3.2 - IoT Security with Post-Quantum Cryptography

Group Members:

Satya Kamala Immidisetty
si2502

Alec Pippas
awp251

Xibo He
xh2774

Suprateek Chatterjee
sc10344

Nico Flores

December 3, 2024

Introduction

The Internet of Things (IoT) is a rapidly evolving domain where interconnected devices communicate to perform tasks such as monitoring, automation, and real-time decision-making. Despite its transformative impact, IoT faces significant security challenges due to its distributed nature, resource constraints, and susceptibility to attacks. Traditional cryptographic methods such as RSA and ECC are vulnerable to emerging quantum computing threats, necessitating the adoption of post-quantum cryptography. This project focuses on implementing and evaluating post-quantum digital signatures using the Open Quantum Safe (OQS) library to secure IoT communication.

Problem Statement

IoT devices often operate in resource-constrained environments, making them vulnerable to message tampering, spoofing, and data breaches. These threats compromise the integrity, authenticity, and confidentiality of communication between devices. The emergence of quantum computing further exacerbates the issue, as conventional cryptographic algorithms such as RSA and ECC are no longer secure against quantum attacks.

This project addresses these challenges by implementing digital signatures with `Dilithium5`, a post-quantum cryptographic algorithm. The solution ensures secure message transmission while maintaining low computational and resource overhead, making it ideal for IoT devices.

Approach to the Solution

This project uses the Open Quantum Safe (OQS) library to simulate secure communication between IoT devices. The steps include:

Key Components

1. **Key Generation:** IoT devices generate private-public key pairs using `Dilithium5`.
2. **Message Signing:** The sender signs messages with a private key, ensuring authenticity and integrity.
3. **Message Verification:** The receiver verifies the signed message using the sender's public key.
4. **Performance Metrics:** Signing time, verification time, memory usage, and CPU overhead are evaluated across multiple iterations.
5. **Security Testing:** The solution tests resistance to spoofing and tampering attacks.

Implementation Workflow

1. **Key Generation:** Devices generate quantum-safe key pairs using `Dilithium5`. The private key is stored securely, and the public key is shared with other devices for verification.
2. **Message Signing:** Messages are signed using the private key. This step ensures authenticity and integrity and measures the computational cost in terms of execution time, memory, and CPU overhead.
3. **Message Verification:** The receiver validates the signature using the public key to confirm the message's authenticity. This process ensures that the message remains unaltered.
4. **Security Testing:**
    - **Spoofing Detection:** Modified messages fail verification.
    - **Tampering Detection:** Altered signatures are detected and rejected.

Challenges

During the implementation of post-quantum digital signatures for IoT communication, several challenges were encountered:

- **Integration with the OQS Library:** Adapting the Open Quantum Safe (OQS) Python bindings for a real-world simulation required understanding and resolving compatibility issues between the library and the Python runtime environment.
- **Performance Trade-offs:** While `Dilithium5` provided robust security, optimizing its performance for resource-constrained IoT devices involved balancing computational cost and memory usage.

- **Key Management:** Ensuring secure and efficient handling of cryptographic keys was critical to maintaining the overall integrity of the system.
- **Testing for Edge Cases:** Simulating scenarios such as tampered signatures and spoofed messages required careful design of test cases to validate system robustness.
- **Resource Monitoring:** Accurately measuring resource usage (e.g., memory and CPU) during signing and verification operations posed challenges due to variations in system activity.

Results and Outputs

The implementation successfully demonstrates the following:

- **Secure Communication:** Messages signed using `Dilithium5` are verified correctly, ensuring authenticity and integrity throughout the communication process.
- **Performance Metrics:**
  - **Average Signing Time: 2-3 ms**, demonstrating efficiency suitable for IoT environments.
  - **Average Verification Time: 1-2 ms**, enabling quick validation for real-time communication.
  - **Memory Usage:** Minimal overhead, ensuring compatibility with resource-constrained devices.
  - **CPU Usage:** Low computational requirements, maintaining system responsiveness during cryptographic operations.
- **Robust Security:**
  - Spoofed messages are successfully detected and rejected during verification.
  - Tampered signatures fail validation, confirming the solution's robustness against integrity breaches.
- **Scalability:** The solution is extensible to larger IoT networks while maintaining secure communication.

Conclusion

This project demonstrates the feasibility of using post-quantum digital signatures to secure IoT communication. By implementing the `Dilithium5` algorithm, the solution ensures message authenticity, integrity, and resistance to both classical and quantum attacks. Performance metrics confirm its suitability for resource-constrained IoT devices, making it a scalable and secure cryptographic solution.

Future Work

The project presents a scalable foundation for securing IoT communication using post-quantum cryptography. Future enhancements and explorations include:

- **Expanding Algorithm Support:** Evaluating other post-quantum cryptographic algorithms such as `Falcon` and `SPHINCS+` to compare performance and security trade-offs in IoT environments.
- **Real-Time Integration:** Extending the implementation to real-world IoT networks with multiple interconnected devices to assess system performance and scalability under realistic conditions.
- **Lightweight Implementations:** Developing more resource-efficient adaptations of `Dilithium5` for ultra-constrained IoT devices such as sensors and wearable devices.
- **Compliance with Standards:** Aligning the framework with industry standards like HIPAA and GDPR to ensure regulatory compliance in sensitive sectors such as healthcare and finance.
- **Long-Term Storage Security:** Investigating post-quantum encryption methods for securely archiving IoT data, ensuring resistance to quantum threats over extended periods.
- **Comprehensive Testing:** Enhancing test cases to include adversarial scenarios such as distributed denial-of-service (DDoS) attacks and side-channel attacks.

Citations

1. Open Quantum Safe Project: `https://openquantumsafe.org/`
2. CRYSTALS-Kyber and CRYSTALS-Dilithium. NIST PQC Standardization: `https://csrc.nist.gov/Projects/post-quantum-cryptography`
3. AES-GCM Encryption (NIST Special Publication 800-38D): `https://nvlpubs.nist.gov/`