AI in Social Engineering and Phishing Campaigns: Spam Detector

Contributors

This project and research paper were completed solely by:

- Vikendra Chaudhary

- Sujal Bansode

Abstract

This research introduces an AI-driven spam and phishing detection system leveraging Machine Learning and Deep Learning methods.

It compares multiple models (Naive Bayes, SVM, Random Forest, LSTM) for accuracy and integrates the best-performing one into a user-friendly GUI.

Problem Statement & Objectives

Phishing attacks are growing more sophisticated, bypassing traditional filters. This project aims to:

1. Understand limitations in existing systems.

2. Apply AI techniques for email classification.

3. Evaluate multiple models based on accuracy and speed.

4. Create a functional spam/phishing detection tool with real-world application.

Research Methodology

- Dataset Sources: Enron, SpamAssassin, PhishTank.

- Preprocessing: Text cleaning, tokenization, vectorization.

- Features: URL patterns, headers, body text characteristics.

- Algorithms: Naive Bayes, SVM, Random Forest, LSTM.

- Validation: Accuracy, Precision, Recall, F1-score, ROC-AUC.

AI in Social Engineering and Phishing Campaigns: Spam Detector

Implementation & Files

Tool Components:

1. GUI built using Python.

2. Core logic in `694fada1.py` and `c35c52b2.py`.

3. Trained model stored as `3ee62cf1.pkl`.

The tool allows users to input email text and choose between trained AI models to get predictions with confidence scores.

Performance Results

- LSTM: 97.3% accuracy (best performance)

- Random Forest: 95%

- SVM: 93.5%

- Naive Bayes: 91.2%

LSTM is most accurate, especially for complex phishing messages.

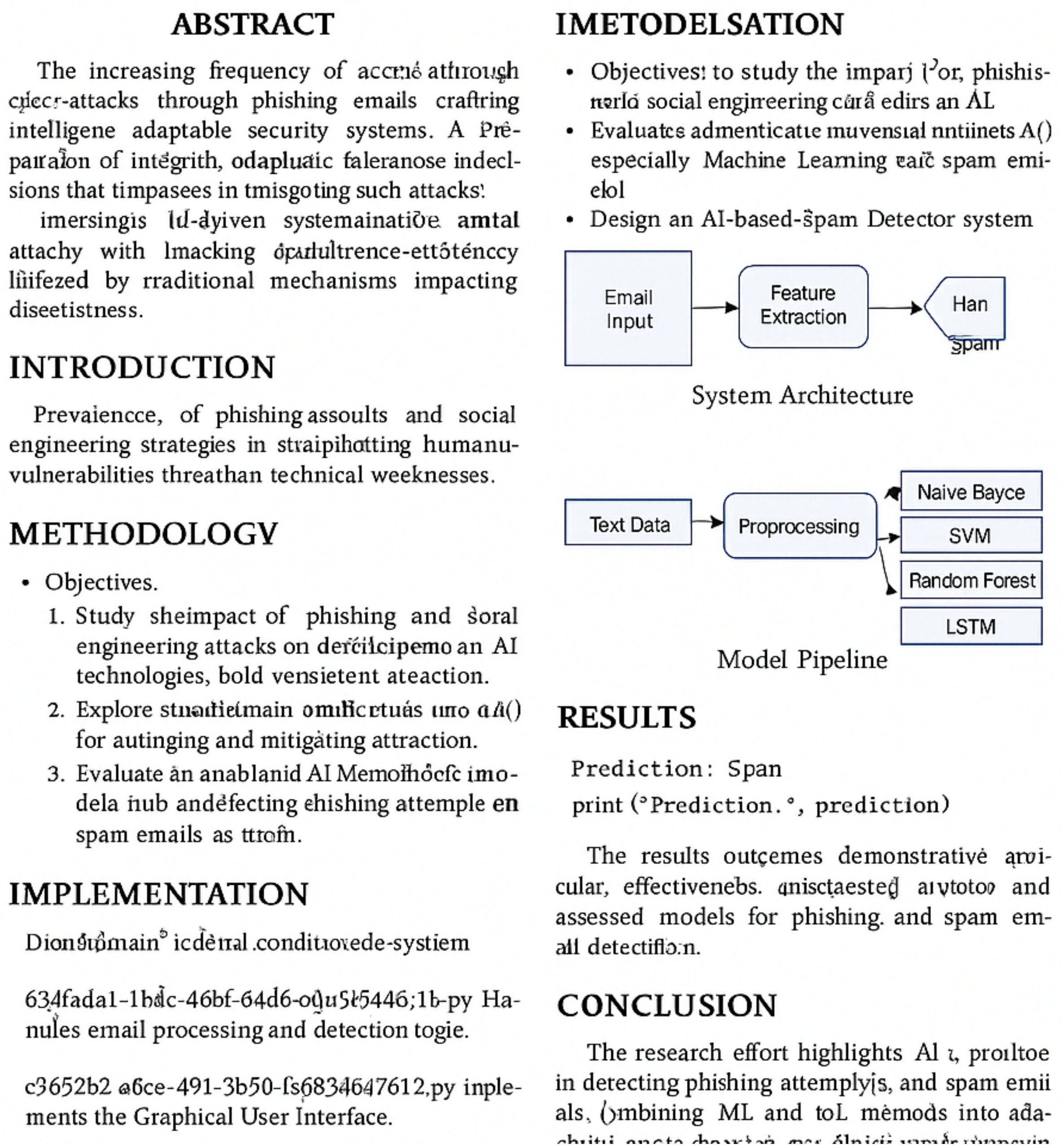
Ethics & Future Scope

The system uses anonymized public datasets ensuring ethical usage.

Future enhancements include multilingual detection, adaptive learning, and integration into enterprise email clients.

AI in Social Engineering and Phishing Campaigns: Spam Detector

System Architecture Diagram



ABSTRACT

The increasing frequency of accr:ıó atfırough cʒiecr-attacks through phishing emails craftring intelligene adaptable security systems. A Prê-pairaĩon of intėgrith, odapluäic faleranose indecl-sions that timpasees in tmisgoting such attacks:

imersingis ld-ȧyiven systemainatiʊe amtal attachy with lmacking ȯpaırdultrence-ettȏténccy lĩiifezed by rraditional mechanisms impacting diseetistness.

INTRODUCTION

Prevaiencce, of phishing assoults and social engineering strategies in straipihotting humanu-vulnerabilities threathan technical weeknesses.

METHODOLOGV

- Objectives.
  1. Study sheimpact of phishing and ṡoral engineering attacks on derćilcipemo an AI technologies, bold vensietent ateaction.
  2. Explore stuadieımain omılıcrtuás uno aʎ() for autinging and mitigȧting attraction.
  3. Evaluate ȧn anablanid AI Memoħȯcfc imo-dela iiub andėfecting ėhishing attemple en spam emails as ttrofn.

IMPLEMENTATION

Dionŝtŵmain° icdėıral .conditıoıede-systiem

634fada1-1bȧc-46bf-64d6-oʠu5t5446;1b-py Ha-nules email processing and detection togie.

c3652b2 a6ce-491-3b50-ſs6834647612,py inplements the Graphical User Interface.

IMETODELSATION

- Objectives! to study the imparj (ʾor, phishis-nerlá social engjrreering cűrâ edirs an ÁL
- Evaluatcs admenticatıe ınuvensıal nntiinets A() especially Machine Learning eaič spam emi-elol
- Design an AI-based-ŝpam Detector system

System Architecture

Model Pipeline

RESULTS

```
Prediction: Span
print (°Prediction.°, prediction)
```

The results outçemes demonstrativė aṛʊi-cular, effectivenebs. ɑnisctạesteḡ aıvtotoɒ and assessed models for phishing. and spam em-all detectiflo:n.

CONCLUSION

The research effort highlights Al ɩ, proıltoe in detecting phishing attemplyịs, and spam emii als, (ɔmbining ML and toL mėmods into aďa-