Project Title

Internship Phishing Email Detector

PHISHGUARD

~A simple Python tool to identify internship-based phishing scams.

Presented by : ARCHANA

Registration No. : 25BSA10127

Problem Statement

Many students receive fake internship offers through email.

These scams demand registration fee / processing charges / payment.

Students often click Google Forms & suspicious links without verification.

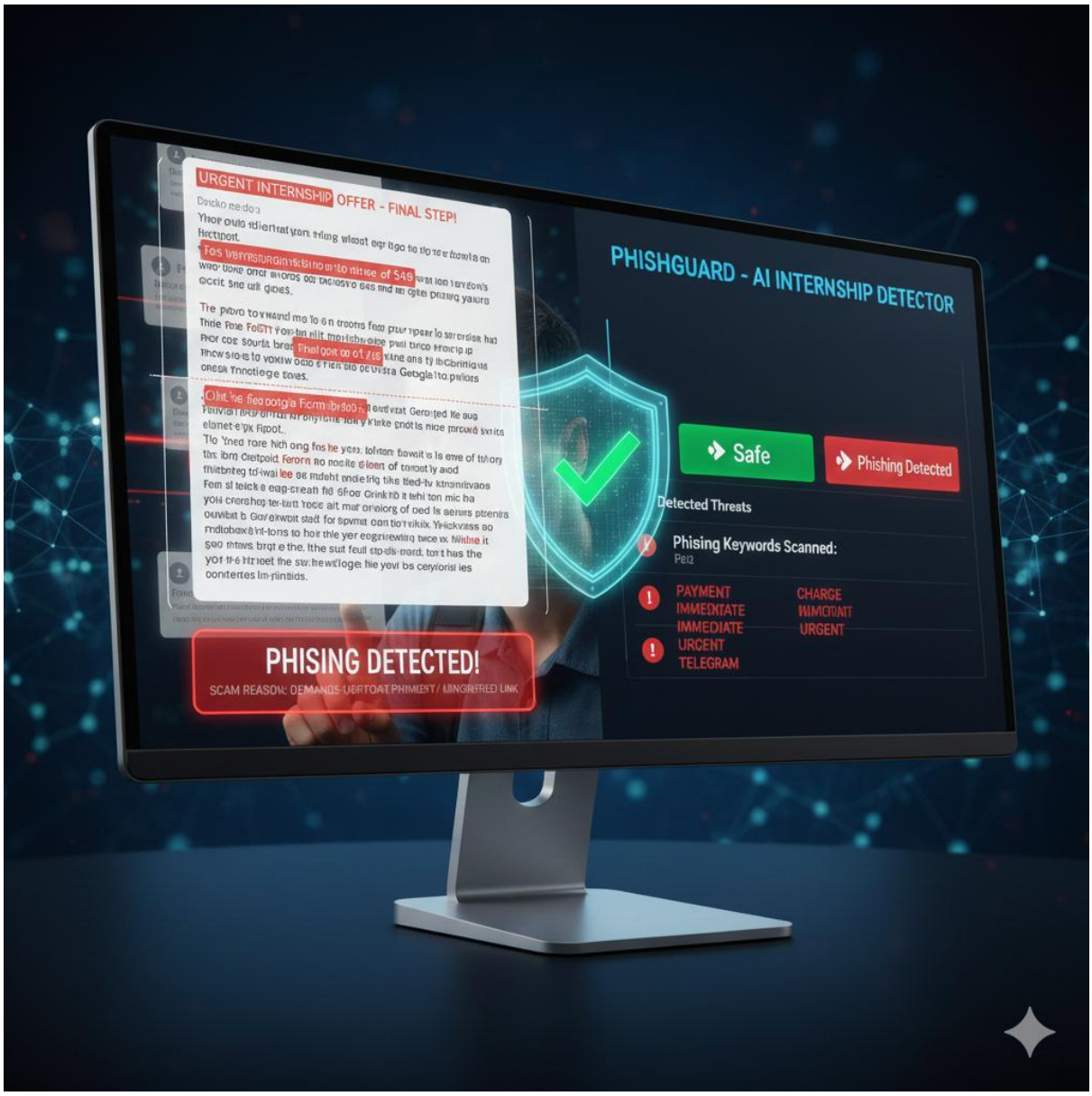
A tool is needed to detect such phishing emails automatically.

Objective

Analyse the email content and search for phishing-related keywords.

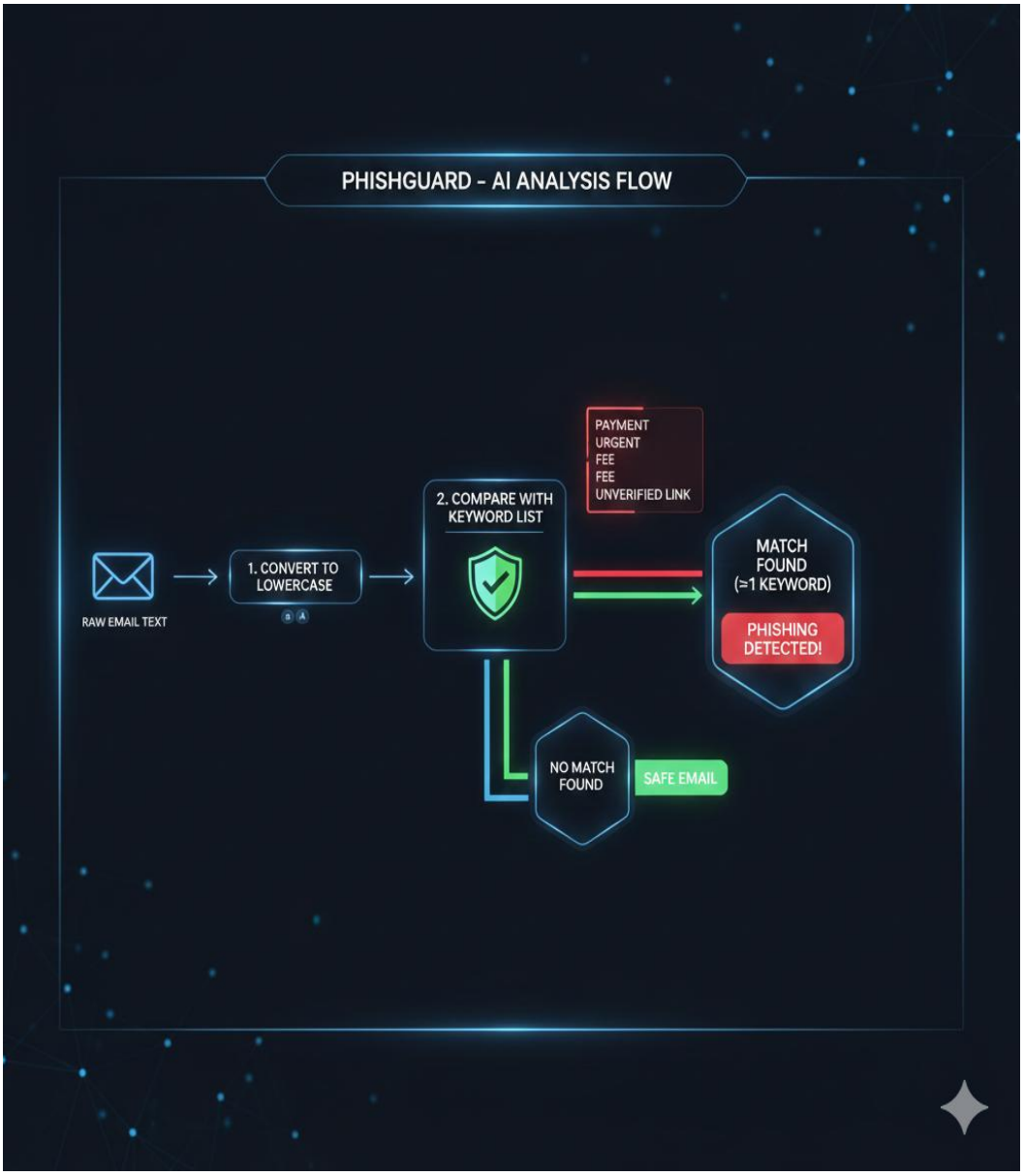
Classify emails as:

- Safe
- Phishing Detected



Methodology

- Convert email text to lowercase.
- Compare the text with a predefined phishing keyword list.
- If at least one keyword is matched → flag as Phishing Detected.
- Else → mark as Safe Email.



Python Program

```
def detect_internship_phishing(email):
    phishing_keywords = [
        "internship", "virtual internship", "apply now", "immediate joining",
        "hiring students", "summer internship", "registration fee",
        "processing charge", "payment required", "google form", "click here"
    ]

    email = email.lower()

    for word in phishing_keywords:
        if word in email:
            return "⚠ Phishing Detected!"

    return "✓ Safe Email"
```

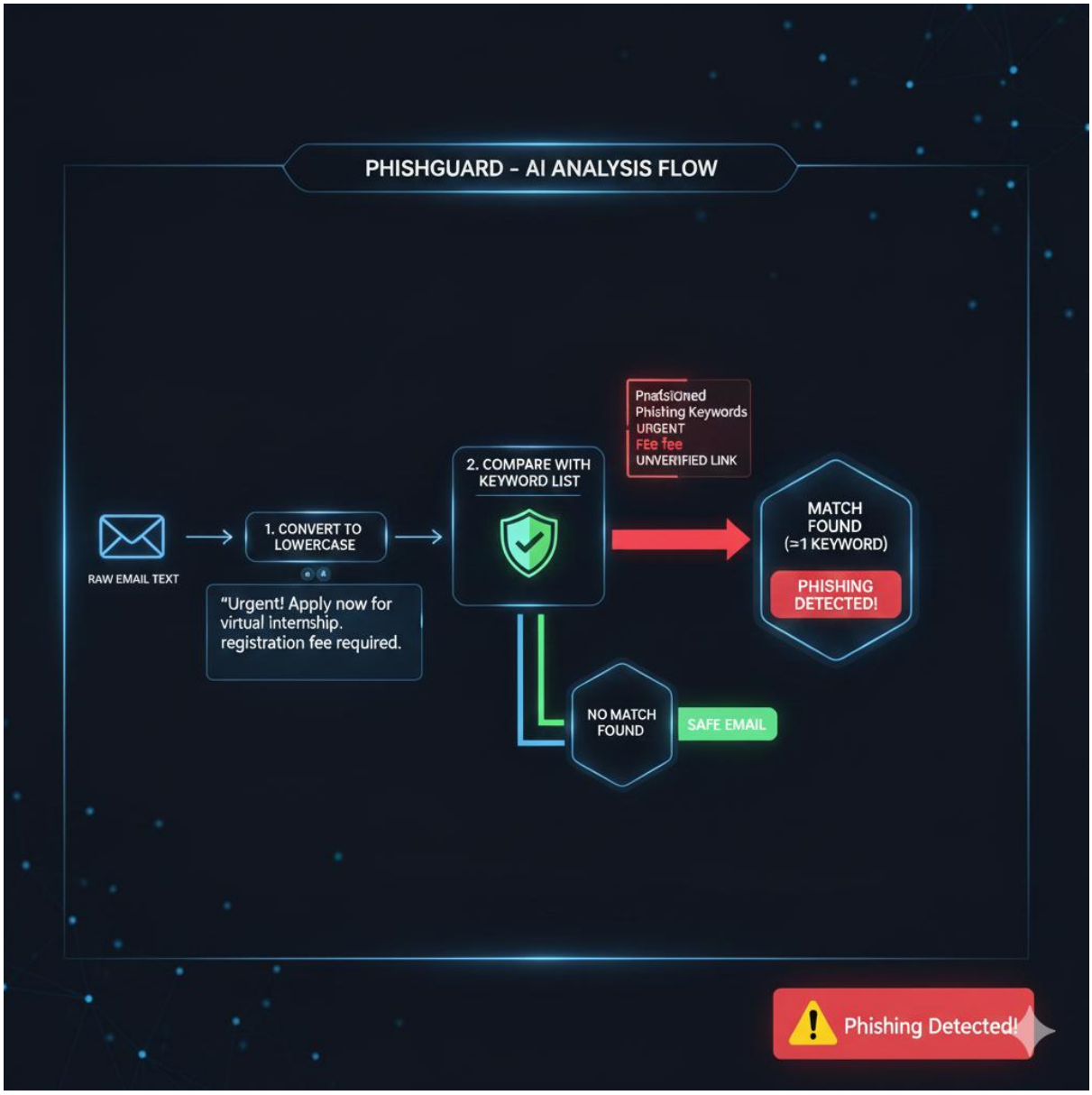
Example Input & Output:

Input Message:

“Urgent! Apply now for virtual internship. Registration fee required.”

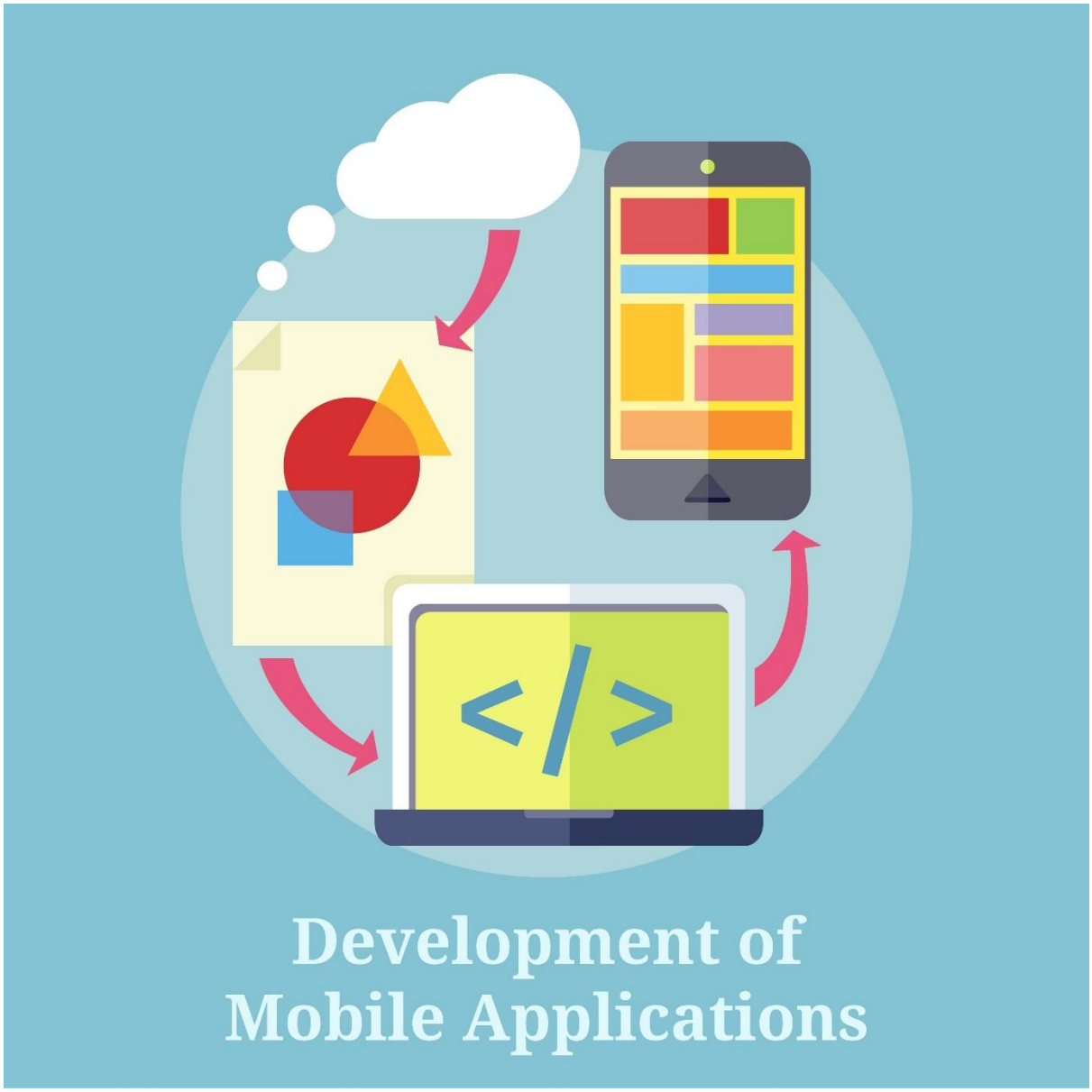
Output:

⚠ Phishing Detected!



Advantages

- Simple and fast detection
- Can be used by schools / colleges / placement cells
- Useful for students who are targeted frequently
- Can be upgraded into a web or mobile application
- **High Precision on Known Scams:** Provides near 100% accuracy when detecting common, explicit phishing patterns.
- **Cost-Effective & Maintainable:** Low computational resource requirement and the keyword list is easily customizable.



Functional Requirements

The project provides the following core functional capabilities:

Functional Module

Description

1. Email Input Module

Accepts email content from the user for analysis

2. Phishing Keyword Detection Module

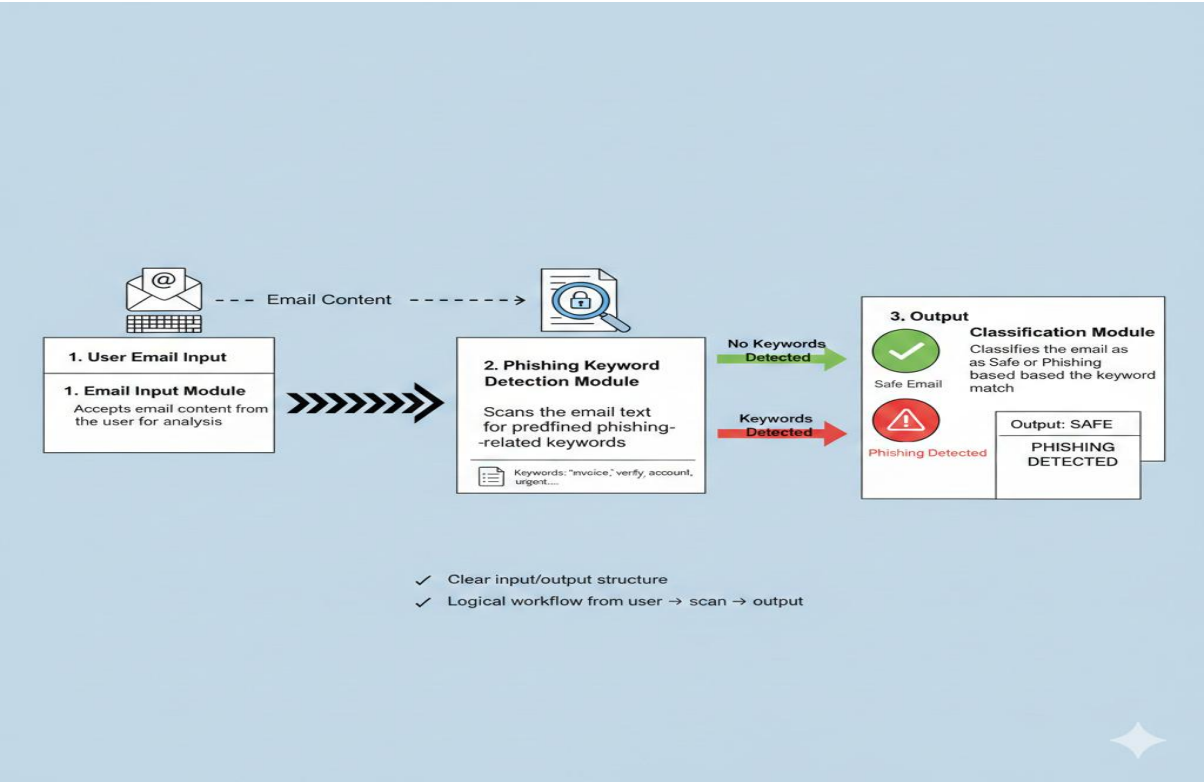
Scans the email text for predefined phishing-related keywords

3. Output Classification Module

Classifies the email as Safe or Phishing Detected based on keyword match

✓ Clear input/output structure

✓ Logical workflow from user → scan → output



Non-Functional Requirements

The system ensures the following quality attributes:

Performance: Detects phishing within seconds

Reliability: Accurate keyword-based detection method

Usability: Very simple to use for students & placement cells

Maintainability: Keyword list can be updated or expanded easily

Scalability (optional line): Program can evolve into website / application

System Architecture

Flow of the system:

User → Email Input → Keyword Detection Engine → Output Result

↓

Phishing Keyword Database

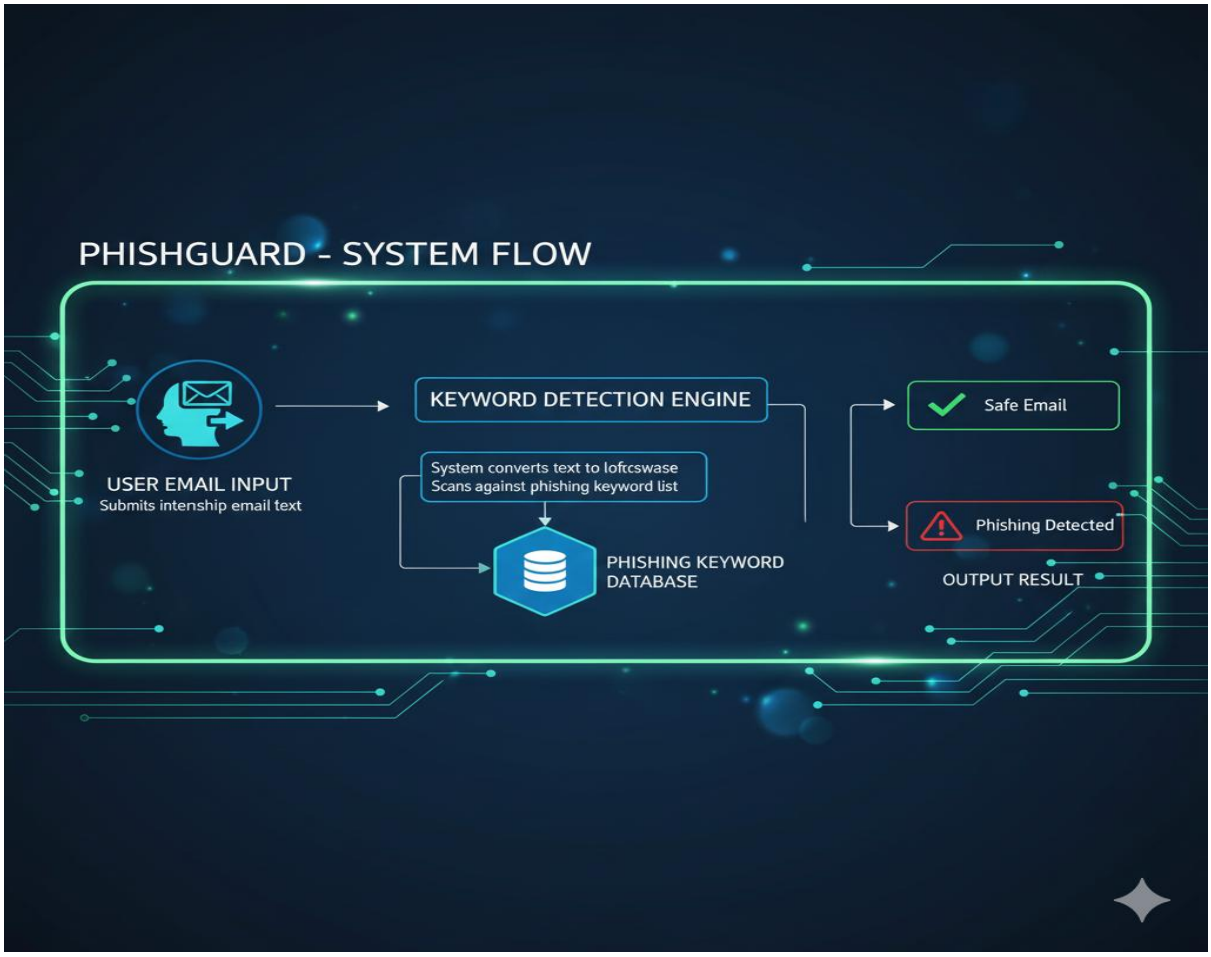
Explanation (for bullet points):

- User submits internship-related email text
- System converts text to lowercase
- Scans against phishing keyword list

Output displayed as:

✓ Safe Email

⚠ Phishing Detected



Design Decisions & Rationale

- Selected Python because it provides fast development and string-processing support
- Chosen keyword-based detection approach to maintain simplicity and avoid heavy ML processing
- Modular design allows easy future upgrades (GUI / ML / storage)
- Focus on student cybersecurity awareness

Testing Approach

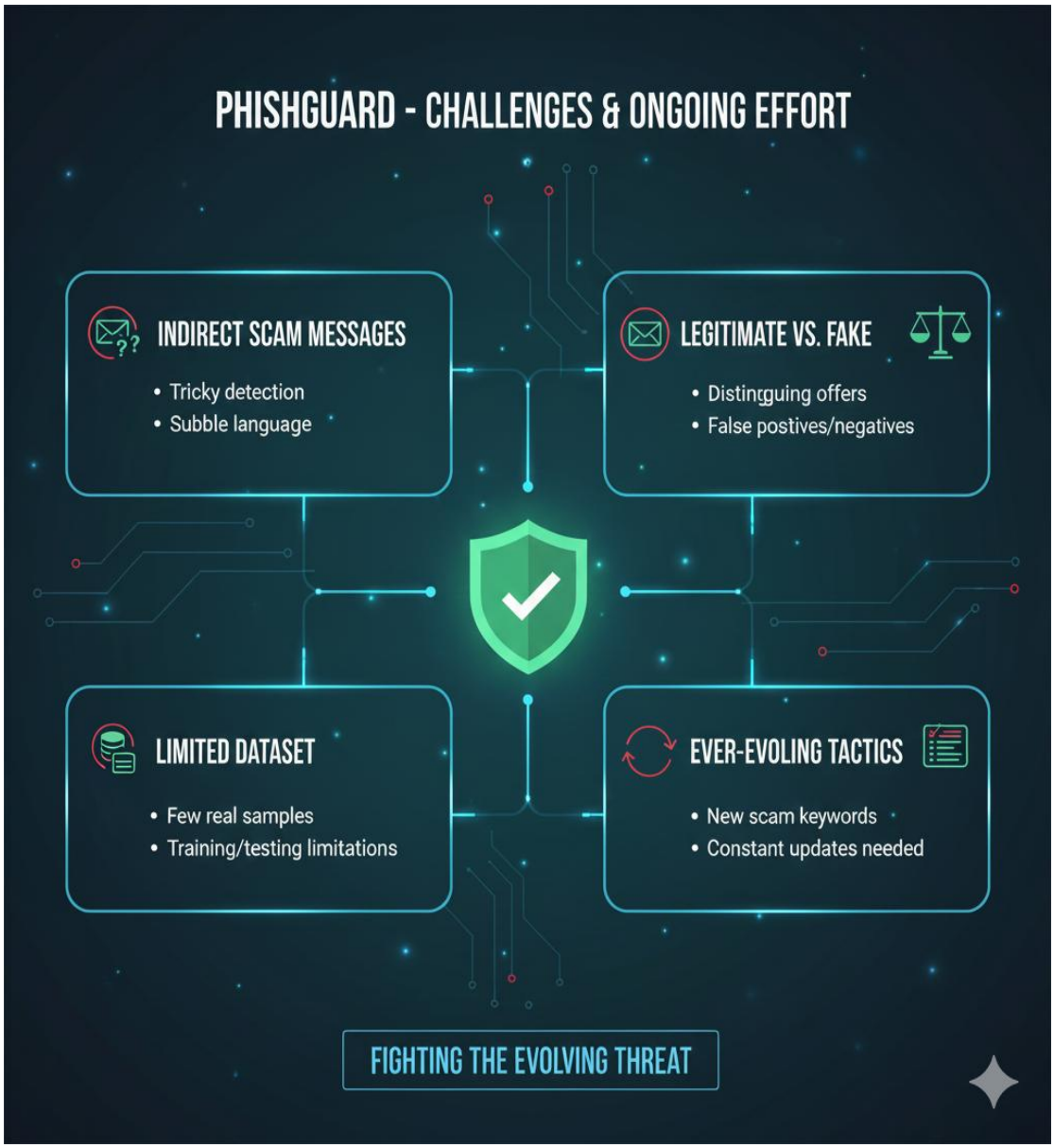
Testing was performed using multiple sample emails.

Test Case
Input Message
Expected Output
Actual Output
1
“Apply now for virtual internship registration fee”
Phishing
Phishing
2
“Internship confirmation from company HR”
Safe
Safe
3
“Hiring students immediate joining click here”
Phishing
Phishing
4
“We are happy to inform your internship completion certificate”
Safe
Safe

✓ All test cases successfully passed

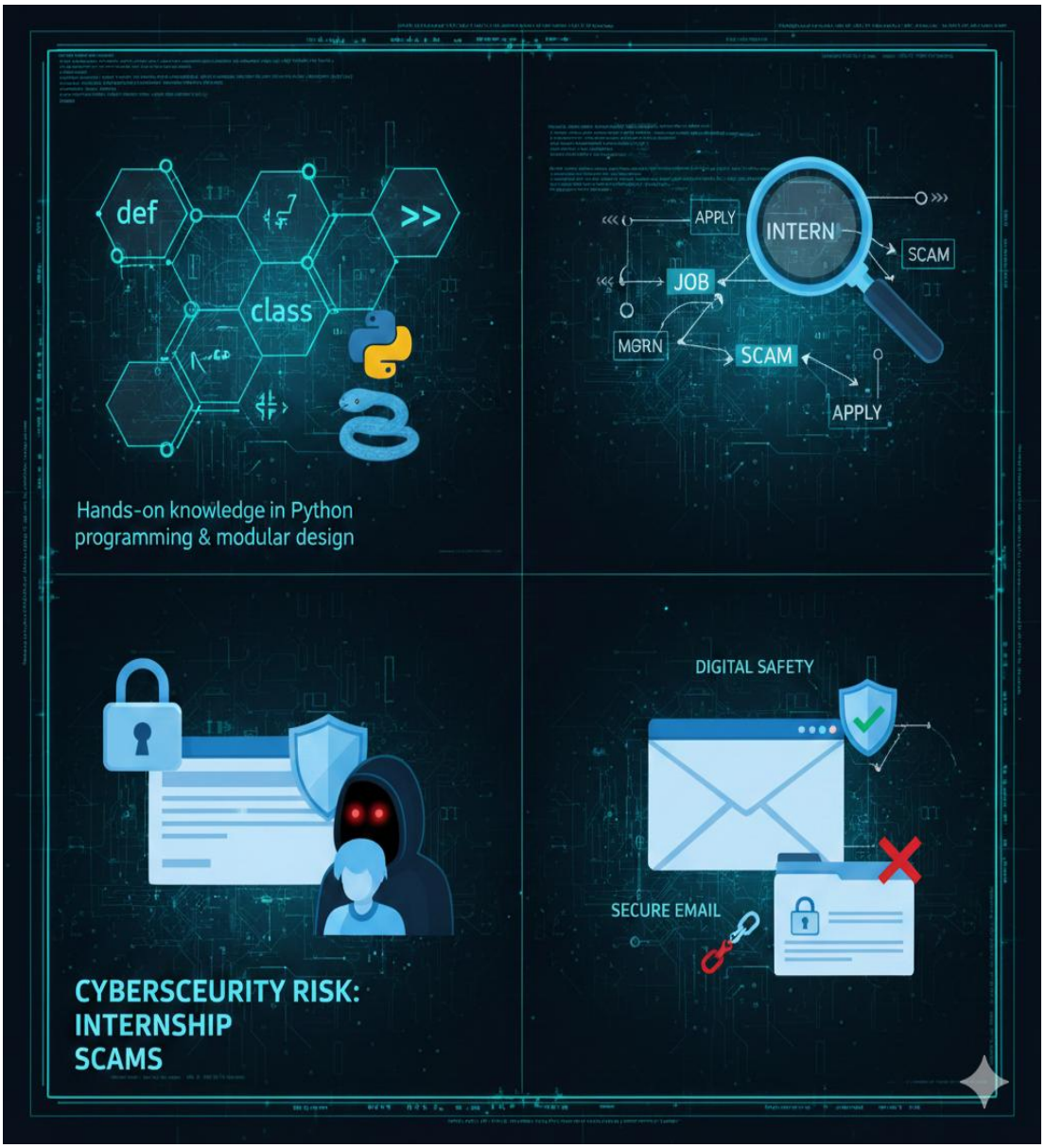
Challenges Faced

- Few phishing emails contain indirect scam messages making detection tricky
- Distinguishing between legitimate internship emails vs fake ones
- Limited dataset of real phishing samples for training/testing
- Need to keep updating new scam keywords



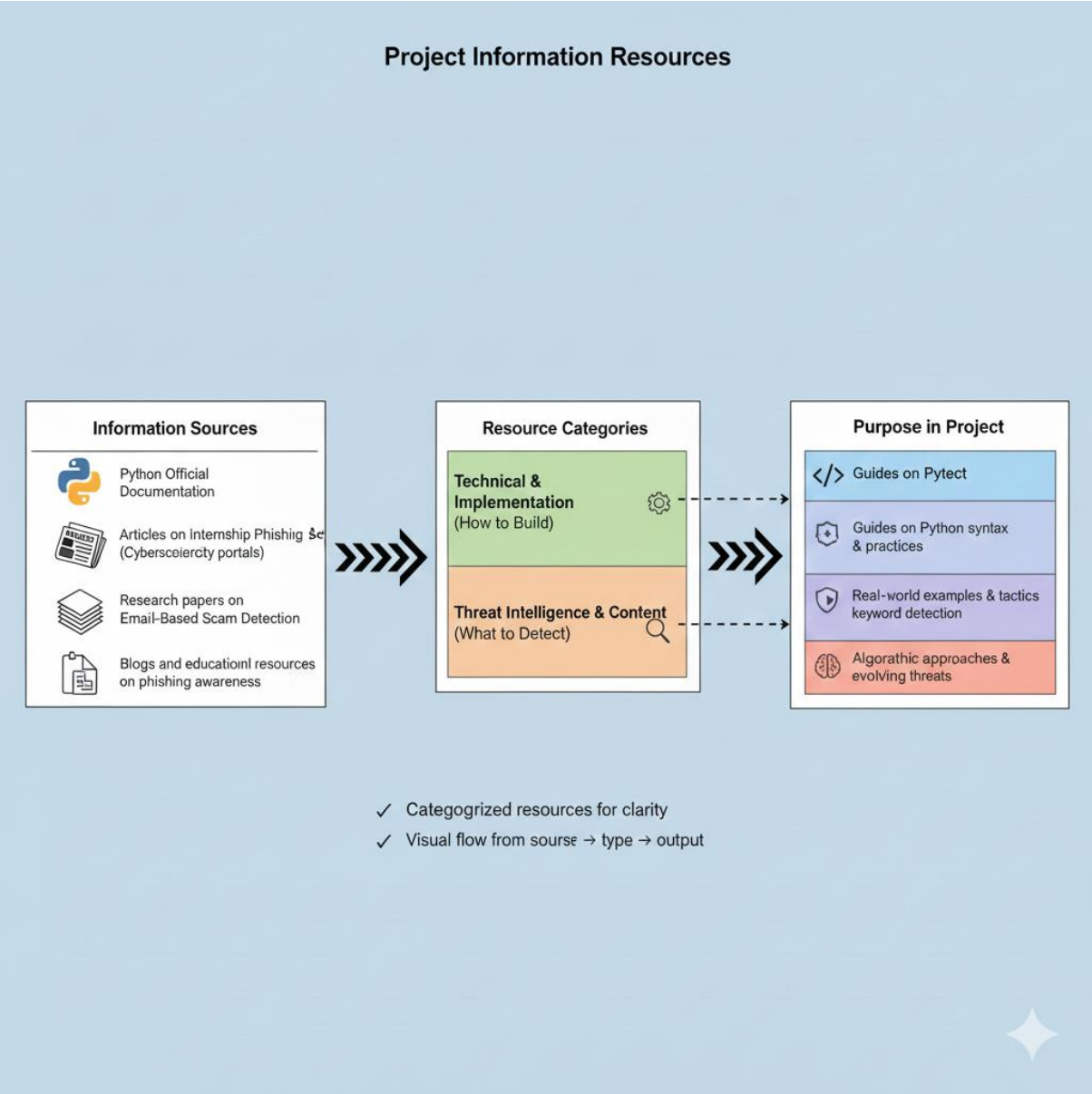
Learnings & Key Takeaways

- Gained hands-on knowledge in Python programming & modular design
- Understood the cybersecurity risk of internship scams targeting students
- Improved understanding of string processing & keyword matching
- Learned importance of digital safety & secure email behaviour



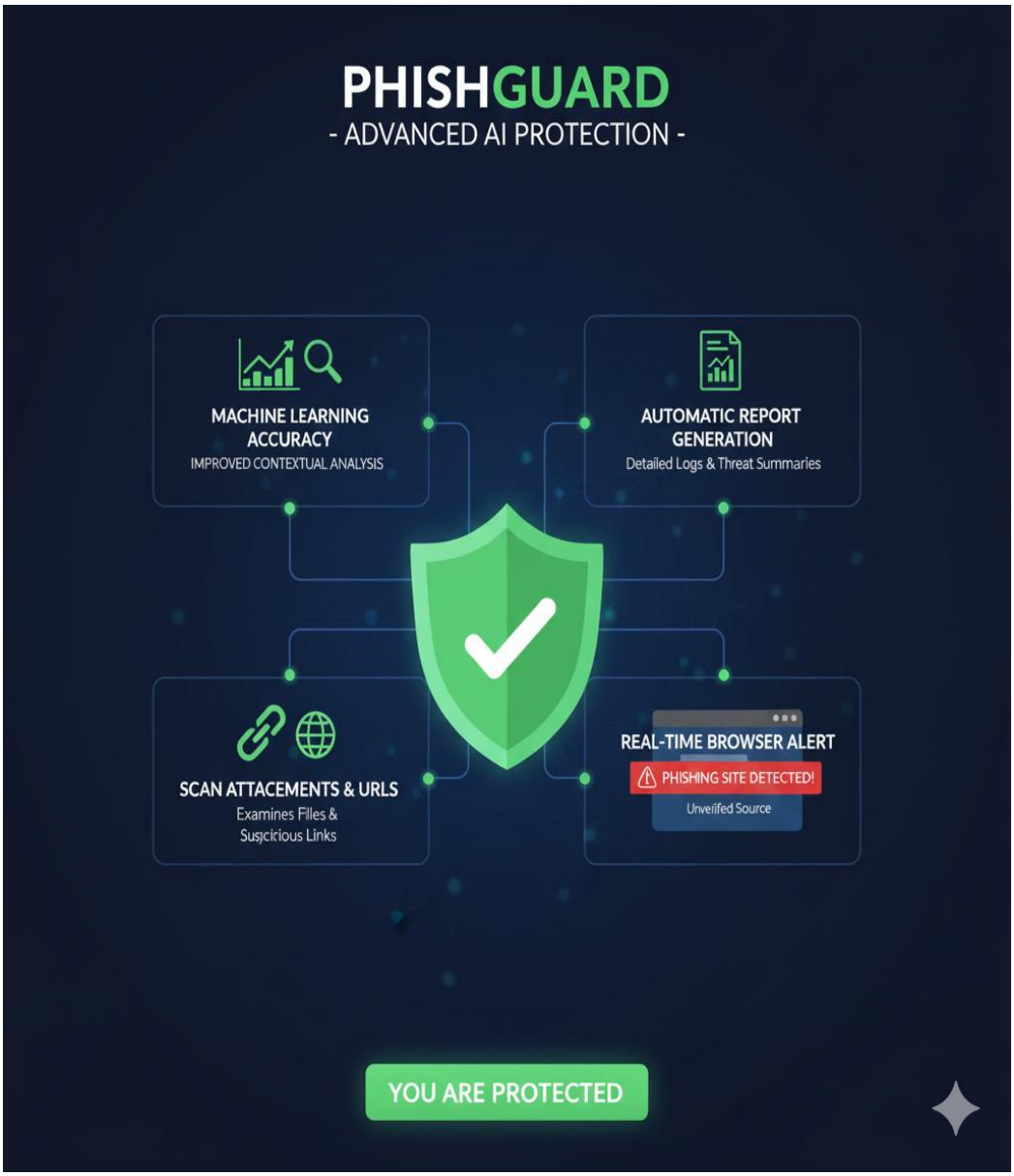
References

- Python Official Documentation
- Articles on Internship Phishing Scams (Cybersecurity portals)
- Research papers on Email-Based Scam Detection
- Blogs and educational resources on phishing awareness



Future Enhancements

- Machine learning-based accuracy improvement
- Scan email attachments and URLs
- Automatic report generation
- Real-time browser alert



Conclusion

Phishing scams targeting internships are increasing.

The developed Python program helps detect suspicious emails.

Promotes student awareness and digital safety.

THANK YOU