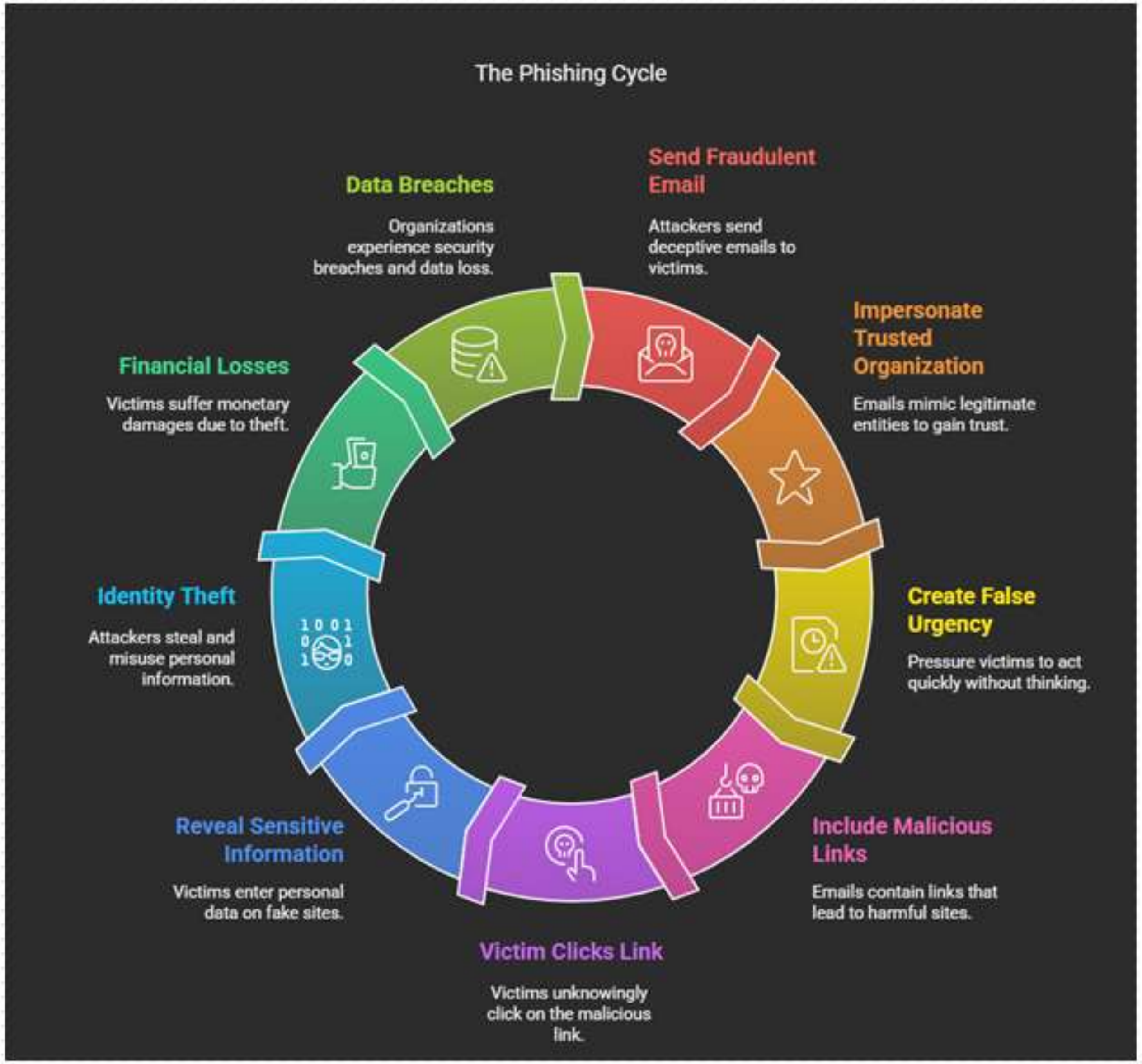
BYTE BASH 2025

DOMAIN : AI/ML

PROJECT NAME: PHISHING EMAIL DETECTOR

TEAM RJ
BY ROHAN JAIN
EMAIL: 23f2002461@ds.study.iitm.ac.in
CONTACT INFO: 8910225465

Introduction to Phishing Attacks



The Phishing Cycle

Send Fraudulent Email

Attackers send deceptive emails to victims.

Impersonate Trusted Organization

Emails mimic legitimate entities to gain trust.

Create False Urgency

Pressure victims to act quickly without thinking.

Include Malicious Links

Emails contain links that lead to harmful sites.

Victim Clicks Link

Victims unknowingly click on the malicious link.

Reveal Sensitive Information

Victims enter personal data on fake sites.

Identity Theft

Attackers steal and misuse personal information.

Financial Losses

Victims suffer monetary damages due to theft.

Data Breaches

Organizations experience security breaches and data loss.

What is Phishing?

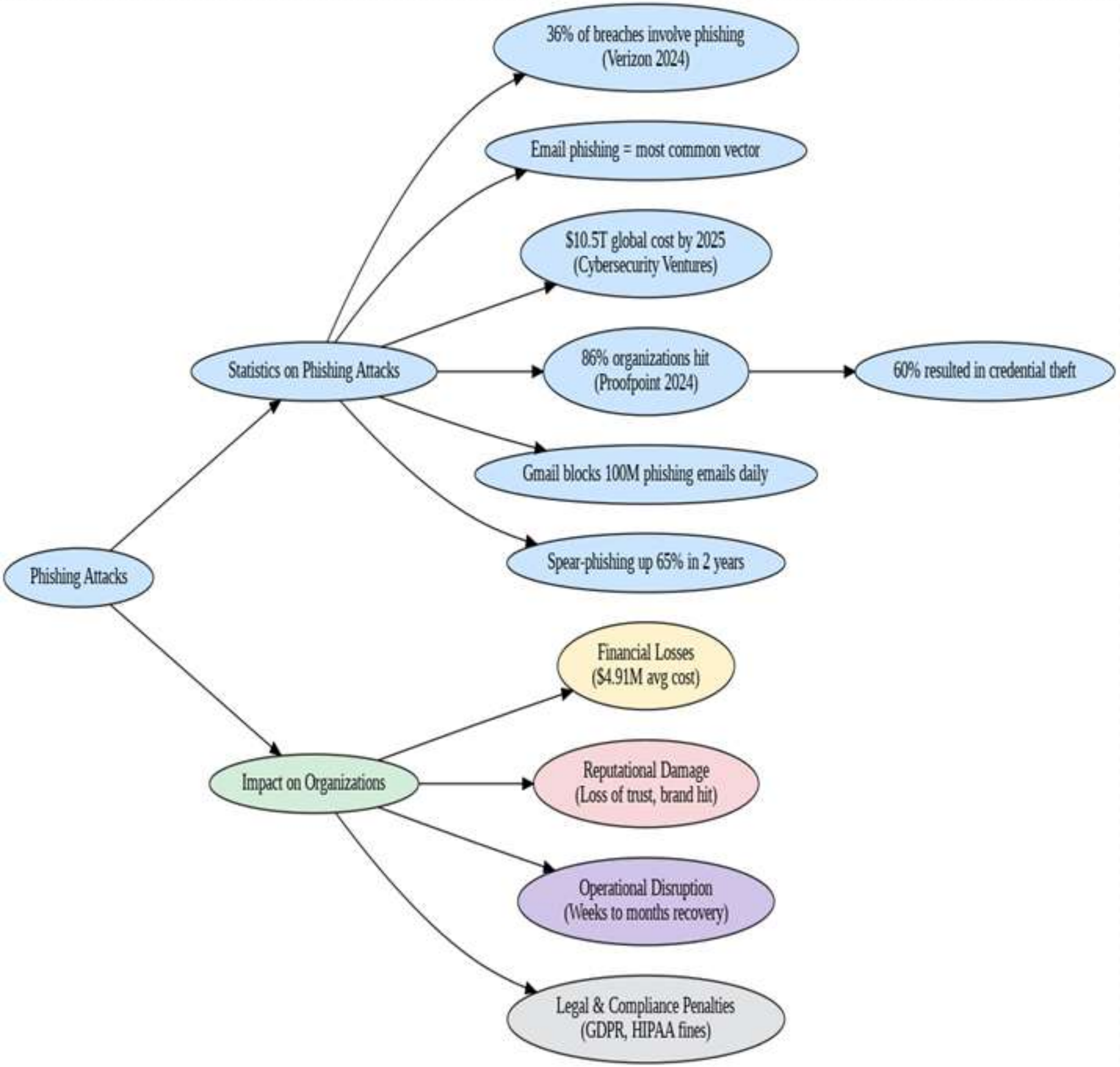
Phishing is a deceptive practice where attackers send fraudulent emails or messages to trick users into revealing sensitive information or performing harmful actions.

Common Phishing Tactics

Phishing emails often impersonate trusted organizations, create a false sense of urgency, and include malicious links or attachments.

Consequences of Phishing

Successful phishing attacks can lead to identity theft, financial losses, and data breaches, causing significant harm to both individuals and organizations.



Phishing Attacks

Statistics on Phishing Attacks

36% of breaches involve phishing (Verizon 2024)

Email phishing = most common vector

$10.5T global cost by 2025 (Cybersecurity Ventures)

86% organizations hit (Proofpoint 2024)

60% resulted in credential theft

Gmail blocks 100M phishing emails daily

Spear-phishing up 65% in 2 years

Impact on Organizations

Financial Losses ($4.91M avg cost)

Reputational Damage (Loss of trust, brand hit)

Operational Disruption (Weeks to months recovery)

Legal & Compliance Penalties (GDPR, HIPAA fines)

<u>**Challenge**</u>	<u>**Explanation**</u>
Sophisticated Phishing Techniques	Attackers use personalized ("spear-phishing") emails that are extremely hard to detect.
Social Engineering Tactics	Attackers psychologically manipulate users to trust and click malicious links.
Bypass of Traditional Filters	Modern phishing emails often evade simple keyword-based or blacklist-based email filters.
Use of Zero-Day Links	Attackers create brand new phishing URLs that aren't recognized by blacklists at the time of attack.
Encrypted Phishing	HTTPS is now used in **over 80%** of phishing websites, making detection harder.
Email Spoofing and Brand Impersonation	Attackers perfectly mimic well-known brands, making fraudulent emails appear legitimate.
Mobile Device Vulnerability	Phishing detection tools are weaker on mobile apps, where users are more likely to click suspicious links.

PROPOSAL

Project Overview

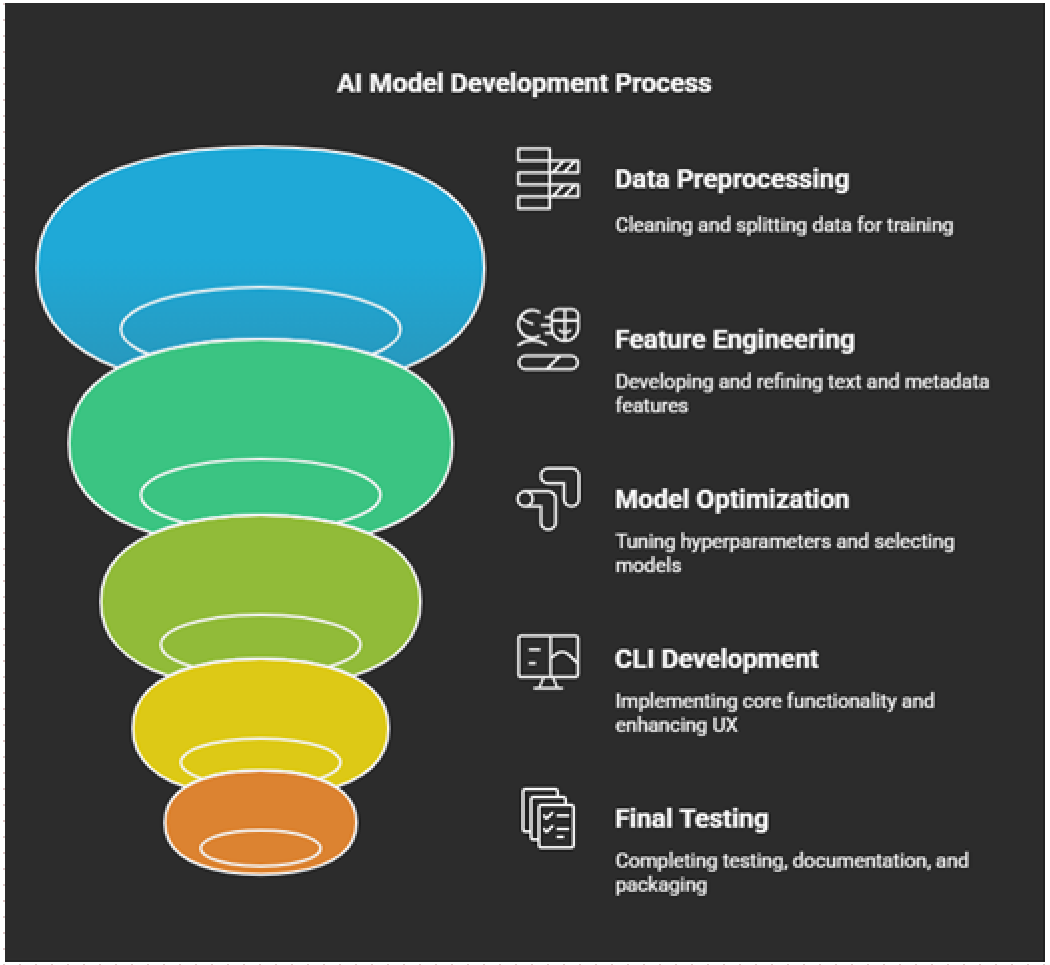
The Phishing Email Detector will analyze email content to determine if it's legitimate or a phishing attempt. Users will paste email text into a CLI application, which will return a binary classification **(PHISHING or LEGITIMATE).**

OBJECTIVE:

•☑ Successfully develop a **Phishing Email Detection System** using Machine Learning techniques.
•☑ Achieve high **accuracy**, **ROC-AUC**, and **reliable classification** between **Phishing** and **Legitimate** emails.
•☑ Build a **Command-Line Interface (CLI) Application** for easy user interaction

Model Building

•Preprocessing: Lowercasing, removing punctuations, stopwords.
•TF-IDF Vectorization.
•Model: Logistic Regression (Best results in text classification).



AI Model Development Process

Data Preprocessing
Cleaning and splitting data for training

Feature Engineering
Developing and refining text and metadata features

Model Optimization
Tuning hyperparameters and selecting models

CLI Development
Implementing core functionality and enhancing UX

Final Testing
Completing testing, documentation, and packaging

Step	Details
1	**Dataset Collection** - CSV of emails and labels.
2	**Preprocessing** - Clean text (remove stopwords, punctuations, lowercase).
3	**Feature Engineering** - Convert text to numerical format using TF-IDF
4	**Model Training** - Train on 80% data, validate on 20% test set.
5	**Model Evaluation** - Use Accuracy, Confusion Matrix, ROC Curve, Classification Report.
6	**Save Model** - Save using joblib or pickle.
7	**CLI App** - Build a command-line app to input email text and predict.

Testing

- **Unit Testing**: Verify model predictions.
- **CLI Testing**: Ensure smooth user experience.

Hyperparameter Tuning

The selected model will be fine-tuned through rigorous hyperparameter optimization, ensuring the best possible performance on both the training and validation datasets.

Model Evaluation

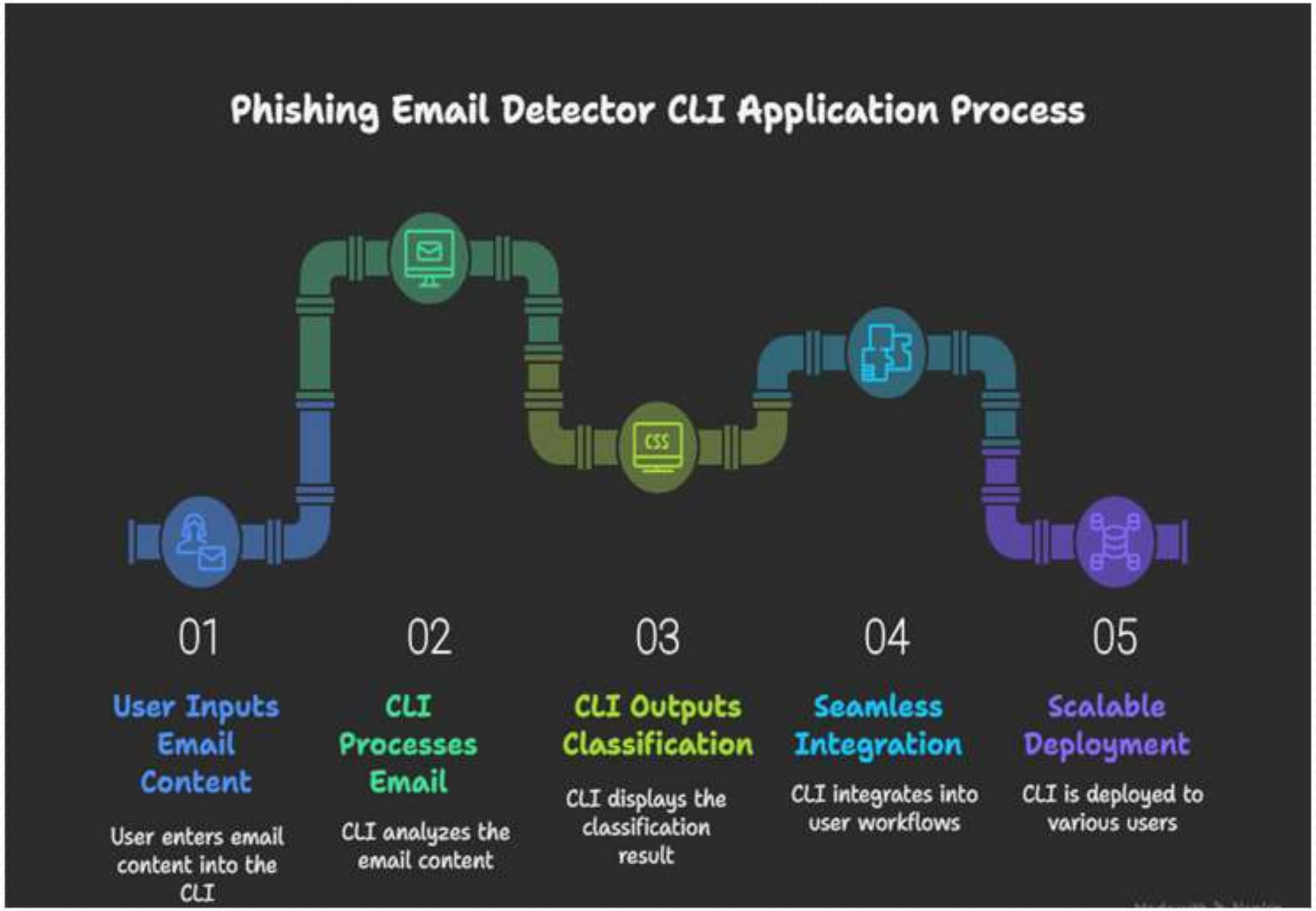
The trained model will be thoroughly evaluated using relevant metrics, such as accuracy, precision, recall, and F1-score, to validate its effectiveness in accurately detecting phishing emails.

Evaluate & Visualize Model Performance

We'll include:

- **Confusion Matrix**
- **Classification Report (Precision, Recall, F1)**
- **ROC Curve & AUC Score**
- **Accuracy Score**

Command-Line Interface (CLI) Application



Phishing Email Detector CLI Application Process

01 User Inputs Email Content

User enters email content into the CLI

02 CLI Processes Email

CLI analyzes the email content

03 CLI Outputs Classification

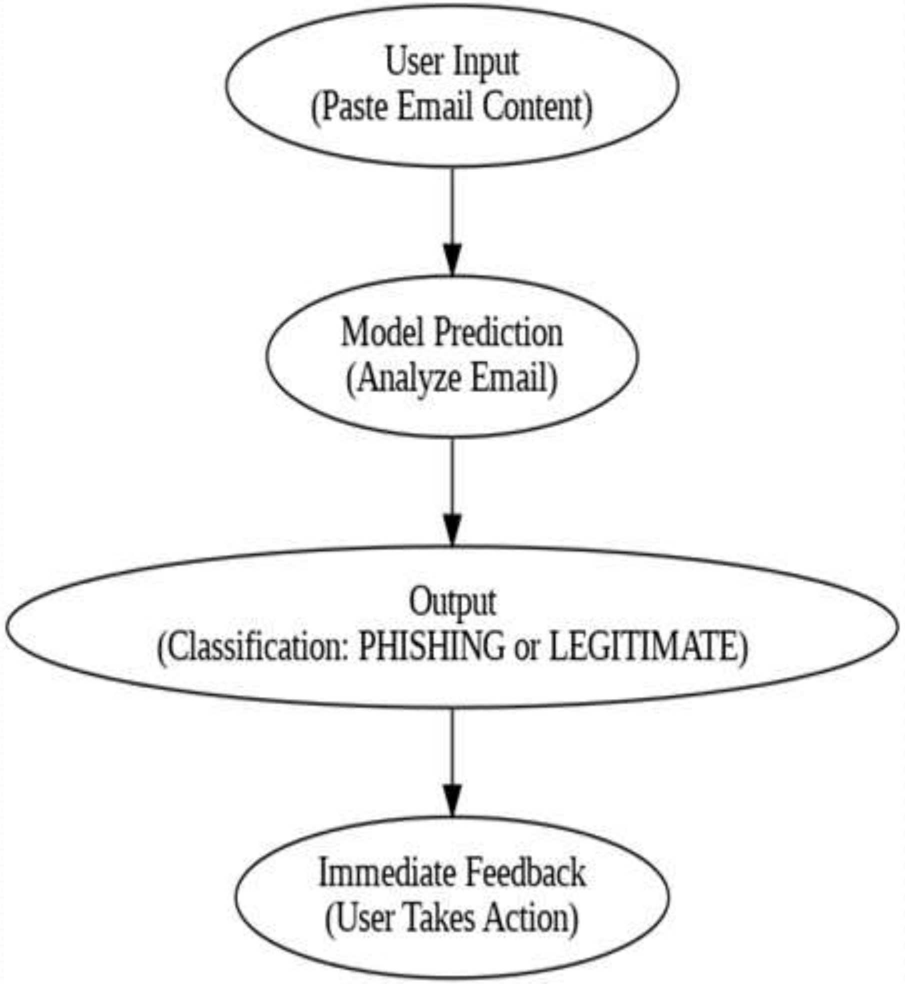
CLI displays the classification result

04 Seamless Integration

CLI integrates into user workflows

05 Scalable Deployment

CLI is deployed to various users



User Input (Paste Email Content)

Model Prediction (Analyze Email)

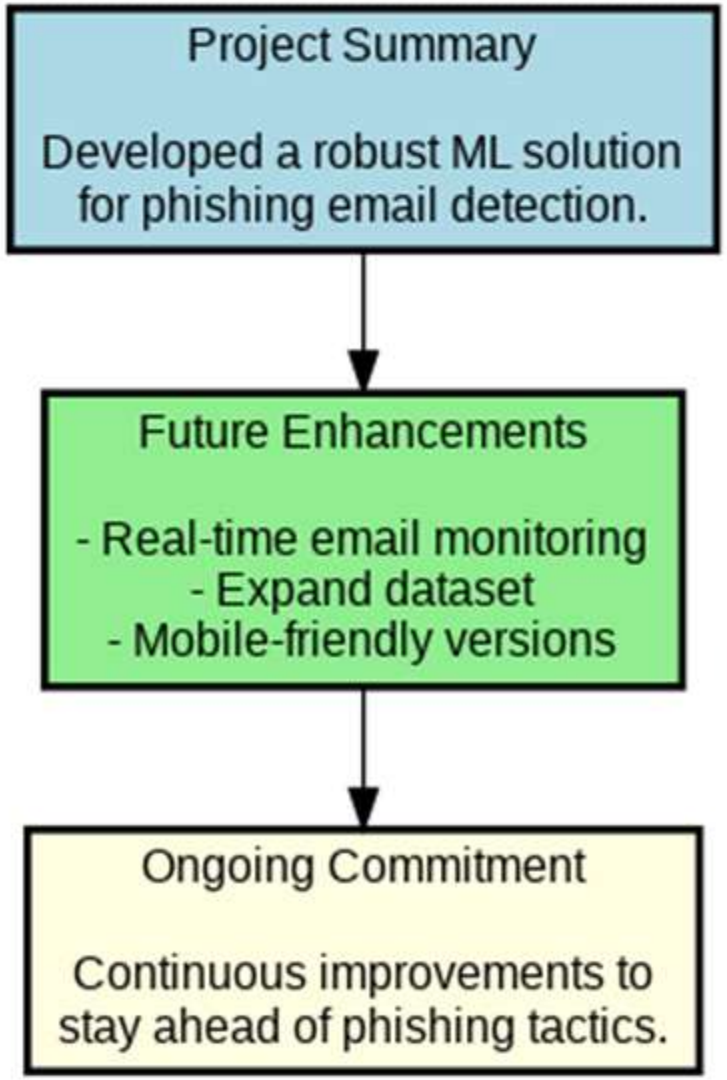
Output (Classification: PHISHING or LEGITIMATE)

Immediate Feedback (User Takes Action)

TECH STACK

Area	Tech Stack
Programming Language	Python 3.x
Machine Learning	Scikit-learn, Pandas, NumPy
Text Processing (NLP)	NLTK or Scikit-learn's TfidfVectorizer
Model Evaluation	Matplotlib, Seaborn
CLI App	Python's argparse / simple input() CLI
Version Control	Git, GitHub
Dataset	Public phishing email datasets (like Kaggle)

Conclusion and Future Enhancements



Project Summary

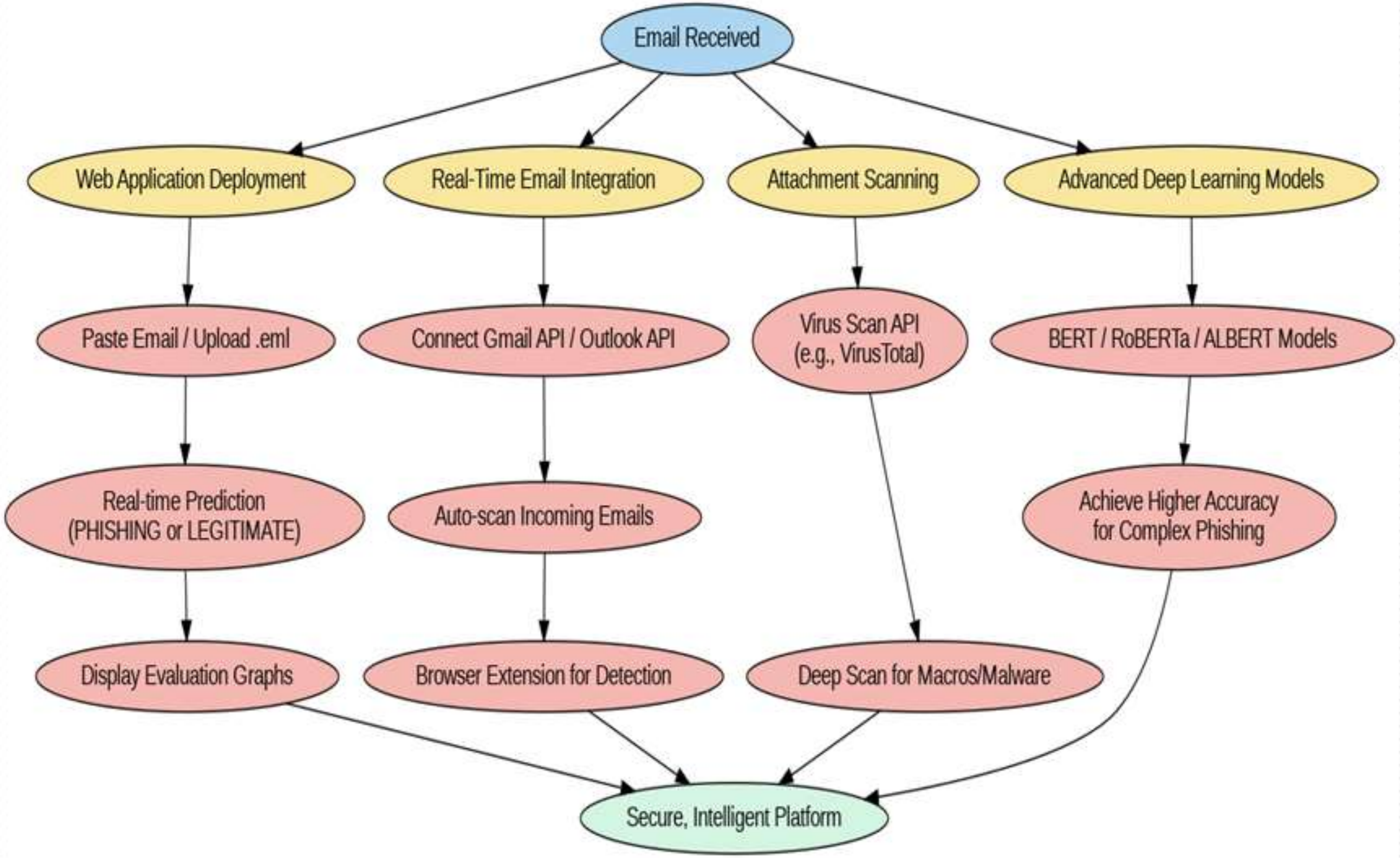
Developed a robust ML solution for phishing email detection.

Future Enhancements

- Real-time email monitoring
- Expand dataset
- Mobile-friendly versions

Ongoing Commitment

Continuous improvements to stay ahead of phishing tactics.



Email Received

Web Application Deployment

Real-Time Email Integration

Attachment Scanning

Advanced Deep Learning Models

Paste Email / Upload .eml

Connect Gmail API / Outlook API

Virus Scan API (e.g., VirusTotal)

BERT / RoBERTa / ALBERT Models

Real-time Prediction (PHISHING or LEGITIMATE)

Auto-scan Incoming Emails

Achieve Higher Accuracy for Complex Phishing

Display Evaluation Graphs

Browser Extension for Detection

Deep Scan for Macros/Malware

Secure, Intelligent Platform

THANK YOU