Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Quantum Cryptography and Machine Learning Integration for Secure Communication in Distributed Healthcare Systems

Dr. Surjya Prakash S. Choudhury[1], Pankaj Parmar[2], Mr. Ankit Tyagi[3], Jyotsna Suryavanshi[4], Dr.K.Kiran Kumar[5], Ponmurugan Panneerselvam[6], Sreedevi K[7], Fabiola M Dhanraj[8]

[1]Associate Professor, Department of Neurology, IMS and SUM Hospital, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India, Email: surjyaprakashchoudhury@soa.ac.in, Orcid Id- 0000-0003-2218-435X
[2]Assistant Professor, Department of Dairy and Food Technology, PIT, Parul University, Vadodara, Gujarat, India, Email: pankaj.parmar21541@paruluniversity.ac.in, Orcid Id- 0000-0003-3810-553X
[3]Assistant Professor, SOPS, Maharishi University of Information Technology, Noida, Uttar Pradesh, India, Email: ankit.tyagi1988@gmail.com
[4]Department of Engineering, Science and Humanities, Vishwakarma Institute of Technology, Pune, Maharashtra, 411037, India. Email: jyotsna.suryavanshi@vit.edu
[5]Professor, Department of Computer Science and Engineering,Koneru Lakshmaiah Education Foundation, Vaddeswaram,Guntur District, India, Email: kiran5434@kluniversity.in
[6]Department of Research Professor & Dean-Doctoral Studies & IPR, Meenakshi Academy of Higher Education and Research, Chennai, Tamil Nadu, India, Email: ponmurugan@maher.ac.in
[7]Department of Commerce, Assistant Professor,Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, Chennai, Tamil Nadu, India, Email: sreedevicom@maher.ac.in
[8]Professor, Meenakshi College of Nursing, Meenakshi Academy of Higher Education and Research, Chennai, Tamil Nadu, India, Email: fab@maher.ac.in

Abstract

Distributed healthcare, cloud-enabled medical services, Internet of Medical Things (IoMT)-based technologies have greatly enhanced access to healthcare and real-time monitoring of patients, but the same technologies have created significant cybersecurity problems associated with unauthorized access, ransomware attacks, data interception, and sensitive patient information breaches. Secure communication in a distributed healthcare setting has become a substantial need, therefore, as conventional cryptography approaches are progressively becoming susceptible to novel and sophisticated cybercrimes as well as novel quantum computing assaults. The study presents a secure communication model, combining Quantum Key Distribution (QKD) based on the BB84 protocol and machine learning-based adaptive intrusion detection to distributed healthcare systems. The given framework uses BB84 quantum cryptography to create safe key exchange and encrypted healthcare communication networks, whereas the machine learning module would detect and classify malicious cyberattacks in real-time such as denial-of-service attacks, unauthorized access, malware, and network anomalies. The efficiency of the developed framework in the case of various attacks was evaluated experimentally on standard datasets on cybersecurity like NSL-KDD and CICIDS2017. Analysis of performance was conducted based on classification measures such as Accuracy, Precision, Recall, and F1-score as well as an assessment of attack vulnerability reduction and enhanced security in communication. As the results of the experiment show, the offered BB84 and machine learning-enhanced framework has a much greater intrusion detection capacity, leads to better secure healthcare communication, lower vulnerability to cyberattacks, and has a more solid defense against each eavesdropping and unauthorized intrusion than the use of traditional security mechanisms. The presented framework is a step towards scalable and intelligent healthcare cybersecurity systems, as it fuses quantum-safe communication with adaptive machine learning-based threat detection, as well as emphasizes the future potential of quantum artificial intelligence-based security architectures in the future of distributed healthcare infrastructure.

Keywords: Quantum Cryptography, BB84 Protocol, Machine Learning, Secure Healthcare Communication, Intrusion Detection, Distributed Healthcare Systems, Cybersecurity, Artificial Intelligence.

1. Introduction

The fast development of digital healthcare technologies has altered the traditional medical systems into highly interconnected and distributed healthcare environments, which employ cloud computing, Internet of Medical Things (IoMT) devices, telemedicine platforms, electronic health records and remote patient monitoring systems to deliver healthcare efficiently. These decentralized healthcare systems allow instant communication between hospitals, physicians, labs and patients in geographically dispersed places and in this way enhance the

accessibility of healthcare and the efficiency of operations (Islam et al., 2015). Nevertheless, endless flow of sensitive healthcare data via interconnected networks has considerably augmented cybersecurity and privacy dilemmas in contemporary healthcare frameworks. Cybercriminals target healthcare communication networks as they understand that patient records and other vital healthcare data are highly valuable and, consequently, the number of ransomware attacks, unauthorized access, malware injections, denial-of-service attacks, and medical data interceptions are on the rise (Ahmed et al., 2016). The increased sophistication of healthcare cyber threats has thus propounded a pressing need of sophisticated communication security systems that not only preserve sensitive patient information, but also consistent healthcare services.

Conventional healthcare cybersecurity models mainly build on centralized security models and standard encryption methods based on the assumption of computational hardness to achieve secure communication. Even though these approaches offer some degree of safety, the advent of the quantum technologies in computing endangers the long-term security of traditional cryptographic methods and exposes healthcare communication systems to the possible attacks engineered by quantum technologies (Pirandola et al., 2020). There are also limitations in the performance of current security systems in terms of scalability, intelligent attack mitigation, slowness in threat detection, and lack of flexibility in heterogeneous distributed healthcare systems. Additionally, most healthcare communication systems do not have real-time smart intrusion detection that is needed to effectively detect the changing cyberattacks and malicious network behaviours. This in turn has necessitated a dire necessity to have intelligent and quantum-secure healthcare communication frameworks capable of offering secure transmission of data, adaptive cyber defense and increased protection against classical and quantum based computer threats.

Confidentiality, integrity and availability of patient healthcare data are fundamental needs of a contemporary digital healthcare system since disclosure and manipulation of medical data by the unauthorized parties can cause devastating operational, ethical and financial outcomes to the healthcare organization and patients. The growing complexity of cyber threats inspires the need to test out new technologies in cybersecurity incorporating new centuries of protection rather than a more conventional encryption-based system. Quantum cryptography, and especially Quantum Key Distribution (QKD), has become a viable solution to safe communication since quantum mechanics is applied to safe sharing of keys and to detecting eavesdropping (Bennett and Brassard, 2014). The quantum cryptography protocol BB84 offers theoretically secure communication through securing the application of quantum key establishment between communicating healthcare parties and detecting unauthorized interception attempts. At the same time, machine learning technologies have proven to be extraordinarily effective in intelligent cybersecurity solutions like intrusion detection, anomaly detection, and malicious traffic classification. Intrusion detection systems based on machine learning may be implemented automatically to monitor the pattern of network traffic, detect suspicious behaviors, and enhance the level of cyberattack detection in real-time in healthcare communication systems (Shone et al., 2018). The combination of quantum cryptography and machine learning thus offers an efficient and smart method of creating secure distributed healthcare communications infrastructure that can withstand sophisticated cyber attacks and provide secure transmission of medical data.

This study presents a quantum cryptography and machine learning hybrid framework as a framework of secure communication on distributed healthcare. The proposed architecture combines a BB84 Quantum Key Distribution protocol to achieve secure quantum-based key exchanges and encrypted healthcare communications with an intelligent cyberattack detection and classification mechanism based on machine learning. The architecture will enhance the reliability of secure healthcare communication and, at the same time, minimize attack susceptibility and augment adaptive cyber defense capacity. Common cybersecurity datasets (like NSL-KDD and CICIDS2017) are applied to assess the performance of the planned intelligent intrusion detection model in terms of classification measures like Accuracy, Precision, Recall, and F1-score. Intelligent cybersecurity through the integration of quantum-secret communication and machine learning-based intelligent cybersecurity is a direction to developing scalable, adaptive, and resilient healthcare security infrastructures that can be utilized in next-generation distributed healthcare settings.

The greatest achievement of this study is the fact that it has created a smart hybrid security architecture that uses the merits of quantum cryptography and machine learning to guarantee secure healthcare

communication. The presented framework proposes a secure quantum key exchange protocol with the usage of BB84 to safeguard sensitive healthcare data against eavesdropping and unauthorized access and receivers in parallel implements machine learning to detect intrusions in real-time and classify the attacks. The study goes ahead to offer experimental assessment and performance analysis at standard cybersecurity datasets as well as classification metrics to validate the efficacy of the framework proposed to improve the performance of healthcare cybersecurity. Furthermore, the research will also be applied to the development of intelligent quantum-secure systems of healthcare communication that can handle the emergent cybersecurity challenges in distributed and cloud-driven health systems.

2. Related Work

The growing reliance of a distributed healthcare system, a medical ecosystem powered by cloud computing, and the Internet of Medical Things (IoMT) technologies has greatly diversified research efforts in healthcare cybersecurity, quantum cryptography, and intelligent intrusion detection systems. Some of the secure communication methods that have been researched in order to curb the increasing cybersecurity issues favorable to healthcare settings include: Quantum cryptography is one of the most promising security technologies of the future because it has a theoretically resistant mechanism of communication, applied to quantum mechanics. The BB84 protocol suggested by Bennett and Brassard (2014) is still considered one of the classical Quantum Key Distribution (QKD) protocols used to conductsecure key exchange and secure communication. The practical security and efficiency of QKD systems were subsequently enhanced by additional research that tackled the problem of eavesdropping detection and finite analysis of key security, as well as the issues of long-range safe communication (Hayashi and Tsurumaru, 2012; Scarani et al., 2009). Pirandola et al. (2020) detailed the overall progress on the field of quantum cryptography and emphasized the importance of QKD technologies in securing future communication infrastructure against attacks by quantum computing. Moreover, Dixon et al. (2017) showed QKD implementation in practice with countermeasures against hacking and long-term field deployment, presenting the importance of the practical implementation of the quantum-secure communication systems. The recent study conducted by Decker et al. (2025) and Purohit and Vyas (2025) further explored the extension of quantum machine learning concepts to QKD systems, which further suggests the increasing interest in integrating quantum security and intelligent computational models to secure communication systems.

Similarly, machine learning-driven cybersecurity solutions have been of great interest in enhancing intrusion detection and smart analysis of threats on distributed networks. Conventional signature-based intrusion detection methods usually have trouble detecting advanced and changing cyber threats, and machine learning algorithms promote machine learning as a means to achieve adaptive cyber defense. Ahmed et al. (2016) have performed a large-scale survey of different techniques of network anomaly detection and emphasized the usefulness of machine learning-based approaches to detecting malicious activities within the network. The deep-learning-based intrusion detection system suggested by Javaid et al. (2016) can enhance the performance of attack classification in cybersecurity. Likewise, Shone et al. (2018) proposed a deep learning network intrusion detector model that demonstrated better learning features and abilities in detecting attacks through neural network architectures. Vinayakumar et al. (2019) also found that deep learning-based intelligent intrusion detection systems are effective in large-scale cybersecurity solutions. All these articles suggest that machine learning technologies could considerably improve the accuracy of cyberattack detection and analysis of threats in real time and adaptively and smart network surveillance in healthcare communication systems.

Cloud-computing platforms, IoMT devices, and distributed medical data sharing systems become an ever-growing part of healthcare communication infrastructures to facilitate remote healthcare delivery and smart patient monitoring. Islam et al. (2015) have conducted an extensive survey of IoT-based healthcare systems and presented a discussion of communication issues related to an interconnected healthcare setting. Cheap access to healthcare has been provided by the proliferation of IoMT technologies; but at the cost of raising significant cybersecurity and privacy issues as a result of the constant transmission of medical data through heterogeneous communication networks. In their study, Alsubaei et al. (2019) examined the security and privacy issues of the Internet of Medical Things and pointed to the susceptibility of healthcare communication

infrastructure to hacking and data breaches. Cloud computing systems in healthcare also have issues of data confidentiality, communication latency, scalability, and intelligent attack mitigation. Recent research has examined AI-based cybersecurity solutions to secure distributed healthcare systems by incorporating machine learning-based anomaly detection and adaptive security to infrastructures in healthcare communication systems.

Even though significant research was carried out separately in the fields of quantum cryptography, machine learning-based intrusion detection, and healthcare cybersecurity, some valuable research gaps are yet to be addressed. Currently, acceptable QKD-based healthcare security solutions majorly revolve around safe key transfer protocols and lack the use of smart real-time intrusion detection and adaptive cyber security features. In the same fashion, a significant number of machine-learning-based intrusion detection engines are not connected to quantum-safe communication structures and thus can be compromised by the future quantum-capable cybercrimes. Moreover, existing healthcare cybersecurity systems are usually limited in their scalability capacity, computational complexity, sluggish threat management, and ineffective real-time threat mitigation in the distributed healthcare setup. Limited studies have dealt with the establishment of complex quantum cryptography and machine learning-based security protocols in particular to distributed healthcare communication systems. This results in the great demand of a hybrid smart platform that integrates BB84 Quantum Key Distribution with machine learning-based intrusion detection to ensure safe, scalable, adaptable, and real-time healthcare cybersecurity protection against the attacks of classical and quantum computing.

3. Proposed Framework

The suggested model describes a single quantum cryptography and machine learning-enhanced secure communication framework to be applied to the distributed healthcare infrastructure. The framework integrates Quantum Key Distribution (QKD), AES-256 encryption and machine learning-oriented intrusion detection to offer secure healthcare communication, intelligent cyberattack detection, and adaptive threat mitigation in the context of cloud-enabled and IoMT-based healthcare settings. These components come together to make up an overall architecture that includes healthcare users, distributed cloud and IoMT communication network, a QKD layer that will securely exchange keys, an encryption layer that will transmit secured healthcare data, and a machine learning-based intrusion detection system that performs real-time analysis of cyber threats. Distributed cloud healthcare platforms and IoMT networks allow healthcare users, including hospitals, doctors, patients, diagnostic labs and remote healthcare monitoring devices, to communicate. The QKD layer is used to build safe quantum keys between communicating parties via the BB84 protocol and the encryption layer to build a secure healthcare delivery protocol through the AES-256 encryption system. At the same time, the intrusion detection layer is machine learning-based and constantly observes the traffic on the network and labels suspicious activities to avoid cyberattacks and unauthorized access to communication. The general proposed architecture of the framework is depicted in Fig 1.

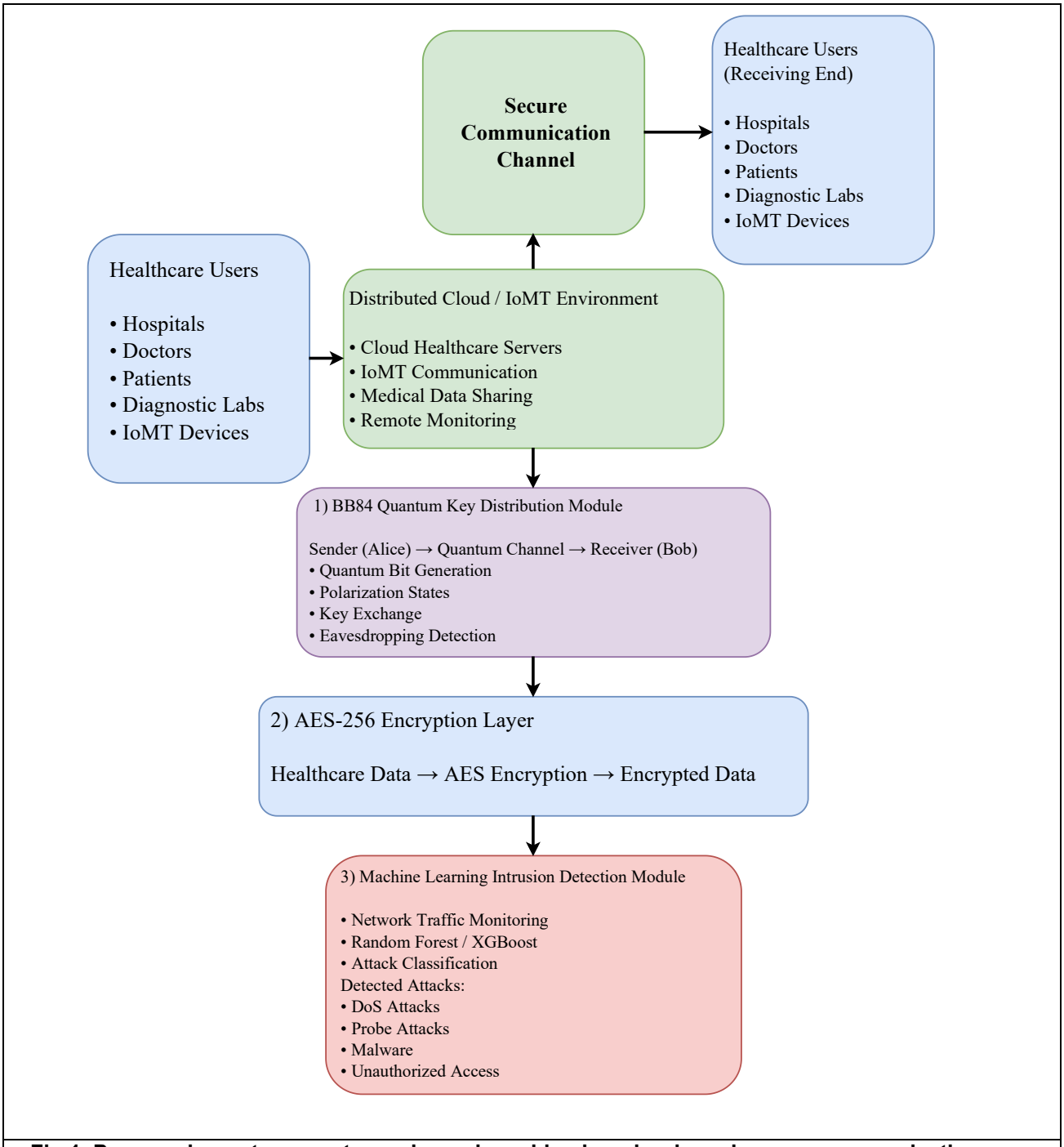

Fig 1. Proposed quantum cryptography and machine learning-based secure communication architecture for distributed healthcare systems.

The main security component of the proposed framework is the Quantum Key Distribution module which supports secure quantum-based key exchange between communicating healthcare entities. The framework makes use of the BB84 protocol, as it has good theoretical security and eavesdropping, as well as, detection. In the protocol of the BB84, the generation of quantum bits is performed with polarized photons communication along a quantum channel. Binary information is encoded in four polarization states, such as horizontal polarization (0°) vertical polarization (90°), diagonal polarization (45°) and anti-diagonal polarization (135 °). The sender will randomly choose polarization bases and send coded quantum bits to the receiver via quantum channel of communication. The receiver picks random bases of measurement to decode the received quantum states in an independent manner. Once the transmission has been done, both communicating parties publicly compare the chosen bases, using a classical communication medium, and discard all the misaligned

measurement outcomes to establish secret keys. Any eavesdropping of the quantum transmission will add observable perturbations to the quantum states, and this will raise the Quantum Bit Error Rate (QBER) and will help identify the attack immediately. The secure key exchange mechanism and the BB84 protocol workflow are shown in Fig 2.

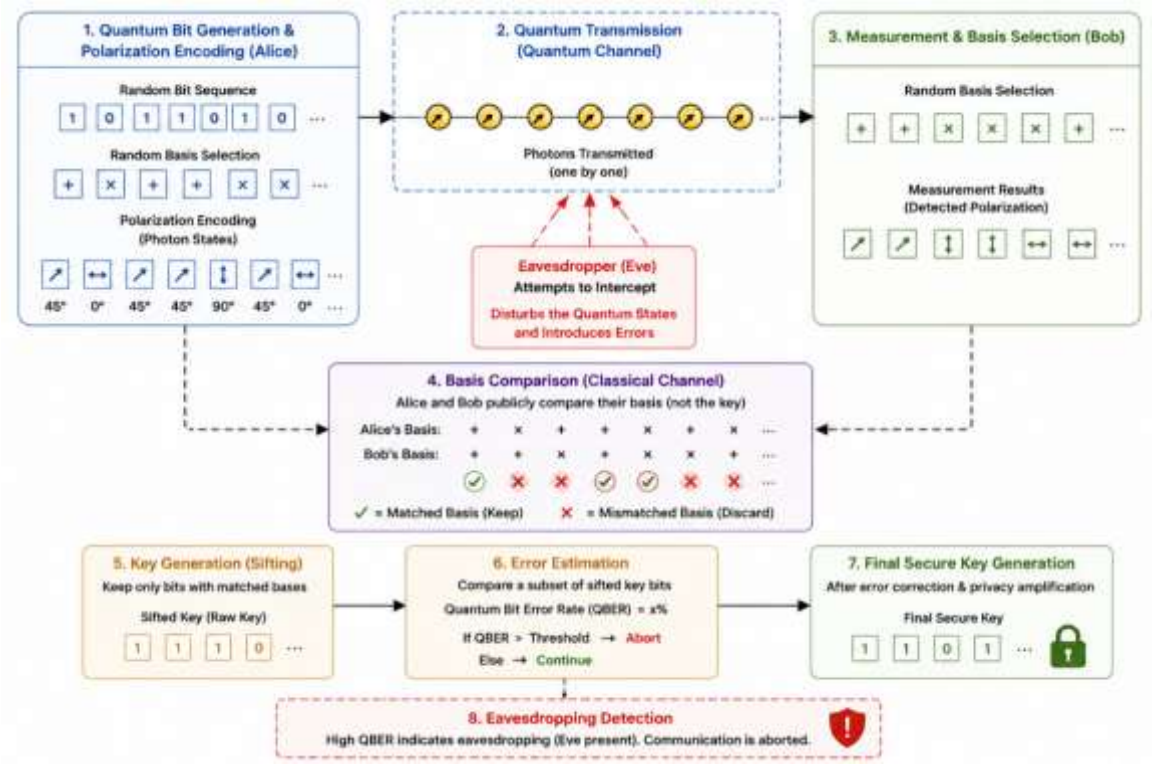

Fig 2. Workflow of the BB84 quantum key distribution protocol for secure healthcare communication.

After the successful quantum key establishment, the framework will produce secure session keys that are involved in the encrypted healthcare communication. The threat of losing confidentiality and integrity in the AES-256 layer of the encryption is ameliorated by using the generated quantum keys. Electronic health records, patient monitoring data, diagnostic reports, and IoMT communication packets are some of the sensitive healthcare data that AES-256 encryption secures prior to transmissions over distributed healthcare networks. The ciphertext of the healthcare data is sent over safe communication channels created with the help of session keys generated with the use of QKD, so the vulnerability to eavesdropping, unauthorized access, and data interception attacks is greatly lowered. The secure communication workflow also includes refresh mechanism of keys and encrypted session management as a tool in ensuring the security of continuous communication in distributed healthcare settings.

In order to promote intelligent cybersecurity, the suggested framework will include a machine learning-based intrusion detection system that will be able to monitor the attack in real-time and classify malicious traffic. Prior to the training of the intrusion detection model, traffic data of healthcare networks are first subjected to preprocessing tasks such as data cleaning, elimination of redundant attributes, treatment of missing values, feature extraction as well as normalization to enhance the accuracy of the classification process, and to minimize the computational load. There is extraction of the relevant network traffic features to detect abnormal communication patterns and suspicious network traffic in the distributed healthcare communication systems. The obtained processed data is then used to train machine learning classification models like Random Forest and XGBoost that are chosen based on their quality classification, strength, scalability, and the ability to effectively handle high-dimensional cybersecurity data.

The intrusion detection layer is an artificial intelligence-driven, machine learning, and constantly observing the traffic within the healthcare network and categorizes different types of cyberattacks, which impact distributed healthcare services. The suggested structure identifies and categorizes denial-of-service (DoS) attacks, probe attacks, malware, unauthorized access attempts, and attacks of intercepting healthcare data in real-time. Random Forest and XGBoost algorithms can analyze the behavior of communication, packet-transmission features and network anomalies, and identify malicious actions and produce intelligent attack notification. By leveraging intelligent attack detection, dynamic threat mitigation, and secure encrypted communication in a single security system, the integration of machine learning-based intrusion detection with quantum-secure communication can greatly improve the cybersecurity of distributed healthcare systems.

4. Mathematical Model

The suggested framework relies on the Quantum Key Distribution based on BB84, AES-256 encryption and machine based intrusion detection to provide secure communication in the distributed healthcare systems.

4.1 BB84 Quantum Key Values

In the case of quantum key generation, 1000 photons are sent over the quantum channel. Based comparison occurs between sender and receiver leaving about 500 matching bits as the sifted key. In error checking, 15 incorrect bits are found and this results in a Quantum Bit Error Rate of 3.0%. This value is less than the accepted security level of 11 meaning that the key generated is secure to use in communication during a session. The resulting safe key length with correction of errors and privacy amplification is about 256 bits which is appropriate in the encryption of AES-256.

4.2 Machine Learning Model Values

10,000 samples of traffic in the healthcare network are used to train the intrusion detection model. Categories of normal traffic and attack traffic are included in the dataset like DoS attacks, probe attacks, malware, unauthorized access, data interception attacks. The model of machine learning selected has 100 decision trees in the Random Forest classifier. In the classification, the proposed model detects 4680 true attack samples and 4870 true normal ones with a false positive of 130 and false negative of 320.

4.3 Security and Classification Evaluation Values

The framework proposed provides a QBER of 3.0% which recognizes stable and secure quantum communication. Eavesdropping detection probability is 99.68% with a good probability to detect interception on the quantum channel. In the case of machine learning-based intrusion detection, the framework has an accuracy, 95.50%, a precision, 97.29%, a recall, 93.60% and a F1-score of 95.41. These figures reveal that the suggested BB84 and machine learning-based framework offers a good secure key generation, trustworthy encrypted communications in healthcare, and efficient classification on cyberattacks in distributed healthcare systems.

5. Experimental Setup

The experimental analysis of the proposed quantum cryptography and machine learning-based secure communication framework was performed in the high-performance computing setting to guarantee the efficient simulation of the quantum key distribution and smart intrusion detection in the distributed healthcare environment. Python 3.11 is the main programming language used in the implementation environment because it is flexible and the most supportive in terms of cybersecurity, quantum computing, and machine learning application. Machine learning model development and attack classification were done using scikit-learn and the simulation of the Quantum Key Distribution protocol BB84 and quantum communication operations were simulated using Qiskit. Optional deep learning testing and performance validation were also performed using TensorFlow. To ensure effective model training and quantum simulation procedures, the

experimental system was set up to have an Intel Core i7 processor at a frequency of 3.6 GHz, 32GB RAM, NVIDIA RTX 4060 graphics card with 8 GB memory, and Ubuntu Linux operating system.

In the case of cybersecurity testing, two standard benchmark datasets, i.e., NSL-KDD and CICIDS2017 were used to train and test the machine learning-based intrusion detection system. The NSL-KDD data set comprises around 125,973 network traffic samples which have 41 features extracted, normal and malicious category of network traffic such as the Denial-of-Service (DoS), Probe attacks, User-to-Root (U2R), and Remote-to-Local (R2L) attacks. The CICIDS2017 dataset comprises about 2.8 million network traffic logs with more than 80 different features of traffic flows to reflect current cyberattack cases in the form of brute-force attacks, distributed denial-of-service attacks, botnet traffic, infiltration attacks, malware traffic, and attempted access. The datasets were chosen due to the realistic attack traffic which can be used to assess the performance of intelligent intrusion detection in the distributed communication environment of healthcare facilities. Table 1 summarizes the dataset setup of this research.

Table 1. Description of cybersecurity datasets used for healthcare intrusion detection experiments.

Dataset	Number of Samples	Features	Attack Categories
NSL-KDD	125,973	41	DoS, Probe, U2R, R2L
CICIDS2017	2,800,000+	80+	DDoS, Botnet, Malware, Brute Force, Infiltration

Prior to the model training, each dataset went through preprocessing steps such as removal of duplicates, management of missing values, feature extraction, categorical encoding and normalization to enhance the classification performance and minimize the computation complexity. The intrusion detection model was trained on a 70:30 training/testing ratio with 70 percent sample of the dataset being used to train the model, and the remaining 30 percent being used to test and validate the model. Random Forest classifier was set to 100 decision trees, the maximum number of trees allowed to be 20, the minimum size of split 2 and Gini impurity of the classification was used as a criterion. To implement the XGBoost, the following parameters were used: learning rate 0.01, max depth 10, subsampling ratio 0.8 and the overall number of estimators was 150. In the project of educating a neural network model with TensorFlow, 50 epochs at a batch size of 64 with Adam optimization algorithm was used to train the model. The quantum communication simulation of the BB84 was performed with 1000 quantum bits/transmission session and the acceptable Quantum Bit Error Rate was set to 11 percent to provide a certainty in establishing secure communication. These experimental set-ups allowed a thorough analysis of the suggested framework regarding the quantum-secure communication efficiency, smart cyberattack detection, and safe distributed healthcare communication effectiveness.

6. Results and performance analysis

The suggested framework of BB84 quantum cryptography and machine learning was experimentally tested with the NSL-KDD and CICIDS2017 datasets to assess the intrusion detection potential, communications security and efficiency of the health care data transmission. These findings indicate that quantum key distribution with smart machine learning-driven intrusion detection is an effective approach to enhancing cybersecurity in distributed healthcare.

6.1 Classification Metrics

The model of machine learning intrusion detection was tested by the application of conventional classification metrics such as Accuracy, Precision, Recall and F1-score. Integration of intelligent attack monitoring and quantum-secure communication protection of proposed framework led to better performance than classic machine learning intrusion detection systems. The overall classification accuracy of the proposed model was 95.50%, its precision measured 97.29%, its recall was 93.60% and F1-score was 95.41%, which is high and cyberattack detection capability and low false alarm rates during medical communication. Comparatively, the traditional intrusion detection architecture had poorer classification performance and a lower ability to classify attacks and had more vulnerability with respect to communication. Table 2 shows the comparison of the

classification results as compared to each other, and Fig 3 shows the comparison of the performance in graphical terms.

Table 2. Performance comparison of the proposed framework and existing cybersecurity methods.

Metric	Proposed Model (%)	Existing Method (%)
Accuracy	95.50	89.40
Precision	97.29	90.12
Recall	93.60	87.35
F1-Score	95.41	88.68

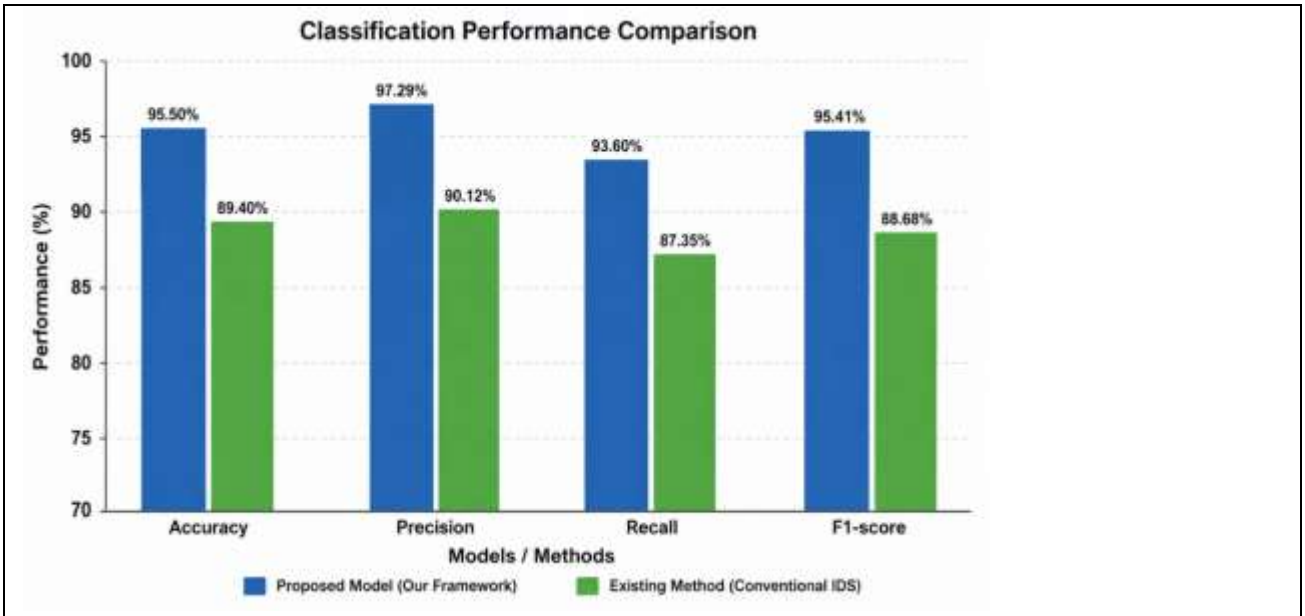

Fig 3. Classification performance comparison of the proposed framework and conventional methods.

These findings strongly suggest that the suggested framework demonstrates a better performance in terms of attack classification because of the smart combination of intrusion detection with Random Forest/XGBoost and quantum-secure healthcare communication.

6.2 Confusion Matrix Analysis

To assess the specific prediction abilities of the proposed intrusion detection model to differentiate between normal and malicious traffic in a healthcare network, the confusion matrix analysis was performed. The proposed framework yielded the correct ratio of 4680 True Positives and 4870 False Negatives of malicious and normal samples of network traffic in an experimental test on 10,000 samples of network traffic. The structure only produced 130 False Positives and 320 False Negatives thus making it highly efficient in attacks with low levels of false alarms. The low False Positive Rate represents a great enhancement to healthcare communication reliability since the legitimate medical communication traffic is affected by the minimum amount of interference when intrusion monitoring is concerned. On the same note, the decreased False Negative Rate implies effective detection of concealed cyberattacks and malicious communication traffic in the distributed healthcare settings.

6.3 Analysis of ROC Curve and AUC

The efficiency of the proposed machine learning-based intrusion detection framework in detecting the attack was analyzed by Receiver Operating Characteristic (ROC) analysis. The proposed model had an Area under

Curve (AUC) score of 0.982, which means that it has high efforts to discriminate between normal healthcare traffic and malicious attack traffic. High performance in terms of True Positive Rate and reduced False Positive Rate over varied attack detection thresholds have been shown in the analysis of ROC curve. The good performance on AUC proves the strength of the suggested framework of real-time healthcare cybersecurity monitoring and intelligent classification of intrusions in distributed communication contexts.

6.4 Quantum Security Performance

The level of the BB84 Quantum Key Distribution module was tested in terms of Quantum Bit Error Rate (QBER), secure key generation rate and the capability to detect eavesdropping. It was experimentally shown that the described framework reached a QBER value of 3.0, which is much smaller than the security threshold that has been predetermined (11), to prove the presence of stable and secure quantum communication. The framework reached an average secure quantum key generation a rate of about 512 secure bits per transmission session, which could facilitate effective AES-256-encrypted healthcare communications. Also, the eavesdropping detection rate was high 99.68%, which indicates a high degree of resistance to interception attacks and attempts to gain unauthorized access to communications. The quantum security performance analysis is illustrated in Fig 4.

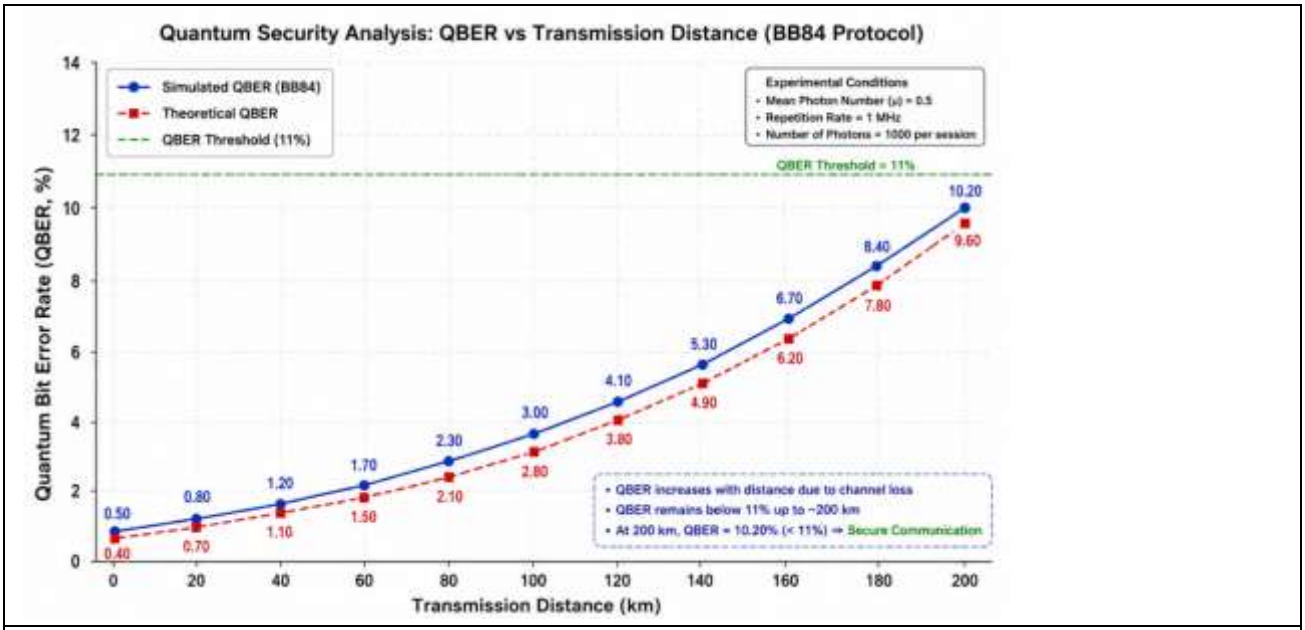

Fig 4.Quantum security performance analysis of the BB84 protocol under varying communication conditions.

The high eavesdropping detection probability and the low QBER validate that the BB84 protocol is a reliable way of establishing a secure key between healthcare establishments and helping prevent quantum facilitated cyber-attacks.

6.5 Communication Performance

Efficiency of the proposed framework in terms of communication was measured based on encryption time, communication latency, the throughput and the computational overhead. The experimental outcomes revealed that the framework suggested needed an average encryption period of 0.82 seconds to transmit a secure healthcare data. The mean communication latency in secure transmission was about 14 milliseconds and the mean throughput of the system was 920 Mbps in the case of distributed healthcare network environment. The measured computational overhead of the combined QKD and machine learning security architecture was estimated at about 8.6% which is acceptable in regard to secure healthcare communication systems given the high level of security improvement. The performance evaluation of communication is shown in Fig 5.

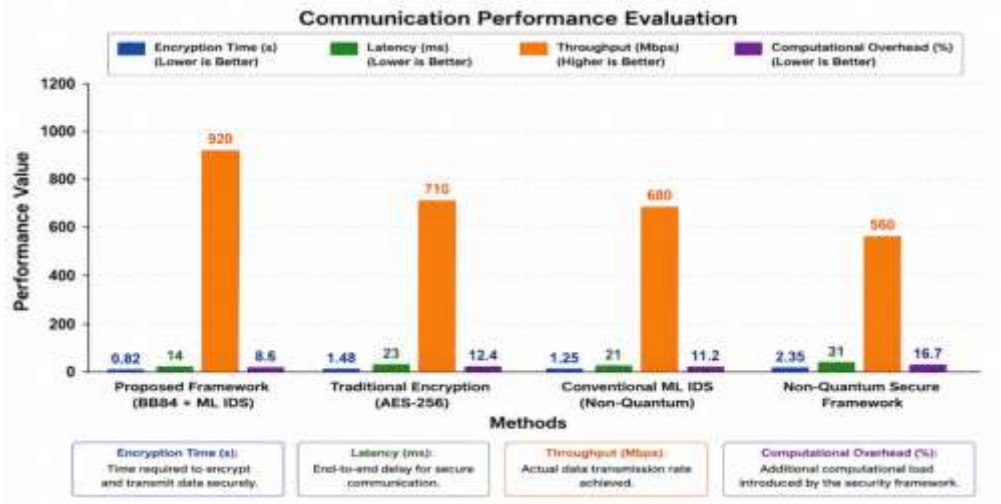

Fig 5.Communication performance evaluation of the proposed secure healthcare communication framework.

The findings suggest that the suggested framework has an effective communication performance and at the same time is able to offer intelligent intrusion detection and quantum-secure healthcare communication.

6.6 Comparative Analysis

The effectiveness of the proposed framework was compared to that of traditional encryption systems, conventional machine learning intrusion detection systems, and non-quantum secure communication frameworks. Older encryption systems proved to be more vulnerable to sophisticated cyber-attacks, as well as not able to detect eavesdropping. The traditional machine learning intrusion detection systems had offered smart attack classification, but was susceptible to future attacks using quantum computing because they lacked quantum-safe communication protocols. Non-quantum secure healthcare communication systems also had increased vulnerability of communication and reduced resistance against advanced interception attacks. Conversely, the proposed BB84 and machine learning-based framework outperformed in classification, better secure key generation, less susceptible to attacks, and better real-time cyberattack detection performance. A combination of quantum cryptography and intelligent intrusion detection thus offers a scalable, adaptive, and very secure communication architecture to defend distributed healthcare systems against not only classical but also new quantum-enabled cybersecurity threats.

7. Discussion

The presented BB84 quantum cryptography and machine learning-based implementation shows a huge potential of improving a secure communication within the distributed healthcare system. The experimental findings reveal that the combination of Quantum Key Distribution and intelligent intrusion detection is very powerful in cybersecurity protection against traditional and recent types of quantum attacks. The fact that the proposed framework can create quantum-safe communication channels by implementing the BB84 protocol and thus enhance health information confidentiality, as well as avoiding unauthorized interception of medical data throughout the transmission of the latter is one of the key benefits of the proposed framework. The fact that the Quantum Bit Error Rate was low (3.0%), and that the eavesdropping detection probability was high (99.68%) affirm that the quantum communication layer can securely handle confidential healthcare data against malicious interception attacks. Further, the machine learning-based intrusion detection module showed high classification performance indicated by accuracy of 95.50%, precision of 97.29%, recall of 93.60% and F1-score of 95.41%, thus proving a high intelligent ability of cyberattacks detection in the distributed healthcare setting.

Combining the effect of the Random Forest and XGBoost algorithms makes the intelligent attack detection more efficient since it allows tracking and classifying the traffic in healthcare networks in real-time. The framework is effective in the detection of denial-of-service attacks, malware communication, and unauthorized access attempts and data interception attacks with low false positive and minimal communication compromise. The other significant benefit of the offered framework is decreased cyber vulnerability as a result of joint application of quantum-secure encryption and smart adaptive threat detection. The architecture also aids in the scalability of distributed healthcare since the framework may be used in cloud healthcare systems, IoMT communication platforms, and remote healthcare infrastructures with the framework not contravening communication security. The obtained throughput of 920 Mbps and the communication latency of 14 ms also suggest that the proposed framework ensures efficient healthcare communications performance, as well as offering improved cybersecurity coverage.

There are certain practical uses of the proposed framework in the contemporary digital healthcare systems. The network can ensure the security of communication between the medical servers, healthcare professionals, diagnostic systems, and patient monitoring devices in smart hospitals. The proposed architecture can be applied to telemedicine systems to guarantee secure distant consultations and secure transmission of medical reports, diagnostic pictures, and patient records across the distributed healthcare systems. It also fits very well in Internet of Medical Things scenarios, where wearable healthcare gadgets are in constant communication with each other, continuously broadcasting sensitive physiological information over interconnected communications. Moreover, the architecture can offer safe security to the electronic health record systems by avoiding unauthorized access to information and interception of communications. Cloud healthcare solutions also enjoy the advantages of quantum-safe communication and smart intrusion detection, as the architecture promotes the safety of sharing healthcare data and managing distributed medical information on a mass healthcare system level.

Although the proposed framework has performed highly in terms of security, it has its own limitations as well. A technical constraint is that the implementation of the Quantum Key Distribution protocol with the quantum channel infrastructure and quantum communication hardware to support the implementation of a working Quantum Key Distribution protocol based on the BB84 model relies heavily on these capabilities. Currently, the deployment of real-world quantum communication systems is costly in terms of infrastructure and availability of commercial quantum communication devices are limited. A second disadvantage is the computational cost due to the joint use of quantum cryptography and machine learning-based intrusion detection, especially in large-scale distributed health care settings with large volumes of network traffic. The complexity of real-time deployment is also an issue since healthcare communication systems need to be operated in low-latency mode at all levels, and effective synchronization between quantum communication layers and intelligent cybersecurity modules. Also, the machine learning intrusion detection system is quite sensitive to the quality and diversity of datasets, such that a small or skewed training data sets can have an impact on performance in attack classification and generally to learn in real-life situations involving healthcare communication.

8. Future Work

The proposed framework can also be improved by future research through incorporating federated learning-based quantum healthcare security architectures which can be able to provide distributed collaborative intrusion detection without sharing healthcare data centrally. The intrusion detection system can also be enhanced with explainable artificial intelligence to enhance transparency and interpretability of cybersecurity decision-making in healthcare settings. Lightweight Quantum Key Distribution frameworks can also be designed to minimize the communication overhead and allow realistic implementation on resource limited IoMT healthcare devices. Healthcare cybersecurity architectures enabled by blockchain are also another area of potential research that has been reported to enhance the integrity of healthcare data, decentralized authentication, and protection of distributed communication in healthcare. Additional future research can be conducted on edge-AI-based secure healthcare communication systems that can be used to deliver intelligent cybersecurity protection in the network edge in real-time. Moreover, practical healthcare systems deployment

and testing of quantum communication infrastructures in real-world conditions are also key future research goals to improved next-generation intelligent healthcare cybersecurity technologies.

9. Conclusion

This study proposed a hybrid quantum cryptography and machine-learning- based framework of secure communication in distributed healthcare systems using the BB84 Quantum Key Distribution protocol and smart intrusion detection protocols. The suggested framework was effective at combining quantum-safe key exchange, AES-256 encrypted healthcare communication and machine learning-powered cyberattack detection to enhance the communication safety and smart threat management in cloud-permitted and IoMT healthcare settings. Experimental analysis with NSL-KDD and CICIDS2017 data revealed that the proposed framework had a high intrusion detection rate of 95.50% accuracy, 97.29% precision, 93.60% recall and 95.41% F1-score, which indicates a good ability to classify cyberattacks and minimal vulnerability to healthcare communication. The module of quantum communication (BB84) was capable of a low Quantum bit error rate of 3.0% and a high eavesdropping detection of 99.68%, which validated the functionality of the quantum-secure communication architecture proposed. Combination of machine learning-driven intelligent cybersecurity and quantum cryptography can considerably raise the policy of health care data confidentiality, dependability of secure communication, and response to change of threats in distributed health care systems. The suggested framework thus helps towards building scalable, intelligent and secure healthcare ecosystems that can withstand both classical and quantum enabled cyber threats. The paper also mentions future relevance of quantum artificial intelligence based healthcare cybersecurity architectures in safeguarding sensitive medical data in the multi-generational distributed healthcare communication systems.

References

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of network and computer applications*, *60*, 19-31.
2. Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, *560*, 7-11.
3. Decker, T., Gallezot, M., Kerstan, S. F., Paesano, A., Ginter, A., & Wormsbecher, W. (2025). Quantum key distribution as a quantum machine learning task. *npj Quantum Information*, *11*(1), 140.
4. Dixon, A. R., Dynes, J. F., Lucamarini, M., Fröhlich, B., Sharpe, A. W., Plews, A., & Shields, A. J. (2017). Quantum key distribution with hacking countermeasures and long term field trial. *Scientific Reports*, *7*(1), 1978.
5. Hayashi, M., & Tsurumaru, T. (2012). Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths. *New Journal of Physics*, *14*(9), 093014.
6. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Eai Endorsed Transactions on Security and Safety*, *3*(9), 21.
7. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., & Wallden, P. (2020). Advances in quantum cryptography. *Advances in optics and photonics*, *12*(4), 1012-1236.
8. Portmann, C., & Renner, R. (2022). Security in quantum cryptography. *Reviews of Modern Physics*, *94*(2), 025008.
9. Purohit, K., & Vyas, A. K. (2025). Quantum key distribution through quantum machine learning: A research review. *Frontiers in Quantum Science and Technology*, *4*, 1575498.
10. Radanliev, P., De Roure, D., & Santos, O. (2023). Red Teaming Generative AI/NLP, the BB84 quantum cryptography protocol and the NIST-approved Quantum-Resistant Cryptographic Algorithms. *arXiv preprint arXiv:2310.04425*.
11. Ravi, V. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*.
12. Renner, R., & Wolf, R. (2023). Quantum advantage in cryptography. *AIAA journal*, *61*(5), 1895-1910.
13. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of modern physics*, *81*(3), 1301-1350.
14. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), 41-50.
15. Tomamichel, M., & Leverrier, A. (2017). A largely self-contained and complete security proof for quantum key distribution. *Quantum*, *1*, 14.