Quantum-based Secure Communication Frameworkfor Telehealth Applications using BB84 Protocol

Harshal Gajjar*, Dirgha Jivani†,
Email:*20bce086@nirmauni.ac.in, †20bce065@nirmauni.ac.in

***Abstract*—This paper introduces a novel telehealth communication system, designed to enhance the security and integrity of medical data exchange. In the rapidly evolving digital healthcare landscape, the protection of sensitive patient information is paramount. To address this, our system uniquely combines quantum cryptography, specifically the BB84 protocol, with blockchain technology, offering a dual-layered security framework. The Quantum Layer, underpinned by the BB84 protocol, establishes quantum-secure communication channels, effectively encrypting data exchanges between patients, doctors, and hospitals. This layer guarantees that medical information remains confidential and safe from potential quantum-level eavesdropping threats. The subsequent Blockchain Layer further strengthens the system by storing these encrypted communications in an immutable blockchain ledger. This approach not only secures the data against unauthorized alterations but also provides a transparent and permanent record of all transactions, thereby enhancing the auditability of medical communications.**

***Index Terms*—Quantum Cryptography, BB84 algorithm, Security, Secure Message**

I. Introduction

Healthcare has continuously evolved with the integration of advanced technological solutions, profoundly reshaping patient-doctor interactions and the broader medical framework [1]. One pivotal result of this tech-healthcare confluence is the rise of telehealth networks, sometimes referred to as telemedicine or e-health networks. These systems serve as conduits, bridging patients with medical institutions and healthcare professionals, ensuring continuity of care even across vast distances. The World Health Organization underscores the significance of telehealth as an invaluable tool in advancing global public health, a stance further emphasized by its undeniable role during the COVID-19 pandemic in mitigating infection spread via remote consultations and care.

However, the path of healthcare's digital transformation isn't devoid of challenges. Managing and transmitting vast amounts of intricate, sensitive health data across these digital networks can occasionally lead to data losses, fragmentation, and more concerningly, breaches. The year 2020 brought this vulnerability into stark relief. From January to October alone, an astonishing 22 billion records found themselves exposed due to 700 data breaches, with the healthcare sector, unfortunately, standing out as the prime target [2].

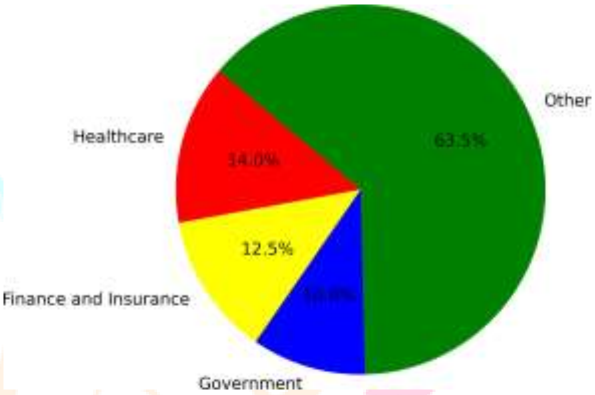

Fig. 1: Distribution of the data leak in 2020

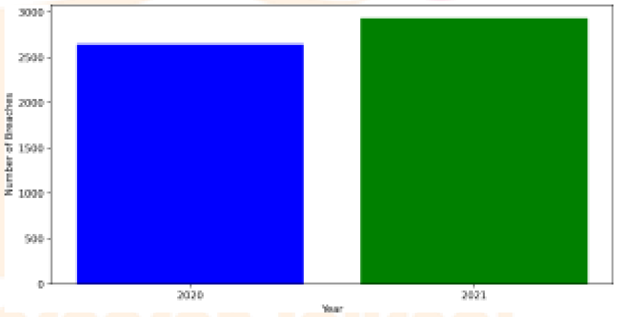

Fig. 2: Increment of data breaches in the US from 2020-2021

The intrinsic value of such data in the black market is noteworthy. While personally identifiable information (PII) might command prices of $1–2, personal health information (PHI), with its detailed health records and diagnostics, can fetch amounts upwards of $363, presenting a tantalizing target for hackers. In a chilling testament to this, a report by IBM Security highlighted that the healthcare sector bore an exorbitant cost for data breaches in 2020, averaging a steep $7.13 million, far exceeding global standards.

Diving deeper into the global landscape reveals distinct regional challenges. Taking the Philippines as an illustrative example, despite proactive steps by its government, such as allocating over P1 billion for cybersecurity in 2021, the country faced an alarming rate of compromised medical devices just the previous year, signaling persistent vulnerabilities and underscoring the need for rigorous, context-specific solutions [3].

In the unceasing endeavor to fortify data transmission, especially within the intricate network of healthcare, cryptographic methods have been pivotal. Recent advances have pushed the boundaries of this domain, adapting it to cater to modern technological innovations. For instance, the integration of the Internet of Things (IoT) in healthcare has opened up avenues for remote monitoring and patient care, but it has also posed new challenges for data privacy and security. Chandani and Sharma's 2023 study provides insight into this very juxtaposition, proposing a Secure Data Transmission Scheme (SDTS) which employs Elliptic Curve Cryptography (ECC) to bolster communication security in Wireless Sensor Networks (WSNs). Such networks form the underpinning for a plethora of contemporary healthcare devices, and ensuring their security is paramount [4]. In parallel, vehicular communications, while not directly related to healthcare, present an illustrative example of the broad spectrum of areas where data security is indispensable. Another research [5] delves into Vehicular Ad-hoc Networks (VANET), advocating for an enhanced ECC methodology optimized with an Adaptive Horse herd Optimization Algorithm (AHOA) to navigate the intricate landscape of data transmission challenges in this space.

Yet, as promising as these innovations might seem, looming on the horizon are quantum machines with the potential to destabilize the very foundations of traditional cryptography. Quantum computers, with their capacity to rapidly process and calculate using quantum mechanics, threaten to decrypt widely-used encryption schemes such as ECC. This means that while current cryptographic solutions offer robust defense mechanisms against contemporary threats, they might be rendered vulnerable in a quantum-dominated future, necessitating the evolution of cryptographic techniques to withstand quantum-driven challenges.

Transitioning into this quantum realm, it becomes evident that a paradigm shift in cryptographic solutions is imperative. Quantum cryptography, unlike its classical counterpart, is equipped to counter the immense computational prowess of quantum machines. Foremost among quantum cryptographic protocols is the BB84, conceived by Bennett and Brassard in 1984. Rather than merely relying on mathematical complexity as traditional methods do, BB84 employs quantum mechanics' intrinsic properties. It uses the principle of superposition to transmit qubits in a mix of different bases. As receivers measure these in varied bases, an eavesdropper's presence becomes evident due to the inherent no-cloning theorem of quantum mechanics, ensuring any intrusion distorts the quantum state. This physical manifestation of security allows parties to detect eavesdropping attempts by merely comparing a subset of their measurements. While BB84 stands as a pioneering quantum protocol, the arena has been enriched by others like the E91, which leans on quantum entanglement, and the six-state and B92 protocols which offer alternative quantum key distribution schemes. Collectively, these quantum methodologies signify a resilient frontier in the face of quantum computational threats, ensuring that the healthcare sector and other data-intensive industries are armored against breaches in a quantum era.

II. Related Works

III. System model and problem formulation

In the contemporary healthcare landscape, the secure exchange of sensitive medical information is of paramount importance. To address this critical need, we propose an innovative solution that leverages the power of Quantum Key Distribution (QKD) and blockchain technology to establish a highly secure communication framework for healthcare data. The patients $P = \{P_1, P_2, P_3, \ldots, P_j, \ldots, P_y\}$ and hospitals $H = \{H_1, H_2, H_3, \ldots, H_i, \ldots, H_x\}$, each playing a vital role in this healthcare communication ecosystem. The communication between these entities is facilitated by a quantum chat application, where QKD takes center stage to ensure the encryption and decryption of data, guaranteeing the utmost data confidentiality as is shown by (1) and (2). Furthermore, we employ blockchain technology (3) to enhance the security and traceability of medical data, offering a robust foundation for the storage and management of healthcare-related information.

$$\psi \xrightarrow{\text{QKD}} ED \tag{1}$$

where, ψ : Original data or decrypted data, QKD : Quantum Key Distribution, method for encryption and decryption and ED : Data encrypted using QKD.
Patients securely communicate with hospitals through the quantum chat application, with QKD mechanisms ensuring data encryption and decryption for privacy and security. Blockchain technology is utilized to securely store and manage patient data and medical files, providing data immutability and traceability, essential for maintaining data integrity. Hospitals make informed decisions to select suitable doctors D_i from a pool of available medical professionals $D = \{D_1, D_2, D_3, \ldots, D_k, \ldots, D_z\}$, ensuring patients receive specialized medical attention tailored to their unique needs.

$$\text{Encrypted Data} \xrightarrow{\text{QKD}} \psi \tag{2}$$

$$\text{Data} \xrightarrow{BCT} Block \tag{3}$$

where, $Data$: Generic data to be stored, BCT : Blockchain Technology used for data storage, and $Block$: Data stored in block.
The selected doctor D_i conducts a comprehensive analysis of the patient's information, including medical records and test results, to facilitate accurate medical diagnosis and treatment planning. Results of the medical analysis provided in (4), along with relevant medical documents, are securely transmitted via the quantum channel to both the patient P_i and the hospital H_i, ensuring data integrity and confidentiality through quantum encryption.

$$\psi \xrightarrow{D^i} I \tag{4}$$

where, D_i : Selected Doctor D_i, I : Insights derived from data analysis.

IV. The Proposed Framework

A. Hospital Layer

Central to the entire medical communication system is the foundational technology embedded within the Hospital-Patient communication framework. These communication nodes $\{H_1, H_2, H_3, \ldots, H_i, \ldots, H_x\}$ representing individual hospitals are connected to multiple patient nodes $\{P_1, P_2, P_3, \ldots, P_j, \ldots, P_y\}$, are fortified with the BB84 protocol ensuring quantum-secure communication. Within the chat app, the data is exchanged securely, ensuring the confidentiality and integrity of the sensitive medical information contained within. The importance of this layer is unmatchable. The secure and organized exchange of medical data offers invaluable insights into the patient's health, enabling timely and accurate medical interventions. The hospitals check the provided info from the patient stores in the blockchain and then pass it on to the selected doctor D_i for further analysis.

B. Doctor Layer

The next integral layer of the medical communication system focuses on the pivotal role of physicians: the Doctor Layer. Upon receipt, the chosen doctor or doctors delve into a meticulous analysis of the information. This involves understanding the patient's health status, diagnosing potential medical conditions, and strategizing an appropriate treatment plan. Following this in-depth assessment, the doctors embark on their medical activities, which could encompass various tasks ranging from prescribing medications to suggesting specialized treatments or procedures. After completing their assessment and medical activities, a comprehensive report is crafted. This report encapsulates the doctor's findings, professional recommendations, and the proposed course of action. Subsequently, this report is securely transmitted to the concerned patient P_i from the set of patients $\{P_1, P_2, \ldots, P_k, \ldots, P_N\}$ and also relayed back to the originating hospital H_i for integration into the broader medical record system.

to

C. Patient Layer

The culmination of the medical communication system rests in the Patient Layer. This layer emphasizes the essential role of the patient, who sits at intersection of both the hospital and the doctor. From the set of patients $\{P_1, P_2, \ldots, P_i, \ldots, P_N\}$, a specific patient P_i initiates the process by transmitting their Personal Health Records (PHR) and other medical information to a chosen hospital via the quantum-secure chat application. Once the hospital receives and processes this data, it's seamlessly relayed to selected doctors from the set $\{D_1, D_2, D_3, \ldots, D_j, \ldots, D\}$. These physicians scrutinize the PHR, undertake relevant medical activities, and generate a comprehensive report detailing their findings and recommendations. This report, vital for the patient's healthcare journey, is then sent back securely to the patient. Upon receipt, the patient is empowered with a clear understanding of their health status, potential medical conditions, and the doctor's advised course of action.

D. Quantum Layer

In the telehealth communication system, the BB84 protocol (Equations (5), (6), and (7) is ingeniously integrated with a chat application, ensuring quantum-secure transmission of medical information. This protocol establishes a secure quantum communication channel between the participants by distributing a cryptographic key that cannot be intercepted without detection. The process begins with one party (the sender) preparing qubits (Fig. 3) in random quantum states as is given in eq.(5) and sending them to the receiver over a quantum channel. These qubits are encoded in either of two bases (Z or X), randomly chosen by the sender. The receiver, upon receipt, measures the qubits in bases also chosen at random (Equation (6)). After the transmission, both parties compare their choice of bases over a public channel and discard the bits where their bases did not match, forming a shared secret key (Equation (7)). This key is then used to encrypt the chat messages. Once the conversation is encrypted, the messages are stored as documents in the blocks of a blockchain. The blockchain serves as a secure, immutable ledger, ensuring the integrity and non-repudiation of the stored medical data. Each block contains a timestamp and a cryptographic hash of the previous block, linking them in a chain and preventing any retroactive alteration of the data. The combination of the BB84 protocol with blockchain technology not only provides an unprecedented level of security for the transmission of sensitive medical data but also ensures the confidentiality and integrity of the data stored. This dual-layered approach – quantum encryption for communication and blockchain for data storage – offers a robust framework for protecting patient information in the rapidly evolving domain of telehealth.

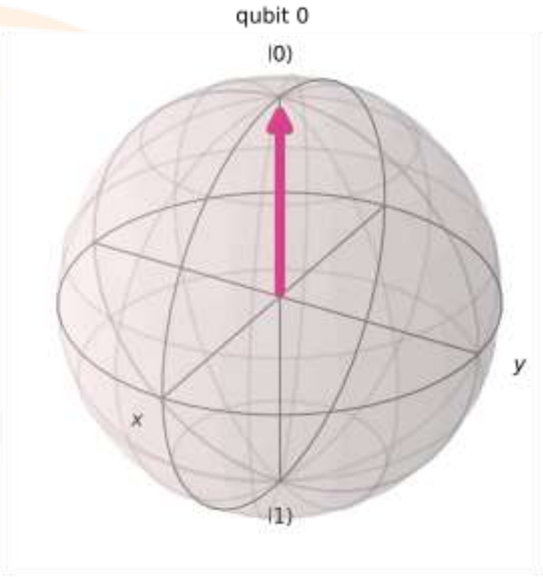

Fig. 3: Visualization of a qubit in 0 state.

$$|\psi_i\rangle = \begin{cases} |0\rangle \text{ or } |1\rangle, & \text{for basis } Z \\ |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), & \text{for basis } X \end{cases} \qquad (5)$$

where, $|\psi_i\rangle$ represents the state of the qubit prepared by Alice, Z is the standard basis $\{|0\rangle, |1\rangle\}$, and X is the superposition basis $\{|+\rangle, |-\rangle\}$.

$$M = \begin{cases} Z, & \text{if Alice used basis } Z \\ X, & \text{if Alice used basis } X \end{cases} \qquad (6)$$

where, M represents Bob's measurement basis, Z is the standard basis, and X is the superposition basis.

Key Sifting Process: After the exchange of qubits, Alice and Bob publicly compare their basis choices. They discard any bits where the bases did not match. This process, known as key sifting, can be represented as:

$$K_i = \begin{cases} \text{Keep}, & \text{if bases match} \\ \text{Discard}, & \text{if bases do not match} \end{cases} \qquad (7)$$

where, K_i represents the decision to keep or discard a bit in the key, based on whether the bases used by Alice and Bob match.

Algorithm 1 Alice's Protocol

```
procedure ALICE
    Initialize socket $s$ on HOST, PORT
    Listen for connections on $s$
    Accept connection as $conn$
    $alice\_bits$ ← GENERATE _RANDOM _BITS(20)
    $alice\_bases$ ← GENERATE _RANDOM _BASES(20)
    Send $alice\_bits + alice\_bases$ through $conn$
    Receive $bob\_bases$ from $conn$
    Calculate shared key from matching bases
    Receive $error\_rate$ from $conn$
    if $error\_rate > 0$ then
        Print "Connection not secure"
    else
        Print "Connection is secure"
        START_CHAT("Alice", $conn$)
    end if
end procedure
```

Security : One of the paramount concerns in the medical domain is the safeguarding of patient data and the assurance of confidentiality in doctor-to-doctor communication. The BB84 protocol's security stems from the fundamental principles of quantum mechanics. If an eavesdropper, often termed Eve, tries to intercept and measure the quantum states sent during the key exchange, this action will introduce discrepancies due to the quantum measurement's invasive nature. As a result, by comparing a subset of their shared key, the communicating parties can detect any eavesdropping and abort the key if necessary. This quantum-enabled security ensures that sensitive medical data remains confidential and uncompromised.

Algorithm 2 Bob's Protocol

```
procedure BOB
    Initialize socket $s$ and connect to HOST, PORT
    Receive data from $s$ as $data$
    Extract $alice\_bits$ and $alice\_bases$ from $data$
    $bob\_bases$ ← GENERATE _RANDOM _BASES(20)
    Measure qubits sent by Alice using $bob\_bases$ to obtain $bob\_results$
    Send $bob\_bases$ through $s$
    Calculate shared key from matching bases
    Calculate $error\_rate$ from mismatched bits
    Send $error\_rate$ to Alice through $s$
    if $error\_rate > 0$ then
        Print "Connection not secure"
    else
        Print "Connection is secure"
        START_CHAT("BOB", $s$)
    end if
end procedure
```

E. Blockchain Layer

The Blockchain Layer introduces an additional tier of security and integrity to the medical communication system. In this layer, transactions, which are the secure messages exchanged between patients and hospitals, are grouped into blocks. Each block $\{B_1, B_2, B_3, \ldots, B_j\}$ contains a set of transactions $T = \{T_1, T_2, T_3, \ldots, T_n\}$ and a unique identifier known as a hash. This hash is a digital fingerprint of the block's contents, including the transactions and the hash of the previous block in the chain, forming an unbreakable link.

When a patient or doctor sends a message, it is encrypted using the BB84 protocol and then broadcasted to the network to be included in a block. A new block is created by compiling these transactions and computing the block's hash. The process of block creation can be represented mathematically as:

$$B_n = \text{Hash}(T_1, T_2, \ldots, T_m, \text{Hash}(B_{n-1})) \qquad (8)$$

where Equation (8) describes the composition of a block, B_n, incorporating the transactions T and the hash of the previous block, B_{n-1}.

Each new block includes the hash of the previous block, $\{B_{n-1}\}$, thus linking it to the chain. This creates an immutable record, as changing any information in a previous block would require recalculating every hash that comes after it, which is computationally infeasible. The block linking process can be mathematically expressed as:

$$B_n \rightarrow B_{n-1} \qquad (9)$$

where Equation (9) signifies the linking of the current block, B_n, to its predecessor, B_{n-1}, thereby ensuring the continuity and immutability of the blockchain.

The integrity of the blockchain can be verified at any time by recalculating and comparing the hashes of the blocks. If the hashes match the recorded values, the integrity of the chain is confirmed. The verification process is represented as:

$$\text{Verify}(B_n) = \text{Hash}(B_n) == \text{Stored Hash of } B_n \qquad (10)$$

where Equation (10) outlines the verification method for a block, B_n, ensuring that its current hash matches the stored hash, thus validating the integrity of the blockchain.
This blockchain layer acts as a secure ledger, recording all communications in a verifiable and immutable manner. It ensures that once a message is recorded in a block, it cannot be altered or deleted without detection, thus providing a robust audit trail for all communications within the medical system.

Algorithm 3 Blockchain Creation and Verification Protocol

```
procedure CREATEBLOCK(transactions)
    block ← new Block()
    block.transactions ← transactions
    block.previousHash ← getLastBlockHash()
    block.hash ← calculateHash(block)
    return block
end procedure
```

```
procedure ADDBLOCKTOCHAIN(block)
    if isValidNewBlock(block, getLatestBlock()) then
        append block to blockchain
    end if
end procedure

function CALCULATEHASH(block)
    data ← concatenate(block.previousHash, block.transactions)
    hash ← hashFunction(data)
    return hash
end function

function ISVALIDNEWBLOCK(newBlock, previousBlock)
    if previousBlock.hash '= newBlock.previousHash then
        return False
    end if
    if calculateHash(newBlock) '= newBlock.hash then
        return False
    end if
    return True
end function

function GETLASTBLOCKHASH
    latestBlock ← getLastBlock(blockchain)
    return latestBlock.hash
end function
```

V. Performance Evaluation

A. Experimental Setup

This research paper describes the experimental setup of a secure chat application, focusing on the amalgamation of quantum cryptography principles with symmetric encryption to ensure message confidentiality. Developed on a MacBook M1 Pro environment, Python was chosen as the primary programming language, ensuring seamless integration of backend logic with a frontend user interface constructed using the Tkinter library. A pivotal phase in the experiment revolves around generating random bits and bases, echoing the foundational principles of Quantum Key Distribution (QKD). Essential to this phase was the creation of random bits, encapsulated as a string of 0s and 1s, and the fabrication of random bases, typically represented by the characters 'X' and 'Z'. These generated bits and bases were then securely exchanged over a communication channel, realized using a socket connection. Upon the successful establishment of a shared secret key via the QKD simulation, the chat session—bolstered with layers of security—was initiated. At its core, the chat system encrypts messages using the Fernet symmetric encryption scheme before transmitting them. On the receiving end, messages are decrypted using the shared key, ensuring confidentiality. For user convenience, a graphical user interface, built using Tkinter, provides an interactive platform for message exchange.

B. Quantum-based results

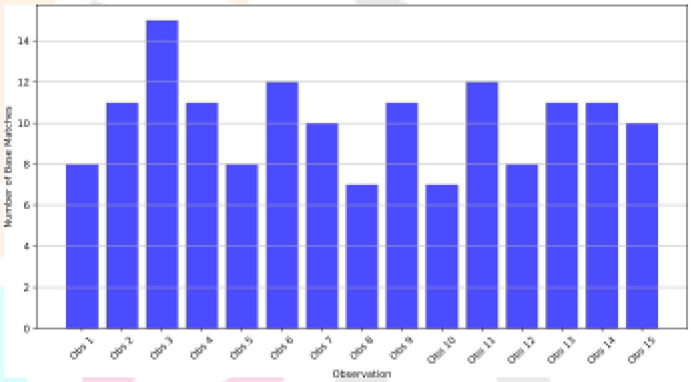

Fig. 4: The frequency of matching bits between Alice and Bob

Fig. 4 represents the frequency of a matched bases between two parties, who independently select between two quantum states—represented as 'X' and 'Z' for a sequence of 20 qubits across 15 observations. The 'X' and 'Z' symbolize two distinct, non-overlapping quantum states, such as differing polarization directions of photons. Upon comparison, the number of matches—where Alice and Bob chose the same state for a given qubit—is recorded. The expected average of matches is 10, given the random selection from two possible states. The bases are random in nature for generation of a shared key, and not revealing it via the public channel. The chart's fluctuating match counts align with the randomness of selection, exhibiting natural variance around the 50% baseline. This distribution is crucial in QKD, as only qubits with matching bases contribute to the raw key material, which, after refining through error correction and privacy amplification, yields the secure cryptographic key.

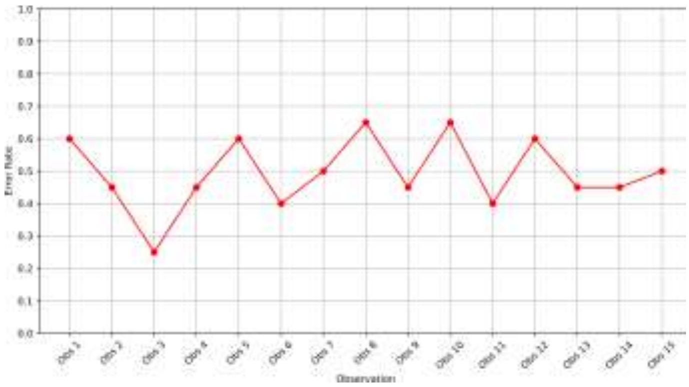

Fig. 5: Error rate of the qubit transfer

Fig. 5 displays variations in error rates across 15 observations. The error rate is calculated (mention equation) and an eavesdropper was simulated in observations 1,5,8,10 and 12 to notice the fluctuaton in the error rate. It is visible that the rate is higher than 50% indicating a potential eavesdropper. In the BB84 protocol, an eavesdropper, known as ’Eve’ could inadvertently disturb qubits when attempting to intercept and measure them, resulting in discrepancies during Bob’s measurements. Observations with notably increased error rates suggest interference by Eve, highlighting the protocol’s effectiveness in detecting unauthorized interception in quantum communications.

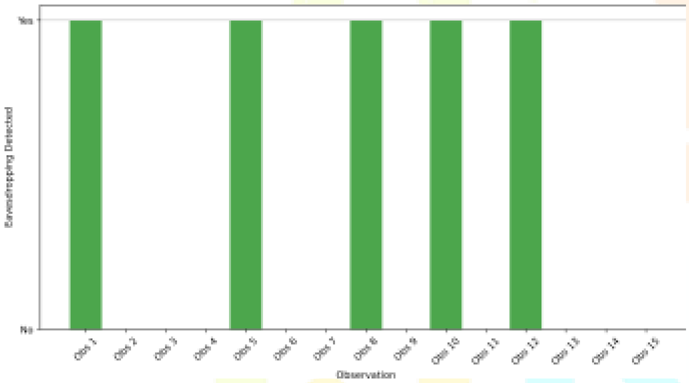

Fig. 6: Detection of the eavsedropper

Fig. 6 illustrates the eavesdropper detection across 15 observations. Marked either as ”Yes” or ”No,” with ”Yes” denoting the detection of an eavesdropper, this plays a pivotal role in assessing the security of the QKD protocol. The criterion for eavesdropper detection is that if the error rate in a specific observation equals or surpasses the 50% threshold, it is marked as ”Yes,” signifying potential external interference. This figure visually encapsulates the protocol’s ability to identify and signal unauthorized access to the quantum communication channel, reinforcing the QKD system’s sensitivity to potential security breaches.

VI. Conclusion

This paper has presented a comprehensive overview of a state-of-the-art telehealth communication system, which incorporates advanced quantum and blockchain technologies to address the critical needs of data security and integrity in medical communications. At the core of this system lies the Quantum Layer, utilizing the BB84 protocol to establish quantum-secure communication channels. This layer ensures that sensitive medical information exchanged between patients, doctors, and hospitals is encrypted and protected against potential eavesdropping, thereby maintaining confidentiality and integrity.The Blockchain Layer adds an additional level of security and auditability. By grouping encrypted messages into immutable blocks and linking them in a chain, the blockchain technology not only secures the data against tampering but also provides a verifiable and permanent record of all transactions. In conclusion, the integration of quantum cryptography with blockchain technology in this telehealth communication system offers a robust, secure, and efficient framework for handling sensitive medical data. It paves the way for a new era in digital healthcare, where the privacy and security of patient information are paramount. As the field of telemedicine continues to evolve, this system stands as a testament to the potential of combining cutting-edge technologies to enhance and safeguard medical communications.

References

[1] T. M. Camarines and J. C. M. Camarines, “Discussing data security and telehealth during the covid-19 pandemic,” *PubMed Central (PMC)*, 2020.

[2] “Over 22 billion records exposed in 2021,” 2021.

[3] A. M. Association, “Interoperability and patient access to health data,” *AMA Journal of Ethics*, 2021.

[4] P. Chandani and M. Sharma, “Secure data transmission using cryptography for internet of things and sensor networks applications,” *Proceedings of the International Conference on Innovations in Computer Science and Engineering (ICoCICs)*, 2023.

[5] M. J. Patil and K. Adhiya, “An enhanced elliptic curve cryptography scheme for secure data transmission to evade entailment of fake vehicles in vanet,” *Computers and Electrical Engineering*, 2023.