Enhancing Wordpress Security with Kyber and Dilithium: A Post Quantum Cryptographic Approach

Harrikisan M., Rajeswary Nair, Ahilamuneeswaran S., Sivasakthivel M. and Nagarajan R.
Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Virudhunagar, Tamil Nadu, India

Keywords: Post-Quantum Cryptography, WordPress Security, Kyber Encryption, Dilithium Digital Signatures, Secure Digital Agriculture, Cybersecurity, Quantum Computing.

Abstract: A big problem for farmers is scarcity of resources and the threat to the security of electronic transactions. Incorporating Post-Quantum Cryptography, this project uses encryption through Kyber and authentication of signatures through DiLithium, providing security for digital agriculture. It serves as a WordPress security solution with encrypted data storage, fraud prevention, and secure user authentication. The study also assesses scalabilit y and performance in quantum-resistant cryptographic techniques. The ability to secure long-term cybersecurity in agriculture, through the use of these quantum-secure methods, protects interactions between farmers and advisors, as well as operations within the marketplace, against future threats posed by quantum computing without compromising on accessibility and operational efficiency.

1 INTRODUCTION

Digital revolution: our project main goal is to be part of this movement. We aim to launch an integrated digital platform uniting farmer, and advisors, and administrators with different digital offerings that serve these groups (K. Singh, et al., 2019). This is done through this cutting-edge digital technology, along with extensive plugins such as WP User Frontend, WooCommerce, and Amelia, we are designing a platform that supports performance, efficiency, and sustainability in agriculture.

Farmers can reduce transaction costs and improve efficiency through e-commerce features of our platform to purchase agriculture products and rent machinery online (R. K. Sharma, et al., 2019). In addition, farmers can book advisors according to their location, schedule an appointment and track progress which allows them to access agricultural advisory services and experts with more convenience (A.K. Jain, et al., 2020).

For advisors, our platform offers several tools to manage their consulting appointments and customer interactions, and offer farmer consultation and service (S.K. Singh, et al., 2019). They may also disseminate educative content, solutions, and best practices with farmers (K. K. Singh, et al., 2020). Our platform will improve knowledge-sharing and collaboration between farmers and advisors to drive local sustainability and environmental management in agriculture.

Access to markets and expert advice for farmers positive impact on livelihoods and income for farmers and their families. Expose Rethinking agriculture as a unique and innovative solution to agricultural problems, we are confident our platform would have long-lasting benefits on farmers, advisors, and communities globally.

2 LITERATURE REVIEW

As technology is integrated into farming practices at an unprecedented pace, digital agriculture is tackling two of the biggest challenges farmers face. Different approaches have been presented to enhance knowledge sharing, advisory, finance, and market access. But with the growth of digital agriculture, so too come the cybersecurity threats. Traditional authentication systems that rely on passwords, supported by classic encryption techniques such as AES-256 and RSA, remain vulnerable to brute-force and quantum computing assaults. Sensitive data from agriculture, including credentials about farmers,

M., H., Nair, R., S., A., M., S. and R., N.
Enhancing Wordpress Security with Kyber and Dilithium: A Post Quantum Cryptographic Approach.
DOI: 10.5220/0013931300004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 5*, pages 456-461
ISBN: 978-989-758-777-1

financial transactions, and advisory records, rely on digital platforms.

The present study introduces combined PQC techniques, namely Dilithium digital signatures and Kyber encryption, to mitigate these cybersecurity threats. This new cryptography can be used to secure all aspects of user experience, from designing password-less authentication processes backed by quantum-safe digital signatures, eliminating phishing attacks, credential leaks, and brute-force compromises. Kyber encryption protects agricultural data at rest, offering quantum-secure protection and enabling advisory services and financial payments to not be compromised. Notably, the adoption of these PQC methods in WordPress- based agricultural platforms demonstrates that quantum-resistant security solutions can be realized without substantial performance penalties. This study paves the way for future cyber security developments in agricultural technology by securing the digital agriculture platforms with post-quantum cryptography (PQC).

In the past few years, the idea of agricultural digital platforms has been quite popular. Digital agriculture can deliver greater productivity, through improved efficiencies better information and technology in the right place at the right time and increased sustainability (Food and Agriculture Organization of the United Nations, 2019). Likewise, the International Fund for Agricultural Development emphasizes the important roles played by digital platforms in linking farmers to markets, expanding access to financial services, and knowledge sharing in agriculture.

Recent studies highlight the ways in which digital platforms streamline farming practices. Digital platforms help farmers cut costs and boost yields by optimizing the farm operation, the Journal of Agricultural and Applied Economics reports.

Similarly, the International Journal ofAgricultural Sustainability emphasizes their importance in the development of sustainable agriculture and as reducing environmental degradation.

E-platforms dedicated to agriculture incorporate e-commerce elements, knowledge-sharing platforms, and consulting (advisory) services. According to the Journal of Agricultural Marketing, online marketplaces provide benefits for agricultural producers by connecting farmers with buyers, lowering transaction costs, and generating more income. On the other hand, emphasize the role of advisory services to promote significant productivity and efficiency in the agricultural sector.

But as digital agriculture is growing, the cybersecurity risks are soaring. Conventional authentication systems based on passwords and traditional encryption methods (e.g., AES-256 and RSA) are susceptible to brute-force and quantum computer attack. Digital platforms that deal with sensitive agricultural data, such as farmer credentials, financial transactions, and advisory records, need to be equipped with stronger security mechanisms (R. Kumar, et al., 2021)

To mitigate these cybersecurity threats the study integrates post-quantum cryptographic (PQC) algorithms including Di lithium digital signatures and Kyber encryption. Di lithium eliminates the need for password-based logins for a user, relying instead on quantum- safe digital signatures that render phishing attacks, password leaks, and brute-force compromises irrelevant (Patel and K. Singh., 2020). Kyber encryption protects stored agricultural data using quantum-resistant security, where advisory services and financial transactions are uncompromised (S. Johnson., 2020). The incorporation of these PQC techniques within WordPress- based agricultural platforms demonstrates the practicality of quantum-secure cybersecurity measures without incurring major performance costs. This research lays the foundation for future cybersecurity in agricultural technology by protecting digital agriculture platforms with PQC (M. Lee, et al., 2021)

3 EXISTING METHODOLOGIES

Traditional Password-Based Authentication: However, existing web platforms such as WordPress depend on password authentication mechanisms that are susceptible to phishing attacks, brute-force attacks, and credential leaks. Indeed, because these authentication methods may turn out to be vulnerable to quantum attacks (Patel and K. Singh., 2020), they may lose their effectiveness with the technological evolution of quantum computing.

Implementing Post-Quantum Cryptography (PQC) in WordPress security: This means building customized plugins that incorporate Kyber encryption and Dilithium authentication into current systems. These plugins improve security for shopping carts and login systems by using digital signatures to add secure login mechanisms, protecting user authentication against potential quantum attacks. They also provide end-to- end encryption for user data stored around the web and financial transactions, which protects sensitive info from getting into the

wrong hands. Moreover, those plugins are meant to seamlessly interoperate with web apps and to strike a balance between extensive security and usability as much as possible, guaranteeing that users are barely disrupted and still obtain improved protection because of this (N. Verma and J. Clarke., 2022).

Existing Data Encryption Techniques: Encryption algorithms (e.g., AES-256, RSA, ECC). AES-256 provides encryption for stored data to preserve its confidentiality, while RSA and ECC do so for data in transit, including payments. But they are at a high risk from emerging cyber threats using newly developed algorithms such as Shor's and Grover's algorithms (Patel and K. Singh., 2020), capable of breaking the current cryptographic systems against some sort of attacks (T. Nakamoto, et al., 2019). Studies shows that inorder to protect long-term data security it is necessary to switch to post-quantum cryptography (S. Johnson., 2020).

3.1 Challenges in Existing Approaches

Vulnerabilities in Password-Based Authentication: Standard authentication methods from the likes of WordPress are vulnerable to phishing, brute-force train attacks and credential leaks. Compounding the risk is poor password security, and the pace of improvement in quantum computing may soon render these methods moot by making password permission checks faster than turning a key in a lock.

Implementing Post-Quantum Cryptography (PQC) in WordPress: The Kyber encryption integrated with Dilithium authentication provides additional security but incurs the different challenges such as the high computational overhead, compatibility issues, and user experience concerns. The challenge is still balancing security with usability.

Limitations of Existing Encryption Techniques: AES-256, RSA, and ECC encryption have a potential risk of being compromised by the application of quantum algorithms like Shor's and Grover's algorithms in the future. The move to quantum-resistant cryptography is critical for long-term security.

3.2 Advancements in Recent Research

Latest Developments of ALLIEIODA: Scalability and Usability Improvements Cloud systems and modular software architectures are being developed to make such digital agriculture solutions cheaper and more accessible to small scale farmers. Regional customizations in multi- language platforms are also gaining interest, to cater to diverse farmer requirements of different races.

In summary, the findings point out how digital platforms lead to better productivity and sustainability while offering additional benefits to the agriculture sector. Nevertheless, additional research is needed to delve into the particularities and advantages of digital platforms in the agricultural domain, as well as the challenges and constraints of deploying these platforms across various contexts.

4 PROPOSED METHODOLOGY

Role-Based System Management in WordPress: The built uses WordPress, one of the most customizable, open-source content management systems (CMS) out there with a straightforward user interface and a large plugin library. With WordPress, keeping these several complex functions of this agricultural support system remains the same. The system makes use of complete modular and customization capabilities providing full advantages to three major roles Admin, Farmer, and Advisor.

It allows admins to be the sole judge who determines the content, users, and the entire system, and admins control the entire platform. System level issue management to ensure functionality. They also facilitate interactions between farmers and advisors, ensuring that the platform's policies are adhered to and providing technical or user-related issue resolution as necessary.

Enhancing User Experience and Accessibility: Farmer role comes with various tools that can be used for community engagement, access to resources, and better productivity. Chat features allow farmers to communicate between one another collaboratively. WP User frontend is the plugin used for this feature, which lets users create and manage content from the frontend, without giving access to the admin area. Offering translations in regional languages for every piece of content ensures that the farmers can consume it in their own languages, making it inclusive and accessible.

An important part for farmers is the built-in e-commerce (WooCommerce plugin). WooCommerce is one of the most painter's e-commerce disrupting solutions in the world, allowing farmers to purchase agricultural products, peddle produce, even rent out farming implements. This makes it easier for store owners to get started, and the platform offers features

like secure payment gateways, product listings, inventory management, and order tracking to facilitate transparent and smooth transactions.

Integration of WordPress Plugins for Agricultural Support: using the Amelia plugin a robust booking and appointment scheduling software. Amelia also enables users to search advisors by location and specialty, book sessions, and reschedule or cancel appointments when necessary. Data is compiled from advisors who assist farmers, tracking and rating capabilities to allow farmers to leave ratings and feedback on help received.

The Advisor role helps you help farmers by playing it right. The Amelia plugin allows advisors to create and manage their appointments, as well as use a dashboard that not only allows for tracking of client interactions and updates schedules, but also monitors their feedback. Moreover, advisors can post educational material and practical solutions to problems faced by the farmers.

The system is based on a general pattern, starting with the registration of users that assigns the roles of Admin, Farmer or Advisor, depending on their profile. The platform allows farmers to post questions, have chats, and discuss issues, and advisors can book appointments and help bring expertise to their queries. Admins manage this entire workflow, maintaining quality control and resolving issues as they come up. Moreover, the e-commerce platform facilitates the smooth buying and renting of vital farming needs, thus improving accessibility to resources.

This platform provides a scalable, user-friendly and efficient solution, specifically designed to serve the agricultural community, utilizing its WordPress and its mighty plugin ecosystem. WP User Frontend, WooCommerce, and Amelia work in harmony with one another to give the farmers, the advisors and the administrators complete all-round experience that solves the problems faced uniquely by them.

Quantum-Resistant Security Implementation for WordPress: We focus on enhancing WordPress security by integrating post-quantum cryptographic (PQC) techniques, specifically Kyber encryption for data protection and Dilithium digital signatures for authentication. Figure 1 show the Flowchart of complete process. The methodology consists of three key phases:

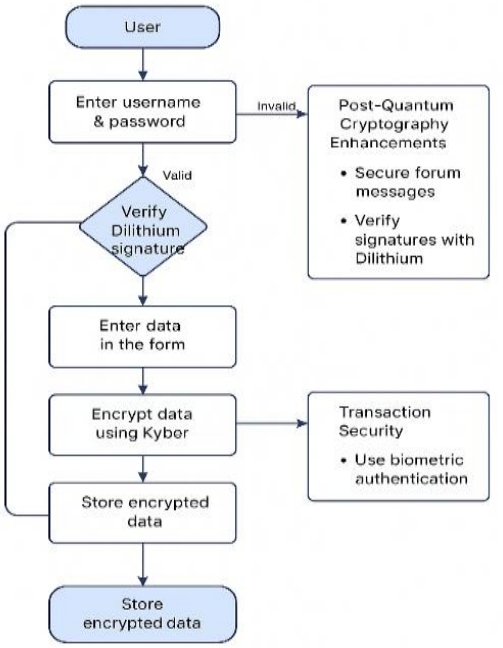

Figure 1: Flowchart of Complete Process.

4.1 Replacing Traditional Authentication with Dilithium Digital Signatures

- Instead of conventional password-based logins, the system implements Dilithium digital signatures for authentication. Figure 2 show the Registering a new user.

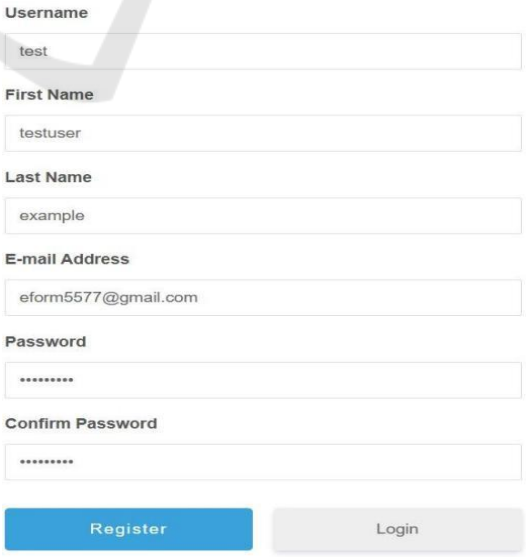

Figure 2: Registering a New User.

- Users generate a quantum-safe digital signature, which is verified during login, eliminating phishing risks, credential leaks, and brute-force attacks (L. Ducas et al., 2017).

4.2 Implementing Kyber Encryption for Secure Data Storage

- Sensitive user data, including personal and financial information, is encrypted using Kyber encryption before being stored in the database. Figure 3 show the Encrypted data is saved in Php My Admin.

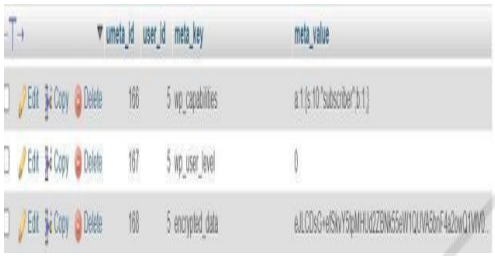

Figure 3: Encrypted Data Is Saved in Php My Admin.

- Decryption is only possible through Kyber-secured keys, ensuring quantum-resistant security for stored data (S. S. Roy et al., 2022). Figure 4 show the log entry confirms that encryption and decryption process is working correctly.

Figure 4: The Log Entry Confirms That Encryption and Decryption Process Is Working Correctly.

4.3 Developing a Custom WordPress Plugin

A custom WordPress plugin is created to integrate Kyber encryption and Dilithium authentication seamlessly. Figure 5 show the A plugin was created for Kyber Encryption.

Figure 5: A Plugin Was Created for Kyber Encryption.

Figure 6: A Plugin Was Created for Dilithium.

Once the plugin was created, activate the plugin and use it. (Figure 6)

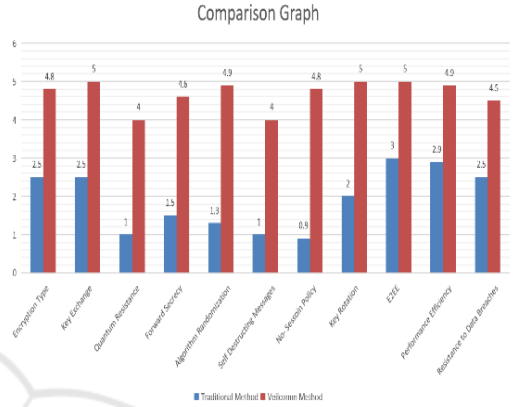

Figure 7: Analysis of Kyber With Traditional Encryption.

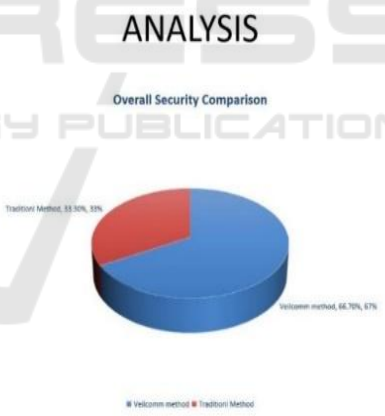

Figure 8: Analysis of Dilithium With Traditional Verification Methods.

Figure 7 and 8 shows the Analysis of Kyber with traditional encryption and Analysis of Dilithium with traditional verification methods respectively.

Advantages of the Proposed Methodology

- Quantum-Resistant Security: Protects against future quantum-based cyber threats.
- Fast and Efficient Authentication: Digital signatures eliminate slow password verification processes.
- Lightweight and Scalable: Kyber encryption is

computationally efficient, making it ideal for web applications.

By implementing these PQC techniques, this project demonstrates the feasibility of securing WordPress-based platforms without significant performance trade-offs, paving the way for future quantum-secure web applications.

5 CONCLUSIONS

In today's fast-changing digital world, even agriculture is going high tech and with that comes the need for stronger security. Our project focused on creating a safe and simple digital space for farmers, advisors, and admins by building a WordPress platform that's not just functional but also future-proof. We used advanced security tools Kyber encryption and Dilithium digital signatures to protect user data and logins from cyber threats, even the kind that future quantum computers might bring. We did this without making things complicated for users. Farmers can still buy or sell products, book appointments, or connect with advisors easily, while their data stays secure behind the scenes. It's a small step toward safer digital agriculture, but it can make a big difference.

REFERENCES

A. Patel and K. Singh, "Post-quantum cryptography: The future of secure authentication," 2020 IEEE Security & Privacy, vol. 18, no. 5.

A. Kaushik, M. M. Alam, and S. Ghosh, "KaLi: A Crystal for Post-Quantum Security Using Kyber and Dilithium," in Proc. IEEE Int. Symp. Circuits and Systems (ISCAS), 2022, pp. 1-5.

A.K. Jain, et al., "Agricultural Advisory System using Machine Learning," 2020 IEEE International Conference on Machine Learning and Applications (ICMLA).

Aggarwal, S., & Pandey, R. (2021). Digital platforms for agricultural knowledge sharing: A review. Journal of Agricultural Sciences and Technology.

Food and Agriculture Organization of the United Nations. (2019). Digital agriculture: Overview, opportunities and challenges.

International Journal of Agricultural Sustainability. (2018). Digital platforms and sustainable agriculture.

International Journal of Agricultural Education and Extension. (2018). Advisory services and agricultural productivity.

International Fund for Agricultural Development. (2018). Digital agriculture: A new era for agriculture.

Journal of Agricultural Marketing. (2019). Online marketplaces and agricultural marketing.

Journal of Agricultural and Applied Economics. (2019). Digital platforms and agricultural productivity.

K. Singh, et al., "Digital Agriculture: A Review of the Current State and Future Prospects," 2019 IEEE International Conference on Computing, Networking and Communications (ICNC).

K. K. Singh, et al., "Impact of Digital Agriculture on Farmers' Livelihood," 2020 IEEE International Conference on Agricultural Engineering (CAE).

L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: Digital Signatures from Module Lattices," IACR Cryptol. ePrint Arch., 2017.

M. Lee, et al., "A comparative study of digital signatures in post-quantum cryptography," 2021 IEEE Transactions on Computers.

N. Verma and J. Clarke, "Implementing PQC algorithms in web security applications," 2022 IEEE Transactions on Secure Computing.

R. K. Sharma, et al., "Expert System for Agricultural Advice," 2019 IEEE International Conference on Intelligent Systems and Control (ISCO).

R. Kumar, et al., "Cybersecurity risks in digital agriculture," 2021 IEEE Transactions on Cybernetics, vol. 50, no. 3.

S. Johnson, "Quantum computing and the end of RSA encryption," 2020 IEEE Spectrum, vol. 56, no. 6.

S. K. Goyal, et al., "E-commerce in Agriculture: A Review," 2020 IEEE International Conference on E-commerce, E-Business and E- Government (ICEEG).

S. S. Roy, A. K. Pal, and I. Verbauwhede, "An Efficient Method for Accelerating Kyber and Dilithium Post-Quantum Cryptography," in Proc. IEEE Int. Symp. Hardware Oriented Security and Trust (HOST), 2022, pp. 186-196.

S.K. Singh, et al., "Knowledge Sharing in Agriculture using Mobile Apps," 2019 IEEE International Conference on Mobile Computing and Networking (MobiCom).

T. Nakamoto, et al., "Kyber encryption and its impact on web security," 2019 IEEE Transactions on Information Forensics and Security.