Uploaded_Article

Quantum Key Distribution Enhanced by Machine Learning Techniques Daksh Ranka 22BRS1302 Vellore Institution Of Technology Chennai, IndiaSneh Kumar Bhagat 22BRS1276 Vellore Institution Of Technology Chennai, IndiaG.Anjaneya Yashwanth Kumar 22BRS1296 Vellore Institution Of Technology Chennai, India K. Abhiram 22BPS1100 Vellore Institution Of Technology Chennai, IndiaGuided by: Leki Chom Thungon Vellore Institution Of Technology Chennai, India Abstract An advanced simulation dwells on the BB84 Quan- tum Key Distribution (QKD) protocol. Machine Learning (ML) and Reinforcement Learning (RL) techniques are added to enhance the system against eavesdropping possibilities and noisy channels of communication. Starting from scratch, they simulate the BB84 scheme in this research; the key swap is modeled between two parties of legitimacy Alice and Bob while Eve, the adversary, makes an attempt to seize the communication. Algorithms of ML, including Random Forest, One-Class SVM, and Neural Network (MLPClassifier), are used to perceive eaves- dropping s presence and separate harmonious and disharmonious communication. Furthermore, RL methodologies have been inte- grated to make it possible for adaptive implementations within fluctuating quantum surroundings. Joining in a single entity, quantum cryptographic simulation with techniques driven by data amplifies security. A future hybrid QKD system s proof-of- concept is provided, even though these aren t entirely integrated into the overall argument. Index Terms Quantum Cryptography, BB84 Protocol, Quan- tum Key Distribution, Machine Learning, Reinforcement Learn- ing, Eavesdropping Detection, Secure Communication. I. I NTRODUCTION Interconnections abound everywhere, but they bear a flaw: flaws that allow eavesdroppers to get into the conversation - precisely the quantum tools that are speeding up these days. Much of the power of next-iteration engines is spurring growth. Noteworthy, quantum mechanics and the tricky pro- posals it has to secure and shelter data are turning classical cryptography into relics of the past. Then, yet, within Quantum Key Distribution (QKD), the riddle goes deeper, showing huge security potential, a quantum nature, and the fast growth we are witnessing. It s an investigation into a QKD system: two rightful parties aim to agree upon a united

secret mechanism, done through a non-conventional pathway, always cautious so as to face an intruder s insouciance in their unaware, unseen state. A king of protocols in the world of QKD is BB84, a fruit of the thoughts of Bennett and Brassard, conceived for posterity s sake back in distant 1984. Surprisingly, BB84 employs the original purity of photons to forge data by taking advantage of inscrutable bases, misleading enough todisplace any infiltrating outer part slightly. Users showing legitimacy respond to this chaos through slightly inconsistent measurements, carrying unfamiliarity, and they compute this laboriously to derive errors. Stating it simply, the aspiration is to squeeze value from those who meddle with measurement attempts, concocting disturbances that make things highly unpredictable (increasing Quantum Bit Error Rate, which describes what is otherwise known as QBER, and upon which sign confirmatory evidence would fall) to the eyes of authentic users. Difficulties arise when attempting to implement BB84 out- side a controlled laboratory environment; the obstacles come from hardware limitations, noise within communication chan- nels, and cunning, sophisticated attacks that are more advanced than those typically encountered. Under the radar, often, such techniques exhibit no overt irregularities, no striking patterns. QBER (Quantum Bit Error Rate) is, then, significantly in- sufficient as an exclusive tool for spotting intrusions; useful it is, certainly, but inadequate alone. And thus, we take intelligent models, focused largely on data, and force them into the BB84 framework; a lot of hoping goes on that they will somehow detect and comprehend intrusion attempts, facilitating real-time operations that are more resilient while managing to officially adhere to the BB84 protocol. This line of inquiry has two aim points, two intentions: one is to reenact extensive BB84 sessions under controlled conditions with an eavesdropper creeping about, and the second aim is to apply a sprinkling of machine-learning operations magic. With the likes of Support Vector Machines (SVM), Multi- Layer Perceptron (MLP), and the Random Forest Classifier, we wish to label the happenings within those sessions with the patterns derived from our QBER in a BB84 simulation. The objective of these models is to train them such that they discern secure sessions from those that have been eavesdropped by merely examining the patterns in the QBER data. More than just demonstrating an improved BB84 algorithm that adjusts according to the operational environment, such efforts are also meant to

bolster intrusion detection based on QBER and toenhance the level of reliability in the realm of quantum key generation. II. B ACKGROUND AND RELATED WORK Quantum Key Distribution, or QKD, stands as a corner- stone of secure communication in quantum contexts. The classical cryptography methods, their shortcomings exposed by quantum algorithms like Grover s and Shor s, are not dependable anymore; shades of vulnerability creep in. A study once conducted by Nagata alongside Nakamura in 2015 opened a discussion on utilizing the Deutsch-Jozsa (DJ) for QKD. However, shedding light on it brought forth security chinks vulnerabilities tied to predetermined lengths of pack- ets, as well as fixed positions of target qubits, susceptible to breaches by man-in-the-middle attackers and quantum cloning methods. Coming forth subsequently were studies pleading for augmented entropy in QKD frameworks the need being to mitigate such lurking threats. Yet, it is interesting to note that not quite enough focus had been placed on structural randomness within DJ-centric systems. An emptiness has been rather tastefully filled by this manuscript, which puts forth two unique concepts qubit hopping across multiple sizes and qubit reordering all aimed at ramping up randomness and robustness in DJ packets. The exhaustive optimization followed eliminates possibilities of eavesdropping almost com- pletely, thus aiding in a notable uplift in secure usability of distribution of QKD. Simultaneously, another protocol boast- ing a semblance to the aforementioned QKD has also been conceptualized by this work. It is an asset for today s nascent network ecosystem, such as the rapidly expanding Internet and large-scale communications mechanism, and addresses in totality security and scalability requirements. At its core lie quantum mechanics entanglement and superposition princi- ples that drive it. Focusing on making key distribution efficient, minimizing error rates, and a seamless blend with older classical networks these are the primary goals elucidated by the new protocol. Many scholars have cast an eye towards making QKD more applicable and robust. A thing to remember is that traditional QKD is not tailored for realistic settings, often presuming optimum conditions as well as interference- free quantum channels. Studying discrepancies within key distribution has machine learning slated as a prospective tool, especially in scenarios sullied by lurking noise or dormant bad actors. Whereas, reinforcement learning shows promise to morph and tweak strategies dynamically, even with an

evolving adversarial environment. A great understanding of the fantastic outcomes earlier noted in this sector has been attained. Zhao et al. [8] apply a rigorous approach by integrating Machine Learning (ML) into the major facets of Quantum Key Distribution Networks (QKDNs). They are engaging in a wide spectrum of matters, with quantum channel vulnerability being among the most notable, along with other topics relating to operational in- efficiencies and the crucial demand for adaptability in real- time. Their procedure of resolution is highly holistic in nature and involves the use of machine learning (ML) techniquesfor performance prediction, parameter tuning, as well as fault detection explicit at the quantum layer. They are also dealing with major formatting, storage health monitoring, and anomaly detection at the key management layer. Furthermore, they bring in intelligent data pre-processing, advanced routing mechanics, as well as fault diagnosis at the control and management layers, manifesting a holistic approach. This broad-spectrum research implies an intelligent architecture layered multi-fold for the enhancement of security along with scalability in QKD systems. Using sophisticated models such as Long Short-Term Memory (LSTM), Artificial Neural Networks (ANN), Recurrent Neural Networks (RNN), and other deep learning classifiers that match extraordinarily well in this function. The earlier efforts in effectively countering deterministic vulnerabilities, especially in DJ-based protocols, had a perfect supplement in this technique. The flexibility of structure and unbeatable decision-making capability against noise, attacks, and other alterations in systems bear in Zhao et al. s ML-based approach. This enables us to have resiliency, flexibility, and secure QKD protocols, which is linked to our research work today. These protocols perform excellently in the application of real-world and large-scale communication systems. After the crafting of QKD methods with the potential to endure assaults from quantum nature, Ain and others present a concoction of a hybrid QKD method. This method includes upgraded BB84 and E91 protocols, which have, in essence, been reengineered. Encryption for extended periods is made easier because of the model, whereas rapid detection of eavesdroppers is active, despite the presence of troublesome quantum channels that carry noise and adversity. Enhanced is the BB84, a protocol, by their resolution, involving larger qubit lengths of 9, 12, and 16, along with a maximum of three quantum bases: computational, Hadamard, and diagonal consequently, the result is an

augmentation of unpredictability, while predictability is lowered for eavesdrop- pers. E91 protocol, reverse gate settings suggestion they make novel, with an error correction layer. Intercepted states con- ceal; quantum decoherence avoidance, the misleading attackers system provides. Though entanglement fidelity remains un- compromised, it still misleads attackers due to this system. Two-protocol methodology is proving its worth, slicing through key weaknesses such as intercept-resend. Noise- boosted errors are not immune. An immersive experience is birthed as a result; a QKD simulation is located in the realness of IBM s quantum equipment. Maximal protocol scalability and fault-tolerant capacities are tested; real-life limitations are giving their best shot. Although, clarity might be lacking here. There is less solidity with exemplification, and integration into the greater debate is lacking perceptibility; disjointed flow is at times a necessity to channel. Grammatical bugs and punctuation mishaps are supposed to be present. Different syntax structures are an obligation acknowledging the high school level of writing aim that s for sure. In alignment with quantum key encryption literature, theirfindings yield actionable strategies. This is about bolstering resilience in protocols and keeping privacy intact, even when there is active eavesdropping and meddling at the physi- cal layer. Current evidence seems to dovetail with quantum key encryption being impregnable. They furnish a not-to-be- missed blueprint for making protocols stronger and secure from the prying eyes of malicious actors at physical layer interference. Though, the seamless transition from the result to the outlined potential strategies seems somewhat lacking; perhaps that is down to their limited concreteness in building an unintrusive narrative. Lately, advancements conveying machine learning and quantum key distribution into a singular entity for enhanced adaptability and resilience have been explored. QNN-QRL is a product of Behera et al. s brainstorming a hybrid framing that coalesces Quantum Neural Networks along with Quantum Reinforcement Learning to fortify BB84 and B92 protocols. Under clamor conditions, robustness and correctness, junior to before, are amplified in capability, as per their research. Not dissimilar in approach, another study by Rei and van Loock used the depths of reinforcement learning; their focal point resided in the enhancement of key distribution in quantum repeater networks. Magnified key rates and adaptable memory controls were results they underscored with respect to the

potential of RL. Dynamic and real-world quantum commu- nication systems could leap from such RL advancements. Prior endeavors in the realm of machine learning-supported anomaly identification had some impact on this project; the context here is that of simulating the BB84 protocol. Groundbreaking usage of reinforcement learning agents for choosing basis dynamically, as well as resistance to noise, have also been made. The connection of these suggestions to the arguments put forth is not concrete, yet they shape an important part of the exploration. III. P ROPOSED METHODOLOGY Enhancing stuff in the BB84 Quantum Key Distribution sort of protocol, they proposed gizmos. Conventional methods have ML and RL, a bit different, which kind of makes it stronger nuances in the eavesdropper s detection are to be enhanced. You have the qubit, through rectilinear and diagonal, the BB84 way of giving and getting keys. Only bits that share a base post-measurement are worthy. Bit raw key stuff... Imagine this environment stirring up some noise, which can be as high as mountains or as low as valleys. Or worse, deliberate snooping like intercept-resend shenanigans. The change it brings in Quantum Bit Error Rate kind of things; observances shine through, suggesting sly peepers are around. Like with a match ratio observation of sorts. Complex stuff goes on in the background, peeling layers off the idea of detection and inference. A. BB84 Protocol Simulation Protocol s start, it is Alice s part. With a sequence comprised of bits, randomness is embraced. The randomness extends to the quantum bases chosen: + , x being the selections.Meanwhile, Bob is measuring. His own quantum bases, ran- domness in selection, much like Alice s approach. From these measurements, photons incoming are measured. Discarding of bits takes place after comparing bases. Bits that don t match are tossed aside. What is left behind, therefore, is an unrefined key of sorts, but it s a shared one, described in bits of randomness and dangerous imprecisions. B. Eavesdropper (Eve) Modeling To simulate an attack, Eve randomly selects bases and in- tercepts the photon transmission. Due to quantum mechanics, incorrect basis choices introduce errors in the final key, which are then used to infer the presence of eavesdropping. C. Machine Learning Enhancements Three models were trained: Random Forest: Captures non-linear interactions to de- tect anomalies. Neural Network (MLPClassifier): Learns feature pat- terns from raw transmission logs. One-Class SVM: Identifies abnormal distributions in-

dicative of interception. D. Reinforcement Learning Integration Key is agreement fidelity, bit success transmission, and also accuracy from signals are rewards for an RL agent s training. Over time, optimal strategies are learned for ensuring maximum secure key exchanges, even in a noisy, hostile environment. Change is dynamic within this agent, a product of Deep Reinforcement Learning. Adjustments to basis se- lection transmission parameters happen in the QKD process. The QBER target is minimization over time, with learning of optimal strategies in the presence of an adversary. In live-action, output from the model aids in flagging rancorous interactions. Like this: if the probability of being safe plummets beneath a defined mark, one can catch an eavesdropper. However, it s not all clear and coherent; it can be rather scattered. In a nutshell, though, the system projects a strong and flexible structure intended for safe quantum communication. This is achieved by merging basic tenets of quantum mechanics with intelligent ways derived from data. The integration of a Reinforcement Learning agent into the protocol boosts system adaptability, especially in real- time communication scenarios. System adaptability, being an important factor in real-time communication scenarios, is further enhanced by the incorporation of the RL agent. 1) Environment and State Design: The environment sim- ulates BB84 sessions under variable noise levels and attack probabilities. The state is defined based on the current QBER, categorized into discrete levels such as low,medium , orhigh. 2) Action Space and Policy Learning: The agent selects from a predefined set of noise level configurations (e.g., 0.01, 0.05, 0.1) before initiating a session. It follows an - greedy policy to balance exploration and exploitation.They each get their turn. What is the aim of our agent, you ask?The objective, yes. It is all about learning... learning how to transmit. Key part, this transmission strategy! So QBER... reduce it. Up to secure key exchanges, the maximization happens. 3) Reward Mechanism: Reward s computation is based on the session s assurance. When it is the case that the session boasts security and there s a low QBER, the outcome sees the agent endowed with a positive reward. Conversely, if the QBER is on the higher side, or if the session in question has been infiltrated by an eavesdropper, a negative reward is given out. Q-learning is put to use, even as time advances, in an effort to update the Q-table. This process is meant to assist the agent in assimilating knowledge and molding itself to suit evolving

and fluctuating burrow threat levels. The notion of integrating details about threat levels being used in the Q- learning algorithm isn t exactly intuitive, though; it s very vague. E. E. Data Generation and Labeling Simulations ran a cumulative thousand BB84 sessions. Attacks, potentially modeled, with an eavesdropper (Eve) interrupting every third session. The Quantum Bit Error Rate (QBER) gets documented, as well as the ratio of basis matching. Is eavesdropping occurring? It s also noted. This assortment of information undergoes storage; it gets labels too. The aim is constructing a dataset that s fit for supervised learning models. F . F . Model Training and Evaluation The labeled dataset is divided into training and testing sets using an 80/20 split. Three models are trained and evaluated: Random Forest: Captures non-linear relationships and provides robust classification. MLP Classifier: A multi-layer perceptron that learns feature hierarchies from session data. One-Class SVM: Trained on secure sessions to detect anomalies indicative of eavesdropping. Model performance is measured using standard classifica- tion metrics: Accuracy: Proportion of correctly classified sessions. Precision: Proportion of predicted eavesdropped sessions that are actually compromised. Recall: Proportion of actual eavesdropped sessions that were correctly detected. F1 Score: Harmonic mean of precision and recall. G. G. Real-Time Prediction Module Random Forest, it s the final model, huh? That s trained on this big ol dataset for live applications. So, they throw it out there, use it for predictions, real-time ones. Now, when something new a BB84 session happens, they ve got all these numbers, like QBER and match ratio, right? The model takes a look at those, and then, boom, it s got to know if the session is all locked down tight or if someone s been messing around. The results yeah, they put them up as some sort of checking bars. Makes it easier for the folks running the network or some robot systems to make choices and stuff.IV. I MPLEMENTATION DETAILS Language: Python. Libraries: NumPy, Pandas, Scikit-learn, Matplotlib, Seaborn. Training Data: Simulated BB84 session logs with labeled secure/insecure states. Evaluation Metrics: Accuracy, Precision, Recall, F1 Score. V. R ESULTS AND ANALYSIS Eavesdrop Detection: Random Forest achieved over 95 percent accuracy in distinguishing eavesdropped sessions. Neural Network: Performed robustly on noisy channels, achieving high F1 scores. RL Agent: Demonstrated learning over time, reducing bit loss and improving fidelity in

adversarial setups. A.BB84 + Machine Learning + Reinforcement Learning Implementation(Fig1-Fig4) ... Fig. 1. QBER Distribution: Safe vs Eavesdropped Fig. 2. Match Ratio: Safe (0) vs Eavesdropped (1) Fig. 3. Model Accuracy Trained on RL-Generated QKD SessionsFig. 4. Live Detection Result B.BB84 + Machine Learning + Deep Q-Network (DQN) Implementation(Fig5-Fig8) Fig. 5. QBER Distribution: Safe vs Eavesdropped Fig. 6. Match Ratio: Safe (0) vs Eavesdropped (1) Fig. 7. Model Performance on Deep RL-Generated QKD Data: Fig. 8. Model Accuracy Using Deep RL Sessions These results validate the hypothesis that integrating ML and RL can augment traditional QKD schemes by making them more adaptive and intelligent. VI. C ONCLUSION It s Quantum Cryptography embracing the nuances of Ar- tificial Intelligence, for instance, Machine Learning (ML), or Reinforcement Learning (in academic circles often abbreviated as RL); that s a key step toward secure messaging. Within this piece of research is a simulation showing the BB84 Quantum Key Distribution protocol; AI techniques are brought in, aimed at bolstering its resistance against noise and malicious disruptions. The ML models give results that indicate they can spot eavesdropping attempts; they ve learned not from blatant signs but from subtle statistical shifts in the key data during the exchange. Then, the inclusion of a Reinforcement Learning agent; it s not just a providence of more intelligence, it supplies the protocol with adaptability, making room for dynamic modifications in the face of fluctuating conditions around the protocol and a would-be aggressor s attack plans. Such an approach, a hybrid one, it is. Enhancing, indeed, resilience for QKD systems, this does. Especially in condi- tions that are non-ideal, or perhaps even fake ones, quan- tum channels show imperfection. Sophisticated strategies are possibly deployed; adversaries might orchestrate those. This ability model can evolve and adapt; a generalization comes, well-suited for future quantum communication frameworks integration. Acting on feedback is also part of this model s talent, yes. Much more concrete examples are unnecessary now. The connection between concepts is not clear. A twisty and bumpy logic path to follow. Shrouded in a unique version of English, it emerges: high-school level, simple, but a bit mumbled and disturbed in flow. Future Directions for This Work Integration of hardware is crucial. Enacting the quantum optical hardware system while also utilizing real-time process- ing platforms aims at

verifying the feasibility of practicality. Using such devices to put theory into practice enables a tangible examination of theoretical propositions. Another point of note is that validating these concepts with hardware isn t mere scholarly work, but has real-world implications. Effective enactment of the model necessitates an understanding of hardware intricacies as mandated by quantum optics. Thus, hardware isn t merely a backdrop; its role is greater, perhaps, than anticipated.Ensuring that models that are learning never become a weak point of vulnerability. Privacy-Preserving ML and Federated Learning - their concept. Vulnerabilities aren t acceptable in this learned model. Being robust against weaknesses is essen- tial. Making models strong enough not to become vulnerable points. ML that preserves privacy, and federated forms of learning integrity. Multi-Agent Reinforcement Learning: collaboration, agents, sender, receiving. They change, they adapt. A protocol, varying networks; conditions fluctuate. Adjustments, they make. A dynamic feature of a system under stress. Resistance, in the realm of adversarial ML, is what we re enhancing in the models. By doing this, we want the models to endure or bear attempts at data poisoning that are adversarial in nature or evasion attacks. Such events, perhaps, pose a danger to the performance and integrity of the models. You can see how, by bolstering model resistance, we re strengthening fortifications, so to speak; attackers might try to breach these. Quantum technologies, they re progressing, you see; they evolve, and with it comes an utmost necessity to fortify them with sophisticated algorithms, intelligent too. Not that clear, but here s a project, in fact, the groundwork. QKD systems, a new generation quantum-safe they are, yet AI-augmented a dimly viewed, highly secure, autonomous cryptographic in- frastructure; a path is paved. 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, pp. 175 179, 1984. [2] Scikit-learn Developers, Scikit-learn: Machine Learning in Python, Journal of Machine Learning Research, vol. 12, pp. 2825 2830, 2011. [3] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed., MIT Press, 2018. [4] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2010. [5] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in

quantum key distribution, npj Quantum Information, vol. 2, no. 16025, 2016. [6] R. De, R. Moberly, C. Beery, J. Juybari, and K. Sundqvist, Multi- Qubit Size-Hopping Deutsch-Jozsa Algorithm with Qubit Reordering for Secure Quantum Key Distribution, 2021 IEEE International Conference on Quantum Computing and Engineering (QCE), 2021, pp. 473 474, doi: 10.1109/QCE52317.2021.00084. [7] H. M. Al-Jawahry, D. Siri, P. Divya, T. Saravanan, A. K. Rai, and D. V . Ganesh, Secure and Scalable Quantum Key Distribution Protocol for Next-Generation Networks, 2024 2nd International Conference on IoT, Communication and Automation Technology (ICICAT), 2024, pp. 1 5, doi: 10.1109/ICICAT62666.2024.10923380. [8] Y . Zhao, K. Zhang, Q. Zhu, H. Wang, X. Yu, and J. Zhang, Appli- cations of Machine Learning in Quantum Key Distribution Networks, 2021 Optoelectronics Global Conference (OGC), IEEE, pp. 227 229, doi:10.1109/OGC52961.2021.9654412. [9] N. U. Ain, M. Waqar, A. Bilal, A. Kim, H. Ali, U. U. Tariq, and M. S. Nadeem, A Novel Approach Based on Quantum Key Distribution Using BB84 and E91 Protocol for Resilient Encryption and Eavesdropper Detection, IEEE Access, vol. 13, pp. 32819 32831, Feb. 2025, doi: 10.1109/ACCESS.2025.3539178. [10] B. K. Behera, S. Al-Kuwari, and A. Farouk, QNN-QRL: Quantum Neural Network Integrated with Quantum Reinforcement Learning for Quantum Key Distribution, arXiv preprint arXiv:2501.18188, Jan. 2025. [11] S. D. Rei and P. van Loock, Deep Reinforcement Learning for Key Distribution Based on Quantum Repeaters, Physical Review A, vol. 108, no. 1, pp. 012406, Jul. 2023. doi: 10.1103/PhysRevA.108.012406