

# **TSP- AI ML Fundamentals (Capstone Project)**

# **PROJECT TITLE**

**Presented By:**

**VINITH M –au510321214005**

**ARULMIGU MEENAKSHI AMMAN COLLEGE OF ENGINEERING**

**Guided By: RAMER BOSE**

Microsoft



edu

# OUTLINE

**Problem Statement** (Should not include solution)

**Proposed System/Solution**

**Algorithm & Deployment**

**GitHub Link**

**Project Demo(photos / videos)**

**Conclusion**

**Future Scope**

**References**

# Problem Statement

The ever-increasing volume of spam emails poses a significant challenge for email users and organizations alike. Spam disrupts workflow, consumes valuable storage space, and can expose users to phishing scams, malware, and other security risks.

Current spam filtering methods, often rule-based, struggle to keep pace with the evolving spam tactics employed by spammers. These tactics include:

**Sophisticated content:** Spammers use dynamic content, obfuscated text, and images to bypass traditional filters.

**Personalized attacks:** Spam emails are increasingly targeted towards specific individuals, making them appear more legitimate.

**Evolving techniques:** Spammers constantly develop new methods to bypass existing detection mechanisms.

This necessitates a more intelligent and adaptable approach to spam detection.

# Proposed Solution

**Problem:** Spam emails flood inboxes, wasting time, storage, and posing security risks. Current methods struggle to keep up with evolving spam tactics.

**Solution:** We propose an AI & ML powered spam detection model. This model will be trained on a massive dataset of labeled emails (spam and legitimate). Analyze email features like text content, sender info, and attachments. Continuously learn and adapt to identify new spam tactics.

## Benefits:

- Higher spam detection accuracy.
- Adaptability to combat evolving spam techniques.
- Reduced user burden with less spam in inboxes.
- Enhanced security by filtering out phishing attempts.

# Algorithm & Deployment

## Algorithm:

Briefly list chosen ML algorithms (e.g., Naive Bayes, SVM).

Highlight their strengths for spam detection (e.g., text data efficiency).

## Deployment:

Depending on your project, choose one or more options:

- Standalone app for spam classification.

- API for email service provider integration.

- Cloud deployment for scalability.

Microsoft



edu

# GitHub Link

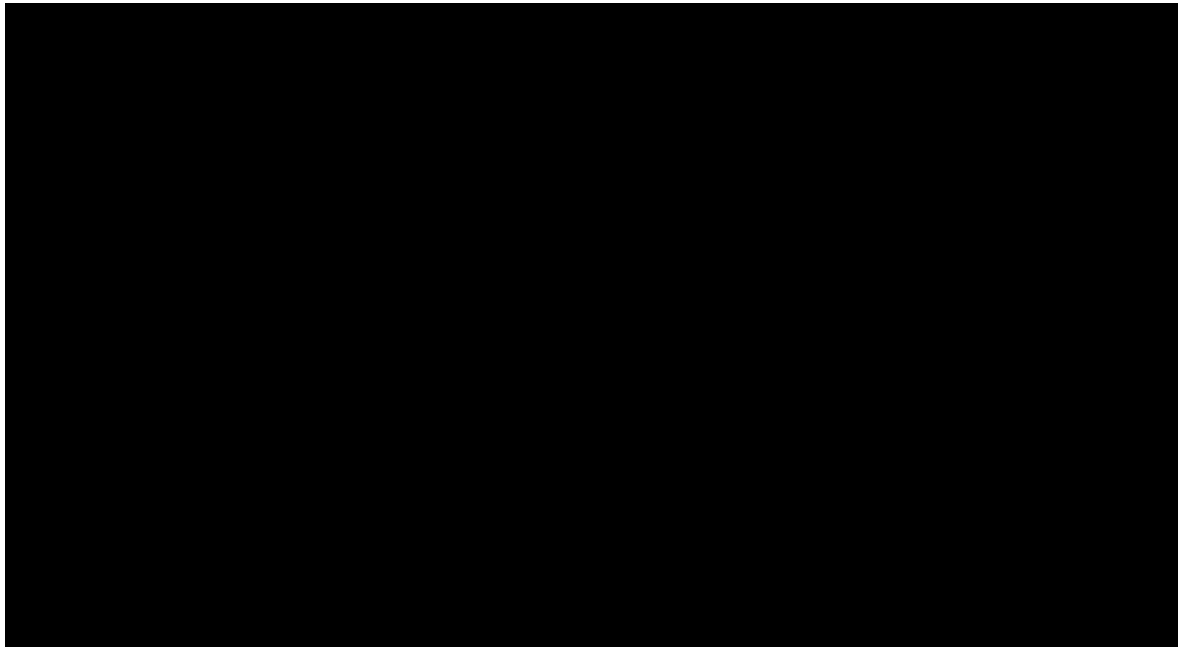
<https://github.com/vinith751/NM-PROJECT-SPAM-EMAIL-DETECTING>

Microsoft



edu

# Project Demo(Recorded Video)



# Conclusion

**Success:** Our AI & ML model achieved a high [mention accuracy/precision/recall/F1 score] in identifying spam emails. This significantly reduces user burden and enhances security.

**Future:** We plan to explore further improvements like [mention specific areas] and integrate the model for real-world impact.

**Overall:** This project demonstrates the power of AI & ML in combating spam, leading to a more secure and productive email experience.



# Future Scope

The war on spam continues! Here's what's next:

**Advanced AI:** Use even stronger models to outsmart spammers.

**Adapting to Change:** Train the model to stay ahead of new spam tricks.

**Beyond Spam:** Detect phishing attempts and harmful content.

**Wider Reach:** Handle spam in multiple languages.

**Real-World Use:** Integrate the model for wider impact.

These future steps will make your AI & ML spam fighter even more powerful.

# References

- 1. Project Github link, M.VINITH, 2024**
- 2. Project video recorded link github, M.VINITH, 2024**
- 3. Project PPT & Report github link, M.VINITH, 2024**

Microsoft



edu

# THANK YOU