AI Based Protocols for Spam Email Detection

B.Tech (AIDS)
UG-II (III-Semester)

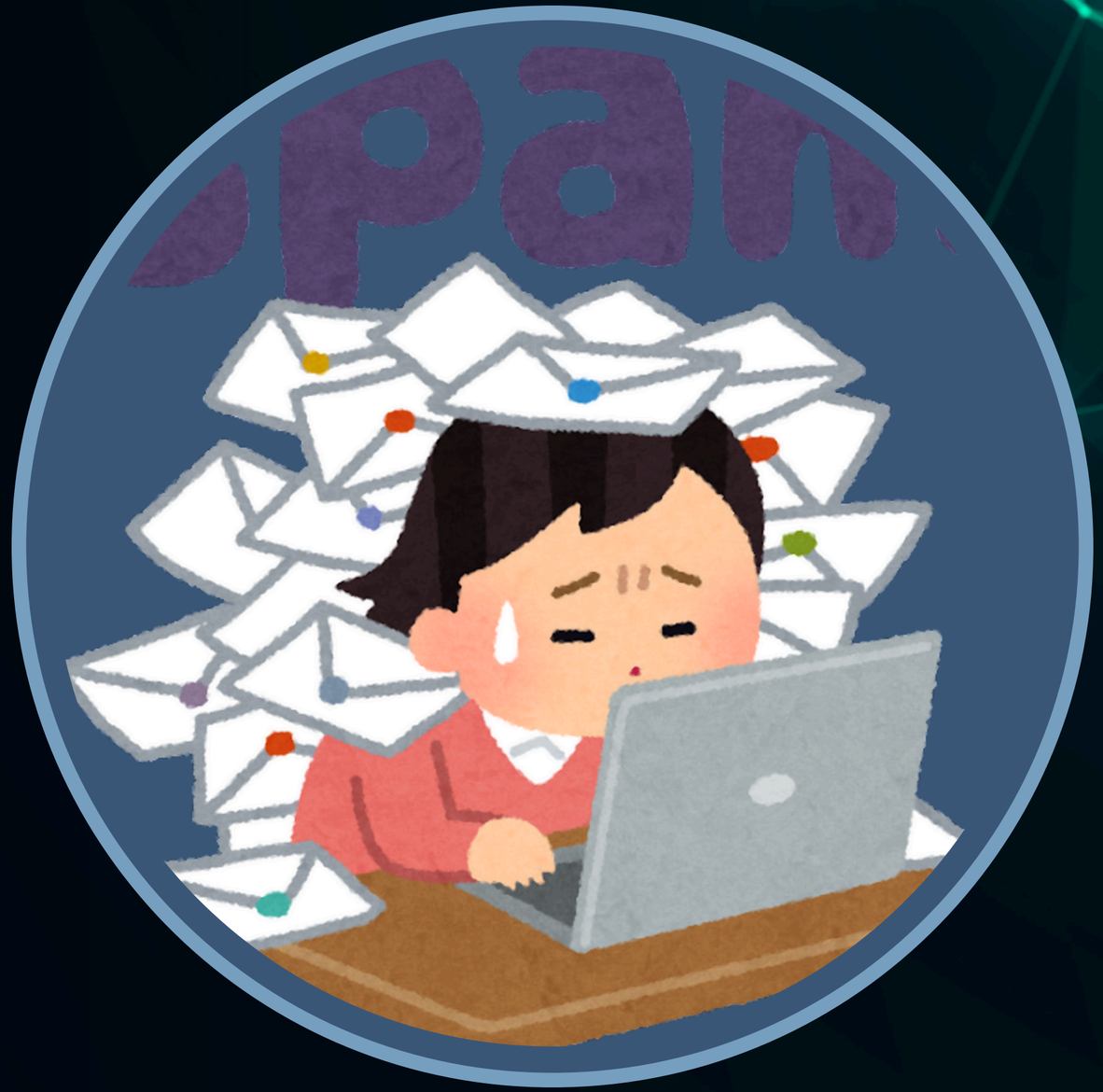
Subject Coordinator
Mr. Vivek Patel
Dr. Divyanshu Sinha

Presented By:
DHWANIT SHARMA (DL.AI.U4AID24111)
KANAN GOEL (DL.AI.U4AID24017)
PARKHI MAHAJAN (DL.AI.U4AID24126)
PUNIT LOHAN (DL.AI.U4AID24127)

AMRITA VISHWA VIDYAPEETHAM, DELHI NCR, FARIDABAD
Department of Artificial Intelligence & Data Science (AIDS)

INTRODUCTION

Email is a fundamental service in computer networks, but its underlying protocol, SMTP, is highly vulnerable to spam attacks. Traditional filtering methods fail against modern, intelligent spam. This project integrates Artificial Intelligence into the email protocol workflow to detect and block spam at the Application Laye

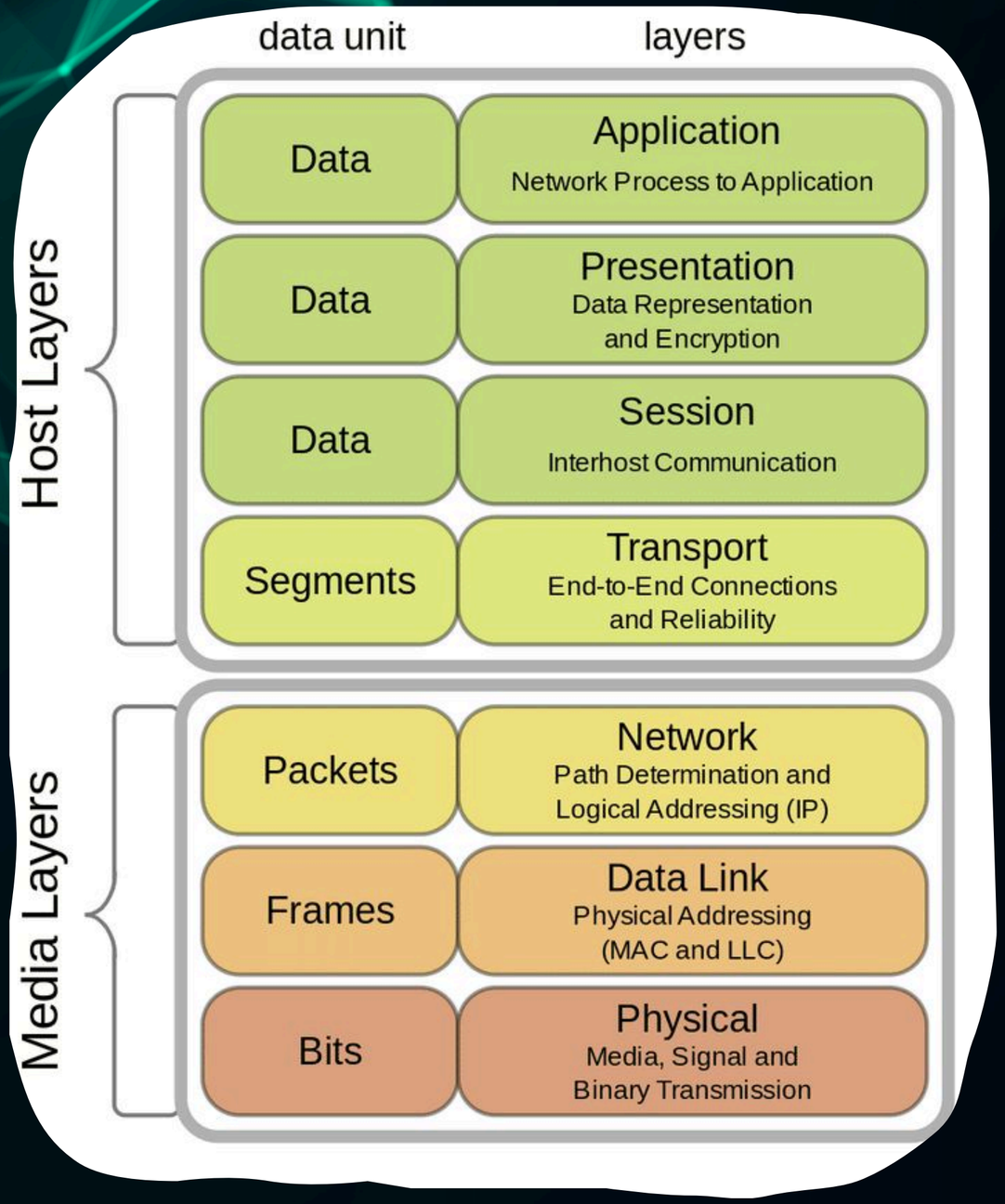


PROBLEM STATEMENT

- Spam emails bypass rule-based filters
- Static firewalls are ineffective
- Need intelligent, content-based detection

OUR MISSION / OBJECTIVES

- Develop AI-based spam classifier
- Simulate SMTP protocol behavior
- Perform real-time email inspection
- Improve network security
- Develop a Real-Time User Interface



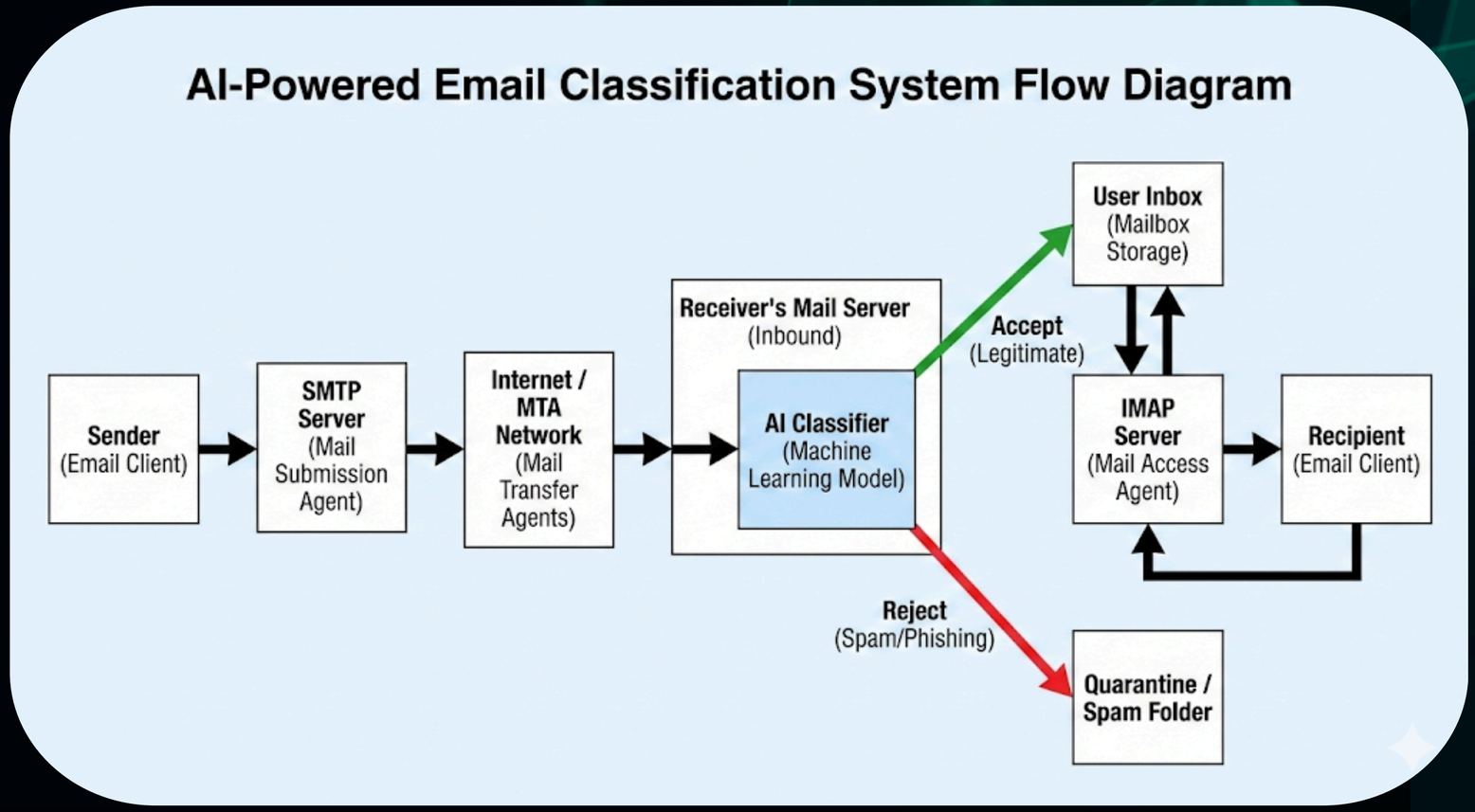
RELEVANCE TO COMPUTER NETWORK

This project operates at the Application Layer (Layer 7 of the OSI Model). It inspects the payload of email packets rather than relying on IP or port-based rules. By integrating AI with SMTP and IMAP protocols, the system demonstrates intelligent packet-level decision-making.

SYSTEM ARCHITECTURE

Two main modules:

- AI Analysis Engine
- Network Protocol Simulation

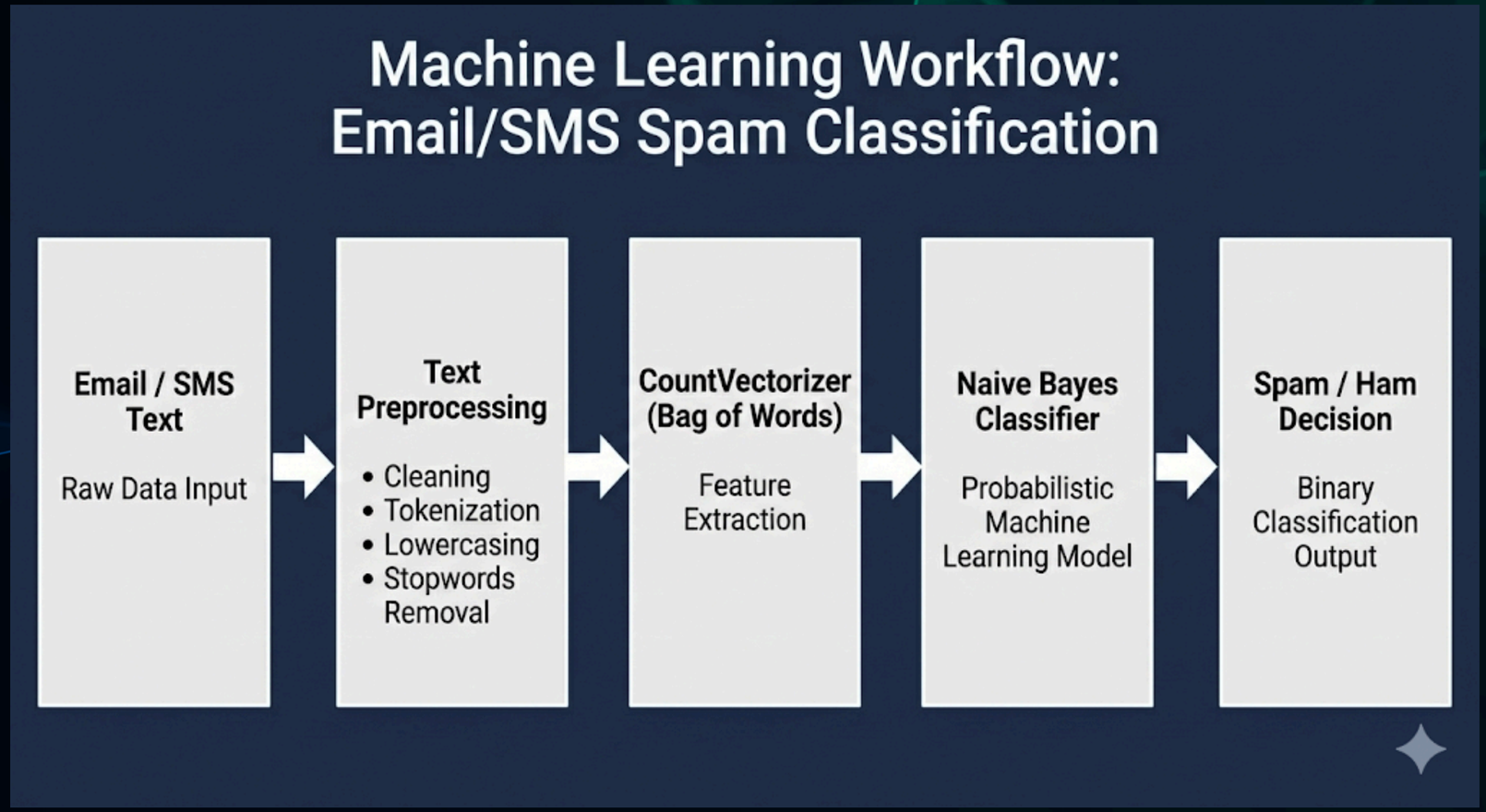


AI ANALYSIS ENGINE

The AI engine uses the Naive Bayes algorithm, chosen for its low computational cost and fast execution. The model is trained on the SMS Spam Collection dataset. Text data is converted into numerical vectors using Bag-of-Words representation before classification.

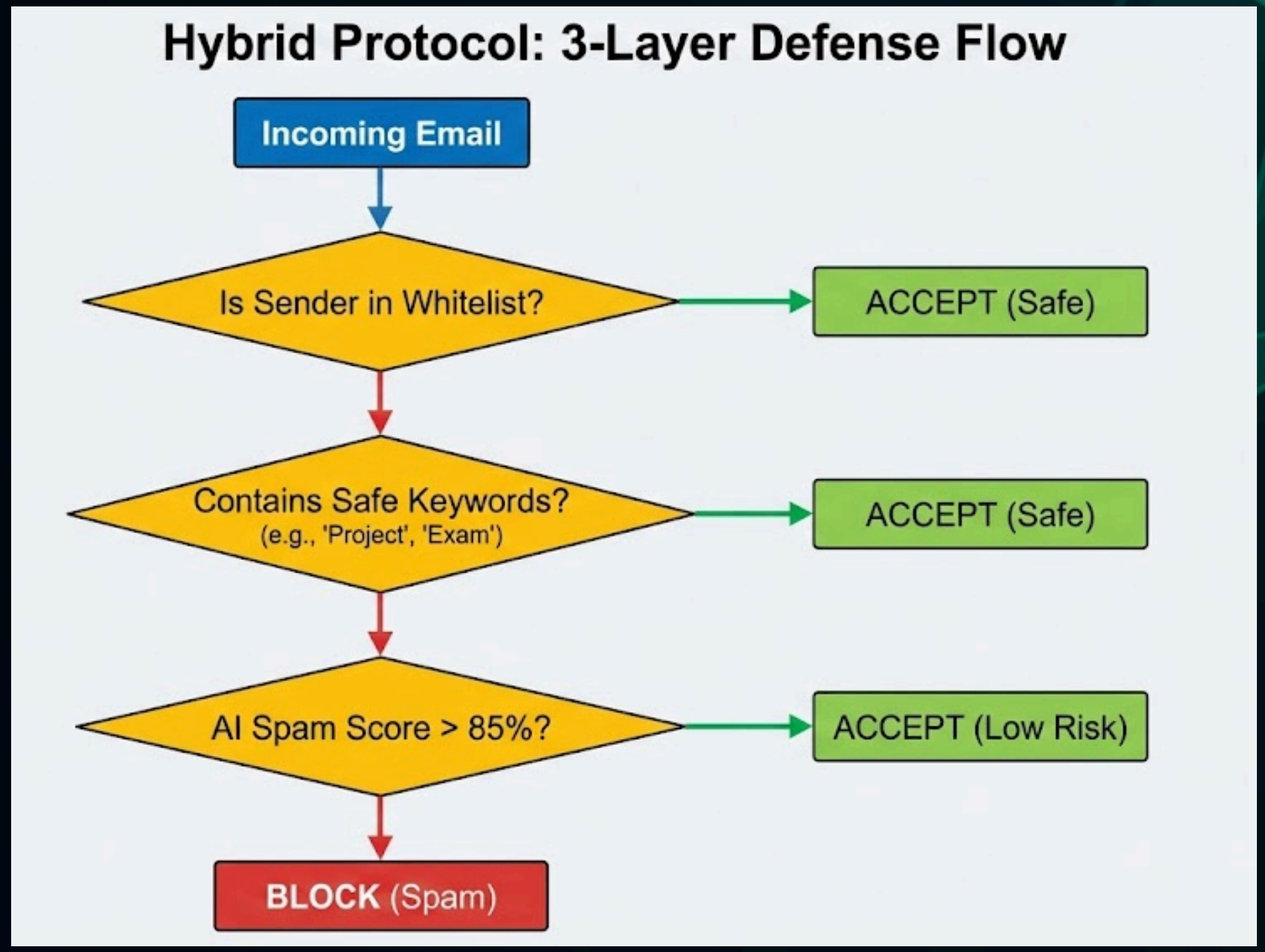
MACHINE LEARNING WORKFLOW

- Dataset collection
- Text preprocessing
- Vectorization
- Model training
- Prediction



THE HYBRID PROTOCOL

- **The Challenge:** Pure AI often blocks legitimate, urgent emails (False Positives).
- **Layer 1 (Whitelist):** Bypasses AI for trusted domains (e.g., google.com) to ensure zero latency.
- **Layer 2 (Heuristics):** Safety override for essential keywords (e.g., "Syllabus", "Interview").
- **Layer 3 (AI Threshold):** Blocks only when confidence exceeds 85% (vs. standard 50%).



SMTP SIMULATION AND IMAP REAL-TIME EMAIL INTEGRATION

This project integrates email protocols at the application layer. SMTP behavior is simulated to inspect incoming email payloads and generate standard response codes such as 250 OK or 550 Rejected based on AI classification. IMAP is used to connect to a real Gmail server to fetch, parse, and analyze live emails securely.

RESULTS

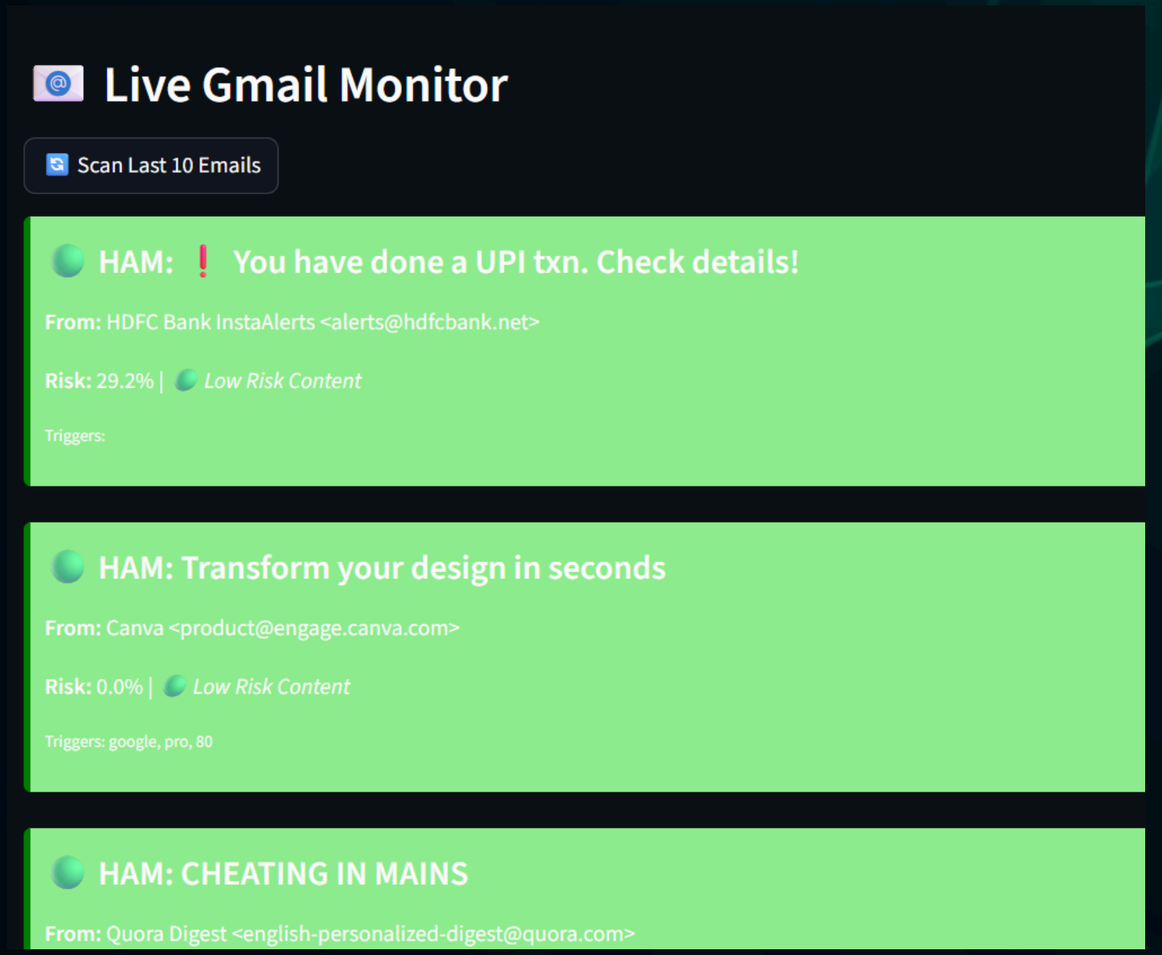
- ## MODEL PERFORMANCE
  - Accuracy: 97.58% (Primary)
  - Accuracy: 92.19% (Primary)
  - High precision & recall
  - Low false positives

- ## NETWORK OUTPUT
  - Spam → 550 Rejected
  - Safe → 250 OK
  - Trigger words detected

Class	Precision	Recall	F1-Score
Ham (Safe)	0.99	0.98	0.98
Spam	0.95	0.96	0.96

REAL-TIME INTELLIGENCE DASHBOARD

- **Real-Time Monitoring:** Streamlit frontend visualizes live IMAP traffic (Port 993).
- **Granular Scoring:** Assigns precise risk percentages (e.g., 97.3%) instead of binary pass/fail.
- **Explainable AI:** Displays specific "Trigger Words" (e.g., lottery, urgent) for full transparency.
- **Hybrid Visualization:** Visually distinguishes between Keyword-safe emails and AI-blocked threats.



CONCLUSION AND FUTURE SCOPE

- AI + CN successfully integrated
- Content-aware filtering
- Better than static firewalls

Future Scope

- Deep learning models
- Proxy server deployment
- Multi-language support

THANK YOU!