**Capstone Project Execution Report**

**Format- 5**

**Capstone Project Name: AIML Tool to Detect Phishing Domains**

**Capstone Project Members:**

* Aditya W
* Abhishek H
* Muzammil S

1. **Design:**

* **Description of Components:**
  + **Input Module:** Responsible for collecting input data such as URLs or domain names.
  + **Pre-processing Module:** Cleans and prepares input data by handling missing values and encoding categorical variables.
  + **Feature Extraction Module:** Extracts relevant features such as URL length, domain age, and keyword presence.
  + **Machine Learning Model:** Utilizes supervised learning algorithms like random forest or deep neural networks for classification.
  + **Output Module:** Displays classification results to users in a user-friendly format.

1. **Description of Technology Used:**

* **Hardware Devices:**
  + No specific hardware requirements; the project primarily involves software development.
* **Software Products:**
  + Programming Environments: Python was the primary development language.
  + Libraries and Frameworks: Utilized TensorFlow for model building, Pandas and NumPy for data manipulation, and Matplotlib and Seaborn for data visualization.
* **Programming Languages:**
  + Python was used for development, covering data processing, model creation, and result visualization.

1. **Fabrication:**

* No physical fabrication involved; software environments and dependencies were set up using provided instructions.

1. **Testing and Validation:**

* **Methodologies:**
  + Laboratory experiments were conducted using labeled datasets containing phishing and legitimate URLs.
  + Employed k-fold cross-validation to assess model performance and generalization.
  + Utilized standard evaluation metrics such as accuracy, precision, recall, and F1-score for result analysis.
* **Datasets:**
  + Utilized publicly available datasets of phishing and legitimate URLs for testing and validation.
* **Results of Testing and Validation:**
  + Testing still going on and software is detecting phishing or legitimate or suspicious.

1. **Results and Inference:**

* **Detailed Results:**
  + Achieved high accuracy in detecting phishing domains, with precision.
  + Performance comparison with existing methods revealed.
* **Inferences:**
  + The AIML tool exhibits robust phishing domain detection capabilities, outperforming existing methods in specific aspects.
  + Identified potential enhancements include feature selection and model optimization to further elevate tool performance.