A logo with text and colors

Description automatically generated with medium confidence

Document Sharing Platform Utilizing Post-Quantum Cryptography

Department Of Science – College of Computer Science

Project Proposal

Prepared by:

Ayad Azad Ali – F200913

Naz Abduljabar Abdulrahman – F201268

Rawa Ghalib Muhammed–F201558

Supervised by:

Dr. Susan AL Naqshbandi

September 12, 2024

Table of Contents

[1-Abstract 2](#_Toc177142402)

[2- Introduction 2](#_Toc177142403)

[3- Background and Justification 3](#_Toc177142404)

[3-1 Quantum Computer Threat 3](#_Toc177142405)

[3-2 PQC algorithms 3](#_Toc177142406)

[4- Aim and Objectives 4](#_Toc177142407)

[5- Methodology: 4](#_Toc177142408)

[5.1. System Architecture: Using Next.js and Django 4](#_Toc177142409)

[Front-End Interface (Next.js): 4](#_Toc177142410)

[Server Backend (Django): 5](#_Toc177142411)

[5.2. Quantum-Safe Cryptography (PQC) 5](#_Toc177142412)

[5.3. Document Sharing Workflow 5](#_Toc177142413)

[6-Time Table 6](#_Toc177142414)

[7-References: 7](#_Toc177142415)

# 1-Abstract

This paper shows the steps and stages of building a secure document-sharing platform using Python. The post-quantum cryptographic method as quantum computers is getting advanced day by day it gives more concern to the users about sharing their sensitive data. Out-of-date encryption methods may become vulnerable and more threats to users, our platform aims to focus on this need by creating a user-friendly platform that the users can access and have a secure environment for exchanging documents by encrypting the documents. This proposal provides a practical and modern method to secure document sharing, ensuring that sensitive documents remain protected against technological threats.[3]

# 2- Introduction

Due to the rise of quantum computers, the classic encryption methods we use these days to secure our data in general are vulnerable. Quantum computers can break many encryption methods, making sharing data among various users difficult. That is why we need to make platforms that make exchanging data more easy and secure.

We present this project as a solution: a secure document-sharing platform using Python and the Kyber post-quantum cryptographic algorithm. Kyber is a post-quantum cryptography algorithm that is designed to make strong encryption even against quantum computers. This platform is a secure platform for exchanging documents between users, the platform will allow users to encrypt documents before sending them and only the intended receiver, who has the correct decryption key, will be able to open and read the document.[3]

# 3- Background and Justification

## 3-1 Quantum Computer Threat

As quantum computers are being worked on to make tasks of computers faster and change the level of computing to another level, the technology world becomes more dangerous[6], because quantum computers has the ability to perform complex computation at an unimaginable time. Common cryptographies like RSA and ECC which secure most online communications, relies on the difficulty of factoring large numbers or solving discrete logarithms, and quantum computers can easily decrypt all of them which makes online presence insecure[4].

## 3-2 Post Quantum Cryptography algorithms

The impact of quantum computing on the security of symmetric keys and hash functions is less relevant, so the greatest focus of research is to find public key algorithms that are resistant to attacks both from classical and quantum computers, The most notable approaches for quantum age cryptography are the following.

* Lattice-based: The security of this algorithm depends on the difficulty of certain problems in lattice mathematics, such as the Shortest Vector Problem (SVP) and the Learning with Errors (LWE) problem, both of which are considered intractable even for quantum computers. Lattice-based algorithms offer versatile cryptographic functionalities, including encryption, digital signatures, and fully homomorphic encryption. Their efficiency and scalability make them suitable for real-world applications, and they are currently considered front-runners in the field of quantum-resistant cryptography[5].
* Hash-based: This cryptography relies on the fundamental security of cryptographic hash functions, which are resistant to quantum attacks. These algorithms are particularly effective for constructing secure digital signature schemes.While hash-based cryptography is highly secure, one of its limitations is that the signature schemes often generate relatively large keys and signatures compared to traditional methods. However, due to their simplicity and robustness, hash-based schemes are among the most trusted methods for digital signatures in a post-quantum world[5].
* Code-based: This cryptography offers strong resistance against quantum attacks. The most famous code-based cryptosystem is the McEliece encryption algorithm, which relies on the difficulty of decoding random linear codes[5]. This problem has been extensively studied and has withstood decades of cryptanalytic attempts, making code-based cryptography a well-established choice for quantum-resistant encryption. The primary challenge of code-based schemes is the large key sizes, which can limit their practicality in some applications. Nonetheless, their security and reliability continue to make them a leading candidate for quantum-safe encryption.

# 4- Aim and Objectives

The primary goal of our project is to assess the security of our document-sharing platform by implementing post-quantum cryptography (PQC). Specifically, we aim to evaluate how well our platformcan withstand attacks from both quantum and classical computers.

Objectives:

* Integrate a post-quantum cryptography algorithm into our document-sharing platform.
* Explore post-quantum cryptography options such as lattice-based, code-based, or multivariate polynomial-based schemes.
* Investigate the vulnerability of our post-quantum cryptography implementation against

quantum computers.

* Creating a user-friendly platform.
* Creating a secure document-sharing platform.
* Creating a scalable and robust platform for document sharing.

# 5- Methodology:

## 5.1. System Architecture: Using Next.js and Django

This DSS architecture is a combination of two powerful frameworks, Next.js and Django. Here’s how they come together to create a robust and user-friendly system:

### Front-End Interface (Next.js):

We’ll be using Next.Js with TypeScript and design it with Tailwind CSS. Next.js the most powerful framework for web development that’s why we’ll use it to make our platform visually appealing and giving the user a good experience.

### Server Backend (Django):

Python is the most powerful language for Cryptography, and Django makes it more special, we’ll be using Django to serve the platform users, and secure the platform, python has a better support for Post Quantum Cryptography, and making the platform backend will be much easier.

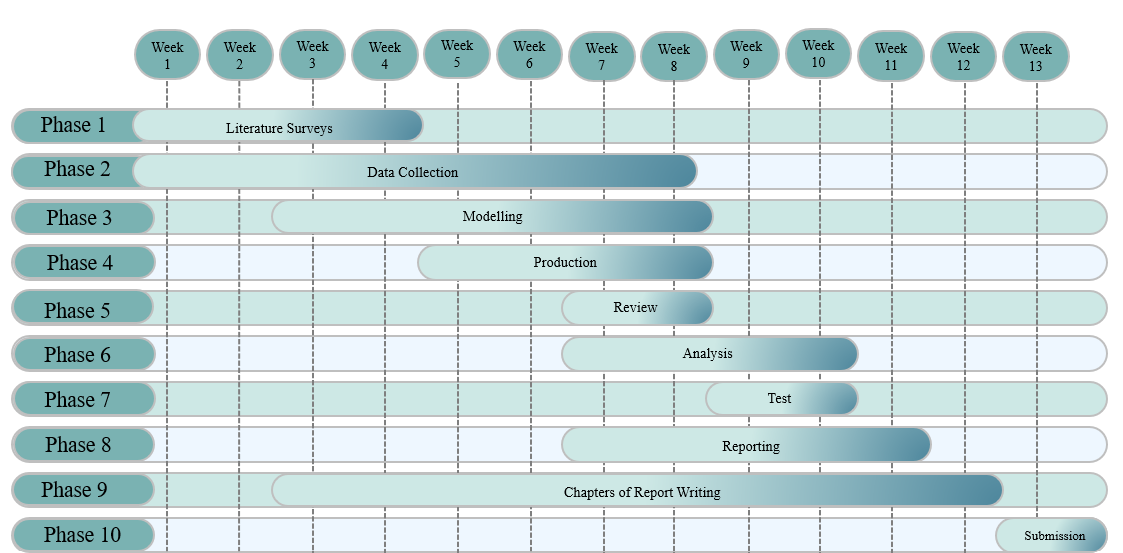
## 5.2. Quantum-Safe Cryptography (PQC)

There are some python libraries available that support Post Quantum Cryptography, but based on our research, we’ll be using QuantCrypt[7], we can apply different Post Quantum Cryptography algorithms by using QuantCrypt and we can also integrate it with other cryptographies to make the platform much more secure.

## 5.3. Document Sharing Workflow

When the users creates an account, they will have the ability to upload a document and share it with another person, the document will be encrypted and be sent to the 2nd person. The document will be decrypted when they receive the file/document using a private key.

# 6-Time Table

****

# 7-References:

1.Hülsing, D. J. Bernstein, and T. Lange, "Post-Quantum Cryptography in Practice: Lessons Learned and Ongoing Work," *arXiv preprint arXiv:2202.02826*, 2022.

2.J. Kumar, A. Sharma, and P. K. Mehra, "Current State of Quantum Cryptography," ResearchGate, June 2022.

3.Kokare, P. N., Vora, D., Patil, S., Kotecha, K., Khairnar, V., & Choudhury, T. Post Quantum Cryptography: A survey of Past and Future.

4.Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. Array, 15, 100242.

5. Pinto, Jose. (2022). Post-Quantum Cryptography. ARIS2 - Advanced Research on Information Systems Security. 2. 4-16. 10.56394/aris2.v2i2.17.

6. Sood, Neerav. (2024). Cryptography in Post Quantum Computing Era. 10.13140/RG.2.2.19691.92964.

7.<https://medium.com/@mattias.aabmets/introduction-to-quantcrypt-a-python-library-for-quantum-resistant-cryptography-00faec1cc032>

8.<https://www.nist.gov/cybersecurity/what-post-quantum-cryptography>

9.<https://www.sciencedirect.com/science/article/pii/S2590005622000777#sec4>