AI and Quantum for Secure Data Transmission

Ishak Tegguiche
Abdelrahmen Abdat
Bahae Medjdoub
Madjda Stambouli

Higher School of Computer Science May 8, 1945-ESI SBA-Sidi Bel Abbes, Algeria
03 Mai 2025

abstract- As Algeria advances digitally, cybersecurity becomes critical. This study proposes a hybrid approach combining AI-based anomaly detection for real-time threat identification with Quantum Key Distribution (QKD) for secure encryption. AI ensures scalable short-term protection, while QKD offers long-term, tamper-resistant security. Together, they form a complementary strategy for a resilient digital future in Algeria

I. INTRODUCTION

As digital transformation accelerates across various sectors, securing sensitive data against evolving cyber threats has become a global priority. Traditional encryption techniques, while effective to a degree, are increasingly challenged by sophisticated attacks and the looming threat of quantum computing. In this context, there is a growing need for hybrid approaches that combine both classical and quantum security mechanisms.

This study explores a dual-layered cybersecurity strategy that integrates artificial intelligence (AI) for real-time data breach detection with Quantum Key Distribution **(QKD)** for next-generation secure communication. The first layer employs AI-based anomaly detection to identify unauthorized access or data exfiltration patterns by analyzing network behavior. The second layer involves the implementation of the **BB84** QKD protocol to ensure the secure transmission of encryption keys, offering theoretically unbreakable security against eavesdropping.

By comparing these two approaches **AI-based detection** and **quantum-secure encryption** this research aims to evaluate their respective strengths, limitations, and potential for integration. The goal is to highlight how such a hybrid model could enhance data protection strategies, particularly in environments facing increasing cybersecurity threats, such as the financial sector.

II. RELATED WORKS

Numerous studies have explored the use of AI for intrusion detection, leveraging datasets such as : **1-UNSW-NB15** and **CICIDS** to classify traffic and detect anomalies with high accuracy.

2-Machine learning techniques like random forests, deep neural networks, and support vector machines have proven effective in identifying classical cyber threats.

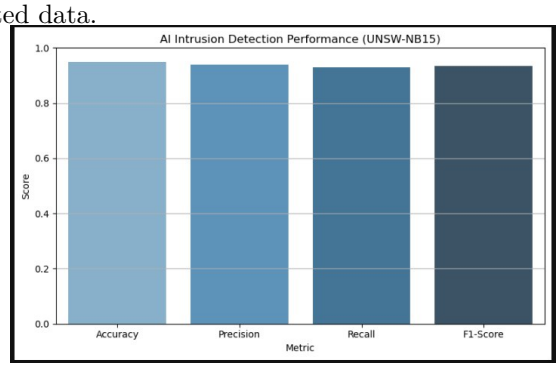
3-QKD, particularly the BB84 protocol introduced by Bennett and Brassard in 1984, has emerged as a promising solution for secure key exchange, leveraging quantum mechanics to guarantee eavesdropping detection.

Prior work has largely focused on either AI-driven detection or quantum-secure communication independently. Our work seeks to bridge the gap by implementing both approaches in tandem and analyzing their comparative performance in practical scenarios.

III. METHODOLOGY

3.1 Classical AI-Based Detection :

To simulate data breach detection, we utilized the UNSW-NB15 dataset, which contains network traffic labeled with various types of attacks and normal behavior. Features such as IP address activity, packet size, protocol type, and session duration were extracted and preprocessed. We trained a supervised machine learning model (e.g., Random Forest or CNN) to classify events as either normal or malicious. The model was evaluated using standard metrics including accuracy, precision, recall, and F1-score, aiming to detect anomalous patterns that could indicate unauthorized access to encrypted data.



UNSW-NB15 : a comprehensive data set for network intrusion detection

3.2 Quantum Key Distribution with BB84

In the quantum part of the project, we implemented the BB84 protocol using Qiskit, simulating secure key exchange between two parties (Alice and Bob). The protocol involved randomly generating bit values and encoding them into quantum states using two bases (Z and X) .

An eavesdropper (Eve) was simulated to interfere with the transmission, measuring qubits in a randomly chosen basis. The disturbance introduced by Eve was quantified using the Quantum Bit Error Rate **(QBER)**. If the QBER exceeded a predefined threshold (typically 11 out of 100), eavesdropping was inferred. The implementation was validated on both local simulators and real **IBM** quantum hardware (e.g., ibm$_b$*risbane*).

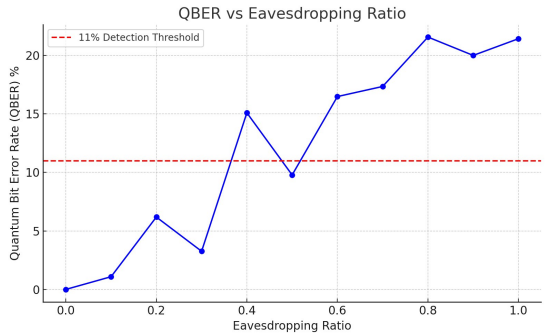
IV. EXPERIMENTS AND RESULTS

5.1 AI Detection Results :

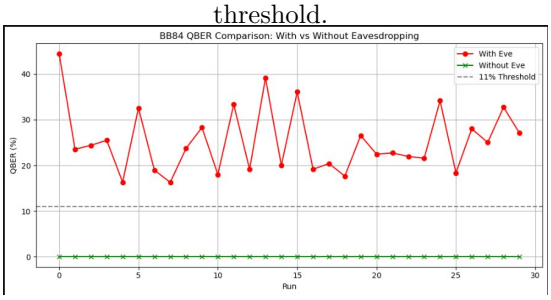
The AI model trained on the **UNSW-NB15** dataset achieved over 95 out of 100 accuracy in classifying network traffic. Precision and recall metrics confirmed its ability to detect malicious access attempts, including botnets, DoS attacks, and unauthorized logins. However, the model required labeled data and could only identify patterns based on historical attacks, limiting its response to novel threats without retraining.

5.2 QKD Detection Results :

The **BB84** simulation showed a clear distinction in **QBER** between scenarios with and without eavesdropping. Without Eves interference, QBER remained below 5 out of 100 , consistent with expected quantum noise. With Eve, **QBER** frequently exceeded 1220 out of 100, reliably indicating eavesdropping activity. These results were consistent across multiple trials on both simulators and real quantum backends. The experiment confirmed that **BB84** can detect live tampering during key exchange, providing proactive rather than reactive security.



QBER increases with higher eavesdropping ratios, surpassing the 11 out of 100 threshold and indicating effective detection through the BB84 protocol.QBER comparison in BB84 protocol showing clear disturbance from eavesdropping, with values consistently above the 11 out of 100 threshold.



AI intrusion detection performance on UNSW-NB15 : high accuracy, precision, recall, and F1-score.

VII. CONCLUSION

This research demonstrates the feasibility and benefit of combining AI-based data breach detection with quantum-secure communication via **QKD**. The AI system trained on **UNSW-NB15** successfully identified patterns of suspicious activity, while the **BB84** protocol implementation showed its ability to detect quantum-level eavesdropping through **QBER analysis**. The hybrid approach offers a dual defense strategy : proactive key protection via **QKD**, and behavioral monitoring via AI. The results suggest that integrating quantum and classical security technologies could offer robust protection in an era where both classical and quantum attacks are becoming increasingly realistic.

VIII. FUTURE WORK

Future work will focus on integrating post-quantum cryptographic algorithms with **QKD** and AI for a more comprehensive security solution. We also plan to train AI models on real-time network logs and extend the **BB84** protocol into full QKD suites including error correction and privacy amplification. Another direction is to deploy this hybrid system in real-world testbeds such as financial institutions or critical infrastructure environments to evaluate its practical scalability and robustness.

IX. APPLICATIONS AND BUSINESS RELEVANCE IN ALGERIA

As Algeria continues its digital transformationparticularly in the banking, telecommunications, and e-government sectorsdata protection is becoming increasingly critical. The nation's financial institutions and public services are digitizing rapidly, introducing both opportunity and vulnerability. Implementing a hybrid security model that combines AI-driven anomaly detection with quantum-safe communication protocols can offer Algeria a strategic advantage in both cybersecurity and innovation.

From a business and national security perspective, deploying such technology locally would :

- Enhance digital trust in online banking and e-payments, helping local banks like BEA, CPA, and CNEP adopt more secure systems resistant to future quantum threats.
- Position Algeria as a cybersecurity leader in North Africa, paving the way for research and tech startups in the field of AI and quantum technologies.
- Secure sensitive state data, particularly in government networks and national ID systems, which are often targets of cyber espionage .
- Stimulate academic and research collaboration, supporting innovation in quantum computing and AI through institutions like the University of Algiers and research centers like CDTA.
- Generate high-skill jobs in AI, quantum programming, and cybersecurity, helping align with the goals of national strategies such as the Algerian Startup Initiative.

By proactively investing in quantum-secure and AI-powered infrastructure, Algeria would not only protect its current digital assets but also future-proof its communication networks in the face of emerging global threats, especially from quantum-capable adversaries.

X. REFERENCE

-UNSW-NB15 : a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set