Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

AI-Driven Threat Detection and Response Using Quantum Cryptography

Prof. Mohini A. Thorat
Department of Computer Engineering
JSPM's Jayawantrao Sawant College of Engineering, Pune

Janhvi Chavan
Department of Computer Engineering
JSPM's Jayawantrao Sawant College of Engineering, Pune

Anushka Kumbhar
Department of Computer Engineering
JSPM's Jayawantrao Sawant College of Engineering, Pune

Mithilesh Kadam
Department of Computer Engineering
JSPM's Jayawantrao Sawant College of Engineering, Pune

Aditya Shinde
Department of Computer Engineering
JSPM's Jayawantrao Sawant College of Engineering, Pune

Abstract—The rapid advancement of quantum computing poses a significant threat to conventional cryptographic systems that rely on computational complexity for security [3]. Quan-tum Key Distribution (QKD) offers a secure communication mechanism based on the principles of quantum mechanics, enabling the detection of unauthorized interception attempts [1]. However, practical QKD deployments remain vulnerable to channel noise, hardware imperfections, and sophisticated eavesdropping attacks [5], [6]. This paper presents an AI-driven threat detection and response framework that combines BB84 Quantum Key Distribution, IBM Qiskit simulation, and machine learning-based anomaly detection [9]. A high-fidelity quantum simulator is developed using IBM Qiskit and AerSimulator to model realistic quantum communication channels with depo-larizing noise. A Random Forest classifier trained on 50,000 simulated transmission sequences identifies malicious activities by analyzing Quantum Bit Error Rate (QBER), noise levels, sifted key lengths, and engineered heuristic features [7]. Experimental analysis demonstrates high detection accuracy while maintaining real-time operational capabilities. The proposed system further incorporates automated mitigation techniques including Privacy Amplification and E91 protocol migration to enhance quantum network resilience [2]. The results demonstrate that integrating artificial intelligence with quantum cryptography significantly improves threat detection, response efficiency, and overall com-munication security.

Index Terms—Quantum Cryptography, QKD, BB84, Random Forest, IBM Qiskit, Threat Detection, Anomaly Detection, Secu-rity Operations Center

I. Introduction

The increasing computational power of modern systems and the emergence of quantum computing technologies have raised serious concerns regarding the long-term security of traditional cryptographic algorithms [10]. Widely deployed encryption schemes such as RSA and Elliptic Curve Cryptography rely on mathematical problems that are computationally infeasible for classical computers. However, quantum algorithms such as Shor's Algorithm have demonstrated the theoretical capa-bility to solve these problems exponentially faster, potentially rendering current cryptographic infrastructures obsolete [3].

Quantum Key Distribution (QKD) has emerged as a promis-ing solution to this challenge. Unlike classical encryption systems that depend on computational hardness, QKD de-rives its security from the fundamental principles of quantum mechanics [4]. The BB84 protocol, introduced by Bennett and Brassard, enables two communicating parties to establish a shared secret key while ensuring that any eavesdropping attempt introduces detectable disturbances into the quantum channel [1].

Although QKD offers theoretically unconditional security, practical implementations face several challenges. Environ-mental noise, transmission losses, hardware imperfections, and malicious attacks can significantly affect communication reliability [6]. Among these threats, intercept-resend attacks remain one of the most important security concerns. In such attacks, an adversary intercepts transmitted photons, performs measurements, and forwards replacement photons to the re-ceiver. Due to the No-Cloning Theorem and wave-function collapse, these actions introduce measurable errors into the communication channel [5].

Machine learning techniques have been proposed to en-hance anomaly detection in network security systems [8],[11]. Integrating machine learning with quantum cryptography creates an intelligent layer capable of distinguishing malicious interception from natural channel noise, enabling automated and adaptive threat response [12].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

II. Literature Survey

BB84 established the foundation of quantum cryptography by enabling secure key exchange with eavesdropping detection [1]. E91 later improved security through entanglement-based communication [2]. Research by Scarani et al. highlighted the importance of Quantum Bit Error Rate (QBER) in evaluating channel security [5], while Pirandola et al. discussed practical deployment challenges in quantum networks [6].

Machine learning techniques have been widely applied in cybersecurity [8]. Random Forest, introduced by Breiman, offers high accuracy and robustness against overfitting, making it suitable for anomaly detection [7]. Although substantial research exists in both quantum cryptography and machine learning, few studies integrate quantum simulation, threat detection, visualization, and automated response within a single framework [11], [12].

A. Research Gap

- Limited intelligent threat detection in QKD systems [5].
- Dependence on static QBER thresholds [6].
- Lack of automated mitigation mechanisms.
- Minimal integration of AI, quantum simulation, and SOC monitoring [8].

III. Proposed System

The proposed system presents an intelligent Security Operations Center (SOC) architecture designed for real-time monitoring, detection, and mitigation of threats in Quantum Key Distribution (QKD) networks. The framework integrates quantum cryptographic simulation, machine learning-based anomaly detection, automated response mechanisms, and interactive visualization to provide end-to-end security management.

A. System Objectives

The primary objectives of the proposed system are:

- To simulate realistic BB84 Quantum Key Distribution channels using IBM Qiskit [9].
- To model environmental noise and intercept-resend attacks using quantum mechanical principles [10].
- To develop an intelligent threat detection framework using machine learning [7].
- To distinguish malicious activities from normal channel degradation [8].
- To provide real-time visualization and monitoring capabilities.
- To automate threat response and channel protection mechanisms.

B. System Architecture

The proposed architecture consists of the following layers:

1) Quantum Simulation Layer
2) Data Generation and Feature Extraction Layer
3) Machine Learning Inference Layer
4) Security Operations Center Dashboard
5) Automated Mitigation Layer

The Quantum Simulation Layer generates quantum communication data using BB84 protocol operations [1]. The generated data is processed to compute Quantum Bit Error Rate (QBER), noise levels, and sifted key lengths [5]. These values are then forwarded to the Machine Learning Layer for threat classification [7]. Finally, the dashboard visualizes system status and initiates mitigation procedures when threats are detected.

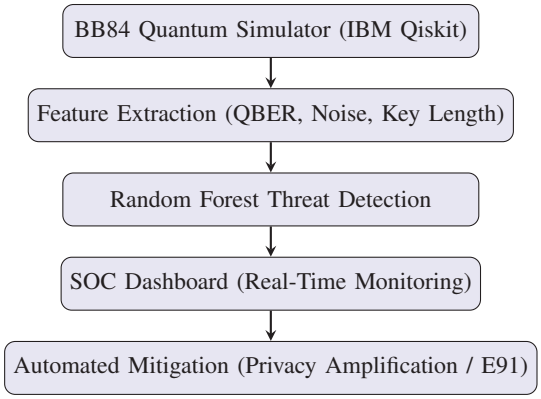

Fig. 1. Architecture of the Proposed AI-Driven QKD Threat Detection Framework.

The system consists of five sequential layers: Quantum Simulation, Feature Extraction, Machine Learning Inference, SOC Monitoring, and Automated Mitigation.

The framework consists of five layers as shown in Fig. 1: Quantum Simulation, Feature Extraction, Machine Learning Inference, SOC Monitoring, and Automated Mitigation. Quantum communication data generated using BB84 [1] is processed into security metrics and classified by a Random Forest model [7]. Threats detected by the classifier trigger automated countermeasures.

IV. Methodology

A. Phase 1: Quantum Simulation

BB84 communication is simulated using IBM Qiskit and AerSimulator [9]. Alice and Bob exchange quantum states through noisy channels, generating realistic communication records [1], [10].

B. Phase 2: Attack Injection

Intercept-resend attacks are introduced by allowing an adversary to measure and retransmit photons. Incorrect basis selection increases QBER and produces identifiable attack patterns [4], [5].

C. Phase 3: Feature Extraction

The extracted features include:

- QBER (Quantum Bit Error Rate) [5]
- Noise Level (Depolarizing noise parameter) [9]
- Sifted Key Length
- Effective Key Rate
- Eve Contribution (engineered heuristic feature)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

$$\text{EveContribution} = \max(0,\ \text{QBER} - 0.66 \times \text{NoiseLevel}) \quad (1)$$

D. Phase 4: Threat Detection

A Random Forest classifier is trained using 50,000 simulated transmission records [7]. The model classifies communication sessions as secure or compromised. Random Forest was selected for its robustness against overfitting, high accuracy on high-dimensional data, and interpretability of feature importance [7], [8].

E. Phase 5: Automated Mitigation

Threats trigger Privacy Amplification and migration to the E91 protocol to maintain communication security [2], [6].

V. Experimental Results and Discussion

The experimental environment consisted of the following components:

- IBM Qiskit for BB84 quantum simulation [9]
- Qiskit AerSimulator for noisy quantum execution [9]
- Python and FastAPI backend services
- Scikit-learn Random Forest Classifier [7]
- React-based Security Operations Center Dashboard
- Dataset consisting of 50,000 quantum transmission records

Each simulation generated communication metrics including Quantum Bit Error Rate (QBER), noise level, sifted key length, effective key rate, and engineered heuristic features.

A. Performance Metrics

To evaluate the effectiveness of the proposed model, standard machine learning performance metrics were employed: Accuracy, Precision, Recall, and F1-Score [7], [8].

Accuracy measures overall prediction correctness, while Precision evaluates the percentage of correctly identified attacks among all detected attacks. Recall measures the model's ability to identify actual attacks, and F1-Score provides a balanced evaluation of Precision and Recall.

B. Classification Results

The Random Forest classifier demonstrated strong performance in distinguishing malicious interception attempts from normal environmental noise.

Metric	Value
Accuracy	93.5%
Precision	95.8%
Recall	94.9%
F1-Score	95.3%

TABLE I
Classification Results of Random Forest Classifier

As shown in Table 1, the Random Forest classifier achieved high accuracy, precision, recall, and F1-score, demonstrating its effectiveness in distinguishing malicious attacks from normal environmental noise [7].

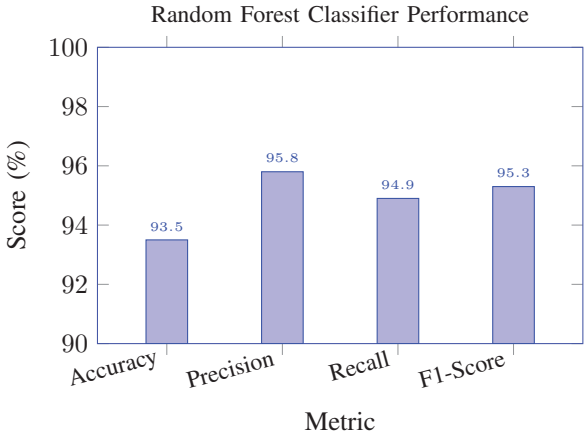

Fig. 2. Comparative performance of the Random Forest classifier

Fig. 2 illustrates the comparative performance of the Random Forest classifier across the four evaluation metrics, highlighting consistently high values for accuracy, precision, recall, and F1-score.

C. Impact of QBER on Threat Detection

Quantum Bit Error Rate (QBER) plays a critical role in determining channel security [5]. Under normal operating conditions, QBER remained within acceptable limits caused by environmental disturbances and transmission imperfections. However, when intercept-resend attacks were introduced, significant increases in QBER were observed [4].

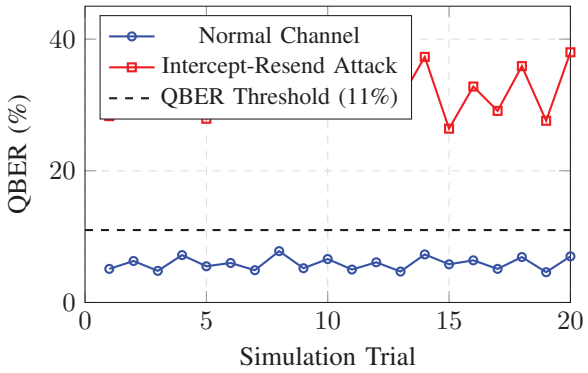

Fig. 3. QBER values under normal channel conditions versus intercept-resend attack conditions across 20 simulation trials.

The machine learning model successfully learned these behavioral patterns and utilized them for reliable attack classification, as illustrated in Fig. 3 [5], [7].

D. Effectiveness of Feature Engineering

A custom heuristic feature was introduced to isolate attacker-induced disturbances from natural channel noise:

$$\text{EveContribution} = \max(0,\ \text{QBER} - 0.66 \times \text{NoiseLevel}) \quad (2)$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

The engineered feature significantly improved classification performance by removing expected environmental depolarization effects and highlighting anomalies caused by malicious interference [5]. Experimental observations indicated that this feature contributed substantially to reducing false alarm rates while improving attack detection accuracy [7].

E. Automated Mitigation Analysis

Upon detection of a high-probability threat, the Security Operations Center automatically initiated mitigation procedures [6]. The first mitigation stage employed Privacy Amplification to reduce attacker knowledge regarding generated keys. Although this process reduced effective key generation rates, it restored communication security. Migration to the E91 protocol was subsequently triggered for sessions under sustained attack [2].

VI. Advantages of the Proposed System

- **Real-Time Monitoring:** Provides continuous monitoring of quantum communication channels [8].
- **Accurate Attack Detection:** Accurately detects intercept-resend attacks using machine learning [7].
- **Noise Differentiation:** Differentiates malicious activities from normal environmental noise using engineered features [5].
- **Realistic Simulation:** Utilizes realistic quantum simulations through IBM Qiskit [9].
- **Automated Response:** Triggers countermeasures automatically without manual intervention [6].
- **Scalability:** The modular architecture allows extension to additional QKD protocols and hardware platforms [4].

VII. Future Scope

Future enhancements can further improve the capabilities of the proposed framework:

- Integration with real quantum hardware available through IBM Quantum platforms [9].
- Support for additional QKD protocols beyond BB84 and E91 [2], [4].
- Application of deep learning models for advanced threat intelligence [11], [12].
- Deployment in enterprise quantum network testbeds for real-world validation [6].
- Federated learning approaches to enable collaborative threat detection across distributed QKD nodes [12].

VIII. Conclusion

This paper presented an AI-driven threat detection and response framework for securing Quantum Key Distribution networks against malicious interception attempts [1], [3]. The proposed architecture integrates IBM Qiskit-based BB84 simulation [9], Random Forest machine learning classification [7], real-time Security Operations Center monitoring, and automated mitigation mechanisms [2].

A dataset consisting of 50,000 simulated transmission sequences was utilized to train and evaluate the detection model. Experimental results demonstrated strong performance with an accuracy of 93.5%, precision of 95.8%, recall of 94.9%, and F1-score of 95.3% [7].

The integration of Privacy Amplification and E91 protocol migration further enhanced communication security by enabling automated defensive responses [2], [6]. The overall results indicate that combining artificial intelligence with quantum cryptography provides an effective and scalable solution for protecting future quantum communication infrastructures [5], [8].

Acknowledgment

The authors express their sincere gratitude to Prof. Mohini A. Thorat, Department of Computer Engineering, JSPM's Jayawantrao Sawant College of Engineering, Pune, for her valuable guidance, encouragement, and continuous support throughout the development of this project and research work.

References

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984.
[2] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.
[3] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.
[4] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.
[5] V. Scarani et al., "The Security of Practical Quantum Key Distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.
[6] S. Pirandola et al., "Advances in Quantum Cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.
[7] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
[8] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Symposium on Security and Privacy*, 2010.
[9] H. Abraham et al., "Qiskit: An Open-Source Framework for Quantum Computing," IBM Research, 2024.
[10] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010.
[11] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung, "Intrusion Detection System: A Comprehensive Review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.
[12] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, "An Empirical Comparison of Botnet Detection Methods," *Computers & Security*, vol. 45, pp. 100–123, 2014.
[13] H.-K. Lo, M. Curty, and K. Tamaki, "Secure Quantum Key Distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014.
[14] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the Rate-Distance Limit of Quantum Key Distribution Without Quantum Repeaters," *Nature*, vol. 557, pp. 400–403, 2018.
[15] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure Quantum Key Distribution with Realistic Devices," *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.
[16] R. Alléaume et al., "Using Quantum Key Distribution for Cryptographic Purposes: A Survey," *Theoretical Computer Science*, vol. 560, pp. 62–81, 2014.
[17] I. Vagniluca et al., "Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution," *Physical Review Applied*, vol. 14, p. 014051, 2020.