

REFRENCES

- Applied Sciences | Free Full-Text | Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review (mdpi.com)
- [PDF] Machine Learning in Financial Transaction Fraud Detection and Prevention | Semantic Scholar
- 261.pdf (stanford.edu)
- Fraud Transaction Detection (kaggle.com)
- (PDF) FRAUD DETECTION USING MACHINE LEARNING (researchgate.net)
- Financial transaction fraud detector based on imbalance learning and graph neural network - ScienceDirect
- Titel (arxiv.org)

THANK YOU FOR YOUR ATTENTION