International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Web based file encryption using quantum computing

Nikita Saidane, Soham Patil *, Sushant Rane and Teerth Shetty

Computer Engineering, Pillai HOC College of Engineering and Technology, Rasayani, India.

International Journal of Science and Research Archive, 2026, 19(02), 186-195

Publication history: Received on 09 March 2026; revised on 19 April 2026; accepted on 22 April 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.19.2.0605

Abstract

Our project, titled "Web-Based File Encryption Using Quantum Computing", presents a secure and innovative approach to data protection by integrating quantum principles into traditional encryption systems. The proposed web application leverages IBM Qiskit, a leading quantum computing framework, to simulate the generation of quantum-based encryption keys that are inherently unpredictable and resistant to classical hacking methods. Users can upload any file format such as text, image, or PDF and have it encrypted using a quantum-generated key, ensuring advanced security through the principles of quantum randomness. The system also provides a downloadable key for safe storage and future decryption. Furthermore, the same interface includes a decryption module, allowing users to decrypt their encrypted files by simply providing the correct key. This seamless integration of encryption and decryption in a web environment demonstrates how quantum computing can revolutionize modern cryptographic techniques, offering a more secure, efficient, and user-friendly solution for data confidentiality and protection in the digital age .

Keywords: IBM Qiskit; Quantum Key Generation; File Encryption; File Decryption; Data Security; Cryptography; Quantum Simulation

1. Introduction

The rapid growth of digital communication and cloud-based storage systems has significantly increased the volume of sensitive data exchanged over web platforms. As organizations and individuals increasingly rely on online services for file storage and sharing, ensuring data confidentiality and integrity has become a critical challenge. Traditional encryption mechanisms primarily depend on mathematical complexity and computational hardness, which are gradually becoming vulnerable due to advances in computing power and emerging cryptographic attacks. Moreover, conventional key generation methods often rely on pseudo-random processes, making them susceptible to prediction and compromise. The increasing frequency of cyberattacks, data breaches, and unauthorized access incidents highlights the limitations of existing security frameworks and emphasizes the urgent need for stronger and more resilient encryption standards. This situation necessitates the development of advanced security systems capable of providing enhanced protection and minimizing the risk of data leakage. [1]

Recent advancements in quantum computing, cryptography, and web technologies have introduced new possibilities for strengthening information security systems. Quantum Key Distribution (QKD) protocols and quantum-inspired random number generation techniques offer theoretically unbreakable security by exploiting the fundamental principles of quantum mechanics. These methods enable the generation of highly unpredictable encryption keys, making eavesdropping and interception practically impossible. In parallel, modern web frameworks and real-time communication technologies facilitate the integration of complex cryptographic mechanisms into user-friendly platforms. However, most existing implementations of quantum cryptographic techniques remain confined to laboratory environments and lack practical web-based deployment models. Current systems often employ classical

* Corresponding author: Soham Patil

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

encryption combined with limited quantum simulations, restricting their effectiveness and real-world applicability. [2]

Existing secure file-sharing platforms can generally be classified into two categories. The first category includes systems that rely solely on traditional cryptographic techniques such as AES and RSA for data protection. These platforms provide basic security functionalities but are increasingly exposed to brute-force attacks, key compromise, and computational advancements. Although suitable for general-purpose applications, such systems offer limited resistance against future quantum-based threats. The second category consists of platforms that incorporate partial quantum cryptographic elements or experimental security models. While these systems demonstrate improved resistance to attacks, they often lack comprehensive integration, scalability, and user accessibility. Additionally, many advanced platforms require specialized hardware or manual intervention for key management and secure communication, which restricts their widespread adoption. Therefore, an integrated and automated framework combining classical and quantum-inspired encryption techniques is essential for building practical and robust security solutions. [3]

This paper presents a comprehensive web-based file encryption system designed to enhance data security by integrating classical cryptography with simulated quantum key distribution and entanglement-based key generation mechanisms. The proposed system employs AES and RSA algorithms for data encryption while leveraging BB84-based quantum protocols and entangled session simulations for generating highly randomized encryption keys. A secure framework for file storage, sharing, and access control has been developed using modern web technologies and real-time communication modules. The key generation module ensures secure provenance tracking, while the quantum telemetry and entropy logging components provide transparency and reliability in key management. Furthermore, the system incorporates noise simulation and quantum laboratory modules to emulate real-world quantum communication environments. By combining quantum-inspired randomness, automated key management, and secure web-based operations, the proposed platform aims to strengthen data confidentiality, reduce vulnerability to cyber threats, and improve the overall reliability of digital file-sharing systems. [4]

2. Literature survey

Recent advancements in quantum cryptography and post-quantum security architectures have emphasized the need for hybrid encryption systems capable of resisting both classical and quantum-era attacks. Classical encryption mechanisms such as AES and RSA provide computational security; however, they rely on pseudo-random number generators and hardness assumptions that may become vulnerable with the development of large-scale quantum computers. Quantum Key Distribution (QKD), particularly the BB84 protocol, introduces information-theoretic security by exploiting quantum superposition and measurement disturbance principles. The detection of eavesdropping through Quantum Bit Error Rate (QBER) analysis provides a provable security advantage over classical key exchange mechanisms.

Entanglement-based cryptographic protocols such as the E91 scheme further extend secure communication by utilizing Bell states and CHSH inequality testing to verify genuine quantum correlations. Unlike classical systems that assume computational difficulty, entanglement-based security ensures that any interception attempt disturbs the quantum channel and becomes detectable. Additionally, privacy amplification techniques based on the Leftover Hash Lemma and Toeplitz matrix hashing strengthen final key secrecy even after partial information leakage during error correction. These mechanisms, combined with Cascade error correction and entropy-based key derivation, establish a mathematically rigorous framework for secure key generation in simulated quantum environments.

Recent developments in quantum simulation frameworks, particularly IBM Qiskit and AerSimulator, have enabled practical implementation of quantum cryptographic protocols without requiring dedicated quantum hardware. By integrating quantum-circuit-based entropy generation, Bell-state verification, CHSH testing, and hybrid post-quantum key encapsulation mechanisms within a full-stack web architecture, it becomes possible to bridge theoretical quantum cryptography and real-world secure file management. The combination of QKD-based key exchange, entanglement verification, Kyber style lattice-based post-quantum simulation, and authenticated AES-GCM encryption forms a multi-layered defense-in-depth security model. Such integration provides not only educational demonstration of quantum principles but also a scalable foundation for future quantum-resistant secure communication systems.

3. Methodology

The methodology of the proposed quantum-based file encryption system follows a structured 9-step approach, starting from user authentication to secure file sharing and continuous security monitoring through quantum-inspired key management and encryption mechanisms.

3.1. User Registration and Authentication

Users create secure accounts through JWT-based authentication, providing essential credentials for identity verification. The system establishes protected user profiles within PostgreSQL/SQLite databases, enabling personalized access control, activity logging, and secure session management.

3.2. Secure File Upload and Metadata Processing

Authenticated users upload digital files through encrypted communication channels. The system validates file formats, generates unique file identifiers, and stores encrypted metadata within the database. File attributes such as size, type, ownership, and access permissions are systematically recorded for secure management.

3.3. Quantum-Based Key Generation

Upon file upload, the system initiates automated key generation using three cryptographic models:

- RSA Key Generation for asymmetric encryption
- Quantum Key Distribution (BB84 Protocol) for secure key exchange
- Entanglement-Based Key Sessions for synchronized encryption keys
- The generated keys utilize quantum-inspired random number generators to ensure high entropy and unpredictability.

3.4. Encryption Algorithm Selection

Based on user preference and security requirements, the platform allows selection among multiple encryption mechanisms:

- AES for symmetric data encryption
- RSA for key encapsulation
- QKD and Entangled Keys for quantum-secured communication
- This hybrid approach ensures compatibility, flexibility, and enhanced resistance against cryptographic attacks.

3.5. File Encryption and Secure Storage

The selected encryption algorithm is applied to uploaded files using PyCryptodome libraries. Encrypted files are securely stored in protected repositories with access-restricted directories. Quantum provenance records are maintained to track key usage and encryption history.

3.6. Secure Sharing and Access Control

Encrypted files can be shared with authorized users through role-based permissions and digital tokens. The system enforces quantum-secured sharing by requiring successful QKD sessions or entanglement verification before granting download access. Real-time communication is managed using Socket.IO for secure session coordination.

3.7. Quantum Telemetry and Entropy Monitoring

The platform continuously monitors key generation and usage patterns through telemetry modules. Quantum entropy logs record randomness levels and protocol performance. Noise simulation mechanisms enable evaluation of system behavior under real-world quantum communication conditions.

3.8. Decryption and Download Authorization

Before file decryption, users must undergo identity verification and key validation procedures. The system ensures that only authenticated recipients with valid quantum session credentials can access decryption keys. Upon successful verification, files are decrypted locally and made available for secure download.

3.9. Continuous Security Evaluation and Optimization

The system supports iterative security assessment through repeated key generation, protocol testing, and performance monitoring. Users can review encryption logs, access historical key sessions, and analyze security metrics. Adaptive configuration mechanisms optimize encryption parameters, ensuring long-term resilience against evolving cyber threats.

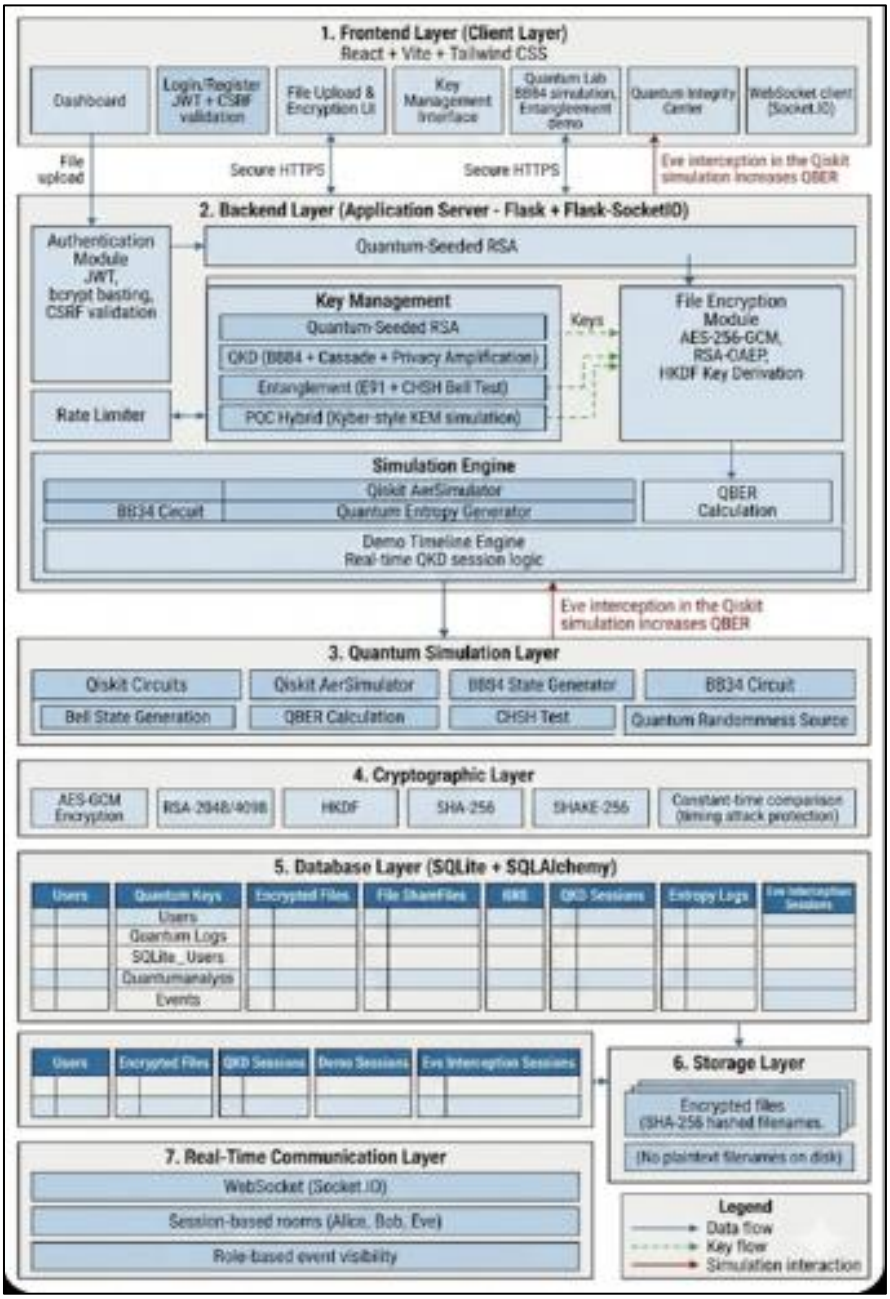

Figure 1 System Architecture

This methodology ensures end-to-end data security by integrating classical cryptographic techniques with quantum-inspired key management, secure storage, controlled sharing, and continuous system evaluation.

4. Result analysis

The proposed quantum-based file encryption system has been successfully implemented and tested, demonstrating effective data security, key management and secure file-sharing capabilities across multiple systems and user interactions.

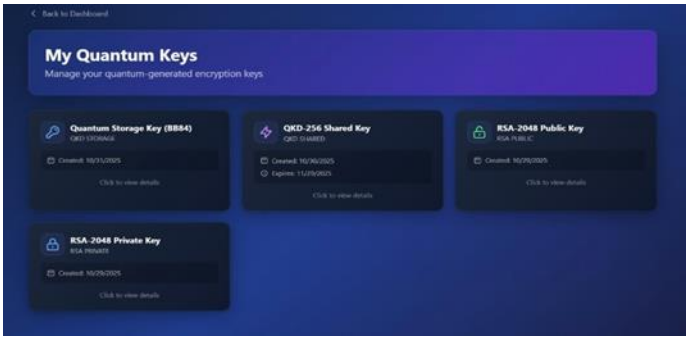

Figure 2 System Interface Implementation

4.1. Dashboard Interface

The main dashboard provides users with a comprehensive overview of system activities, including encrypted file statistics, active key sessions, sharing status and security alerts. It displays real-time information on file uploads, encryption history, key generation events and quantum session logs, enabling users monitor system performance and security status efficiently.

Figure 3 Dashboard Interface

4.2. File Upload and Encryption Interface

The file upload interface enables users to securely upload digital files and initiate encryption processes. Users can select preferred encryption mechanisms and quantum key models before uploading. The system performs automated validation and encryption, ensuring that files are securely processed and stored with minimal user intervention.

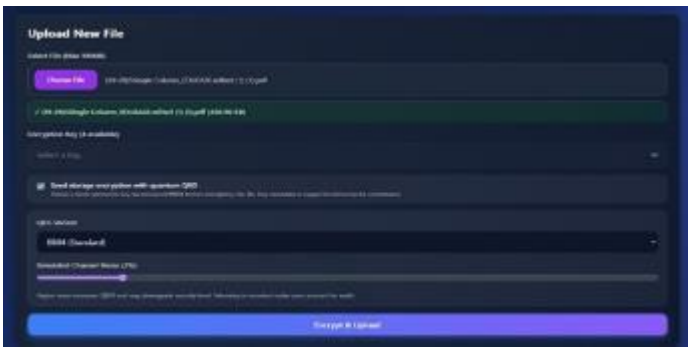

Figure 4 File Upload and Encryption Interface

4.3. My Quantum Keys Interface

The quantum key management interface displays all generated cryptographic keys, including Quantum Storage Keys (BB84-based keys), QKD 256-bit shared keys, RSA 2048-bit public keys, and RSA 2048-bit private keys. The interface allows users to view, download, and manage keys securely, ensuring controlled access and preventing unauthorized exposure.

Figure 5 My Quantum Keys Interface

4.4. Quantum Lab Interface

The Quantum Lab module provides a simulation environment for visualizing and analyzing quantum communication processes. It demonstrates key generation, entropy levels, and protocol behavior under varying conditions. Users can introduce controlled noise to observe system responses, facilitating experimental evaluation and educational understanding of quantum security mechanisms.

Figure 6 Quantum Lab Interface

4.5. BB84 Quantum Key Distribution Simulation

The BB84 simulation interface illustrates the complete quantum key exchange process between communicating entities. It presents photon polarization states, basis selection, key reconciliation stages, and error rates. The simulation enables users to verify protocol correctness and analyze system resilience against interception attempts.

Figure 7 BB84 Quantum Key Distribution Simulation

4.6. Quantum Entanglement Simulation Interface

This interface demonstrates entanglement-based key generation using Bell states and synchronized measurements between Alice and Bob. The system visualizes measurement correlations and entanglement stability, ensuring reliable key synchronization. Performance evaluation confirms consistent key agreement under controlled simulation conditions.

Figure 8 Quantum Entanglement Simulation Interface

4.7. Quantum Integrity Center

The Quantum Integrity Center monitors system security by assessing BB84 channel health, entangled lock status, and communication anomalies. It provides real-time alerts when simulated noise, interception attempts, or abnormal behaviors are detected. The live channel overview enables rapid response to potential security threats, enhancing system reliability.

Figure 9 Quantum Integrity Center

4.8. Secure Communication Channel and Interception Demonstration

A dedicated communication channel simulation module demonstrates secure data transmission between authorized users. The system includes an interceptor simulation mechanism that emulates eavesdropping and man-in-the-middle attacks. When interception attempts are detected, the platform generates real-time security alerts and logs abnormal channel behavior. This demonstration validates the effectiveness of quantum key distribution and entanglement-based security in preventing unauthorized access.

Figure 10 Secure Communication Channel Demonstration

4.9. Quantum Concept Demonstration Modules

The platform incorporates multiple interactive modules for demonstrating fundamental quantum computing and cryptographic concepts. These modules visualize quantum states, basis selection, measurement collapse, entanglement

correlations, and noise effects on transmission. By providing conceptual demonstrations, the system enhances user understanding of quantum security principles and supports experimental evaluation of protocol performance.

Figure 11 Quantum Concept Demonstration Module

4.10. Scope of research

The scope of this research focuses on the design and development of a quantum-based web encryption and secure file-sharing platform that integrates classical cryptographic techniques with quantum-inspired security mechanisms. The proposed system aims to enhance data confidentiality and transmission security by incorporating Quantum Key Distribution (BB84 protocol), entanglement-based key generation, and high-entropy random number generation for secure encryption. It supports secure file upload, storage, sharing, and controlled access through hybrid AES-RSA encryption models and quantum-secured authentication procedures. The platform also includes simulation modules such as the Quantum Lab, noise injection environment, and interception demonstration tools for evaluating protocol behavior under real-world conditions.

Furthermore, the research emphasizes the development of a scalable, user-friendly, and cost-effective security framework that can be deployed using standard web technologies without requiring specialized quantum

hardware. By integrating telemetry monitoring, entropy logging, and integrity assessment mechanisms, the system ensures continuous security evaluation and threat detection. The platform supports multi-user collaboration, role-based access control, and provenance tracking for secure data management. This research aims to provide a practical foundation for implementing quantum-resistant encryption systems in web environments, contributing to improved cybersecurity resilience, secure digital communication, and long-term data protection against emerging quantum-era threats.

5. Results and discussion

The implementation of the proposed quantum-based file encryption system demonstrates clear improvements over traditional data security and file-sharing approaches. The platform effectively integrates classical cryptographic algorithms with quantum-inspired key generation, secure key exchange, and entanglement-based authentication mechanisms to enhance data confidentiality and transmission reliability. Features such as BB84-based key distribution, quantum entropy monitoring, secure file sharing, and real-time integrity assessment provide a comprehensive security framework, while simulation modules, noise injection environments, and interception demonstrations enable practical evaluation under realistic conditions.

Figure 12 Result

The system's automated key management, provenance tracking, and anomaly detection mechanisms assist users in identifying potential security risks and maintaining secure communication channels. Its modular and scalable architecture ensures compatibility with standard web technologies while supporting multi-user collaboration and controlled access management. Furthermore, the user-friendly interface simplifies complex cryptographic operations, making advanced security mechanisms accessible to non-expert users. Overall, the proposed platform proves to be a practical and effective solution for strengthening digital data protection, improving resistance to cyber threats, and supporting the adoption of quantum-resistant security practices in modern web environments.

6. Conclusion

The integration of quantum-inspired cryptographic techniques in web-based security systems has become essential for ensuring data confidentiality, integrity, and resilience against emerging cyber threats in modern digital environments. Existing file encryption and secure data-sharing platforms primarily rely on classical cryptographic algorithms and pseudo-random key generation methods, which are increasingly vulnerable to advanced computational attacks and future quantum-based intrusions. Many conventional systems lack secure key exchange mechanisms, real-time integrity monitoring, entanglement-based authentication, and adaptive security evaluation, thereby limiting their effectiveness in providing long-term data protection and reliable access control. To overcome these limitations, the proposed quantum-based file encryption platform implements a hybrid security framework integrating AES and RSA encryption with simulated Quantum Key Distribution (BB84 protocol), entanglement-assisted key generation, and high-entropy random number generation mechanisms. The system features secure file upload, encrypted storage, quantum-secured sharing, provenance tracking, and real-time anomaly detection through the Quantum Integrity Center.

Experimental testing and system deployment demonstrated improved key randomness, secure transmission reliability, and enhanced resistance to interception and unauthorized access attempts. Users were able to securely manage encryption keys, monitor security status, and exchange sensitive files with minimal risk of compromise. The platform's user-friendly interface and scalable web architecture further support practical adoption in academic and organizational environments. Overall, this project demonstrates that integrating quantum-inspired cryptographic mechanisms with modern web technologies can significantly enhance data security and establish a foundation for quantum-resistant communication systems. By providing automated key management, continuous security monitoring, and comprehensive simulation capabilities, the proposed platform contributes to advancing secure digital communication practices. Future enhancements may include integration with real quantum hardware, implementation of post-quantum cryptographic algorithms, advanced intrusion detection models, and cross-platform deployment to further improve system effectiveness and long-term cybersecurity resilience.

6.1. Future scope

In the future, the proposed quantum-based file encryption platform can be enhanced by integrating real quantum communication hardware and quantum processors to support true quantum key distribution beyond software-based simulation. The system can also be extended to incorporate advanced post-quantum cryptographic algorithms, enabling stronger resistance against emerging quantum-era attacks. Support for multi-user enterprise environments with hierarchical access control, automated policy enforcement, and large-scale data management can further improve system applicability in organizational settings.

Additionally, the platform may be expanded with intelligent threat detection models based on machine learning to enable predictive security analysis and proactive defense mechanisms. Integration with distributed ledger technologies can improve key provenance tracking and auditability. Further development of cross-platform support, mobile accessibility, and cloud-native deployment architectures will enhance scalability and usability. These advancements will make the proposed system more intelligent, robust, and comprehensive, contributing to the development of next-generation quantum-resistant cybersecurity solutions.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Markku-Juhani Saarinen and Daniel Smith-Tone, "Post-Quantum Cryptography: Proceedings of PQCrypto 2024 (Part I)," Lecture Notes in Computer Science, Springer, 2024.

[2] Markku-Juhani Saarinen and Daniel Smith-Tone, "Post-Quantum Cryptography: Proceedings of PQCrypto 2024 (Part II)," Lecture Notes in Computer Science, Springer, 2024.

[3] M. Khalil et al., "Experimental Demonstration of Quantum Encryption in Phase-Modulated Coherent Optical Systems," EPJ Quantum Technology, 2024.

[4] A. Shafique et al., "A Hybrid Encryption Framework Leveraging Quantum and Classical Methods," Scientific Reports (Nature), 2024.

[5] Arman Sykot and M.R.C. Mahdy, "Combining Entangled and Non-Entangled Based Quantum Key Distribution Protocol with GHZ State," Preprint (Simulations with Qiskit), 2024.

[6] N. Sharma, "Unleashing the Potential of Quantum Key Reconciliation," arXiv Preprint, 2024.

[7] P. Pathak, "The Evolution of IBM's Quantum Information Software Kit (Qiskit)," arXiv Preprint, 2025.

[8] IBM Quantum Research Group, "Quantum Key Generation and Qiskit Applications," IBM Quantum Documentation and Research Notes, 2024.

[9] I. Kong, "Realizing Quantum-Safe Information Sharing," ScienceDirect Journal of Information Security, 2024.

[10] Peddi Gowtham Balaji et al., "Optimizing Compiler for Quantum Computing Using Qiskit Terra," Proceedings of ICCCNT 2024 (IEEE Conference), 2024.

[11] Qiskit Machine Learning Team, "Qiskit Machine Learning: An Open-Source Library," ResearchGate Publication, 2025.

[12] A. Mehra and S. Bansal, "A Survey on Design and Implementation of Quantum Computing Circuit Optimization Using Qiskit," ResearchGate, 2025.

[13] S. Patel et al., "Simulation of an Entanglement-Based Quantum Key Distribution Protocol," ResearchGate, 2024.

[14] K. Choudhary et al., "Quantum Secure Key Generation for QKD Protocols Using Quantum Gates," ResearchGate, 2024.

[15] V. Sharma and P. Ghosh, "Develop a Quantum Key Distribution Application Based on the BB84 Protocol Combined with a Classical Channel," ResearchGate, 2024.

[16] R. Kumar et al., "Investigating Quantum Entanglement by Using IBM's Qiskit," ResearchGate, 2024.

[17] M.-J. Saarinen, "Practical Implementations and Transition Strategies in Post-Quantum Cryptography," PQCrypto 2024 Proceedings, Springer, 2024.

[18] T. Nguyen and A. Gupta, "Adaptive Attacks and Overview of Post-Quantum Cryptography," Springer Professional Collection, 2024.

[19] S. Chen et al., "W3ID: A Quantum Computing-Secure Digital Identity System," arXiv Preprint, 2025.

[20] J. Patel et al., "Qiskit as a Simulation Platform for Measurement-Based Quantum Computation," ResearchGate, 2024.