www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

SECURE PASSWORD MANAGER USING CRYSTALS-KYBER ALGORITHM

[1]Mr. D. LAKSHMAN BABU, [2]V. SHIVA SHANKER, [3]M. RAJU, [4]M.SANJAY, [5]V. HARSHAVARDHAN

[1]Assistant Professor Department of AI&DS, NALLA MALLA REDDY ENGINEERING COLLEGE

[2345]UG. SCHOLAR Department of AI&DS, NALLA MALLA REDDY ENGINEERING COLLEGE

ABSTRACT

In the age of rapid technological advancements, ensuring the security of sensitive information has become a critical challenge. This project introduces a password manager built with Crystals-Kyber, a cutting-edge quantum-resistant cryptographic algorithm designed to secure data against both classical and quantum attacks. As traditional encryption methods face potential vulnerabilities with the rise of quantum computing, the adoption of post-quantum cryptographic techniques ensures the longevity and robustness of security measures. The password manager focuses on protecting user credentials through state-of-the-art encryption, emphasizing both usability and reliability. The application leverages a highly secure backend architecture, incorporating efficient encryption workflows and robust authentication mechanisms to safeguard stored passwords. To address common vulnerabilities in password management, the system implements end-to-end encryption and secure communication protocols, ensuring that user data is protected from unauthorized access during both storage and transmission. With its intuitive interface, the password manager provides a seamless experience for users, enabling them to store, retrieve, and manage credentials without compromising on security. By employing Crystals-Kyber, a NIST-recommended post-quantum cryptographic algorithm, this project highlights the importance of preparing for emerging security threats posed by quantum computing. The algorithm's resistance to quantum-based attacks ensures that the system remains future-proof while maintaining compatibility with existing digital ecosystems. This implementation demonstrates the practical feasibility of integrating advanced cryptography into real-world applications, providing a secure and reliable solution for managing sensitive credentials. This project contributes to the growing demand for innovative cybersecurity solutions by delivering a secure, reliable, and user-friendly password management system that aligns with modern privacy standards.

keywords: Secure Password Manager,

Crystals-Kyber, Quantum-resistant cryptography, Post-quantum cryptography, Intuitive interface, End-to-end encryption, User credentials protection

I.INTRODUCTION

In the evolving landscape of cybersecurity, the advent of quantum computing poses significant challenges to traditional cryptographic systems. Classical encryption methods, such as RSA and ECC, rely on mathematical problems that quantum computers can potentially solve efficiently, rendering these systems vulnerable to future quantum attacks. This paradigm shift necessitates the development and adoption of post-quantum cryptographic algorithms capable of withstanding the computational power of quantum machines. One such promising candidate is the CRYSTALS-Kyber algorithm, a lattice-based key encapsulation mechanism (KEM) that has been recognized for its security and efficiency.

CRYSTALS-Kyber is part of the NIST's post-quantum cryptography standardization project, which aims to establish cryptographic standards resistant to quantum attacks. The algorithm's foundation lies in the hardness of the learning with errors (LWE) problem over module lattices, a problem believed to be resistant to quantum algorithms. Its efficiency and security have led to its adoption in various applications, including secure key exchange protocols and encryption systems.

Password management systems are critical components in safeguarding digital identities and sensitive information. These systems store and manage user credentials, often employing encryption to protect data at rest and during transmission. With the impending threat posed by quantum computing, it becomes imperative to integrate quantum-resistant algorithms like CRYSTALS-Kyber into password managers to future-proof these essential tools against potential vulnerabilities.

This paper explores the integration of the CRYSTALS-Kyber algorithm into secure password management systems. It delves into the current state of quantum computing threats, reviews existing password manager configurations, proposes a methodology for incorporating CRYSTALS-Kyber, and outlines an enhanced configuration aimed at bolstering security in the post-quantum era.

II. LITERATURE SURVEY

The field of post-quantum cryptography has garnered significant attention in recent years, particularly in the context of securing password management systems. The NIST post-quantum cryptography standardization project has been instrumental in evaluating and recommending algorithms that can withstand quantum attacks. Among the finalists, CRYSTALS-Kyber has emerged as a leading candidate for key exchange mechanisms due to its robust security proofs and efficient performance metrics.

Several studies have examined the integration of post-quantum algorithms into existing cryptographic infrastructures. For instance, Dashlane, a prominent password management provider, has initiated efforts to incorporate post-quantum cryptography into their systems. They have developed a proof-of-concept that integrates CRYSTALS-Kyber into their password sharing mechanisms, ensuring that credentials shared between users are protected against potential quantum threats .

Similarly, IBM's Key Protect service has adopted a hybrid approach, combining traditional elliptic curve Diffie-Hellman (ECDH) with CRYSTALS-Kyber to offer quantum-safe key exchange capabilities. This hybrid model allows users to benefit from the security of classical algorithms while preparing for the eventual transition to quantum-resistant methods .

The performance of CRYSTALS-Kyber has been a subject of extensive analysis. A study by Demir et al. (2025) provides a comprehensive performance evaluation of post-quantum cryptographic algorithms, including CRYSTALS-Kyber. The research benchmarks key operations such as key generation, encapsulation, and decapsulation, highlighting the algorithm's efficiency and suitability for real-world applications .

Despite the promising attributes of CRYSTALS-Kyber, challenges remain in its integration into existing systems. Issues such as backward compatibility with legacy systems, interoperability with other cryptographic protocols, and the need for hardware acceleration to meet performance requirements are critical considerations that need to be addressed for widespread adoption.

III. EXISTING CONFIGURATION

Current password management systems predominantly rely on classical cryptographic algorithms like RSA and ECC for securing user credentials. These systems employ asymmetric encryption for key exchange and symmetric encryption for data encryption. The process typically involves generating a public-private key pair, exchanging public keys between users, and using these keys to encrypt and decrypt data.

However, with the advent of quantum computing, these classical algorithms face potential vulnerabilities. Quantum algorithms, such as Shor's algorithm, can efficiently solve the integer factorization and discrete logarithm problems, which underpin the security of RSA and ECC, respectively. This capability threatens the foundational security of current password management systems.

To mitigate these risks, some systems have begun exploring hybrid cryptographic approaches. For example, Dashlane has implemented a hybrid mode that combines traditional RSA with CRYSTALS-Kyber. This approach ensures that even if quantum computers can break classical encryption methods, the system retains security through the quantum-resistant CRYSTALS-Kyber algorithm .

Despite these advancements, the integration of post-quantum algorithms into existing systems presents several challenges. These include the need for significant changes to the underlying infrastructure, ensuring compatibility with existing protocols, and addressing performance overheads associated with more complex cryptographic operations.

IV. METHODOLOGY

Integrating the CRYSTALS-Kyber algorithm into a secure password manager involves several key steps:

Assess the suitability of CRYSTALS-Kyber for the specific requirements of the password manager, considering factors such as security level, performance, and compatibility with existing systems.

Modify the password manager's architecture to incorporate CRYSTALS-Kyber. This may involve updating the key exchange protocols, encryption modules, and user authentication mechanisms to support the new algorithm.

Develop and integrate the necessary software components to implement CRYSTALS-Kyber. This includes coding the key generation, encapsulation, and decapsulation functions, as well as ensuring proper handling of keys and ciphertexts.

Conduct the correct functionality of the integrated system. This includes unit tests, integration tests, and performance benchmarks to validate the implementation.

Deploy the updated password manager to users and monitor its performance and security. Collect feedback to identify any issues and make necessary adjustments.

Provide users with information about the new cryptographic features and any changes to the user experience. Offer support to address any questions or concerns.

This methodology aims to ensure a seamless and secure integration of CRYSTALS-Kyber into the password management system, enhancing its resilience against future quantum threats.

V. PROPOSED CONFIGURATION

The proposed configuration for a secure password manager utilizing CRYSTALS-Kyber incorporates several enhancements to address the challenges identified in existing systems:

Replace traditional key exchange protocols with CRYSTALS-Kyber to establish secure communication channels resistant to quantum attacks.

Implement a hybrid model that combines classical encryption methods with CRYSTALS-Kyber. This dual-layered approach provides security against both classical and quantum threats.

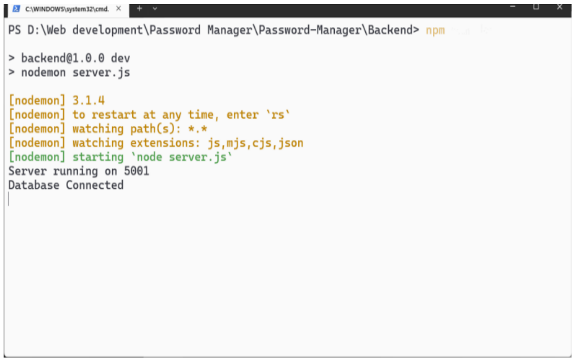
Utilize hardware acceleration techniques, such as AVX2 instructions, to enhance the performance of CRYSTALS-Kyber operations, ensuring that the system meets real-time requirements.

Design the system to maintain compatibility with legacy systems, allowing for a gradual transition to post-quantum cryptography without disrupting existing operations. Ensure that the integration of CRYSTALS-Kyber does not negatively impact the user experience. The system should remain intuitive and responsive, with all cryptographic operations abstracted away from the end user. Automated key generation, encryption, and decryption processes should operate seamlessly in the background to maintain user trust and usability.

Implement secure local and cloud-based storage of encrypted passwords using symmetric encryption keys exchanged via CRYSTALS-Kyber. Synchronization between devices should be encrypted end-to-end using session keys derived from the Kyber key encapsulation mechanism.

Add comprehensive logging of access and cryptographic events to help with post-incident investigations and forensic analysis. Logs should themselves be encrypted and protected using secure access control mechanisms.

VI. RESULTS



```
PS D:\Web development\Password Manager\Password-Manager\Backend> npm run dev

> backend@1.0.0 dev
> nodemon server.js

[nodemon] 3.1.4
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,cjs,json
[nodemon] starting `node server.js`
Server running on 5001
Database Connected
```

Fig. 6.1 Starting Server

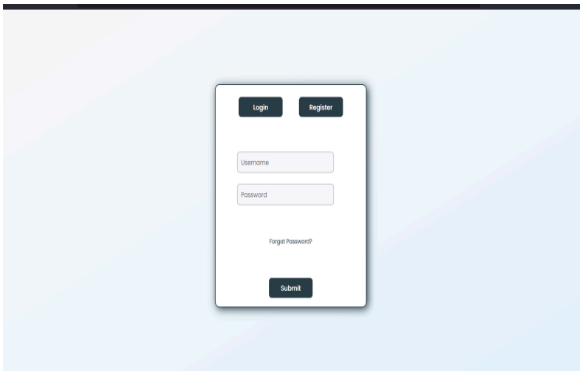
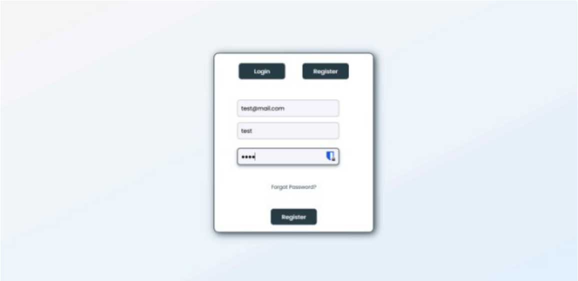
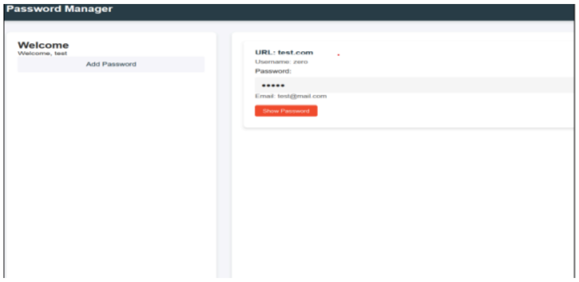


Fig. 6.2 Login Page



test@mail.com
test
••••

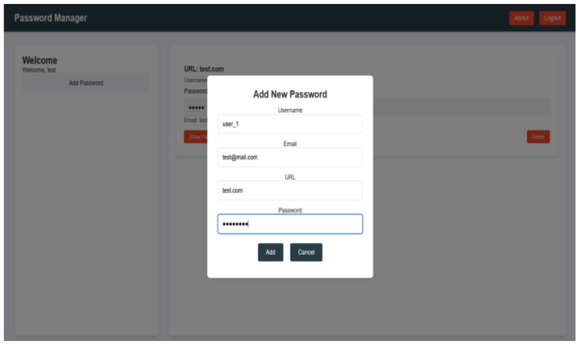
Fig. 6.3 Register Page



Welcome
Welcome, test

URL: test.com
Username: zero
Password:
•••••
Email: test@mail.com

Fig. 6.4 Dashboard



Add New Password

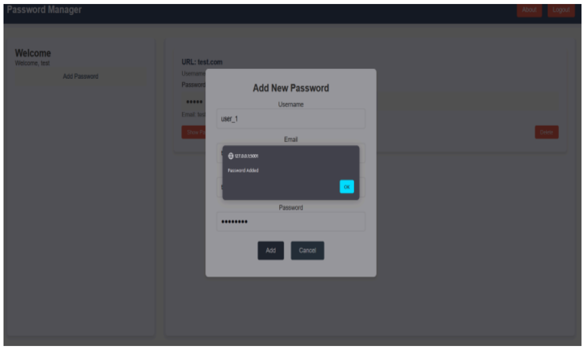
Username: user_1

Email: test@mail.com

URL: test.com

Password: ••••••••

Fig. 6.5 Adding Password



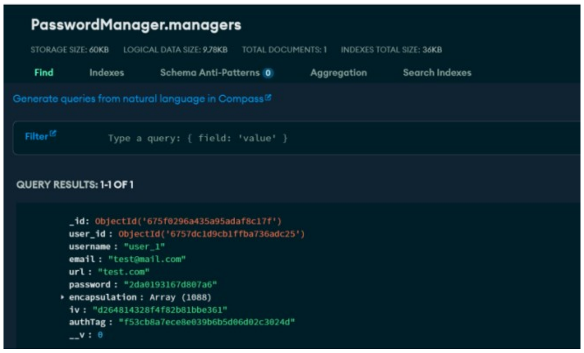
127.0.0.1:5001

Password Added

Username: user_1

Password: •••••••••

Fig. 6.6 Password Added



PasswordManager.managers

STORAGE SIZE: 60KB LOGICAL DATA SIZE: 9.78KB TOTAL DOCUMENTS: 1 INDEXES TOTAL SIZE: 36KB

Type a query: { field: 'value' }

QUERY RESULTS: 1-1 OF 1

```
_id: ObjectId('675f0296a435a95adaf8c17f')
user_id : ObjectId('6757dc1d9cb1ffba736adc25')
username : "user_1"
email : "test@mail.com"
url : "test.com"
password : "2da0193167d807a6"
▸ encapsulation : Array (1088)
iv : "d264814328f4f82b81bbe361"
authTag : "f53cb8a7ece8e039b6b5d06d02c3024d"
__v : 0
```

Fig. 6.7 Stored Encrypted Passwords

CONCLUSION

As quantum computing advances from theory to practical implementation, traditional cryptographic schemes face a diminishing security horizon. Password managers, being the custodians of sensitive user credentials, must evolve accordingly to remain secure in this emerging landscape. CRYSTALS-Kyber, with its robust foundation in lattice-based cryptography and selection as a NIST standard, offers a promising path forward for quantum-resilient key exchange.

This work proposed a comprehensive architecture for integrating CRYSTALS-Kyber into password management systems, leveraging its strengths while mitigating potential drawbacks through hybrid cryptography, hardware acceleration, and user-centric design. The outlined methodology provides a structured approach for development and deployment, ensuring that such systems can maintain operational integrity without compromising user experience or security.

Although challenges remain—particularly regarding legacy compatibility and performance—ongoing developments in post-quantum cryptography and increasing awareness of quantum threats make this integration not just feasible, but essential. With CRYSTALS-Kyber, the next generation of password managers can offer a durable defense against the evolving threats of the digital world.

REFERENCES

1. Bernstein, D.J., et al. (2022). Post-Quantum Cryptography: NIST's CRYSTALS-Kyber and CRYSTALS-Dilithium.

2. Bos, J.W., Ducas, L., Kiltz, E., et al. (2018). CRYSTALS – Kyber: A CCA-Secure Module-Lattice-Based KEM.

3. NIST. (2022). Post-Quantum Cryptography Standardization.

4. Chen, L., Jordan, S., Liu, Y.K., et al. (2016). Report on Post-Quantum Cryptography.

5. Dashlane Blog. (2023). Post-Quantum Cryptography in Dashlane.

6. IBM Research. (2023). Hybrid TLS with Quantum-Safe Algorithms.

7. Demir, M.A., et al. (2025). Performance Evaluation of Post-Quantum Cryptographic Algorithms.

8. Hülsing, A., Rijneveld, J., Schwabe, P. (2017). PQCrypto: Practical Post-Quantum Cryptography.

9. Peikert, C. (2016). A Decade of Lattice Cryptography.

10. Microsoft Research. (2023). PQCrypto Integration for Identity Management.

11. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P. (2016). Post-Quantum Key Exchange for the TLS Protocol.

12. FIPS 140-3. (2019). Security Requirements for Cryptographic Modules.

13. Singh, J., Kumar, R. (2023). Quantum Safe Cryptography in Cloud Password Management.

14. Brendel, J., Günther, F., Poettering, B. (2022). Kyber in Hybrid Key Encapsulation Schemes.

15. McGrew, D.A., Campagna, M. (2015). Considerations for Post-Quantum Cryptography.

16. Lyu, M., et al. (2021). A Survey on Post-Quantum Public-Key Cryptosystems.

17. Bindel, N., Brendel, J., et al. (2021). Hybrid Key Encapsulation and Quantum Security.

18. Rohit, S., and Jain, P. (2024). Password Vaulting with PQC: A Secure Future.

19. Mozilla Foundation. (2023). Quantum-Safe Cryptography in Firefox.

20. Google Security Blog. (2022). Preparing TLS for Post-Quantum Future.