ACROPOLIS INSTITUTE OF TECHNOLOGY AND RESEARCH

Department of IT, CSE (DS), CSE (IoT)

Synopsis

On

Privy-Post: Cutting-Edge Security for Email Communication

1. Introduction

1.1 **Overview:** The Encrypted Email System is designed to address the significant vulnerabilities inherent in traditional email communication by implementing robust encryption techniques. Email remains a crucial tool for both personal and professional communication, but its susceptibility to interception and unauthorized access poses substantial risks. This project aims to mitigate these risks by providing a comprehensive solution that not only encrypts email content and attachments but also simplifies key management. By leveraging advanced cryptographic methods, the system ensures that communications are secure, confidential, and tamper-proof, while maintaining user convenience.

1.2 **Purpose:** The purpose of the Encrypted Email System is to create a secure and user-friendly environment for email communications. Key objectives include:

- **Confidential Communication:** Guaranteeing that only intended recipients can access and read the content of emails and attachments.
- **Protection Against Data Breaches:** Enhancing security measures to minimize the risk and impact of unauthorized email access.
- **Simplified Key Management:** Eliminating the complexity associated with traditional Public Key Infrastructure (PKI) by providing an intuitive key management process.

2. Literature Survey

2.1 **Existing Problems:** Traditional email encryption systems, such as S/MIME (Secure/Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy), rely heavily on PKI, which brings several challenges:

- **High Cost and Complexity:** The need for certificate authorities and the management of digital certificates adds significant overhead. Users must navigate complex processes for key creation, distribution, and revocation.
- **Scalability Challenges:** As the user base grows, maintaining and updating certificates becomes increasingly cumbersome. This complexity can lead to inefficiencies and errors, particularly in large organizations.

- **User Adoption Issues:** The intricacies involved in PKI can deter users from adopting encryption practices. Without user engagement, the effectiveness of encryption is compromised, leaving communications vulnerable.

2.2 **Proposed Solution:** The Encrypted Email System introduces a novel approach that aims to overcome the limitations of existing encryption methods:

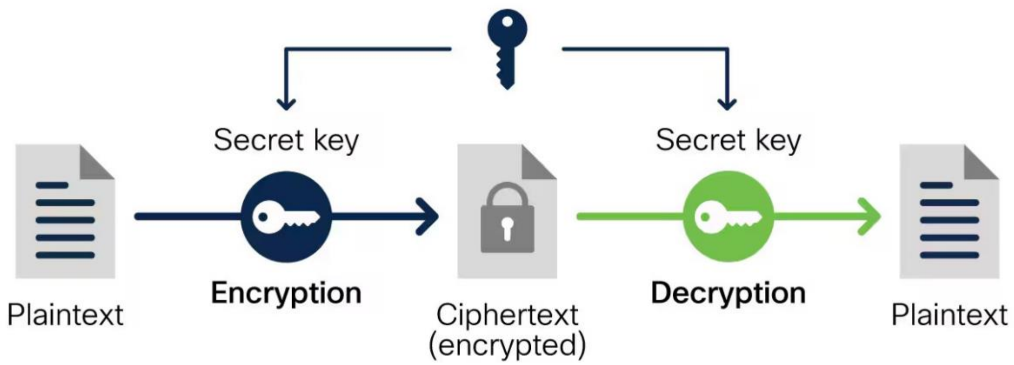
- **Identity-Based Encryption (IBE):** By utilizing IBE, the system removes the dependency on traditional PKI infrastructure. In IBE, encryption keys are derived from user identities, simplifying key management and distribution. This approach reduces the need for certificates and the associated administrative overhead.
- **Dynamic Key Generation:** Keys are generated on-demand based on user-specific identities, streamlining the process and eliminating the need for pre-existing certificates. This dynamic approach enhances flexibility and scalability.
- **End-to-End Encryption:** The system employs the Java Cryptography Extension (JCE) to encrypt and decrypt email content and attachments. This ensures that messages remain confidential and intact during transmission, protecting them from unauthorized access.
- **Two-Factor Authentication (2FA):** To further secure user accounts, the system incorporates 2FA during the login process. This additional layer of security helps prevent unauthorized access and enhances overall protection.

Additional Features:

- **User-Friendly Interface:** The system is designed with a focus on user experience, offering an intuitive interface that simplifies the process of sending and receiving encrypted emails. Users can manage their keys and settings with ease, without needing extensive cryptographic knowledge.
- **Integration with Existing Email Clients:** To facilitate seamless adoption, the system can be integrated with popular email clients, allowing users to benefit from enhanced security without altering their existing workflows.
- **Auditing and Compliance:** The system includes features for auditing and compliance, enabling organizations to track and monitor email transactions to ensure adherence to security policies and regulatory requirements.
- **Scalable Architecture:** Designed to accommodate growth, the system's architecture can handle an increasing number of users and transactions efficiently, making it suitable for both small businesses and large enterprises.

3. Theoretical Analysis

3.1Block Diagram:



The system is divided into the following blocks:

1. **User Authentication**: Includes two-factor authentication for secure access.
2. **Email Composition**: The user drafts an email and attaches files.
3. **Encryption Process**: The system encrypts the email and attachments using the user's public/private key pairs generated through IBE.
4. **Email Transmission**: The encrypted email is sent through secure channels.
5. **Decryption Process**: The recipient decrypts the email using their private key.
6. **Email Display**: The decrypted content is displayed to the recipient.

3.2 Hardware/Software Designing:

- **Hardware Requirements**:
  - Server to host the email platform and manage encryption/decryption processes.
  - Personal computers or devices (laptops, smartphones) for users.
- **Software Requirements**:
  - **Programming Language**: Java 17
  - **Frameworks and Libraries**:
    - **Java Mail API**: For handling email operations (sending/receiving).
    - **BouncyCastle or JCE**: For encryption and decryption algorithms.
    - **Spring Boot**: Backend development.

        - **JSP**: Front-end rendering.

- **Database**: MySQL for storing user data and email metadata.
- **Web Server**: Apache Tomcat for managing server-side processes.
- **Front-End**: HTML, CSS, JavaScript for a user-friendly interface.
- **Build Tools**: Maven for project and dependency management.

4. Applications

The Encrypted Email System has applications in various sectors where secure communication is essential:

- **Government and Public Sector**: Ensures the secure transmission of classified information between government agencies.
- **Education Sector**: Protects student records and academic communications from unauthorized access.
- **Personal Use**: Enables individuals to secure their personal emails and attachments.
- **Financial Services**: Safeguards sensitive financial data, such as transaction records, reports, and client information, ensuring compliance with regulations like **GDPR** and **HIPAA**.

References

List the Sources used in the study.

- Java Cryptography Architecture (JCA) Reference Guide
  https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html
  Cipher Input
- Spring Boot Official Documentation
  https://spring.io/projects/spring-boot
- https://www.cisco.com/c/en/us/products/security/encryption-explained.html
- https://www.researchgate.net/publication/372909532_Email_Security_Issues_Tools_and_Techniques_Used_in_Investigation

Guided By: Pro. Vishal Trivedi

Group Members:

Jayshree Gupta(0827IT211051)

Himanshi Dashore (0827IT211043)

Dev Goyal(0827IT211033)

Kanhai Kumar(0827IT223D02)