iNeuron

PHISHING DOMAIN DETECTION

(Machine Learning)

Architecture Document

Project Members:

1. Adarsh Maurya
2. Akash Kumar
3. Sachin Sharma
4. Priya Singh

iNeuron.ai

July 2023

What is Architecture?

An architecture document in project is a technical document that describes the overall design of the project. It includes information about the project's components, their interactions, and the technologies that will be used. The architecture document is used to communicate the project's design to stakeholders, and to ensure that everyone is on the same page.

INTRODUCTION:

Phishing Domain Detection is a method that utilizes sophisticated algorithms and machine learning models to ascertain the authenticity of a domain, enabling accurate prediction of whether the domain is real or fake.

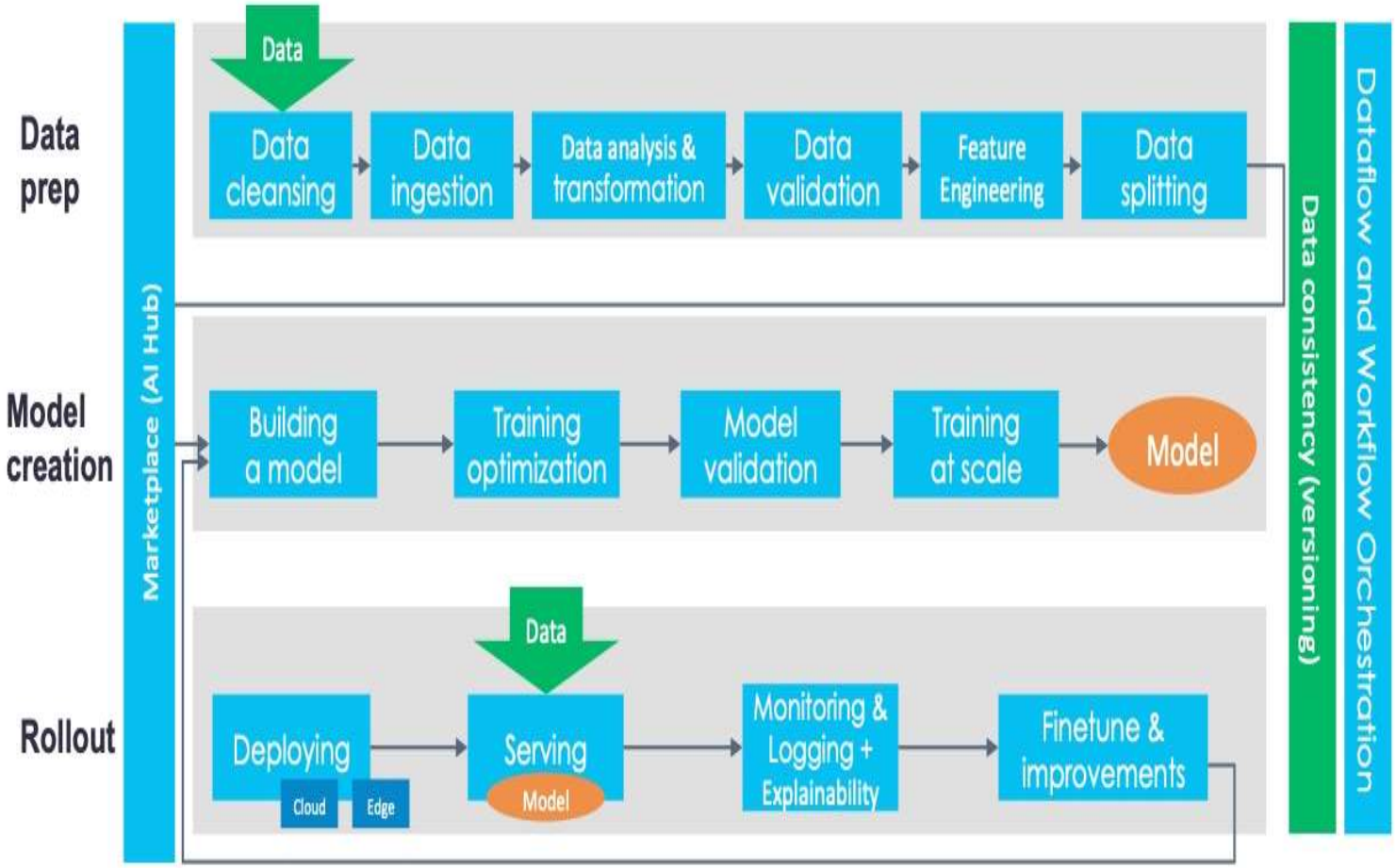
PROBLEM STATEMENT:

Phishing is a fraudulent technique where attackers mimic trusted entities or individuals to deceive unsuspecting targets into divulging sensitive information, typically through email or other communication channels. Attackers prefer phishing due to its effectiveness in convincing individuals to click on seemingly genuine links, circumventing the security measures implemented on their devices.
The main goal is to predict whether the domains are real or malicious.

APPROACH:

- The project involved classical machine learning tasks: Data Exploration, Data Cleaning, Feature Engineering, Model Building, and Model Testing.
- Different machine learning algorithms such as Logistic Regression, SVM, Gradient Boosting, Adaboost, and Random Forest classifier were applied.

- The best-fit model for the project was identified as Random Forest classifier after evaluating the performance of all the tested algorithms.



Data Preprocessing to Deployment Flow Diagram

DATASET:

The dataset comprises both legitimate and phishing website instances, with each website represented by a set of features indicating its legitimacy. This dataset can be utilized as input for machine learning procedures, enabling the development of models to classify websites as

legitimate or phishing based on their feature patterns.

The dataset had two variants of the Phishing Dataset are presented

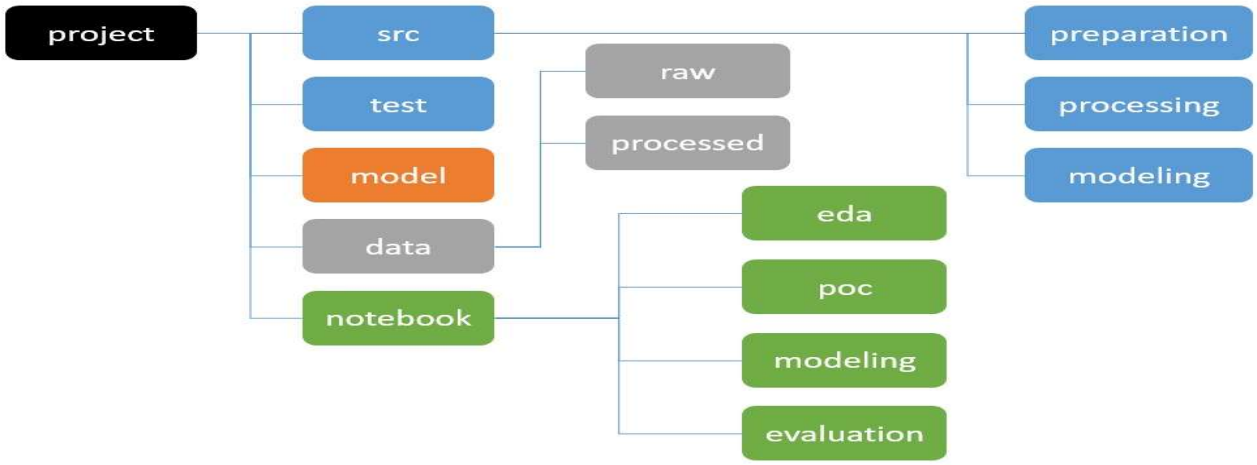
Full variant - dataset_full.csv

- Short description of the full variant dataset:
- Total number of instances: 88,647
- Number of legitimate website instances (labeled as 0): 58,000
- Number of phishing website instances (labeled as 1): 30,647
- Total number of features: 111

Small variant - dataset_small.csv

- Short description of the small variant dataset:
- Total number of instances: 58,645
- Number of legitimate website instances (labeled as 0): 27,998
- Number of phishing website instances (labeled as 1): 30,647
- Total number of features: 111

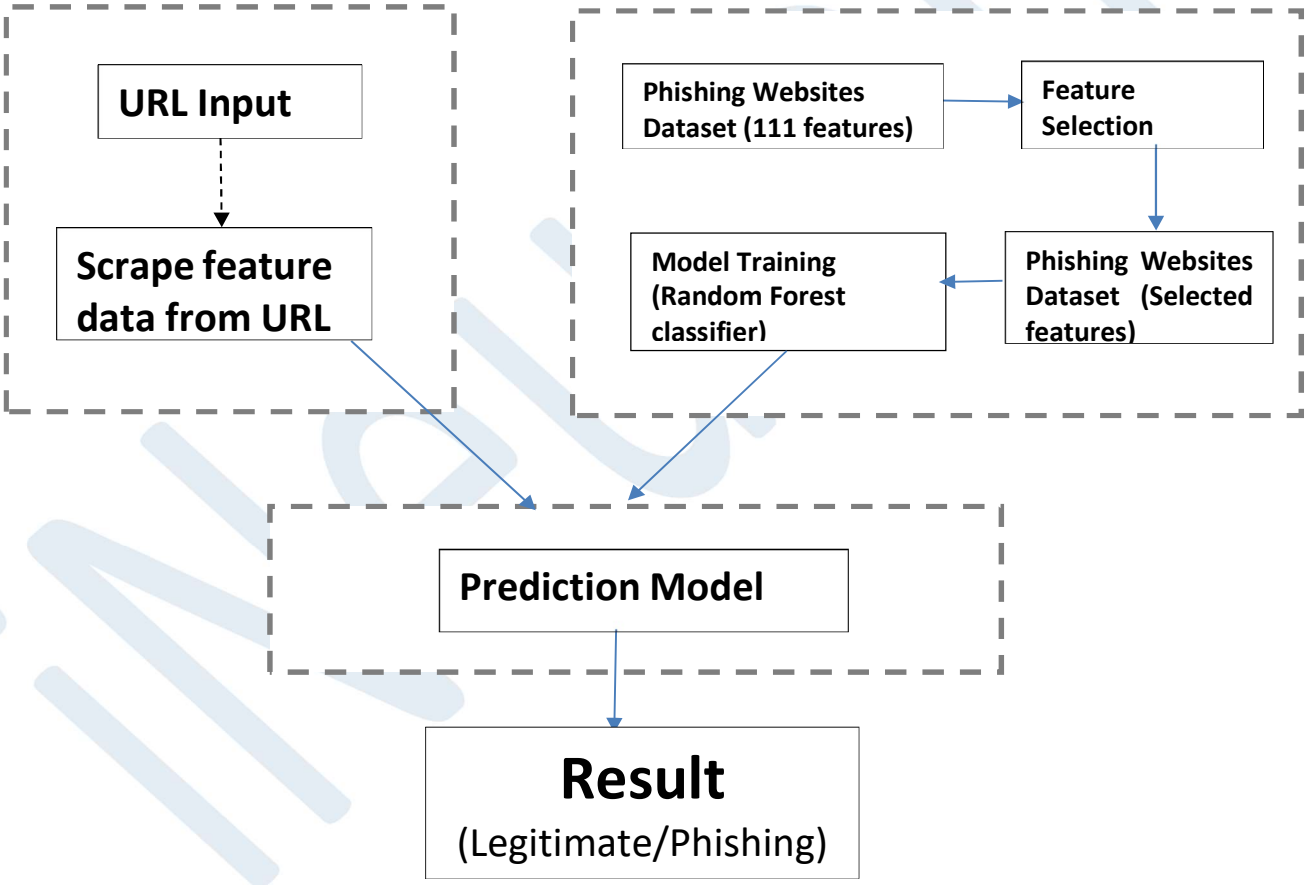
Folder Structure of the Project



TOOLS USED:

- The model development process involved the use of Python programming language.
- Essential libraries such as NumPy, Pandas, Matplotlib, Seaborn, and Scikit-learn were utilized for data manipulation, analysis, and model building.
- Flask, a lightweight Python web framework, was employed for seamless integration of the model into a web application.
- HTML, CSS, and JavaScript were used for front-end development, enabling the creation of an interactive and visually appealing user interface

Machine Learning Model Architecture



CONCLUSION:

- The phishing domain detection using the random forest model yieldedhighly promising results.
- The model achieved an impressive accuracy of 95.08%, precision of 92%,and recall of 93.1%.
- These performance metrics demonstrate the model's exceptional ability toaccurately identify phishing domains.
- The high accuracy and precision of the model make it a robust and reliabletool for predicting the legitimacy of domains.
- The high precision of the model indicates its ability to minimize false positives, reducing the chances of mistakenly flagging legitimate domainsas phishing.
- The model's high recall signifies its capacity to identify a significant portionof actual phishing domains, minimizing the risk of false negatives.
- The excellent overall performance of the model makes it a robust solutionfor organizations and individuals seeking effective phishing domain detection capabilities.
- The model's accuracy and precision contribute to enhanced cybersecuritymeasures, protecting users from falling victim to phishing attacks and preserving sensitive information.

The reliable predictions provided by the model can aid in proactive threat mitigation strategies and support prompt action against potential phishing threat.