RAMAIAH
Institute of Technology

Department of Computer Science and Engineering
V Semester, Cryptography and Network Security
Course Code: CSE555

Quantum-Resilient Phishing Detection:

A Post-Quantum Secure Framework for Email URL Analysis Using AI-Driven Models

By:

Shamanth M Hiremath (1MS22CS128)
Sanchit Vijay (1MS22CS122)
Ashutosh Kumar (1MS22CS036)
Trijal Shinde (1MS22CS153)

Under the Guidance of

Sangeetha V
Soumya CS
Het Joshi

Agenda

- Introduction
- Objectives
- Methodology Used
- Technology Stack
- Comparison to Existing Solution
- Results
- References

Introduction

- **Phishing Attacks:** Phishing is a major cyber threat. It involves using deceptive URLs in emails to trick users.
- **Novel Solution:** Introduces a new method for detecting phishing attacks. Combines quantum-resilient encryption with AI-driven URL analysis.
- **Secure Processing:** URLs from emails are securely processed. Protects the detection model and its parameters from future quantum computing threats.
- **High Predictive Accuracy:** Maintains a high level of accuracy in predicting phishing threats.
- **Research Contribution:** Connects cybersecurity with advanced cryptographic methods. Aims to provide robust solutions in an evolving cyber threat environment.

Introduction

This research introduces a quantum-secure phishing detection framework that combines:

1. An **AI-driven Random Forest model**, trained on 30 critical URL features, to classify URLs as phishing or legitimate with high accuracy.
2. A **post-quantum cryptographic layer** to encrypt and secure the model's weights and parameters, ensuring resilience against future quantum threats.
3. A **browser extension** that extracts URLs from incoming emails, performs real-time phishing analysis, and safeguards user data.

This innovative integration addresses the dual challenge of effective phishing detection and future-proof cybersecurity.

Objectives

- To develop an AI-based phishing detection model using **30 features extracted from email URLs** like **Length of the URL, Number of special characters, Presence of IP address in URL, Count of subdomain, HTTPS usage, Length of the hostname, Age of domain.**
- To **secure the model's parameters** and predictions using **post-quantum cryptography.**
- To demonstrate the feasibility of real-time deployment via an email-parsing browser extension.
- To compare the proposed solution with existing methods in terms of **accuracy, security, and operational efficiency.**
- To establish the model's resilience against both **classical** and **quantum-based attacks**.

Methodology

Dataset Preparation

Source: URLs sourced from repositories such as PhishTank, OpenPhish, and legitimate domains from Alexa Top 1 Million Sites.

Size: ~100,000 labeled URLs, evenly distributed between phishing and legitimate classes.

Features: Extracted 30 parameters from each URL, encompassing both lexical (URL structure) and host-based (domain-related) features.

Model Development

- Algorithm: Random Forest Classifier
- Optimization: GridSearchCV with:
  - n_estimators = 100
  - max_features = log2
  - criterion = entropy
- Performance: Achieved an accuracy of 97.24% with balanced precision and recall metrics.

Methodology

Quantum-Secure Encryption

1. Encryption Methodology:
   - Model weights and parameters are encrypted using AES-256 for speed and efficiency.
   - AES keys are secured using Kyber, a post-quantum key encapsulation mechanism, ensuring quantum resistance.
2. Workflow:
   - At runtime, the model is decrypted for predictions, and the parameters are re-encrypted after use.
   - Encryption and decryption add a latency of ~50ms per operation without significant performance degradation.

3.5 Integration with Email Parsing

- Developed a browser extension to:
  a. Parse email content.
  b. Extract embedded URLs.
  c. Send URLs for phishing prediction using the quantum-secure framework.

Technology Stack

- **Programming:** Python (backend), JavaScript (browser extension).
- **AI/ML:** scikit-learn, pandas, NumPy
- **Cryptography:** PyCryptodome (AES-256), pqcrypto (Kyber).
- **Email Parsing:** Python Email library, Gmail API, IMAP/SMTP protocols.
- **Deployment:** Google Colab for training, AWS cloud services for hosting, browser extension for real-world testing, VS Code for development.

Comparison to Existing Solution

Aspect	Existing Solutions	Proposed Solution
Features Analyzed	10–15 features in most cases	30 comprehensive URL-based features
Encryption	Standard (AES or RSA)	Post-quantum secure (Kyber + AES-256)
Quantum Resistance	Not addressed	Fully quantum-resilient encryption
Deployment	Cloud/local	Browser extension with real-time URL parsing
Accuracy	~80-93%	97.24% with enriched features and RFA optimization

Results

- **Model Performance:**
  a. Accuracy: 97.24%
  b. Precision: 96.89%
  c. Recall: 98.11%
  d. F1-Score: 97.49%
- **Feature Importance:**
  Key contributors: URL length, DNS record validity, and number of special characters.

Results

- **Encryption Performance:**
  Encryption/decryption overhead: ~50ms per operation.
  Ensured end-to-end model security with no compromise on prediction speed.
- **Real-World Deployment:**
  Browser extension successfully parsed emails, extracted URLs, and delivered real-time predictions.

References

1. **Bernstein, D. J., et al.** Post-Quantum Cryptography: A NIST Perspective. NIST, 2022.
2. **PQClean:** A Collection of Clean Implementations of Post-Quantum Cryptographic Algorithms.
3. **scikit-learn developers and documentation.** Machine Learning in Python: Random Forest Implementation.
4. **Kaggle for Dataset:** Open Database of Phishing URLs.
5. **PyCryptodome Library.** Python Cryptography Toolkit.
6. **YouTube**
7. **Google GMail Documentation**
8. **ChatGPT**

Thank You