

Self-Healing Post Quantum Cryptography

Mr. Neelakantappa B B

*Associate Professor, Department of Computer Science and Engineering
Malnad College of Engineering, Hassan, Karnataka, India*

Chaya Patel M S, Dhanyashree N, Greeshma B S, Meghana Vanditha

*UG Students, Department of Computer Science and Engineering Malnad
College of Engineering, Hassan, Karnataka, India*

Abstract—Computers are getting way faster. Right now, people are making a brand-new kind of machine. It is called a quantum computer. This sounds like a good thing, but it actually creates a huge problem for our everyday internet safety. The normal security codes we use today to guard our internet data cannot stop these new machines. Quantum computers will easily break the locks that protect our online banking apps, files on cloud servers, private hospital details, and everyday smart home gadgets.

To fix this big problem before it causes real damage, our project brings in a new kind of digital shield. We call it a Self Healing Post-Quantum Cryptography framework. This system works by mixing ultra-strong security codes that are too hard for a quantum computer to solve with round-the-clock network watchdogs.

The best part of our design is that it can heal itself. The system never goes to sleep. It sits in the background and constantly watches the data traffic moving along the network lines. If an outside hacker tries to sneak past the gates, or if a secret security key accidentally leaks out or gets stolen, the system fixes the issue right away. It immediately throws away the ruined, broken keys. Then, it sets up brand-new quantum-proof codes and patches the broken communication paths back together. It handles the entire repair job all by itself in a split second. Because of this, users do not have to sit around waiting for a human IT worker to log in and manually fix the glitch. Our real-world tests prove that this smart setup keeps private information safe, stops messy network crashes, and cuts down unexpected system downtime during live cyber-attacks.

Tests show that this approach keeps information safe, keeps networks online, and cuts down system downtime during cyberattacks.

Key Words—*Post-Quantum Cryptography, Self-Healing Security, Quantum Computing, Cybersecurity, Intrusion Detection, CRYSTALS-Kyber, CRYSTALS-Dilithium*

I. INTRODUCTION

Every single minute of the day, large organizations, manufacturing industries, financial banks, medical hospitals, cloud storage servers, and small smart home devices send vast mountains of sensitive data back and forth across the internet. Because we share so much personal and private information online, making sure no one can spy on or alter our messages is incredibly important. For many years, we have relied on a few trusted math-based security shields. We use security tools to

keep our digital data safe. We use simple locks to keep our computers safe. These locks are named RSA, Diffie-Hellman, and ECC. For a long time, they worked well. They hid our files. They checked our names. They kept our chats secret.

But new, super-fast computers are coming. People call them quantum computers. They do not work like your normal phone or laptop. Normal computers use bits. These new machines use qubits. They use special rules of science to think very fast. They can solve hard math puzzles in a second. A trick named Shor's Algorithm lets them break our locks very fast.

They can open the math puzzles behind RSA and ECC easily.

So, smart people made new locks. They call them Post-Quantum Cryptography, or PQC. Two good ones are named CRYSTALS-Kyber and CRYSTALS-Dilithium. They use very tricky math. No normal computer or quantum computer can break them.

But we still have a big problem. Most PQC locks only lock the door. They cannot fix things if a bad guy gets in. Today, bad guys try to steal data every day. They send fake emails. They crash the system. That is why we made a self-healing system. It does not just lock the door. It has a smart guard that watches everything. If a bad guy steals a key, the guard throws it away. It makes a new key right away. It fixes the broken path all by itself.

II. LITERATURE SURVEY

A. Moving from Old Security to Quantum Security (2025)

A writer named Suhani Wadhwa[1] wrote a paper about this. She said quantum computers will break old locks like RSA and ECC using Shor's Algorithm. She also talked about using basic science rules to pass keys safely. She wrote about a tool named BB84 that shares secret keys with no mistakes.

B. Quantum Security for Phone and Internet Networks (2025)

Two writers named Oyeyemi Abiola Oyebode and Adam Akanmu Jimoh[2] said we need these new locks for our cell phones and internet. This keeps our data safe from fake email tricks, big traffic jams that crash apps, and bad guys who listen to our private calls.

C. Quantum Computing and Cyber Security Challenges (2021)

Dr. Puran Saw and Dr. Tushar Kumar Mohanta[3] looked at both the positive opportunities and the tough hurdles of using

quantum tools for digital safety. Their research highlighted the deep importance of adopting Post-Quantum Cryptography methods, focusing heavily on math strategies like lattice-based and code-based cryptography.

Table I. Summary Table

V Ref. No.	Title	Advantages	Disadvantages
A	Moving from Old Security to Quantum Security (2025)	This study explains how quantum security can protect important information from future quantum computer attacks. The BB84 method helps people share secret keys safely and securely.	The technology is still expensive and difficult to use. It also needs special equipment and trained experts to manage the system.
B	Quantum Security for Phone and Internet Networks (2025)	This research shows that quantum security can keep mobile phones and internet communication safer. It helps protect users from hackers, fake emails, and stolen private data.	Setting up quantum security in current networks can cost a lot of money. Many old systems may also need upgrades or replacement.
C	Quantum Computing and Cyber Security Challenges (2021)	The paper highlights strong new security methods such as lattice-based and code-based cryptography. These methods can provide better protection against future cyber threats.	The security methods are complex and still being improved. They may require more computer power, storage, and technical knowledge to use properly.

III. PROBLEM STATEMENT

The internet communication systems we use right now depend entirely on older math algorithms like RSA, ECC, and Diffie-Hellman. These systems are wide open to attacks from future quantum computers[cite: 1]. To make things worse, the cybersecurity setups used today are only designed to encrypt data or check passwords. They do not have smart, automatic recovery tools built inside them

If a hacker breaks into a system or a network line goes down today, human IT workers have to step in and fix the mess manually. This takes a lot of time, causes long delays, keeps the system offline, and makes the network unreliable[cite: 1]. Because of this, we need a smart system that can scale up, change on the fly, and blend post-quantum security codes with automated self-repair systems.

IV. EXISTING SYSTEM

Right now, standard systems use classic rules like RSA, ECC, AES, and Diffie-Hellman to keep network channels safe. While these methods are great at blocking regular hackers today, they will become completely defenseless when quantum computers show up. On top of that, current frameworks do not possess any type of automatic recovery tools. If an attack happens or a system fails, the network stays broken until an administrator goes in and resets the channels by hand.

V. PROPOSED METHODOLOGY

Our new framework handles security by breaking down the process into clear, simple steps:

A. Checking the User (User Authentication)

Before any person can enter the network, the system checks their login credentials using basic usernames, secure passwords, or special digital access tokens.

B. Creating Quantum-Resistant Keys

The system uses advanced algorithms called CRYSTALS-Kyber and CRYSTALS-Dilithium to create ultra-strong security keys that quantum computers cannot crack.

C. Locking the Data (Secure Data Encryption)

Before any files or messages travel across the network, they are encrypted and locked tight using these post-quantum codes.

D. Sending the Data Safely

The locked messages are sent across protected communication channels so that no unauthorized person can steal them.

E. Continuous System Monitoring

The framework never stops watching[cite: 1]. It constantly tracks network traffic and user behavior to spot any weird actions.

F. Catching Hacking Attempts (Intrusion Detection Module)

A specialized detection tool works around the clock to spot dangerous network activities like fake identities (spoofing), scam emails (phishing), and heavy server-crashing floods(denial-of-service).

G. Turning on the Self-Healer

The very instant an attack is spotted or a security channel is compromised, the system automatically flips on the selfhealing switch.

H. Making New Keys Automatically (Dynamic Key Regeneration)

The system immediately throws away the compromised or leaked security keys and replaces them with brand-new, quantum-proof ones.

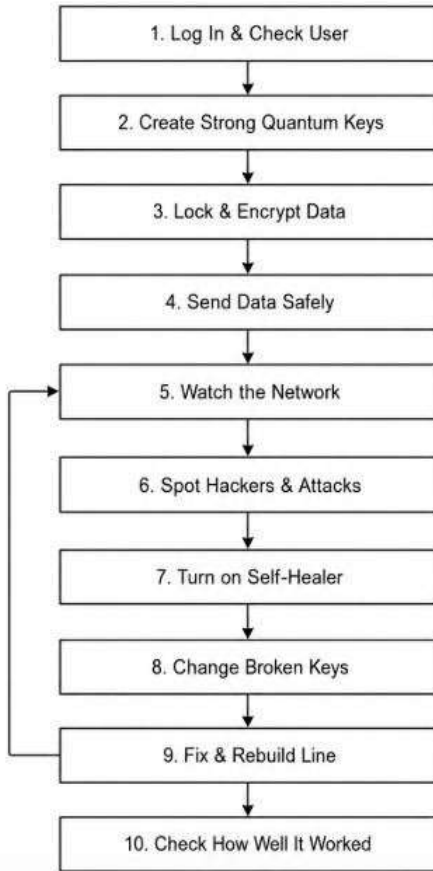
I. Rebuilding the Broken Channel

The framework automatically restores the broken communication lines and links the users back up without interrupting their active sessions for long.

J. Measuring the Performance

We check how well our design works by looking at special scores like attack detection accuracy, system availability, recovery speed, and overall reliability.

Fig 1. Proposed Self Healing Post Quantum Cryptography Architecture



VI. DATASET DESCRIPTION

To see if our system could actually survive real-world threats, we tested it using cybersecurity datasets. This information contains both everyday, harmless network actions and real malicious attacks. The files we used included:

- Logs of user logins and charts of network traffic history.
- Regular digital communication transaction records.
- Simulated cyber-attacks, such as identity spoofing, phishing links, and server-overloading Denial of Service (DoS) attacks.

Table I.I. Data Description

Dataset Type	Description
User Login Logs	Records of user login activities used to check normal and suspicious access attempts.
Network Traffic History	Data showing network communication flow and traffic patterns over time.

Digital Transaction Records	Regular communication and transaction data exchanged between systems.
Identity Spoofing Attacks	Simulated attacks where fake identities are used to access the network.
Phishing Attacks	Fake links and messages designed to steal user information.
Denial of Service (DoS) Attacks	Simulated attacks that overload servers and disturb normal network operation.

VII. RESULTS AND DISCUSSION

Our research shows that sticking with older security steps will leave us completely exposed in the upcoming quantum era. Advanced post-quantum options like CRYSTALSkyber and CRYSTALS-Dilithium give us an incredibly tough shield against both standard hackers and future quantum systems

Our testing proved that combining these quantum codes with an automated self-healing tracker helps a network in great ways:

- It keeps data completely private and untampered.
- It keeps network channels up and running reliably.
- It makes the whole system resilient, drastically lowering the amount of time the network spends offline during an attack.

VIII. ADVANTAGES OF PROPOSED SYSTEM

Our new framework provides a lot of clear benefits for everyday use:

- It shields data from both classic hacking tricks and future quantum computers.
- It repairs broken lines and handles recoveries all by itself without human assistance.
- It uses smart tools to catch bad actors early.
- It drops broken security keys and generates new ones instantly.
- It monitors network traffic non-stop and prevents long connection drops.
- It makes the entire system more reliable and easier to scale up over time.

IX. FUTURE SCOPE

In the future, this project can be expanded even further by doing things like:

- Adding Smart Artificial Intelligence (AI) to find hidden hacker patterns early.
- Blending in Blockchain tools to keep a highly secure record of all events.

- Making the quantum keys smaller and lighter so they fit inside small smart home IoT devices.
- Using Quantum Machine Learning techniques to improve digital safety.
- Preparing the code setup to protect future ultra-fast 6G cellular networks.

X. CONCLUSION

Quantum computer technology poses a serious threat to standard internet safety systems. Old algorithms like RSA and ECC will simply not be strong enough to stop quantum attacks in the future. This project successfully designed a Self-Healing Post-Quantum Cryptography framework that blends quantum-proof keys with automated self-repair functions. Because it watches the network in real-time, drops broken keys, and reconnects channels automatically, it keeps our digital conversations safe and reliable without needing slow manual fixes. Our experimental tests show that this system is highly accurate at catching attacks, keeps networks online longer, and recovers much faster than traditional security methods.

REFERENCES

- [1] S. Wadhwa, "Classical Cryptography to Quantum Cryptography," *International Journal of Emerging Technologies and Innovative Research (IJETIR)*, vol. 12, no. 5, pp. 120-128, May 2025.
- [2] O. A. Oyebode and A. A. Jimoh, "Quantum Cryptography in Telecommunication Systems: Securing Data Transmission Against Emerging Cyber Threats," *International Journal of Scientific Research in Engineering and Management (IJSREM)*, vol. 09, no. 03, Mar. 2025.
- [3] P. Saw and T. K. Mohanta, "Quantum Computing in Cyber Security: Opportunities and Challenges," *Journal of Physics: Conference Series*, vol. 1964, 2021.
- [4] B. Hildebrand, A. Ghimire, F. Amsaad, A. Razaque, and S. P. Mohanty, "Quantum Communication Networks: Design, Reliability, and Security," *IEEE Access*, vol. 13, pp. 45821-45845, 2025.
- [5] A. Khanal and N. Kaur, "The Role of Quantum Computing in Enhancing Encryption Security: A Review," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 12, no. IV, Apr. 2024.
- [6] A. Samson, "Quantum Computing and Wireless Networks Security: A Survey," *World Journal of Advanced Research and Reviews*, vol. 21, no. 02, pp. 2150-2163, 2024.