AN ARTIFICIAL INTELLIGENCE PROJECT PROPOSAL

on

SMS SPAM SHIELD: MULTI-CATEGORY XAI SPAM DETECTOR

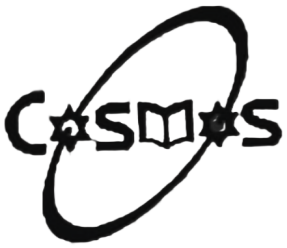
Submitted By

Alok Kumar Jha (230302)
Bibek Kumar Jha (230310)
Kushal Prasad Joshi (230345)

Submitted To

Er. Ranjan Raj Aryal

in partial fulfilment of requirement for the practicals of
Artificial Intelligence (CMP 346) course.



Cosmos College of Management & Technology
(Affiliated to Pokhara University)
Sitapaila, Kathmandu, Nepal

January 18, 2026

Cosmos College of Management & Technology
(Affiliated to Pokhara University)
Sitapaila, Kathmandu, Nepal

APPROVAL

This is to certify that the project proposal titled:

SMS Spam Shield:
Multi-Category XAI Spam Detector

has been reviewed and approved by the project assigner Er. Ranjan Raj Aryal for the further working on project in partial fulfilment of requirement for the practicals of Artificial Intelligence (CMP 346) course.

Project group memebers of Bacholer of Engineering in Computer Engineering named as Alok Kumar Jha (230302), Bibek Kumar Jha (230310) and Kushal Prasad Joshi (230345) can work on the project titled SMS Spam Shield: Multi-Category XAI Spam Detector and submit the final report to fulfill the requirement for the practicals of Artificial Intelligence (CMP 346) course by Pokhara University.

_____

Er. Ranjan Raj Aryal
Course Lecturer

Date of approval: _____

ABSTRACT

This project proposes **SMS Spam Shield: Multi-Category XAI Spam Detector**, an intelligent and explainable system for classifying SMS messages into multiple actionable categories such as *spam, phishing, promotional, transactional, and legitimate* messages. Unlike conventional binary spam filters, the proposed system aims to provide fine-grained classification while offering transparent, human-interpretable explanations for each prediction.

The system is designed to combine classical machine learning models, including Logistic Regression, Naive Bayes, and SVM, with a deep learning-based recurrent neural network (RNN/LSTM). An ensemble-based aggregation strategy is employed to improve robustness and generalization across diverse SMS patterns. To address the black-box nature of automated text classifiers, explainable artificial intelligence techniques such as LIME and SHAP are incorporated to generate token-level explanations and confidence measures for classification decisions.

The project focuses on English-language SMS messages and utilizes offline-trained models evaluated using standard multi-class performance metrics, including precision, recall, F1-score, and confusion matrices. By integrating ensemble learning with explainable AI (XAI), the proposed system aims to enhance both the accuracy and transparency of SMS spam detection, benefiting end users, system administrators, and researchers seeking interpretable and trustworthy text classification solutions.

Keywords: SMS spam detection, multi-category classification, explainable AI (XAI), ensemble learning, LSTM, LIME, SHAP.

PREFACE

This document is submitted in partial fulfillment of the requirements for the Bachelor of Engineering degree in Department of Information Communication and Technology (ICT). The proposed project, *SMS Spam Shield: Multi-Category XAI Spam Detector*, aims to address the increasing variety and sophistication of unsolicited SMS messages by developing an accurate and interpretable SMS classification system. The motivation for this work arises from the growing societal and economic impact of SMS-based spam, phishing, and fraudulent communication, as well as the increasing demand for transparency in automated decision-making systems used in security and communication domains.

Through this project, we seek to explore practical applications of artificial intelligence in cybersecurity, design a robust and user-friendly SMS spam detection framework, and contribute towards improving message safety and user trust through explainable classification mechanisms.

This project is intended to be carried out under the supervision of Er. Ranjan Raj Aryal, whose expertise and guidance are expected to be invaluable throughout the development process. With this proposal, we formally seek approval to proceed with the proposed work and look forward to the opportunity to contribute to academic learning and applied research in artificial intelligence.

We, Alok Kumar Jha (230302), Bibek Kumar Jha (230310) and Kushal Prasad Joshi (230345), hope that this proposal clearly communicates the objectives and planned approach of the proposed SMS Spam Shield: Multi-Category XAI Spam Detector, and serves as a strong foundation for its successful execution under the guidance of Er. Ranjan Raj Aryal.

ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to our respected supervisor, Er. Ranjan Raj Aryal, for his continuous support, encouragement, and expert guidance throughout the process of preparing this project proposal. His valuable feedback and insights have been instrumental in shaping the direction of our work.

We are also thankful to the Department of Information Communication and Technology (ICT) and all the faculty members of Cosmos College of Management & Technology (Affilated to Pokhara University), Sitapaila, Kathamandu, Nepal for their continuous support and for providing us with the opportunity and resources to carry out this proposed project.

We would also like to express our kind regards to the people around us who have directly or indirectly contributed to the successful completion of this proposal. Also we will thank our college friends who gave us valuable suggestions and feedback during the preparation of this project proposal.

Parts of this proposal were drafted and refined with the assistance of AI-powered language models, including ChatGPT [1]. The AI tools were used solely to help with structuring, phrasing, and clarity of the text. All research, analysis, design, and conclusions presented in this proposal are entirely the author's own work.

Finally, we extend our sincere thanks to our family and friends for their unwavering support and encouragement during this endeavour.

We are grateful to all of you.

Alok Kumar Jha (230302), Bibek Kumar Jha (230310) and Kushal Prasad Joshi (230345)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
LIME	Local Interpretable Model-Agnostic Explanations
LR	Logistic Regression
LSTM	Long Short-Term Memory
NB	Naive Bayes
RNN	Recurrent Neural Network
SHAP	SHapley Additive exPlanations
SMS	Short Message Service
SVM	Support Vector Machine
TF-IDF	Term Frequency-Inverse Document Frequency
URL	Uniform Resource Locator
XAI	Explainable Artificial Intelligence

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND AND MOTIVATION

Short Message Service (SMS) remains one of the most widely used communication mediums due to its simplicity, low cost, and universal availability across mobile devices. However, this widespread adoption has also made SMS an attractive channel for unsolicited and malicious messages, including spam, phishing attempts, and fraudulent promotions. Traditional SMS filtering solutions often focus on binary classification: labeling messages as either spam or legitimate; which is increasingly insufficient in modern threat landscapes [2].

Recent advances in machine learning have enabled more accurate text classification techniques, yet most deployed systems operate as black boxes, offering limited insight into why a particular message was flagged. This lack of transparency raises concerns regarding trust, accountability, and regulatory compliance, especially when automated systems influence user communication [3]. These challenges motivate the development of an intelligent, transparent, and multi-category SMS spam detection system.

1.2 PROBLEM STATEMENT

Existing SMS spam detection systems suffer from three primary limitations:

1. **Binary classification constraint:** Most systems classify SMS messages only as spam or non-spam, failing to distinguish between different spam categories such as phishing, promotional, or scam messages.
2. **Limited explainability:** Users and administrators are rarely provided with understandable explanations for classification decisions, reducing trust in automated filtering systems.
3. **Model rigidity:** Single-model approaches struggle to generalize across diverse message structures and evolving spam patterns [4].

Therefore, there is a need for a robust SMS filtering system that supports multi-category classification while providing interpretable and explainable outputs.

1.3 PROJECT OBJECTIVES

The primary objective of this project is to design and implement **SMS Spam Shield: Multi-Category XAI Spam Detector**, an explainable and extensible SMS classification system.

The specific objectives are:

- To collect and preprocess SMS data suitable for multi-category classification.
- To extract meaningful textual features using statistical and sequential representations.
- To train and evaluate multiple machine learning and deep learning models, including Logistic Regression, Naive Bayes, Support Vector Machines, and Recurrent Neural Networks.
- To design an ensemble-based result aggregation mechanism for improved prediction robustness [4].
- To integrate XAI techniques that provide human-interpretable explanations for each prediction [5, 6].

1.4 SCOPE OF THE PROJECT

The scope of this project includes:

- SMS messages written in the English language.
- Offline model training and evaluation using publicly available datasets.
- Explainability at the word or token level for classification decisions.

The project does not address multilingual SMS detection, real-time telecom network deployment, or encrypted message platforms.

1.5 SIGNIFICANCE OF THE PROJECT

By combining ensemble learning with explainable AI techniques, this project aims to improve both the accuracy and transparency of SMS spam detection systems. The proposed solution benefits:

- **End users**, by providing understandable reasons for message blocking.
- **System administrators**, by enabling debugging and model auditing.
- **Researchers**, by offering a modular framework for experimenting with hybrid models and XAI techniques.

CHAPTER 2: LITERATURE REVIEW

"SMS spam detection has evolved from rule-based systems to data-driven and explainable machine learning approaches."

2.1 OVERVIEW OF SMS SPAM DETECTION

SMS spam detection has been an active research area due to the increasing misuse of mobile communication channels for unsolicited and fraudulent activities. Early approaches relied heavily on rule-based systems and manually crafted keyword filters. Although effective for simple spam patterns, such systems lacked adaptability and failed to generalize against evolving spam strategies [2].

With the growth of labeled SMS datasets, machine learning-based text classification techniques became the dominant approach. These systems leverage statistical properties of text to learn discriminative patterns between legitimate and malicious messages.

2.2 TRADITIONAL MACHINE LEARNING APPROACHES

2.2.1 Naive Bayes Classifier

The Naive Bayes (NB) classifier is one of the most widely used algorithms for text classification due to its simplicity and computational efficiency. It assumes conditional independence between words given the class label. Despite this strong assumption, Naive Bayes has shown competitive performance in SMS spam filtering tasks, particularly when combined with bag-of-words or TF-IDF representations [7].

However, NB models are limited in capturing contextual relationships between words, which restricts their effectiveness in detecting sophisticated spam messages such as phishing attempts.

2.2.2 Logistic Regression

Logistic Regression (LR) is a discriminative linear model commonly applied in binary and multi-class text classification. It estimates class probabilities directly and is less sensitive to irrelevant features when regularization is applied. LR-based spam filters have demonstrated stable and interpretable performance in SMS classification tasks [2].

The linear nature of Logistic Regression limits its ability to model non-linear patterns

inherent in complex spam messages.

2.2.3 Support Vector Machines

Support Vector Machines (SVMs) are margin-based classifiers that aim to maximize the separation between classes. SVMs have been extensively used for spam detection due to their robustness in high-dimensional feature spaces [8]. When combined with TF-IDF features, SVMs often outperform simpler probabilistic models.

Despite their effectiveness, SVMs suffer from high computational cost during training and lack inherent probabilistic interpretability, which poses challenges for explainability.

2.3 DEEP LEARNING APPROACHES FOR SMS CLASSIFICATION

2.3.1 Recurrent Neural Networks

Recurrent Neural Networks (RNNs) are designed to model sequential data by maintaining temporal dependencies across inputs. In the context of SMS classification, RNNs capture word order and contextual information that traditional bag-of-words models ignore.

Long Short-Term Memory (LSTM) networks address the vanishing gradient problem in standard RNNs and have demonstrated improved performance in text classification tasks [9]. However, deep learning models require larger datasets and are often criticized for their black-box behavior.

2.4 ENSEMBLE LEARNING TECHNIQUES

Ensemble learning combines multiple models to improve generalization and robustness. Techniques such as voting, averaging, and stacking leverage the strengths of individual classifiers while mitigating their weaknesses [4]. In spam detection, ensemble models have been shown to outperform single-model approaches, particularly when datasets contain diverse message patterns.

This project adopts an ensemble-inspired strategy by aggregating predictions from classical and deep learning models.

2.5 EXPLAINABLE ARTIFICIAL INTELLIGENCE (XAI)

2.5.1 Need for Explainability

As machine learning systems increasingly influence user-facing decisions, explainability has become a critical requirement. Black-box models undermine user trust and complicate debugging, auditing, and regulatory compliance [3].

2.5.2 Model-Agnostic Explanation Techniques

Local Interpretable Model-agnostic Explanations (LIME) generate local surrogate models to explain individual predictions by approximating the decision boundary around a specific instance [5]. Similarly, SHAP values provide a unified framework for feature attribution based on cooperative game theory [6].

These techniques are particularly suitable for SMS classification, as they allow token-level interpretation regardless of the underlying model.

2.6 RESEARCH GAP AND JUSTIFICATION

From the reviewed literature, the following gaps are identified:

- Most existing works evaluate accuracy but do not assess interpretability quality.
- Limited focus on multi-category SMS spam classification.
- Lack of integrated explainability in ensemble-based SMS filters.
- Insufficient emphasis on user-understandable explanations in deployed systems.

The proposed **SMS Spam Shield: Multi-Category XAI Spam Detector** addresses these gaps by combining multi-model classification with explainable AI techniques in a unified framework.

CHAPTER 3: REQUIREMENT ANALYSIS

This chapter presents the requirement analysis for the proposed SMS Spam Shield: Multi-Category XAI Spam Detector system. Requirement analysis is a critical phase of the software development lifecycle that focuses on identifying, analyzing, and documenting the functional and non-functional requirements of the system. A clear understanding of system requirements ensures that the developed solution meets user expectations, remains feasible, and achieves its intended objectives.

3.1 FEASIBILITY STUDY

A feasibility study was conducted to evaluate the practicality and viability of the proposed system before development. The study considers technical, economic, operational, and time feasibility aspects.

3.1.1 Technical Feasibility

The proposed system is technically feasible as it relies on well-established machine learning and deep learning techniques. The required tools, libraries, and frameworks such as Python, scikit-learn, TensorFlow, and explainability libraries are freely available and widely supported. The computational requirements are moderate and can be fulfilled using standard personal computing hardware.

3.1.2 Economic Feasibility

The system is economically feasible since it uses open-source software tools and publicly available datasets. No proprietary software or paid services are required, minimizing overall development costs.

3.1.3 Operational Feasibility

The system is designed to be user-friendly and does not require extensive technical expertise to operate. The classification results and explanations are presented in an understandable format, ensuring acceptance by end users and stakeholders.

3.1.4 Time Feasibility

The project is feasible within the given academic timeline. The use of an incremental development model allows the system to be developed in stages, ensuring timely completion of each module.

3.2 FUNCTIONAL REQUIREMENTS

Functional requirements describe the specific functionalities and services that the proposed system must provide. The key functional requirements of the system are as follows:

- The system shall allow users to submit SMS messages and view predictions in real time using web interface.
- The system shall preprocess input messages using tokenization, stop-word removal, and lemmatization techniques.
- The system shall extract textual features using Bag-of-Words and TF-IDF methods.
- The system shall classify SMS messages into multiple categories such as legitimate, promotional spam, and phishing messages.
- The system shall implement classical machine learning classifiers including Naive Bayes, Logistic Regression, and Support Vector Machine.
- The system shall support deep learning models such as Recurrent Neural Networks or Long Short-Term Memory networks.
- The system shall aggregate predictions from multiple models using an ensemble strategy.
- The system shall generate explainable outputs using model-agnostic explanation techniques such as LIME and SHAP.
- The system shall display classification results along with token-level explanations.
- The system shall allow inference on previously unseen SMS messages.

3.3 NON-FUNCTIONAL REQUIREMENTS

Non-functional requirements define the quality attributes and performance constraints of the system. The following non-functional requirements are identified:

3.3.1 Performance Requirements

The system shall classify SMS messages with acceptable response time suitable for real-time or near real-time usage.

3.3.2 Accuracy and Reliability

The system shall provide consistent and reliable classification results across different SMS categories with minimal classification errors.

3.3.3 Usability Requirements

The system interface shall be simple and intuitive, allowing users to easily input messages and understand the output and explanations without prior training.

3.3.4 Scalability Requirements

The system shall be capable of handling an increasing number of SMS messages without significant degradation in performance.

3.3.5 Security Requirements

The system shall ensure that input SMS data is processed securely and is not stored or shared without authorization.

3.3.6 Maintainability Requirements

The system shall be modular in design, allowing easy updates, model replacement, and extension of functionality in future iterations.

3.3.7 Portability Requirements

The system shall be portable and capable of running on different operating systems such as Windows and Linux with minimal configuration changes.

3.4 HARDWARE REQUIREMENTS

The minimum hardware requirements for implementing the proposed system are:

- Processor: Intel Core i5 or equivalent
- RAM: Minimum 8 GB
- Storage: Minimum 10 GB free disk space
- Optional GPU support for deep learning model training

3.5 SOFTWARE REQUIREMENTS

The software requirements for the proposed system are as follows:

- Operating System: Windows / Linux / MacOS
- Programming Language: Python (version 3.x)
- Development Environment: Jupyter Notebook or any Python IDE (VS code)
- Frontend Technologies: HTML, CSS, and JavaScript
- Backend Framework: Flask or equivalent Python web framework

3.6 TOOLS, LIBRARIES, AND ENVIRONMENT

The following tools and libraries are used in the development of the system:

- HTML and CSS for designing the web-based user interface
- JavaScript for client-side interactivity
- Flask for integrating the frontend with the backend
- NumPy and Pandas for data manipulation
- Scikit-learn for classical machine learning models
- TensorFlow (KerasAPI) for deep learning models
- NLTK for text preprocessing
- LIME for local interpretability
- SHAP for global and local model explanations
- Matplotlib and Seaborn for visualization

3.7 SUMMARY

This chapter presented the requirement analysis of the proposed SMS Spam Shield: Multi-Category XAI Spam Detector system. It discussed the feasibility of the project, identified functional and non-functional requirements, and specified the necessary hardware, software, tools, and libraries. A clear definition of these requirements provides a strong foundation for the subsequent design, implementation, and evaluation phases of the project.

CHAPTER 4: METHODOLOGY

4.1 OVERVIEW OF THE PROPOSED METHODOLOGY

The methodology of the proposed **SMS Spam Shield: Multi-Category XAI Spam Detector** system follows a structured and incremental development approach aligned with Software Development Life Cycle (SDLC) principles [3]. The system follows an **incremental model**, where machine learning models are introduced sequentially one at a time and integrated progressively into the system.

The complete workflow consists of data acquisition, preprocessing, feature extraction, model training, evaluation, result aggregation, and explainability generation. This approach ensures modularity, traceability, and ease of validation at each development stage.

The methodology is divided into two major operational phases:

- **Training Phase**: Offline dataset preparation, model training, validation, and optimization.
- **Inference Phase**: Real-time SMS classification, ensemble aggregation, and explanation generation.

Additionally, each increment undergoes **component testing** to evaluate individual model performance, followed by **system testing** after integrating the new module.

4.2 INCREMENTAL DEVELOPMENT MODEL

The Incremental Model is a type of software development life cycle (SDLC) model where the system is designed, implemented, and tested incrementally (in small portions or modules) rather than developing the entire system at once. Each increment adds functional capabilities until the complete system is ready.

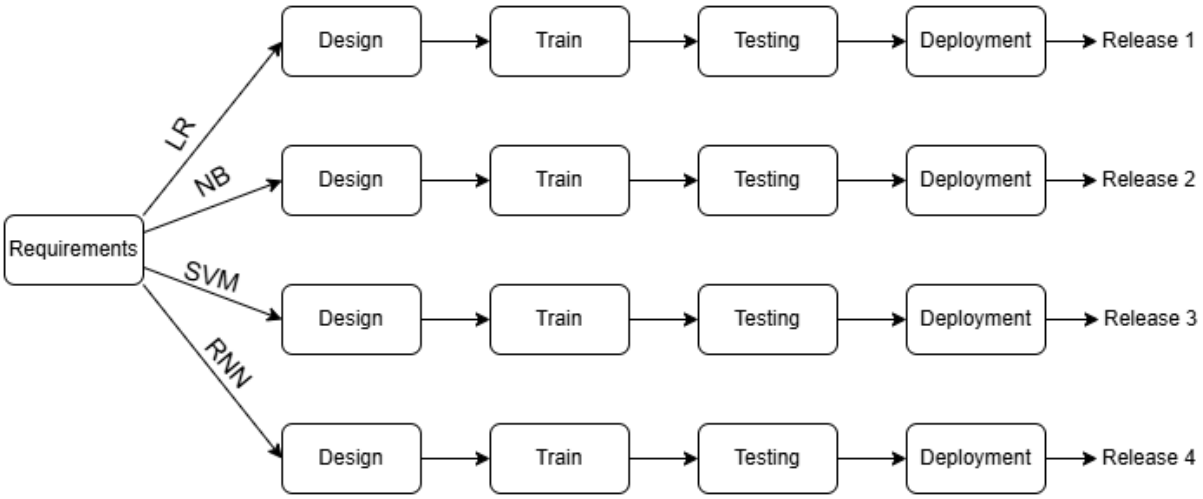


Figure 4.2 : Incremental Development Model of Proposed System

The system follows an incremental development strategy in which one machine learning model is added and evaluated per increment. A total of four increments are defined:

4.2.1 Increment 1: Logistic Regression

Logistic Regression is introduced as the baseline model due to its simplicity, interpretability, and efficiency. Component testing is performed to evaluate its classification accuracy and stability.

4.2.2 Increment 2: Naive Bayes

The Naive Bayes classifier is integrated in the second increment. Its probabilistic nature and low computational cost complement Logistic Regression. Component testing is conducted before integration.

4.2.3 Increment 3: Support Vector Machine

Support Vector Machine is added to handle high-dimensional feature spaces and improve decision boundaries. After component testing, system testing is performed with LR, NB, and SVM integrated.

4.2.4 Increment 4: Recurrent Neural Network

A Recurrent Neural Network with Long Short-Term Memory (LSTM) units is introduced in the final increment. This model captures sequential dependencies in SMS text and enhances performance for complex patterns [9]. Full system testing is performed after integration.

4.2.5 Reason for Incremental Approach

Each increment consists of:

- Model implementation and training
- Component-level accuracy testing
- Integration with existing modules
- System-level testing after integration

This strategy allows early validation, controlled complexity growth, and improved fault isolation during development.

4.3 ARCHITECTURE OF PROPOSED SYSTEM

The system architecture diagram defines the structural organization of software components and their interactions. The architecture is designed to ensure modularity, scalability, and maintainability, following established software engineering principles within the Software Development Life Cycle (SDLC) [3].

The overall system is divided into two primary architectural views:

- **Model Training Architecture**
- **Runtime (Inference) Architecture**

This separation allows independent optimization of training workflows and real-time message classification.

4.4 MODEL TRAINING ARCHITECTURE

The model training architecture illustrates the workflow used to prepare, train, evaluate, and store machine learning models. This process is performed offline to ensure efficient and stable deployment.

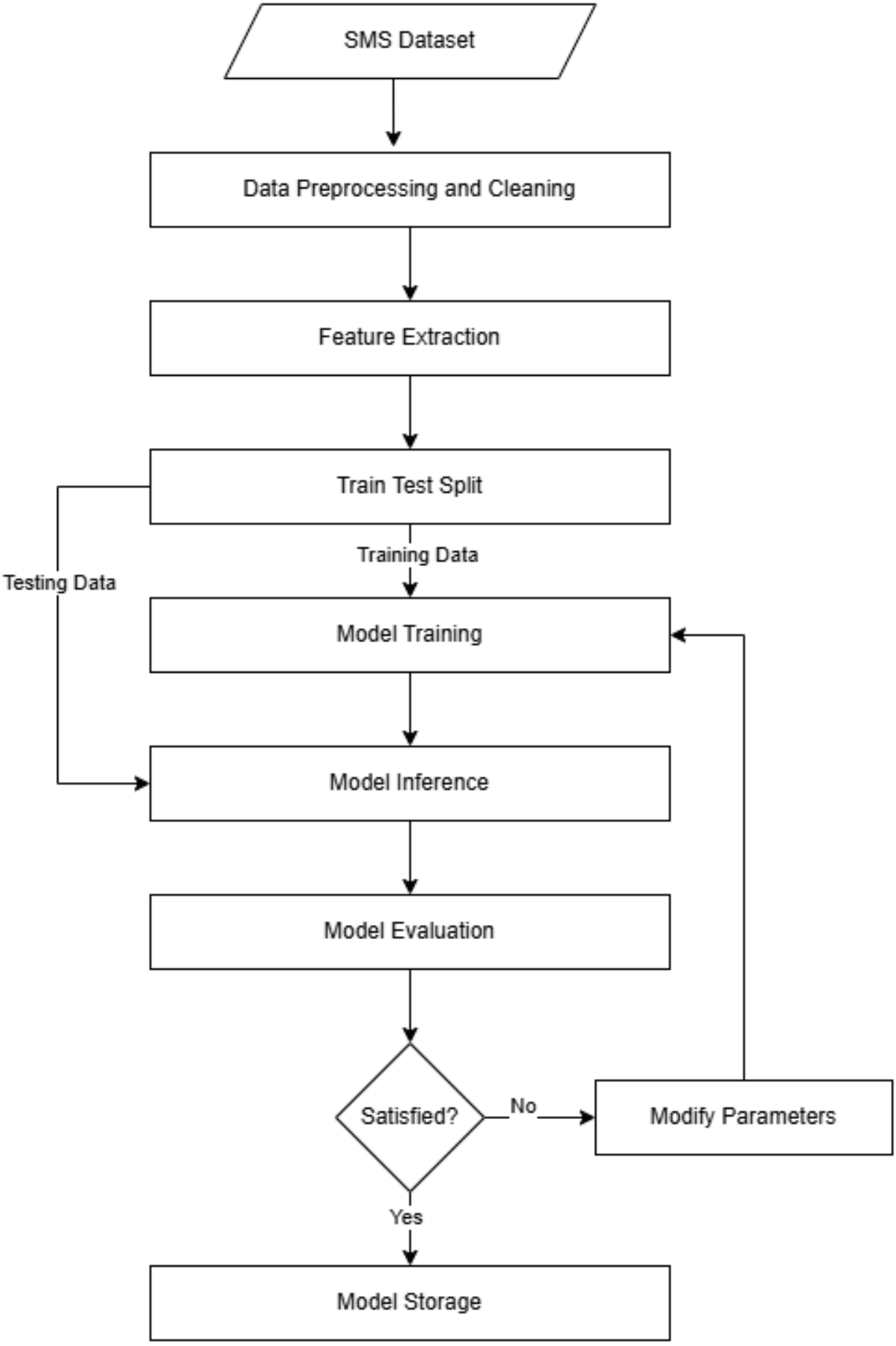


Figure 4.4 : Model Training Architecture of Proposed System

4.4.1 SMS Dataset

The system utilizes publicly available SMS datasets containing labeled text messages. Originally binary-labeled datasets are extended or re-labeled to support multi-category classification such as legitimate, promotional, phishing, scam, and transactional messages [2].

Each dataset record consists of:

- A unique identifier
- Raw SMS text
- Corresponding class label

The dataset serves as the foundation for supervised learning across all increments.

4.4.2 Data Preprocessing and Cleaning

SMS messages often contain noise such as punctuation, numbers, URLs, and inconsistent casing. A unified preprocessing pipeline is applied during both training and inference to maintain consistency.

The preprocessing steps include:

1. Conversion to lowercase
2. Removal of punctuation and special characters
3. Tokenization into individual words
4. Stop-word removal
5. Lemmatization or stemming

These steps reduce vocabulary size, remove noise, and improve model generalization [7].

4.4.3 Feature Extraction

Feature extraction transforms preprocessed SMS text into numerical representations suitable for machine learning algorithms.

Two separate feature extraction strategies are implemented:

1. **Statistical Features:** For classical machine learning models (LR, NB, and SVM), the following representations are used:
   - Bag-of-Words (BoW)
   - Term Frequency-Inverse Document Frequency (TF-IDF)

   TF-IDF assigns lower weights to frequent but less informative words, improving classification performance [2].
2. **Sequential Features:** For the deep learning model, SMS messages are encoded as

sequences of word indices. Padding and truncation are applied to ensure uniform sequence length. This enables the model to capture word order and contextual dependencies [9].

This separation allows each model type to operate on suitable feature representations.

4.4.4 Train-Test Split

The dataset is divided into training and testing subsets to enable unbiased performance evaluation. The training subset is used for model learning, while the testing subset is reserved for inference validation.

The dataset is divided into training and testing subsets using a fixed ratio (e.g., 80:20).

4.4.5 Model Training

Multiple classifiers are trained independently in each increment:

1. Logistic Regression
2. Naive Bayes
3. Support Vector Machine
4. Recurrent Neural Network (LSTM)

Training multiple models improves system robustness and reduces dependency on a single algorithm [4].

4.4.6 Model Evaluation and Optimization

Trained models are evaluated using standard classification metrics:

1. **Accuracy:** Measures the proportion of correct predictions over total predictions.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

2. **Precision:** Measures the proportion of true positives among predicted positives.

$$Precision = \frac{TP}{TP + FP}$$

3. **Recall:** Measures the proportion of true positives among actual positives.

$$Recall = \frac{TP}{TP + FN}$$

4. **F1-score:** Harmonic mean of precision and recall, balancing both metrics.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

5. **Confusion Matrix:** A table displaying true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) across all SMS categories.

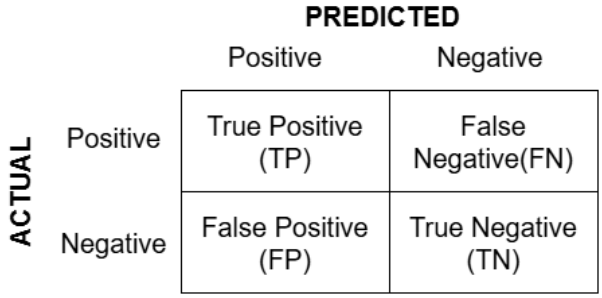


Figure 4.4.6 : Confusion Matrix

These metrics provide a comprehensive assessment of both component-level and system-level performance across SMS categories [2]. If performance is unsatisfactory, model parameters are modified and retraining is performed. This feedback loop continues until acceptable results are achieved.

4.4.7 Model Storage

Once validated, trained models are serialized and stored for deployment in the runtime system.

4.5 RUNTIME (INFERENCE) ARCHITECTURE

The runtime architecture describes how incoming SMS messages are processed and classified in real-time or near real-time.

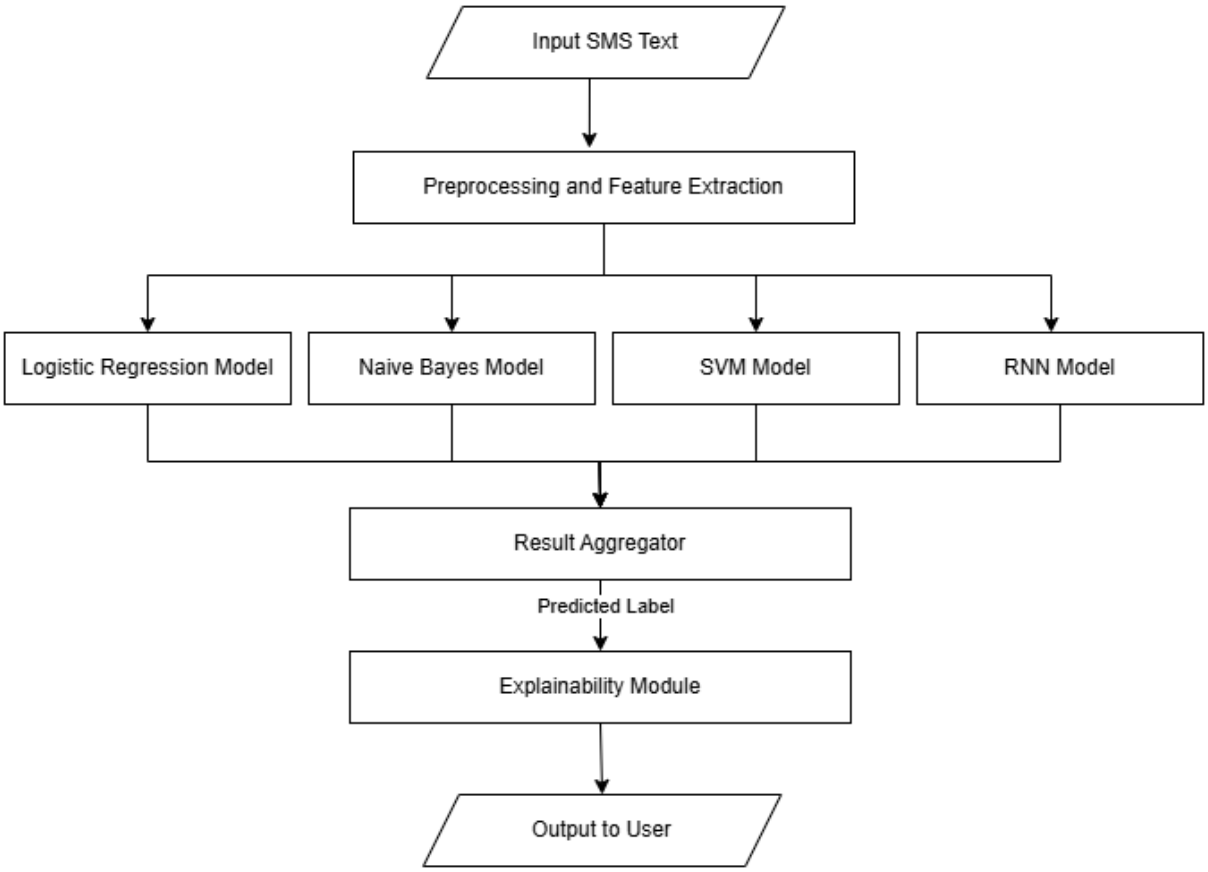


Figure 4.5 : Runtime Architecture for SMS Classification and Explainability

4.5.1 Input SMS Text

The system accepts raw SMS text as input from the user through the provided interface.

4.5.2 Preprocessing and Feature Extraction

Incoming messages undergo the same preprocessing and feature extraction steps used during training to maintain consistency.

4.5.3 Parallel Model Inference

The processed SMS is simultaneously passed to all trained models:

- Logistic Regression Model
- Naive Bayes Model
- SVM Model
- RNN Model

Each model independently generates a probability distribution over the defined SMS categories.

4.5.4 Result Aggregator

The result aggregator combines outputs from all models using ensemble techniques such as weighted averaging or majority voting. This improves prediction reliability and reduces individual model bias [4].

4.5.5 Predicted Label

The aggregated output produces a final predicted SMS category along with confidence scores.

4.5.6 Explainability Module

The explainability module applies XAI techniques to generate human-interpretable explanations for the prediction. Token-level importance values highlight influential words contributing to the decision [5, 6].

To address transparency and trust concerns, explainable artificial intelligence (XAI) techniques are integrated into the system.

4.5.7 Output to User

The final output consists of:

- Predicted SMS category
- Confidence score
- Explanation highlighting key textual features

This output enhances transparency and user trust in the system.

4.6 ARCHITECTURAL ADVANTAGES

The proposed architecture offers:

- Modular design enabling easy model replacement or extension
- Improved accuracy through ensemble learning
- Transparency through integrated explainability
- Clear separation of training and inference concerns

CHAPTER 5: TIME SCHEDULE

5.1 PROJECT TIMELINE

The project is planned to be completed over a period of **eight weeks**. Gnatt Chart in Figure 5.1.1 illustrates the week-wise breakdown of tasks and milestones. Table 5.1.2 presents the week-wise implementation schedule and deliverables.

5.1.1 Gantt Chart

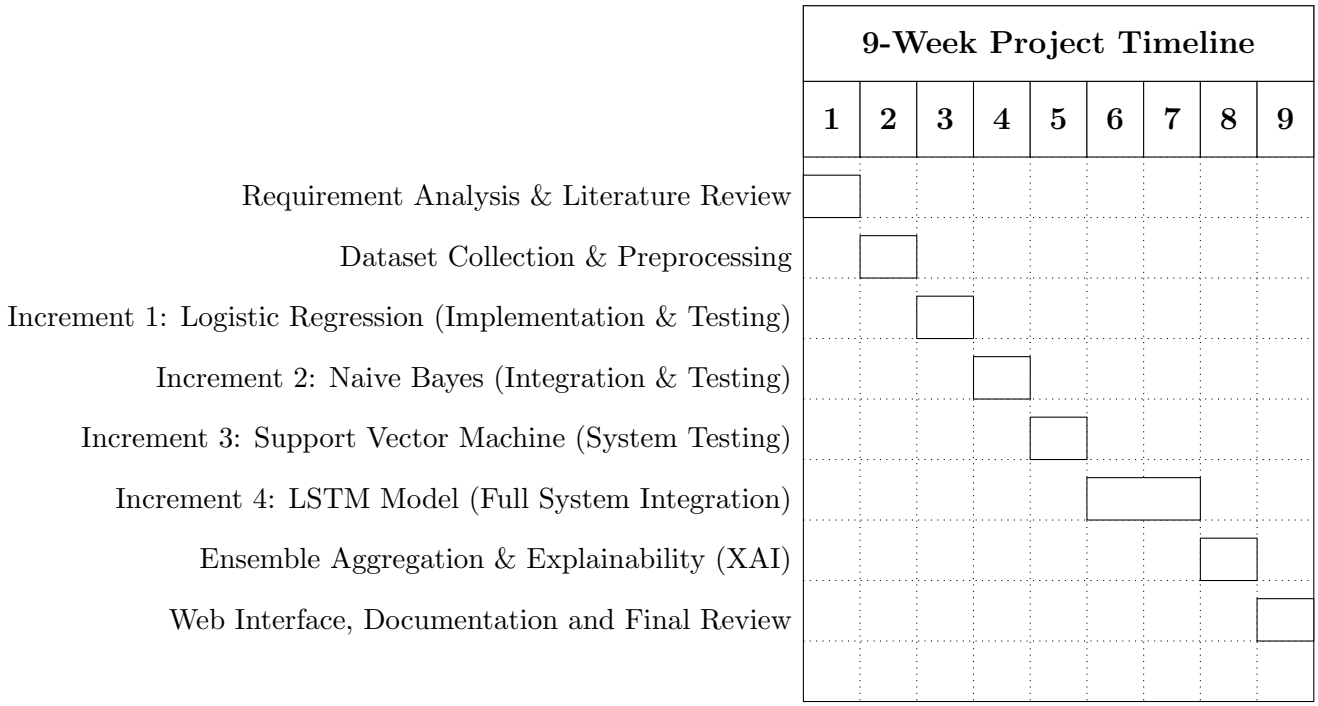


Figure 5.1.1 : Gantt Chart Representing Incremental Development Model

5.1.2 Timeline Deliverables

Week	Activities	Deliverables
Week 1	Requirement analysis and literature survey	Problem definition, system objectives, and finalized methodology
Week 2	Dataset collection, cleaning, labeling, and preprocessing	Cleaned, preprocessed, and ready-to-use SMS dataset
Week 3	Increment 1: Logistic Regression implementation, training, and component testing	Baseline Logistic Regression model with evaluation results
Week 4	Increment 2: Naive Bayes integration, training, and component testing	Integrated LR + NB models with comparative performance analysis
Week 5	Increment 3: Support Vector Machine implementation and system testing	LR, NB, and SVM integrated system with validated metrics
Week 6–7	Increment 4: LSTM model implementation, training, and full system testing	Complete system with LSTM-based classification
Week 8	Ensemble aggregation and explainability (XAI) integration	Final ensemble model with explainable outputs
Week 9	Web interface, documentation, validation, and final review	Final report, results validation, and project submission

Table 5.1.2 : Incremental Timeline Deliverables

5.2 MILESTONES

Major project milestones include:

- Completion of dataset preparation and preprocessing
- Successful training and validation of all classification models
- Integration of ensemble methods and explainability modules
- Comprehensive performance evaluation and validation against benchmarks
- Submission of final documentation and project deliverables

5.3 DELIVERABLES

The final project deliverables encompass:

- Fully trained SMS classification models with performance metrics
- Explainable prediction outputs for enhanced interpretability

- Comprehensive project documentation detailing methodologies and results
- Web interface for user-friendly spam detection and prediction

5.4 SCHEDULE FEASIBILITY

The proposed schedule is feasible within the allocated timeframe and available resources. Leveraging established machine learning frameworks, parallel development of incremental components, and a modular design reduces implementation risk and supports timely completion. Contingency buffers are incorporated for model tuning and integration.

CHAPTER A: RISK ANALYSIS AND MITIGATION

A.1 INTRODUCTION

Risk analysis is a critical component of the Software Development Life Cycle (SDLC) that identifies potential uncertainties which may negatively impact project objectives. Early identification and mitigation of risks improves project reliability and success rate [3]. This chapter discusses the major risks associated with the development of the proposed SMS Spam Shield system and outlines appropriate mitigation strategies.

A.2 RISK IDENTIFICATION

The risks identified in this project are categorized into technical, data-related, operational, and ethical risks.

A.2.1 Technical Risks

Technical risks pertain to challenges in model development, integration, and performance:

- **Model performance degradation:** Trained models may fail to generalize to unseen SMS patterns.
- **Overfitting:** Complex models such as LSTM may overfit limited datasets.
- **System integration issues:** Difficulty in integrating multiple models and explainability tools.

A.2.2 Data-Related Risks

Data-related risks involve issues with the quality and representativeness of the SMS dataset:

- **Class imbalance:** Uneven distribution of SMS categories can bias model predictions.
- **Data quality issues:** Noisy or mislabeled data may degrade classification accuracy.

A.2.3 Operational Risks

Operational risks relate to deployment and maintenance challenges:

- **Computational constraints:** Limited hardware resources may restrict model training or inference speed.
- **Scalability limitations:** The system may not scale efficiently for high message volumes.

A.2.4 Ethical and Explainability Risks

Ethical risks arise from the need for transparency and user trust in automated spam detection:

- **Lack of transparency:** Users may distrust automated decisions without clear explanations.
- **Privacy concerns:** SMS data may contain sensitive personal information.

A.3 RISK MITIGATION STRATEGIES

Table A.3 summarizes identified risks and corresponding mitigation approaches.

Risk Category	Identified Risk	Mitigation Strategy
Technical	Model overfitting	Apply cross-validation, regularization, and early stopping techniques
Technical	Integration complexity	Adopt modular architecture and incremental integration
Data	Class imbalance	Use resampling techniques and class-weighted loss functions
Data	Poor data quality	Perform data cleaning and manual verification of samples
Operational	Hardware limitations	Optimize models and use lightweight classifiers for inference
Operational	Scalability issues	Design stateless inference modules and batch processing
Ethical	Lack of transparency	Integrate explainable AI techniques (LIME, SHAP) [5]
Ethical	Privacy concerns	Anonymize data and avoid storing personally identifiable information

Table A.3 : Risk Analysis and Mitigation Strategies

A.4 RESIDUAL RISK ASSESMENT

Despite mitigation measures, some residual risks may remain, particularly due to evolving spam patterns and data drift. These risks are monitored through periodic model

retraining and performance evaluation.

A.5 SUMMARY

Effective risk management ensures system robustness, ethical compliance, and long-term sustainability. The integration of explainability mechanisms further reduces user trust-related risks and supports responsible deployment of machine learning systems.

CHAPTER B: TECHNICAL DETAILS

B.1 OVERVIEW

This chapter provides detailed technical specifications for the **SMS Spam Shield: Multi-Category XAI Spam Detector** system. It covers the dataset structure, preprocessing methodology, feature extraction techniques, and classification pipeline architecture that form the foundation of the spam detection model.

B.2 DATASET STRUCUTURE

The SMS dataset used in this project follows a structured tabular format. Each record represents a single SMS message with an associated category label.

Field Name	Description	Data Type
sms_id	Unique identifier for SMS	Integer
message_text	Raw SMS content	String
category	SMS classification label	Categorical

Table B.2 : SMS Dataset Schema

B.3 SMS CATEGORY DEFINATIONS

The system supports multi-category classification. The primary categories used are:

- **Legitimate:** Personal or informational messages
- **Promotional:** Marketing or advertising messages
- **Phishing:** Messages attempting to steal sensitive information
- **Scam/Fraud:** Messages involving financial deception
- **Transactional:** One-time password (OTP) or service notifications

B.4 PREPROCESSING PIPELINE PSEUDOCODE

```
Input: Raw SMS Text
Output: Cleaned Token List

1. Convert text to lowercase
2. Remove punctuation and special characters
```

```
3. Tokenize text into words
4. Remove stop-words
5. Apply lemmatization
6. Return cleaned tokens
```

B.5 FEATURE VECTOR REPRESENTATION

TF-IDF Vector Example:

- SMS: "Win a free prize now"
- Extracted Features: [win, free, prize, now]
- TF-IDF Vector: Sparse numerical representation

Sequence Encoding Example:

- Tokenized SMS: [win, free, prize, now]
- Encoded Sequence: [45, 112, 78, 203]
- Padded Sequence Length: 50

B.6 SAMPLE INPUT AND OUTPUT

Sample Input SMS:

"Congratulations! You have won a free gift card. Click the link to claim now."

System Output:

- Predicted Category: Phishing
- Confidence Score: 0.94
- Important Tokens: win, free, click, claim

B.7 ADDITIONAL NOTES

All sample data shown in this appendix is anonymized and used solely for academic and experimental purposes. No personally identifiable information is stored or processed by the system.

GLOSSARY

Short Message Service (SMS): A text messaging service component of mobile communication systems used for exchanging short text messages between mobile devices [2].

Spam: Unsolicited or unwanted messages sent in bulk, often for advertising, fraudulent, or malicious purposes [2].

Phishing: A form of cyberattack in which deceptive messages attempt to obtain sensitive information such as passwords, banking details, or personal data [10].

Machine Learning (ML): A field of artificial intelligence that enables systems to learn patterns from data and make predictions without explicit programming [10].

Binary Classification: A classification task in which input data is assigned to one of two possible classes, such as spam or non-spam.

Multi-Category Classification: A classification task in which input data is assigned to one of several predefined categories rather than a binary decision [11].

Explainable Artificial Intelligence (XAI): Methods and techniques that make the predictions and internal behavior of artificial intelligence models understandable to humans [5].

Black-Box Model: A machine learning model whose internal decision-making process is not directly interpretable or transparent to human users.

Logistic Regression: A supervised machine learning algorithm used for classification that estimates class probabilities using a logistic function [11].

Naive Bayes Classifier: A probabilistic machine learning algorithm based on Bayes' theorem with an assumption of conditional independence among features [7].

Support Vector Machine (SVM): A margin-based supervised learning algorithm that separates data points using an optimal hyperplane in a high-dimensional feature space [8].

Recurrent Neural Network (RNN): A neural network architecture designed for sequential data processing by maintaining internal memory states across time steps [10].

Long Short-Term Memory (LSTM): A specialized type of recurrent neural network capable of learning long-range dependencies by mitigating the vanishing gradient problem [9].

Ensemble Learning: A machine learning technique that combines predictions from multiple models to improve accuracy, robustness, and generalization [4].

Local Interpretable Model-Agnostic Explanations (LIME): An explainability technique that explains individual predictions by approximating the model locally using an interpretable surrogate model [5].

SHapley Additive exPlanations (SHAP): A unified framework for model interpretation based on cooperative game theory that assigns contribution values to individual features [6].

Software Development Life Cycle (SDLC): A structured process for planning, designing, developing, testing, and maintaining software systems [3].

Data Preprocessing: A set of techniques applied to raw data to improve quality, consistency, and suitability for machine learning models [7].

Tokenization: The process of splitting text into smaller units such as words or tokens for further analysis [11].

Stop Words: Commonly occurring words (e.g., "the", "is") that are often removed during text preprocessing to reduce noise [7].

Lemmatization: The process of reducing words to their base or dictionary form to normalize textual data [11].

Bag-of-Words (BoW): A text representation technique that converts text into a fixed-length vector by counting word occurrences while ignoring word order [7].

Term Frequency-Inverse Document Frequency (TF-IDF): A statistical measure that evaluates the importance of a word in a document relative to a collection of documents [7].

Ensemble Aggregation: The process of combining outputs from multiple machine learning models using methods such as majority voting or weighted averaging to produce a final prediction.

Token-Level Explanation: An explainability approach that identifies and highlights the contribution of individual words or tokens to a model's prediction.

Inference: The process of using a trained machine learning model to generate predictions on previously unseen data.

Precision: A performance metric that measures the proportion of correctly predicted positive instances among all predicted positives [11].

Recall: A performance metric that measures the proportion of actual positive instances correctly identified by the model [11].

F1-Score: The harmonic mean of precision and recall, used to evaluate overall classification performance [11].

Confusion Matrix: A tabular representation that summarizes the performance of a classification model by comparing predicted and actual class labels [11].

Model Explainability: The ability to understand, interpret, and justify how a machine learning model arrives at its predictions [5].

Deep Learning: A subset of machine learning that uses multi-layered neural networks to model complex and hierarchical patterns in data [10].

Class Imbalance: A condition in which some classes in a dataset are significantly underrepresented compared to others, potentially biasing model performance.

REFERENCES

[1] OpenAI, "Chatgpt (gpt-5.1)," aI assistant used for drafting and analysis. [Online]. Available: https://chat.openai.com

[2] T. A. Almeida, J. M. G. Hidalgo, and A. Yamakami, "Contributions to the study of sms spam filtering: new collection and results," *arXiv preprint arXiv:1103.4678*, 2011, https://arxiv.org/abs/1103.4678.

[3] I. Sommerville, *Software Engineering*, 9th ed. Addison-Wesley, 2011.

[4] T. G. Dietterich, "Ensemble methods in machine learning," *Multiple Classifier Systems*, pp. 1–15, 2000.

[5] M. T. Ribeiro, S. Singh, and C. Guestrin, "Why should i trust you? explaining the predictions of any classifier," *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016.

[6] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," *Advances in Neural Information Processing Systems*, 2017.

[7] A. McCallum and K. Nigam, "A comparison of event models for naive bayes text classification," in *AAAI-98 Workshop on Learning for Text Categorization*, 1998.

[8] C. Cortes and V. Vapnik, "Support-vector networks," in *Machine Learning*. Kluwer Academic Publishers, 1995.

[9] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[10] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. Dorling Kindersley (India) Pvt. Ltd., 2014.

[11] E. Rich and K. Knight, *Artificial Intelligence*, 2nd ed. Tata McGraw-Hill Publishing Company Limited, 2006.