

TSP- AI ML Fundamentals (Capstone Project)

DETECTING SPAM EMAILS

Presented By:
Shree Amritha J - au61772111093

OUTLINE

- **Abstract**
- **Problem Statement**
- **Proposed System/Solution**
- **Algorithm & Deployment**
- **Project Demo(photos / videos)**
- **Conclusion**
- **Future Scope**
- **References**



ABSTRACT

- Email has become an indispensable mode of communication in both personal and professional spheres. However, the ubiquitous nature of email also attracts unwanted communication in the form of spam. Spam emails not only clutter inboxes but also pose security risks, including phishing attacks and malware distribution. Hence, effective email spam detection mechanisms are crucial to maintain the integrity and security of email communication systems.



PROBLEM STATEMENT

- i. The primary objective of email spam detection is to accurately differentiate between legitimate emails and spam, thereby preventing unwanted or potentially harmful messages from reaching users' inboxes.
- ii. This problem is exacerbated by the sheer volume of emails exchanged daily, making manual filtering impractical and necessitating automated solutions.
- iii. Email spam remains a persistent and widespread issue, posing significant challenges to users, businesses, and email service providers. Despite the advancements in spam filtering technologies, spammers continually adapt their tactics to evade detection, leading to an ongoing arms race between spammers and spam filters.



AIM

AIM :

The aim of email spam detection is to accurately and efficiently differentiate between legitimate emails and unsolicited or potentially harmful spam messages. This process involves the development and implementation of algorithms and techniques that can automatically identify and filter out spam emails, thereby minimizing the impact of spam on users, businesses, and email service providers.



OBJECTIVES

OBJECTIVES :

- a. **Maximizing Detection Accuracy:** The primary goal is to accurately identify and classify spam emails while minimizing false positives (legitimate emails incorrectly classified as spam) and false negatives (spam emails incorrectly classified as legitimate).
- b. **Improving User Experience:** By filtering out spam emails, the aim is to enhance user experience by reducing inbox clutter and minimizing the time and effort required to sift through unwanted messages.
- c. **Enhancing Security:** Spam emails often contain malicious content, such as phishing links, malware attachments, or fraudulent schemes. Effective spam detection helps protect users from security threats and prevent them from falling victim to cyber attacks
- d. **Preserving Privacy:** Spam emails may also contain attempts to collect sensitive information or engage in identity theft. By detecting and filtering out such emails, email spam detection systems help safeguard user privacy and prevent unauthorized access to personal or confidential data.

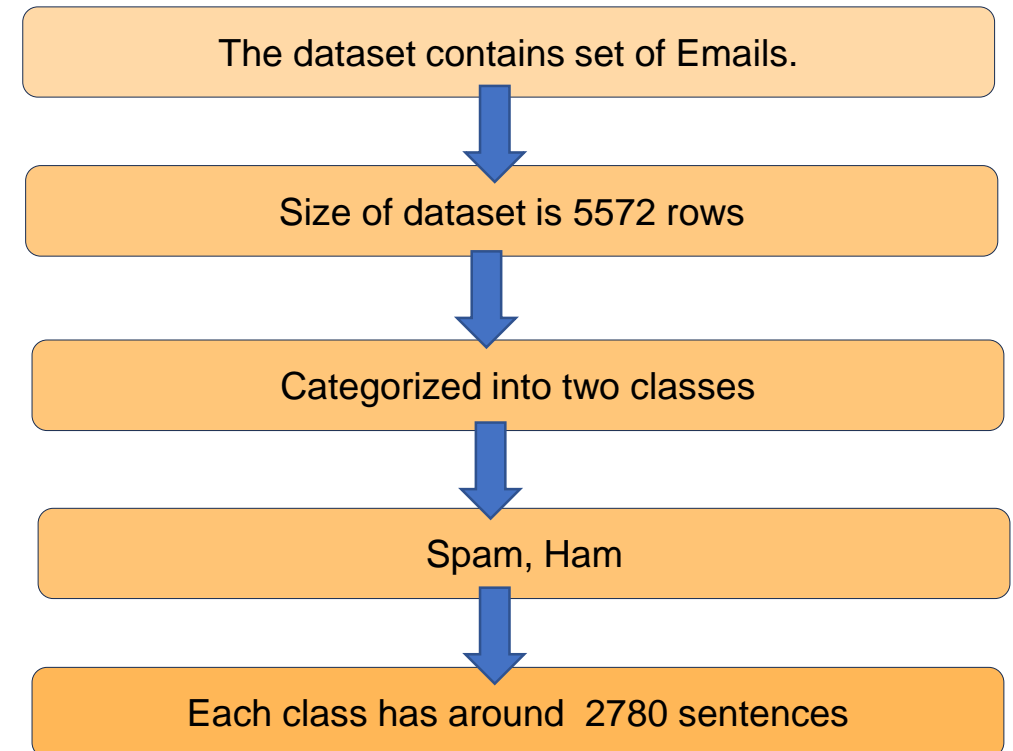
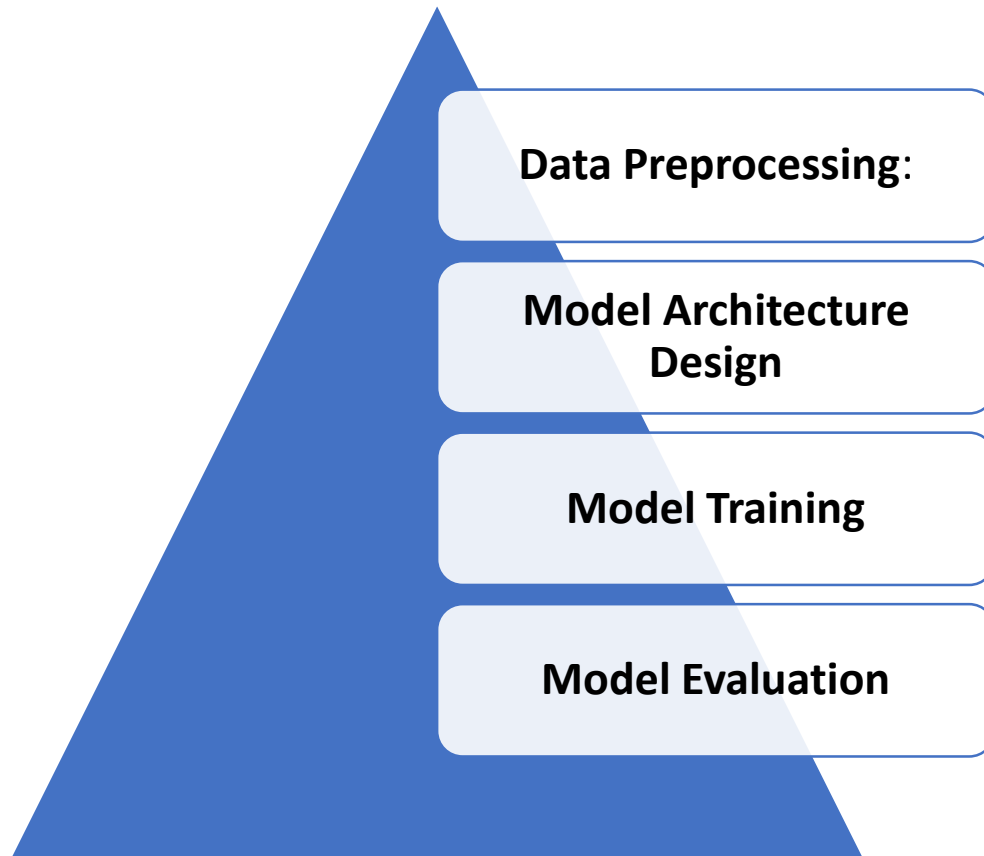
PROPOSED SOLUTION

- i. A novel email spam detection solution leveraging the Tensor Flow framework, a versatile tool for building and training deep learning models.
- ii. Feature engineering techniques such as tokenization, word embeddings, and feature scaling are applied to transform raw data into a format suitable
- iii. We train the deep learning model on a labeled dataset of spam and legitimate emails using Tensor Flow's powerful optimization algorithms
- iv. Our solution combines deep neural networks with feature engineering and real-time monitoring to achieve high detection accuracy to evolving spam tactics.



ALGORITHM

ALGORITHM :



DEPLOYMENT



Trained Logistic Regression model




Spam
(or)
Ham

Prediction

PROJECT DEMO(RECORDED VIDEO) & RESULT

Result :


Detecting Spam Emails SK.ipynb

File Edit View Insert Runtime Tools Help Commit & save changes

+ Code + Text Copy to Drive

```

import numpy as np
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import accuracy_score

```

```

[5]: # loading the data from csv file to pandas Dataframe
raw_mail_data = pd.read_csv('/content/mail_data.csv')

[ ] print(raw_mail_data)

```

	Category	Message
0	ham	Go until jurong point, crazy.. Available only in jurong point area...
1	ham	OK lar... taking wifi a bit...
2	spam	Free entry in 2 a wkly comp to win FA Cup final tkts 21st May 6pm-6pm. Text FA to 87121 to receive entry. Valid only for standard mobile phones. T&Cs apply.
3	ham	U dun say so early hor... U c already then say...
4	ham	Nah I don't think he goes to usf, he lives around here.
...
5562	spam	This is the 2nd time we have tried to contact u... please reply so we can stop trying.
5568	ham	Will u b going to esplanade fr home?
5569	ham	Pity, * was in mood for that. No...any other s...
5570	ham	The guy did some hitching but I acted like I'd...
5571	ham	Nuff. It's true to its name.
...

```

[5572 rows x 2 columns]

```

```

[6]: # replace the null values with a null string
mail_data = raw_mail_data.where((pd.notnull(raw_mail_data)), '')

```

Done compiled at 12:08 PM

```

input_mail = ["SIX chances to win CASH! From 100 to 20,000 pounds txt> CSH11 and send to 87575. Cost 150p/day, 6days, 16+ Txts apply Reply HL 4 info"]

# convert text to feature vectors
input_data_features = feature_extraction.transform(input_mail)

# making prediction

prediction = model.predict(input_data_features)
print(prediction)

if (prediction[0]==1):
    print('Ham mail')

else:
    print('Spam mail')

[0]
Spam mail

```

CONCLUSION

In conclusion,

The future scope of email spam detection using Tensor Flow is vast and promising, with opportunities for advancements in model architectures, multi-modal learning, adversarial robustness, interpretability, semi-supervised learning, privacy preservation, and real-time adaptation. By leveraging the capabilities of Tensor Flow and exploring these avenues of research, we can develop more effective, robust, and privacy-preserving spam detection systems to combat the ever-evolving threat of email spam



FUTURE SCOPE

- i. **Enhanced Model Architectures** : Future research in email spam detection using Tensor Flow will likely focus on designing more complex and efficient deep learning architectures tailored specifically for email data.
- ii. **Adversarial Robustness** : Adversarial attacks pose a significant threat to spam detection systems, as spammers continuously devise evasion tactics to bypass filters.
- iii. **Interpretability and Explainability** : As email spam detection systems become more complex, ensuring interpretability and explain ability of model decisions becomes increasingly important.

Email spam detection, an essential aspect of cyber security, has witnessed significant advancements in recent years, driven by innovations in machine learning and deep learning technologies.



REFERENCES

- <https://ieeexplore.ieee.org/document/10170187>
- [https://www.cell.com/heliyon/pdf/S2405-8440\(18\)35340-4.pdf](https://www.cell.com/heliyon/pdf/S2405-8440(18)35340-4.pdf)
- <https://www.coursera.org>
- https://www.researchgate.net/publication/363589502_SpamDL_A_High_Performance_Deep_Learning_Spam_Detector_Using_Stanford_Global_Vectors_and_Bidirectional_Long_Short-Term_Memory_Neural_Networks



THANK YOU