Simulated Quantum Entangled Firewall for Preventing Insider Data Leakage

Abstract— Insider data leakage remains a significant cybersecurity problem which existing firewalls have difficulty detecting. The paper presents an integrated firewall system which simulates quantum entanglement email verification along with end-point activity monitoring and WhatsApp-based approval. The email verification process utilizes Qiskit's simulated two-qubit states to produce deterministic quantum entangled amplitude values for basis states through hashed RY rotation angles which stop mismatches from passing through. The system employs Python tools to track USB insertion activities, capture screens and monitor clipboard functionality along with cloud accessibility. A Tkinter interface delivers warning notifications and Firebase provides secure storage for user credentials. Higher-level authorities must approve every login attempt through WhatsApp to maintain human intervention in the process. The system integrates multiple defence layers that provide scalable, proactive protection against insider threats across all industrial sectors, including those related to environmental operations.

Keywords—Quantum Entanglement, Cryptography, Insider Data Leakage, Hybrid Firewall, Simulated Quantum State, Deterministic Fingerprint, Endpoint Monitoring, WhatsApp Approval

I. Introduction

Insider data breaches are still one of the largest cybersecurity threats, accounting for a significant percentage of reported threats. While external attacks come from outside, insider threats are from legitimate users like employees, contractors, or third parties, who may leak confidential data intentionally or unintentionally. Since their behavior mimics normal activity, conventional security controls have difficulty detecting them. Environmental technology firms are particularly vulnerable with quick digitalization, global infrastructures, and proprietary clean energy technologies. Of all the channels through which exfiltration takes place, Email is the most common and dangerous channel.

Insider threats typically take one of four forms: (a) malicious insiders who use information for private or competitive gain; (b) opportunistic insiders gathering sensitive information without specific intent; (c) careless insiders transmitting inadvertent disclosures, like misplaced emails; and (d) cooperative insiders working in concert with outsiders. Human error accounts for almost 60% of breaches, and email's susceptibility underscores this. Examples from the real world display these threats: In 2019, a GE Power engineer illegally sent shielded turbine technology by email, slowing cleaner system rollouts. In 2023, former Tesla employees leaked 100 GB of data, including battery architecture, boosting data center power consumption. In 2022, a phishing ransomware attack required Nordex Wind Turbine to take IT systems offline, temporarily using diesel generators that increased emissions. These events indicate insider threats can prevent environmental gains, as well as produce financial or reputation loss.

Quantum entanglement—where particles correlate their states independent of distance—supports secure communication protocols like the BB84 quantum key distribution scheme[1] and QKD-Enhanced Cybersecurity Protocols[2]. These utilize non-local correlations for identity verification and data security but real-world use is still rare due to high costs and complexity of Physical quantum systems. This paper puts forward a simulated quantum entanglement–insider threat detection framework for email, attaching to each recipient a SHA-512–derived quantum entangled amplitude values for basis states . Deviating emails are immediately blocked. Built-in behavior monitoring catches anomalies such as insertion of USB, screen capture and higher-authority WhatsApp approvals prevent sensitive data transmission without supervisor approval. The proposed firewall boosts cybersecurity strength.

II. Related work

Legacy insider threat defence and secure communication protocols are rooted in classical cryptography and

post-event reactive controls like auditing and rule-based access. These are a bare minimum starting point for defence but are insufficient in dynamic environments where insiders can exploit credentials or go around static defence. Legacy systems have no real-time anomaly detection, leading to late responses and more data exfiltration attacks. The quantum computing revolution has also undermined the trust in classical cryptography, which has initiated research in quantum key distribution (QKD), post-quantum cryptography (PQC), and quantum-aided threat modelling. These solutions provide promising alternatives through quantum-resilient communication and identity verification based on entanglement and superposition.

Some research efforts have taken this approach and motivated this work:

Ramesh et al. employed Quantum Random Number Generators and post-Quantum VPNs to enhance IoT communication security, demonstrating improved encryption strength and resilience against quantum attacks but without focusing on endpoint-level integration [3]. Sahana et al. developed a Quantum Network Simulator to simulate entanglement generation and single-qubit teleportation with improved fidelity analysis. However, it does not fully address experimental scalability or broader entanglement distribution across real-world networks [4]. Vijayaraj et al. proposed a protocol on non-maximally entangled states for secure teleportation under ideal conditions but not endpoint integration [5]. A comparative study in 2025 compared QKD and PQC but was theoretical without deployment testing [6]. Ye and Jiang proposed a dialogue protocol on entanglement swapping, which works well for passive eavesdropping but not endpoint threat detection [7]. Farokhi and Kim simulated quantum leakage through gentle probing, offering theoretical metrics but no real-world applications [8]. Ahmed et al. proposed a Zero Trust framework on quantum neural networks, but it has not been implemented yet [9]. Wang and Wang evaluated SPF, DKIM, and ARC email forwarding and suggested header-chain validation enhancements without behaviour analysis and encryption [10]. Hureau et al. DMARC settings were stress-tested and found to be vulnerable, yet mitigation was not comprehensive [11].

While such efforts are a step in the right direction, most are isolated—either on quantum simulations or standalone behavioural analysis without integration. None of them incorporate simulated quantum entanglement with user-specific verification and real-time endpoint scanning. This paper bridges these gaps by simulating quantum entanglement in Qiskit [12] to generate identity-bound fingerprints, coupled with behavioural and device-level monitoring. We also utilize Firebase-backed secure authentication and real-time USB, screenshot, and clipboard monitoring—offering an integrated, real-world zero-trust system beyond the theoretical and disjointed nature of existing systems.

III. System Architecture

The architecture framework depicted in Figure 1 operates as a secure data access system which targets corporate environments along with industrial settings. Employees can access confidential information through native approval workflows with endpoint monitoring and simulated quantum entanglement-based verification mechanisms while following this safe data access protocol. The architecture provides user-friendly interaction and strong access management, and dependable data handling through multiple layers which integrate graphical user interfaces , firewall protocols , database operations and external communication platforms.

The Key components of system architecture are discussed below:

(A) The Employee - Who serves as the initial party. Any employee seeking data access begins the process by launching the built-in GUI application to send a WhatsApp request. Users can easily interact with the system through this multi-channel entry which offers both convenience and user choice. Every request needs to undergo administrative approval for verification of its authenticity and organizational policy compliance before data access becomes possible. The Administration Approval module evaluates both the authenticity and appropriateness of employee data access requests after they have been submitted. The approval process functions as the first line of defence to stop unauthorized access. When the approval occurs, the main GUI receives the notification through WhatsApp which allows employees to resume their tasks. Human-in-the-loop validation takes place during this process to maintain data retrieval accountability.

(B) The GUI Module - Functions as the system's front interface which users find easy to use. Through its login feature, employees obtain secure access to the backend infrastructure. After signing in , users can access displayed information before selecting specific data to share. The GUI provides simple user interactions with backend systems as well as security features that limit access to administrator- approved permissions.

(C) The Firewall - Functions as the fundamental security layer which protects the system architecture. The firewall performs two primary functions that include watching endpoint operations and validating simulated quantum entanglement. The module which tracks endpoint activity performs ongoing monitoring of user interactions through the GUI and multiple access points. The system immediately detects unauthorized or suspicious activities during its operation. Simultaneously , the system uses a simulated quantum entanglement validation layer which replicates the quantum security principles. The system verifies both data integrity and authenticates entangled trusted emails before sending them externally through email to prevent interception.

(D) The database - Functions as the main storage facility which stores all operational and employee data. The database functions as both an entry point and exit point for handling data transactions. The firewall sends the requested database information back to the graphical user interface after receiving an authorized request which passes through the firewall. The firewall enforces database access by blocking any unapproved connections that could compromise data protection .

The system starts the Email Notification Module automatically after successful evaluation of the simulated quantum entanglement and data validation without human interaction. After data confirmation through the module, it sends the information to the intended recipient through email which completes the entire process of data delivery. The final step ensures that data acquisition receives proper documentation and traceability and secure delivery to the respective recipients which completes the fully controlled process of data access.

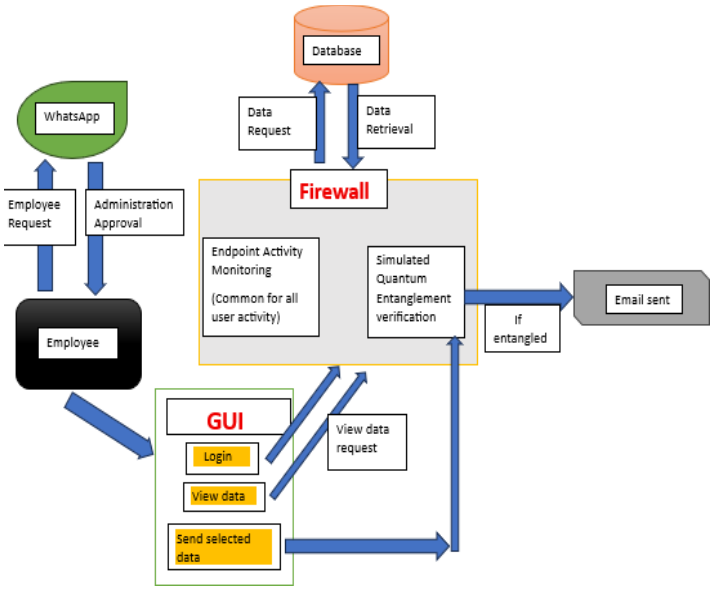


Figure 1: Block diagram of System Architecture

IV. System Design and Components

The Design proposed in Figure 2 is one that will cater to the problem of insider data breaches through a hybrid solution combining simulated quantum entanglement with continuous monitoring of the system. It consists of two operational phases: the Quantum Entanglement Simulation Phase and the Login and Monitoring Phase. The multi-tiered design is characterized by a zero-trust security posture, where no process or user is ever presumed to be trusted in itself, and must be expressly validated for every request for access or transmission. In the Quantum Entanglement Simulation Stage, the system begins the process by loading a configuration file (data.txt), which contains a seed value and a list of trusted recipient email addresses. For each recipient, a unique cryptographic hash is created using the seed in combination with both the sender's and receiver's email addresses (hash (seed+ receiver +sender)). This hash is then merged with a rotation angle that plays a crucial role in the creation of a simulated quantum circuit through the Qiskit platform. Quantum gate RY is used to implement this rotation in the quantum state. The amplitude values obtained from the simulated state vector generates quantum entangled amplitude values for basis states that represent the entangled state corresponding to each recipient. These amplitude values are encrypted and securely stored in a file named entanglement_state.txt. To prevent residual access to the raw seed or identity data and minimize the risk of possible tampering, the original input file is deleted after processing.

The Login and Monitoring Phase as follows .

An Administration Employee must first respond to an approval message sent via WhatsApp, and this is enabled by Vonage APIs. Then, once approved, the Employee must authenticate by providing a UID and password, and these are cross- checked against the Firebase Realtime Database. Once authenticated, the system launches the SecureFirewallGUI, a custom interface that allows for real-time monitoring functionality.

The system is constantly searching for significant threat vectors, such as the insertion of USB gadgets, the use of screen capture software, and the access of cloud-synchronized folders like Dropbox or OneDrive. The system cross-verifies the e-mail address of the recipient against the pre-approved list of entangled addresses stored encrypted before permitting the transfer of data. If the e-mail address is cross-checked against an entangled identity, the transfer is permitted but with continuous monitoring. If not, the operation is refused to avoid unauthorized transfer of data—even by already authenticated users. This approach ensures that confidential information is shared with trusted, verified parties only, subjecting it to stringent communication boundaries even in an already authenticated session.

The system comprises several core components.

1) Cryptographic attributes consist of SHA-512 hashing and Fernet encryption for safe data management.
2) Quantum simulation is performed using Qiskit, circuit building through rotation gates and state vector examination.
3) System monitoring is based on Python libraries like psutil for USB insertion detection and watchdog for file monitoring.
4) Authentication is handled through Firebase Realtime Database.
5) Pre-login approval is done via WhatsApp APIs such as Vonage API.

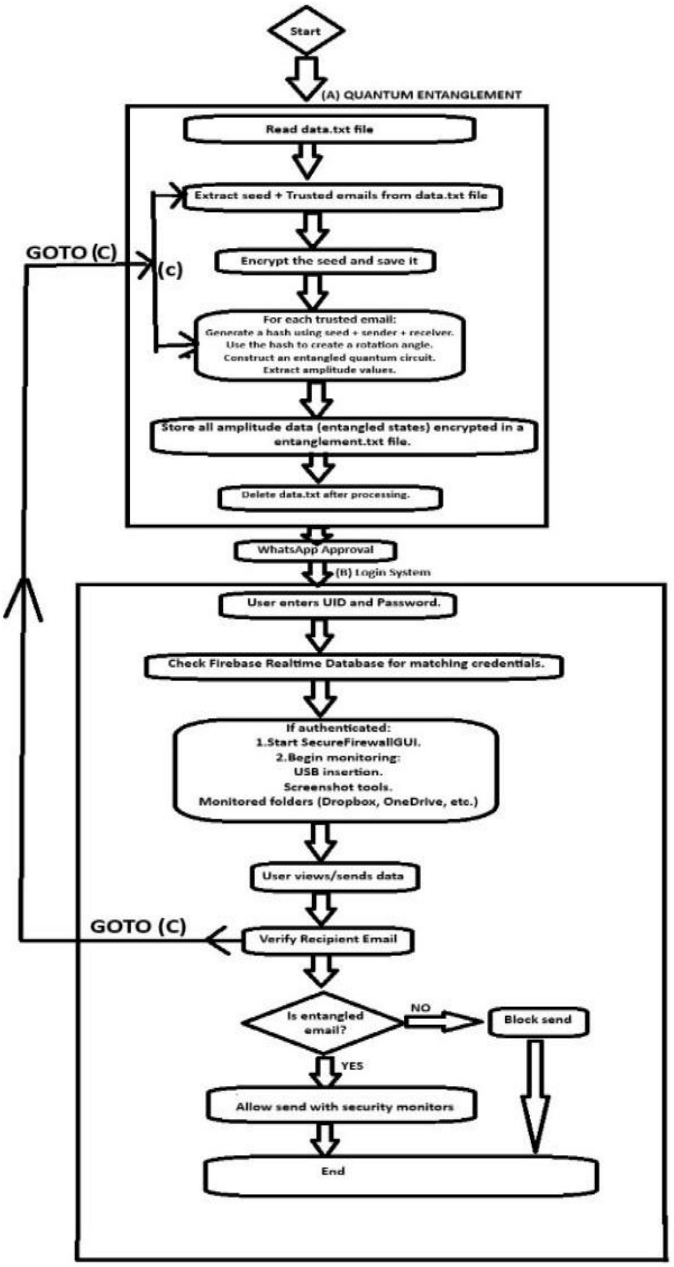


Figure 2: System Flowchart

V. Circuit design

Figure 3: Circuit diagram

The recipient verification system is based on a two-qubit quantum circuit which enables secure email authentication operations. Each (sender, recipient) pair receives unique amplitude values through entanglement combined with parameterized rotation. The initial operation of the circuit applies a Hadamard gate (H) on qubit 0 to create superposition. A Controlled-NOT (CNOT) gate creates an entanglement between the two qubits resulting in a Bell state that establishes secure quantum correlation. The rotation gate RY(θ) operates on qubit 1 to establish uniqueness. The secret seed combined with sender and recipient email is hashed through SHA-512 before converting the output hash to a 0-2π range to obtain angle θ. The method generates a consistent transformation pattern for every communication pair. The circuit execution produces complex amplitude values for basis states "00", "01", "10" and "11" which are normalized before removing imaginary components to produce quantum entangled values. After being encrypted through Fernet symmetric encryption these values get stored securely. The system generates new amplitude values during each email transmission to match them against the stored values . The system only allows transmission when the values match exactly; otherwise any small difference in sender email or recipient information results in a distinct amplitude pattern and results in a blocked operation. This quantum circuit enforces recipient-specific, cryptographically secure authentication, introducing a level of complexity that cannot be replicated by conventional methods. By grounding identity validation in deterministic, quantum-generated amplitudes, the system offers a tamper resistant, future-ready foundation for secure communications in high-risk environments.

VI. Mathematical formula

The quantum circuit under consideration involves the following operations:

1. Hadamard gate (H) on qubit 0
2. CNOT gate with control on qubit 0 and target on qubit 1
3. RY(θ) rotation on qubit 1

The initial state of the two-qubit system is:

$|\psi_0\rangle = |00\rangle$ (1)

Step 1: Apply Hadamard Gate on Qubit 0

The Hadamard gate creates a superposition on qubit 0:

$H|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ (2)

Thus, the state of the system becomes:

$|\psi_1\rangle = (1/\sqrt{2})(|00\rangle + |10\rangle)$ (3)

Step 2: Apply CNOT Gate

Applying the CNOT gate (control: q_0, target: q_1) yields:

$|\psi_2\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ (4)

This is the standard Bell state.

Step 3: Apply RY(θ) to Qubit

The RY(θ) rotation is applied to the second qubit (q_1). The matrix form is:

$RY(\theta) = [[\cos(\theta/2) \quad -\sin(\theta/2)]]$

$[[\sin(\theta/2) \quad \cos(\theta/2)]]$ (5)

Applying this to the entangled state:

$|\psi\_final\rangle = (1/\sqrt{2})(|0\rangle \otimes RY(\theta)|0\rangle + |1\rangle \otimes RY(\theta)|1\rangle)$ (6)

Substituting the matrix actions gives:

$|\psi\_final\rangle = (1/\sqrt{2})(|0\rangle \otimes [\cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle] + |1\rangle ([-\sin(\theta/2)|0\rangle + \cos(\theta/2)|1\rangle])$ (7)

Final Generalized Expression

The final quantum state can be written as:

$|\psi(\theta)\rangle = (1/\sqrt{2})(\cos(\theta/2)|00\rangle + \sin(\theta/2)|01\rangle - \sin(\theta/2)|10\rangle + \cos(\theta/2)|11\rangle)$ (8)

VII. Results

To assess the performance and reliability of the hybrid firewall, a series of simulations were conducted using the developed Python-based prototype. The primary focus is the recipient verification mechanism, which employs simulated quantum entanglement to bind authorized email addresses to specific amplitude patterns derived from quantum circuits. The amplitude states act as cryptographically deterministic values for each recipient, with endpoint monitoring providing an additional behavioral safeguard.

Metric Analysis: After giving different testcase inputs to our prototype ,metric value determined is
Mean Time to Detect(MTTD) is in the range of 100 to 200 microseconds (Illustrated in Figure4) which proves that this proposed firewall is highly secure.

```
--- Firewall Security Metrics Report ---
Timestamp: 2025-10-13 12:09:17
MTTD (Mean Time to Detect): 0.0001 sec
Total Incidents Detected: 15
Latest Threat Detected: [BLOCKED] Email not entangled. Send denied.
```

```
--- Firewall Security Metrics Report ---
Timestamp: 2025-10-12 23:17:10
MTTD (Mean Time to Detect): 0.0002 sec
Total Incidents Detected: 2
Latest Threat Detected: [BLOCKED] Email not entangled. Send denied.
```

Figure 4:

The bar graphs illustrate the quantum amplitude profiles generated for four distinct target email addresses: krishna@gmail.com,bob@gmail.com,krishnaa@gmail.com ,mailtocarol@gmail.com and sender email address : alice@trusted.com (common for all target addresses). For each address, a unique two-qubit state vector was generated using a hash function (seed + sender + receiver) to parameterize the RY gate rotation applied to a Bell-state quantum circuit, implemented via Qiskit. The resulting state vector amplitudes for computational basis states ("00", "01", "10", and "11") were extracted, normalized, and visualized.

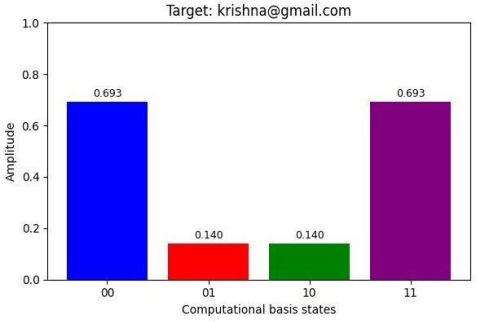


Figure 5:

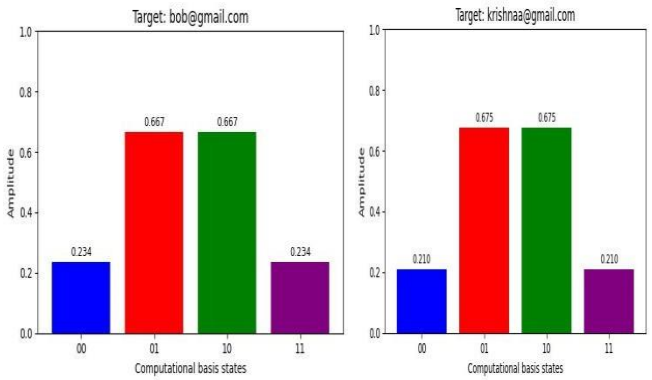


Figure 6:

Figure 7:

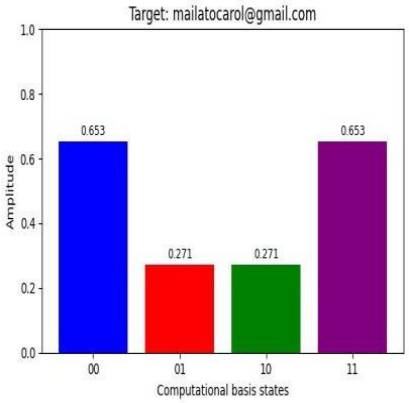


Figure 8:

[A] Distinctive Amplitude Patterns-The amplitude vectors reveal recipient-specific patterns. consider 4 graphs(Figure5,Figure 6,Figure 7,Figure 8) 1.krishna@gmail.com 2.bob@gmail.com 3.krishnaa@gmail.com and 4.mailtocarol@gmail.com

[B] Spoof-Resistance and Determinism-The firewall performs quantum amplitude recalculations through recipient input during sensitive data transmission. The email access depends on an exact match between the recipient's calculated amplitude vector and the pre-stored (entangled) profile. The system immediately blocks any typographical errors or spoofing attempts or recipients who do not match the stored profiles. The system proves its deterministic nature by performing recipient-specific verification.

[C] Endpoint Vigilance -The Python codebase keeps an ongoing watch of endpoint actions through psutil and watchdog modules which monitor USB access, screenshot tools, clipboard activities and cloud folder utilization. The system performs immediate logout or process termination upon detection of unauthorized actions to protect users from data leakage through physical or alternative channels.

[D] Comparison-The evaluation of amplitude profiles for different recipient email addresses indicates that the system exhibits excellent responsiveness to input modifications. The quantum circuit produces a distinct amplitude profile when a single character- ‘a’ in the recipient address changes from krishna@gmail.com to krishnaa@gmail.com. The bar graphs show immediate changes in amplitude patterns because peaks move between basis states so that all email addresses with minor differences generate separate non-overlapping values .All changes made to one email address appear in all amplitude profiles which guarantees recipient-specific and deterministic verification. The firewall operates through this mechanism to recognize only exact pre-approved email addresses while any form of spoofing or address alteration or typographical error will result in a mismatch that blocks data transfer. The system achieves its spoof-resistance capabilities through highly sensitive amplitude patterns that avoid redundancy making it resistant to both unintentional mistakes and malicious insider tampering profiles. The system proves its deterministic nature by performing recipient-specific verification.

Collision Resistance of SHA-512: Probability Analysis for Large-Scale Inputs

To illustrate the collision resistance of SHA-512, we use the birthday bound formula to estimate the probability that any two outputs collide when hashing 1 trillion (n = 10^ {12}) distinct inputs. SHA-512 produces 512-bit outputs, giving: M = 2^ {512}
possible hash values.
According to the birthday paradox and its approximation, the probability P of at least one collision is given by:
P(collision) ≈ 1 - e^ (-n² / (2M)) • n =
10^ {12} • M = 2^{512} ,
P(collision) ≈ 1 - e^(-(10^12)^2)/ 2 x 2^(512)) ≈
7.39x10^(-131)
This means the probability of any two different inputs colliding in their SHA-512 hash is essentially zero, even with 1 trillion inputs. Experimentally, this result ensures that each hash output for 1 trillion unique inputs will be different with overwhelming probability. Each time the system hashes a different "seed + sender + receiver" combination, the amplitude pattern—derived from the hash—will be unique. This mathematically supports and justifies the claim: for practical purposes, no two input combinations will ever produce the same fingerprint when using SHA-512 at this scale. This statistical certainty is foundational to the security of our recipient-specific verification

Table Explanation:

Table 1 proves the following mathematical explanation that the possibility of collision is in 7.39x10^(-131) , so we can also see in the table that all emails have unique values, for each email the results table will also show different values for upper and lower case letters.

Table 1: Quantum Entangled Amplitude Values for Basis States

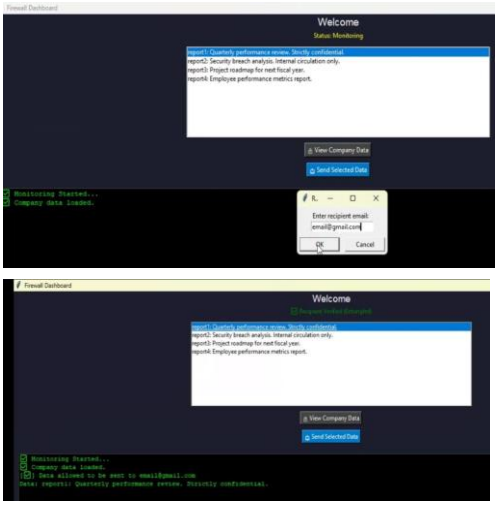
Gmail	Value 1	Value 2	Value 3	Value 4
Sid@gmail.com	0.29563	0.642342	0.642342	0.29563
sid@gmail.com	0.417874	0.570422	0.570422	0.417874
Aryan@gmail.com	0.660338	0.252892	0.252892	0.660338
aryan@gmail.com	0.700223	0.098429	0.098429	0.700223
leader@gmail.com	0.295784	0.642271	0.642271	0.295784
cr@gmail.com	0.569481	0.419156	0.419156	0.569481
heigan@gmail.com	0.044211	0.705723	0.705723	0.044211
arjun.mitra2025@gmail.com	0.255499	0.659333	0.659333	0.255499
kavya.shenoy88@gmail.com	0.013646	0.706975	0.706975	0.013646
raghavtech01@gmail.com	0.627686	0.325591	0.325591	0.627686
meera.kumarx@gmail.com	0.584553	0.397866	0.397866	0.584553
devansh.creative@gmail.com	0.276758	0.650696	0.650696	0.276758
tanishq.works09@gmail.com	0.472366	0.526184	0.526184	0.472366
neha.sundar29@gmail.com	0.369885	0.602648	0.602648	0.369885
rajdeepcoder@gmail.com	0.119829	0.696879	0.696879	0.119829
anjali.artworld@gmail.com	0.156792	0.689504	0.689504	0.156792
vivekrajvlogs@gmail.com	0.693099	0.140047	0.140047	0.693099
priyanka.writer7@gmail.com	0.669842	0.22652	0.22652	0.669842
harsh.itzone23@gmail.com	0.697947	0.113446	0.113446	0.697947
nidhi.sharmax1@gmail.com	0.112439	0.69811	0.69811	0.112439
abhinav.gamingpro@gmail.com	0.447456	0.547524	0.547524	0.447456
snehaofficial08@gmail.com	0.400207	0.582953	0.582953	0.400207
karthik.musicmail@gmail.com	0.70258	0.079882	0.079882	0.70258
isha.projects2024@gmail.com	0.429206	0.561945	0.561945	0.429206
rohit.champ001@gmail.com	0.701076	0.092153	0.092153	0.701076
diya.photogenius@gmail.com	0.633332	0.314468	0.314468	0.633332
adityaverma.creations@gmail.com	0.075591	0.703055	0.703055	0.075591
émail@gmail.com	0.173794	0.685416	0.685416	0.173794
email@gmail.com	0.669337	0.228009	0.228009	0.669337

Functional Prototype Demonstration:

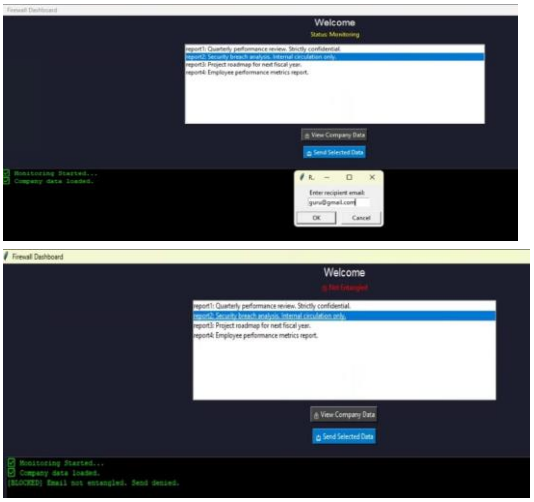
Storing of State ,Key and Seed

Figure 9:

Trusted Email Input: krishna@gmail.com



Authorised email and its output



Unauthorised email and its output

Figure 10

VIII. APPLICATIONS

General Use Applications

Where:

Telecom (Airtel, Jio), Manufacturing (Tata, Reliance), IT, Healthcare, and Government data centers.

Data Protected:

Customer information, user information, payment data, employee directories, in-office emails, project documents, and company intellectual property.

The Quantum-Inspired Insider Threat Detection and Fingerprint Firewall System prevents insider data leaks and unauthorized access, validating every transaction and blocking abnormal activities with advanced safeguards.

Environment-Related Organizations

Where:

NASA, ISRO, IPCC, Renewable Energy Enterprises, Environment Research Institutions, Meteorological Departments, and Forest Departments.

Data Protected:

Remote sensing data, user information, climate projections, sensor data, emission reports, biodiversity reports, and environmental reports.

In scientific and environmental institutions, the firewall system blocks unauthorized leaks and secures critical datasets, making sure research and operational data cannot be improperly accessed or shared

IX. CONCLUSION

The proposed simulated quantum hybrid firewall demonstrates a major breakthrough for insider threat prevention through its unified approach of quantum verification alongside real-time behavioral monitoring and human approval protocols. The system performs real-time verification of email recipients through quantum entangled amplitude values for basis states and constantly monitors endpoint activity patterns to detect suspicious behavior that traditional security systems either respond to breaches after the fact or fail to differentiate genuine user actions from malicious actions. The WhatsApp-based session approval system adds a crucial human supervision component that improves organizational responsibility while protecting against automated system misuse. The verification process demonstrates strong resistance to spoofing attacks and exact verification capabilities that protect against even the smallest unauthorized modifications. The system combines quantum simulation with behavioral analytics and multi-factor authentication to create a new scalable cybersecurity solution that protects dynamic enterprise data assets and establishes a path towards future-proof security infrastructure

X. FUTURE WORKS

A) Extending the same concept to other data leakage tools like WhatsApp, Slack, Telegram.

B) Integration of Webcam to detect mobile photo captures.

C) Dynamic modification of entangled states values (creating UI to add new emails and delete old emails).

D) Using AI technologies to integrate CCTV footage to detect any data leakage outside the system like writing sensitive data on paper.

REFERENCES

[1] A. Sharma, V. Ojha, And S.K. Lenka, "Security Of Entanglement Based Version Of BB84 Protocol For Quantum Cryptography," In IEEE International Conference On Computer Science And Information Technology (ICCSIT), IEEE, 2010.

[2] I. B. Djordjevic, "QKD-Enhanced Cybersecurity Protocols," In IEEE Photonics Journal, Vol. 13, No. 2, Pp. 1-8, April 2021.

[3] P. Ramesh, N. Saranya, Shantha Shalini K., S. Leela, Eric Howard, and Bala Sundara Ganapathy N., "Quantum Cryptography in Secure IoT Communications," in International Conference on Frontier Technologies and Solutions (ICFTS), IEEE, 2025.

[4] Sahana Dermal, Asvija Balasubramanyam, and Gudapati Naresh Raghava,"Simulation of Quantum Entanglement and Quantum Teleportation for Advanced Networks," IEEE, 2025.

[5] Vijayaraj et al., "Quasi-Deterministic Secure Quantum Communication," Journal of Quantum Information Systems, 2021.

[6] M. Zhao and T. Chen, "Comparison: QKD vs Post-Quantum Crypto," Quantum Security Review, vol. 14, no. 3, pp. 45–53, 2025.

[7] Ye and Jiang, "Quantum Dialogue Without Information Leakage," arXiv:2204.12345, 2022.

[8] Farokhi and Kim, "Measuring Quantum Info Leakage Under Detection Threat," arXiv:2402.08123, 2024.

[9] Ahmed et al., "Quantum-driven Zero Trust Framework for Insider Threats," arXiv:2501.09876, 2025.

[10] S. Wang and T. Wang, "Authenticated Email Forwarding Security," Journal of Email and Internet Security, vol. 10, no.1, pp.30–38,.2022.

[11] C. Hureau et al., "Stress Testing DMARC Policies for Phishing Protection," Cyber Defence Journal, vol. 8, no. 3, pp. 91–104, 2024.

[12] IBM Quantum, "Qiskit: An Open-source Framework for Quantum Computing," [Online]. Available: https://qiskit.org/