

QUANTUM SECURE EMAIL CLIENT APPLICATION

Yallapragada Naga Sai Padma Sri

Department of CSE NRI Institute of Technology, padmasriyallapragada08@gmail.com

P. Aravind, Asst. Prof

Department of CSE NRI Institute of Technology, aravind.penamaka@gmail.com

ABSTRACT

The rapid growth of digital communication has increased the need for highly secure email systems capable of protecting sensitive information from evolving cyber threats. Traditional encryption techniques such as RSA and ECC are becoming vulnerable due to advancements in quantum computing, which can potentially break conventional cryptographic algorithms. To address these challenges, this project proposes a Quantum Secure Email Client Application that integrates post-quantum cryptography (PQC) techniques to ensure end-to-end secure communication.

The proposed system employs quantum-resistant encryption algorithms such as lattice-based cryptography, hash-based signatures, or code-based encryption to secure email content, attachments, and user authentication processes. The email client ensures that messages are encrypted before transmission and can only be decrypted by the intended recipient, thereby preventing unauthorized access, interception, and data leakage.

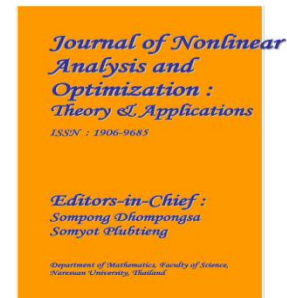
Additionally, the system incorporates secure key exchange mechanisms resistant to quantum attacks, ensuring safe communication even in the presence of quantum adversaries. The user interface is designed to be simple and user-friendly, allowing seamless sending and receiving of secure emails without requiring deep technical knowledge.

The application enhances confidentiality, integrity, and authentication in email communication, making it suitable for defense, banking, healthcare, and government sectors where data security is critical. By integrating quantum-safe cryptographic techniques, the system provides a future-ready solution that safeguards communication against both classical and quantum computing threats.

INTRODUCTION

Email communication has become an essential part of modern digital interaction,

widely used in personal, academic, business, and government domains. However, traditional email systems are increasingly vulnerable to cyber threats such as phishing, spoofing, man-in-the-



middle attacks, and data breaches. To protect sensitive information, encryption techniques like RSA and ECC have been widely used for secure communication.

With the rapid advancement of quantum computing, these conventional cryptographic methods are at risk of becoming obsolete. Quantum computers have the potential to solve complex mathematical problems much faster than classical computers, which could break widely used encryption algorithms. This creates an urgent need for developing quantum-resistant security solutions to ensure the safety of digital communication in the future.

A Quantum Secure Email Client Application is designed to overcome these limitations by implementing post-quantum cryptographic techniques. These algorithms are resistant to attacks from both classical and quantum computers, ensuring stronger security for email transmission. The system focuses on encrypting email content, securing attachments, and protecting authentication processes using advanced cryptographic methods.

The main goal of this project is to develop a secure and user-friendly email client that provides end-to-end encryption with quantum-safe algorithms. It ensures that only authorized users can access the message content, thereby maintaining confidentiality, integrity, and authenticity of communication.

This system is particularly useful in domains where security is critical, such as banking, healthcare, defense, and corporate communication. By integrating quantum-

resistant encryption techniques, the proposed application prepares email communication systems for the future era of quantum computing threats.

LITERATURE SURVEY

1. Title: Post-Quantum Cryptography for Secure Communication Systems

Author: Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen

Description:

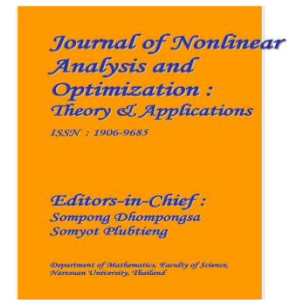
This work provides a comprehensive study of post-quantum cryptographic algorithms designed to resist attacks from quantum computers. It discusses lattice-based, hash-based, and multivariate cryptographic systems. The study emphasizes that traditional encryption methods like RSA and ECC will become insecure in the presence of quantum computing, and it highlights the need for developing quantum-resistant security protocols for future communication systems such as email and messaging platforms.

2. Title: Quantum Computing and Its Impact on Cryptography

Author: Peter W. Shor

Description:

This research introduces Shor's algorithm, which demonstrates that quantum computers can efficiently factor large integers and compute discrete logarithms. These mathematical capabilities directly threaten widely used public-key cryptographic systems. The paper is



foundational in showing why current encryption methods used in email security must be replaced with quantum-safe alternatives to maintain data confidentiality.

3. Title: NIST Post-Quantum Cryptography Standardization Process

Author: National Institute of Standards and Technology (NIST) Researchers

Description:

This study outlines the ongoing standardization process for post-quantum cryptographic algorithms. It evaluates multiple encryption schemes based on security, performance, and implementation feasibility. The selected algorithms aim to replace current cryptographic standards in real-world applications, including secure email systems, ensuring resistance against both classical and quantum attacks.

4.Title: Secure Email Communication Using Hybrid Encryption Techniques

Author: Ahmad Reza Sadeghi, et al.

Description:

This paper discusses hybrid encryption methods combining symmetric and asymmetric cryptography to enhance email security. It explains how combining multiple cryptographic techniques improves performance and security. However, it also notes that such systems may still be vulnerable in a post-quantum environment, motivating the need for quantum-secure email clients.

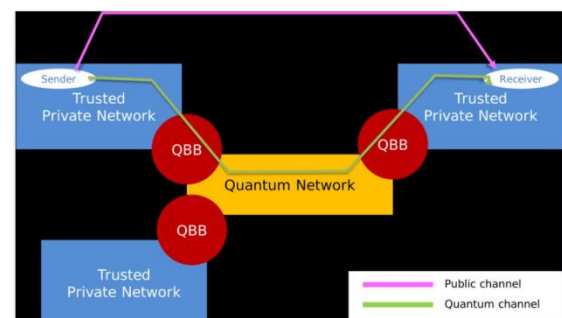
5.Title:Lattice-Based Cryptography for Post-Quantum Security

Author: Oded Regev

Description:

This research introduces lattice-based cryptography as one of the most promising approaches for post-quantum security. It explains that lattice problems are computationally hard even for quantum computers, making them suitable for secure communication systems. The study forms the foundation for many modern quantum-safe encryption schemes used in secure email applications.

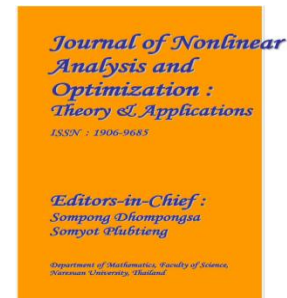
SYSTEM ARCHITECTURE



IMPLEMENTATION

SCREEN SHOTS

To run project double click on 'run.bat' file to get below screen



```

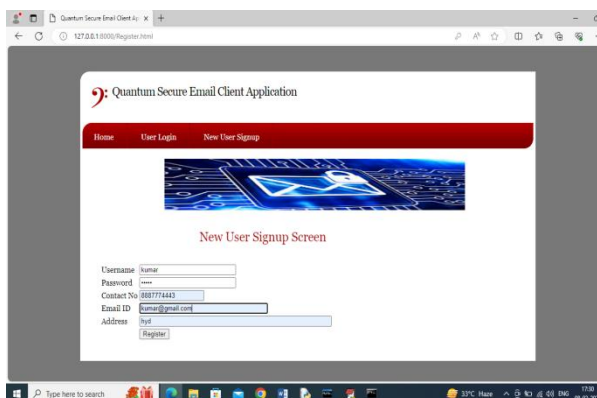
C:\Windows\system32\cmd.exe
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\psycopg2\__init__.py
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\psycopg2\__init__.py
Performing system checks...

System check identified no issues (0 silenced).
You have 15 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin,
auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
February 09, 2024 - 17:28:57
Django version 2.1.7, using settings 'email.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
    
```

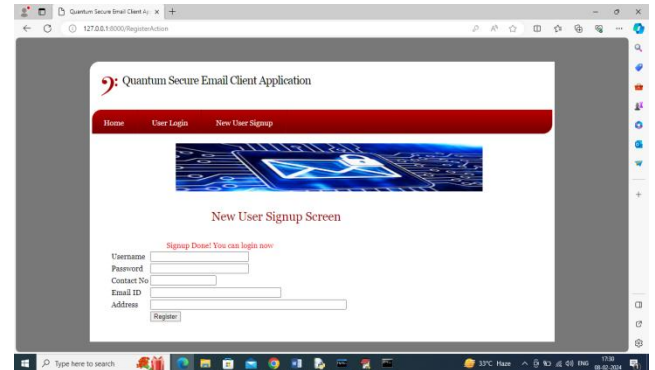
In above screen python server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and press enter key to get below page



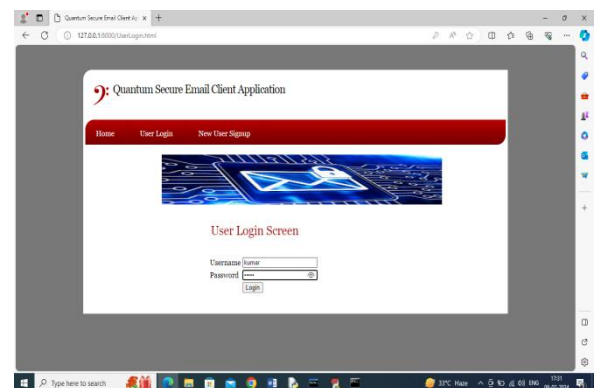
In above screen click on 'New User Sign up' link to get below page



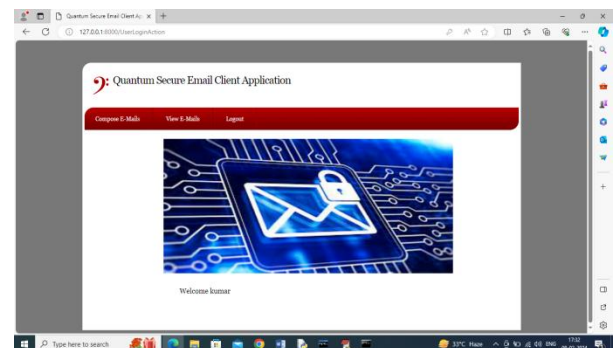
In above screen user is entering sign up details and then click on 'Register' button to complete sign up and get below output



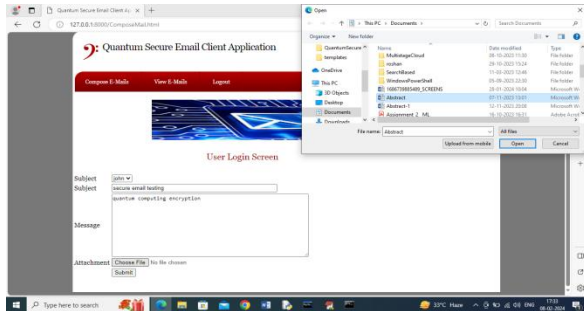
In above screen sign up completed and similarly you can add any number of users and now click on 'User Login' link to get below page



In above screen user is login and after login will get below page



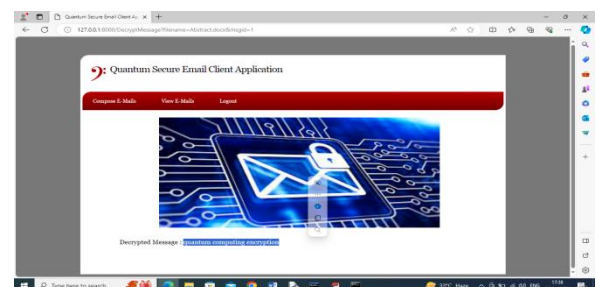
In above screen user can click on 'Compose E-Mails' link to get below page



The screenshot shows the Quantum Secure Email Client window titled "Quantum Secure Email Client (x)". The address bar displays "127.0.0.1:8000/viewEmail". The top navigation bar includes links for "Compose E-Mails", "View E-Mails", and "Logout". Below the navigation bar is a large graphic featuring a blue envelope icon with a white padlock, set against a background of glowing circuitry.

Mail ID	Sender Name	Receiver Name	Mail Date	Subject	Encrypted Message	Decrypt Message	Decrypt & Download Attachment
1	jumar	jaha	2024-02-08 17:33:00.343903	secure mail starting	0'1'000'1000'1000'1000'1000'1000'1000'1000'1000'	Click Here	Click Here

The bottom status bar shows system information: Windows taskbar icons, "Type here to search", system clock at "12:23 PM", date "Feb 8, 2024", and network status.



JNAO Vol. 17, Issue. 2: 2026

Similarly by following above screens you can send secure mails from sender to receiver

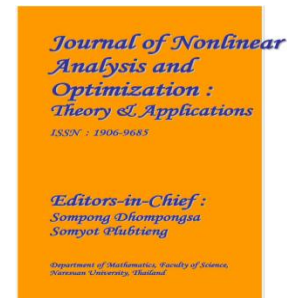
The Quantum Secure Email Client Application addresses the growing need for highly secure communication in the era of advancing quantum computing. Traditional encryption methods such as RSA and ECC are expected to become vulnerable due to the computational power of quantum algorithms. To overcome this limitation, the proposed system integrates post-quantum cryptographic techniques that are resistant to quantum attacks.

In conclusion, the proposed system offers a future-ready solution that strengthens email security against both classical and quantum threats, ensuring safe and reliable communication in the evolving digital landscape.

The proposed Quantum Secure Email Client Application can be further enhanced to meet evolving security demands and technological advancements in the field of cybersecurity and quantum computing.

One major area of future improvement is the integration of **advanced post-quantum cryptographic standards** as they are finalized by organizations such as NIST. This will ensure the system remains up to date with the most secure and efficient quantum-resistant algorithms.

The application can also be extended by implementing **multi-factor authentication (MFA)** and **biometric verification** such as fingerprint or facial recognition to further strengthen user identity verification and prevent unauthorized access.



Another possible enhancement is the development of a **cloud-based secure email service**, enabling users to access encrypted emails across multiple devices while maintaining end-to-end security.

Future versions may also include **AI-based threat detection systems** to identify phishing attempts, spam emails, and malicious attachments in real time, improving overall system intelligence and user protection.

Additionally, support for **blockchain-based email verification** can be explored to ensure message integrity and prevent tampering or spoofing of email content.

In conclusion, future enhancements aim to make the system more robust, intelligent, scalable, and fully prepared for next-generation quantum-secure communication environments.

REFERENCES

- [1] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*, Springer, 2009.
- [2] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.
- [3] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization Project," 2016–2024.
- [4] O. Regev, "On lattices, learning with errors, random linear codes, and

cryptography," *Journal of the ACM*, vol. 56, no. 6, 2009.

- [5] A. Reza Sadeghi et al., "Secure Email Communication Using Hybrid Encryption Techniques," *IEEE Security & Privacy*, 2018.