**PHASE 2**

**BUILDING A SMARTER AI-POWERED SPAM CLASSIFIER**

**TEAM MEMBERS:**

1. NALINKUMAR S - (2021504304)
2. DINESHKUMAR S - (2021504710)
3. PRAVEEN G R - (2021504307)
4. VENGADESHWARAN S - (2021504708)

**INTRODUCTION:**

In Phase 1, we identified a design solution to address a specific problem. Now, in Phase 2, we will outline the comprehensive steps required to transform this design into a practical innovation.

Creating a mail spam classifier AI involves several steps. Here is a high-level step-by-step procedure to build a basic email spam classifier using machine learning:

**STEP 1. Gather and Preprocess Data:**

Collect a dataset of labeled email messages, with spam and non-spam (ham) categories.

Preprocess the text data, including tokenization, lowercasing, and removing stopwords, to convert emails into numerical features.

**STEP 2. Feature Extraction:**

Convert the preprocessed text data into numerical features. Common methods include:

* **Bag of Words (BoW):** Representing each email as a vector of word frequencies.
* **TF-IDF (Term Frequency-Inverse Document Frequency):** Assigning numerical values to words based on their importance.
* **Word Embeddings:** Using pre-trained word embeddings like Word2Vec or GloVe.

**STEP 3. Split the Dataset:**

Divide your dataset into training and testing subsets to evaluate your model's performance.

**STEP 4. Choose a Machine Learning Algorithm:**

Select a machine learning algorithm to train your model. Common choices include:

* **Naive Bayes:** A simple and effective algorithm for text classification.
* Support Vector Machines (SVM): Effective for binary classification tasks.

**Random Forest**, **Logistic Regression**, or more advanced models like **Deep Learning** with neural networks.

**STEP 5. Train the Model:**

Feed the training data into the chosen algorithm and train the model.

**STEP 6. Evaluate the Model:**

Use the testing dataset to evaluate the model's performance. Common evaluation metrics include accuracy, precision, recall, and F1-score.

**STEP 7. Tune Hyperparameters:**

Optimize the model's hyperparameters to improve its performance. You can use techniques like cross-validation and grid search.

**STEP 8. Feature Engineering:**

Experiment with different feature engineering techniques and model variations to improve accuracy. Feature selection, dimensionality reduction, and ensemble methods can help.

**STEP 9. Handling Imbalanced Data:**

Deal with class imbalance issues if present by using techniques like oversampling, undersampling, or synthetic data generation.

**STEP** **10. Regularization:**

Apply regularization techniques to prevent overfitting, like L1 and L2 regularization.

**STEP 11. Model Interpretation:**

If necessary, interpret your model's predictions to understand which features or words contribute to the classification.

**STEP 12. Deployment:**

Once you have a satisfactory model, deploy it as a service, an API, or integrate it into your email system.

**STEP 13. Continuous Monitoring and Improvement:**

Spam email patterns change over time, so it's essential to continuously monitor and update your model to adapt to new spamming techniques.

**STEP 14. User Feedback:**

Collect feedback from users to improve the accuracy of the classifier and reduce false positives/negatives.

**STEP 15. Legal and Ethical Considerations:**

Ensure your spam classifier complies with relevant legal and ethical guidelines.

**CONCLUSION:**

creating a spam email classifier AI involves data collection, preprocessing, feature extraction, model selection, training, evaluation, and deployment. Key steps include gathering labelled data, converting text to numerical features, choosing a classification algorithm, and ensuring continuous monitoring and adaptation to changing spamming techniques. Legal compliance and user feedback are also important considerations in maintaining an effective spam classifier.