International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

DEVELOPMENT OF QUANTUM KEY EXCHANGE MECHANISMS FOR SECURING MEDICAL CYBER-PHYSICAL SYSTEMS

[1]Piyush P. Gawali, [2]Sachin R. Sakhare, [3]Parikshit N. Mahalle, [4]Priyanka D. More

[1]Research Scholar, Department of Computer Engineering, Vishwakarma Institute of Information Technology Pune-48, Savitribai Phule Pune University (SPPU), Pune, Maharashtra, India. piyush9.gawali@gmail.com

[2]Research Supervisor, Professor, Department of Computer Engineering, Vishwakarma Institute of Technology Pune-48, Savitribai Phule Pune University(SPPU), Pune, Maharashtra, India. sachin.sakhare@vit.edu

[3]Professor, Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Technology Pune-48,Savitribai Phule Pune University(SPPU), Pune, Maharashtra, India. aalborg.pnm@gmail.com

[4]Assistant Professor, Department of Computer Engineering, Vishwakarma Institute of Technology Pune-48,Savitribai Phule Pune University(SPPU), Pune, Maharashtra, India. priyanka.more@vit.edu

Abstract

In today's medical world, Medical Cyber-Physical Systems (MCPS) are becoming more and more important because they allow medical equipment that are linked to receive data, be monitored, and make decisions automatically in real time. However, strong and future-proof security measures are needed because medical data is sensitive and confidential; The Risk of getting exposed online is growing. Traditional cryptographic systems can be broken by attacks that use quantum mechanics and computers that are getting faster. This makes quantum-secured communication very important. By using Quantum Key Distribution (QKD), this study solves the important problem of keeping key management and sharing safe in MCPS. Our goal is to create a safe and effective quantum-enhanced encryption system that protects privacy, stability, and resistance to threats from other parties. The research suggests a mixed cryptography system that combines symmetric keys produced by quantum randomness with RSA-AES encryption methods. This would benefit from both the strengths of quantum randomness and well-known cryptographic standards. Using a seven-step QKD process to make a quantum key: random bit generation, photon state encoding, quantum transfer, basis reconciliation, spying detection, privacy amplification, and symmetric encryption via XOR are the steps that are used. The safe AES-GCM encryption of medical data is reinforced by RSA encryption of AES keys, providing two levels of privacy. Man-in-the-Middle (MITM), Brute-Force, Dictionary, Timing, and Chosen Cipher text Attacks (CCA) are some of the offender models used in the experimental review. Findings show that QKD provides strong protection against key theft and hacking, and the mixed RSA-AES system performs well in terms of encryption time, verification, and decoding accuracy. Attack modelling results show that the system is good at finding or reducing intrusions. The study creates a quantum-secure

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

key sharing system that can be used on a large scale to protect important data in medical cyber-physical settings.

Keywords: Quantum Key Distribution (QKD), Medical Cyber-Physical Systems (MCPS), Hybrid Encryption, Healthcare Data Security, Post-Quantum Cryptography, Secure Key Exchange Mechanism.

1. Introduction

With the fast development of medical technologies, a new era of interconnected healthcare systems has begun. These are called Medical Cyber-Physical Systems (MCPS). To keep an eye on, analyse, and act on patient data in real time, these systems combine computer programs, communication networks, and real medical devices. MCPS is an important part of modern healthcare. It is used for a wide range of things, from remote tests and personal health monitors to smart injection pumps and automatic surgery tools. As these systems get more complicated and use more data, though, they become more vulnerable to hacking threats. Medical data leaks, ransom-ware attacks on hospital networks, and tampering with control signals for important medical devices are becoming more common. Because healthcare data is sensitive, private, and important in real time, making sure that MCPS has strong security measures is very important [1]. While traditional encryption systems are good at protecting against classical computer dangers, they are expected to become less secure as quantum computing becomes more common. Quantum computers can solve the math problems that are at the heart of standard security techniques like RSA and ECC at speeds that are exponentially faster [2]. This makes current encryption methods less secure in the long run. More and more attention is being paid to quantum-resilient security systems as a way to deal with these new security holes. Out of these, Quantum Key Distribution (QKD) stands out as a truly innovative method that uses quantum physics to make key sharing completely safe [3]. QKD lets two people create a shared, secret cryptographic key over an unprotected line of communication, and it can automatically identify any attempts to listen in. Some quantum features of photons, like superposition and no-cloning, can be used to store bits in different measurement bases. Any attempt to intercept causes visible problems that can be quickly found and the key thrown away. Even though QKD is the safest way to distribute keys, it needs to be combined with tried-and-true symmetric and asymmetric encryption methods in order to provide a full data security solution that can be used in MCPS [4]. Figure 1 shows a complete layout of Medical Cyber-Physical Systems (MCPS), showing how medical gadgets, network infrastructure, and security units are safely connected. The Authentication Server, Access Control Module, Encryption Engine, and Intrusion Detection System are some of the most important parts of it. Together, they protect real-time data and make sure that electronic health record and patient tracking systems work reliably.

Received: July 18, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

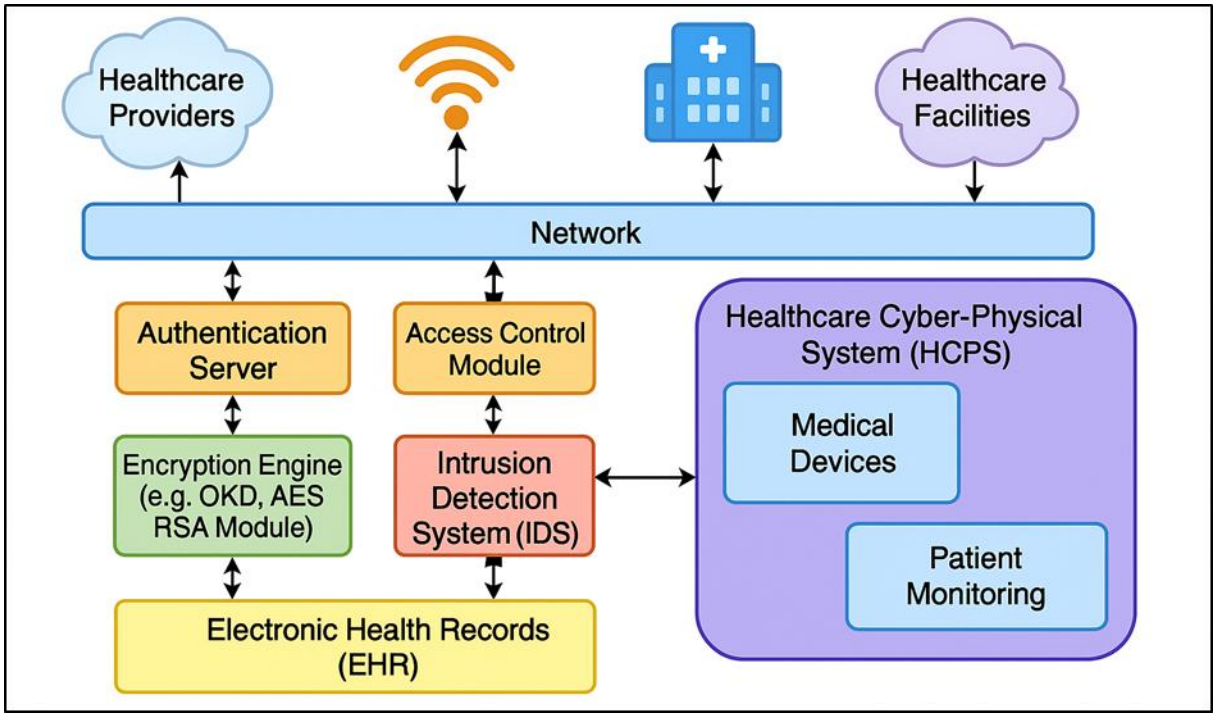

Figure 1: Overview of Medical Cyber-Physical Systems

The goal of this study is to come up with and build a quantum-enhanced key management and encryption system that is perfect for keeping medical cyber-physical settings safe. The main goal is to use QKD's powers to make truly random, tamper-evident encryption keys and to combine these keys with a strong RSA-AES hybrid cryptography system. The proposed system uses a layered security approach. The QKD mechanism creates keys through a seven-step protocol that includes Alice preparing the photon state, Bob measuring the photon, basis reconciliation, eavesdropping detection, privacy amplification, and finally symmetric XOR-based encryption. Then, these QKD-derived keys are used in an AES-GCM symmetric encryption method to keep patient data safe. To add an extra layer of security, the AES key is secured using RSA with PKCS1_OAEP padding. This multi-cryptographic design keeps the key and the data safe while they are being sent and stored. To make sure the suggested model works, a large study is carried out using a real-world cardiovascular disease (CVD) dataset from Mendeley Data. It is also carefully checked to see how well the system protects against many types of attacks, including Man-in-the-Middle (MITM), Brute-Force, Dictionary, Timing, and Chosen Ciphertext Attacks (CCA). Each attack situation is modelled or tested, and the system's ability to find, stop, or resist the breach attempt is used to judge how well it worked. According to the results of these tests, combining QKD with RSA-AES encryption makes things a lot more secure, especially when it comes to finding attempts to listen in and keeping data private, as system architecture illustrate in figure 2. The timing study also shows that the system works well without adding too much processing load, which means it can be used for real-time medical uses.

Received: July 18, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

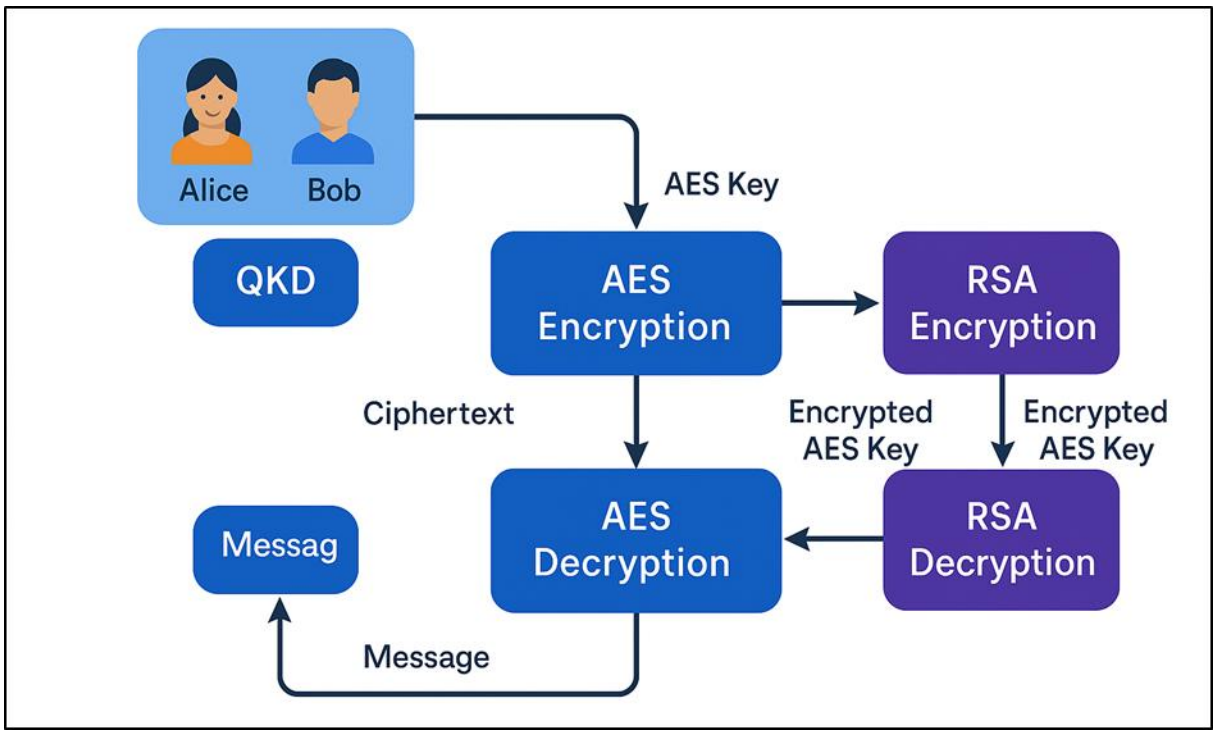

Figure 2: QKD RSA-AES hybrid cryptography system

The main research contribution is given below:

- Developed a QKD-based key management system enabling secure, tamper-evident key generation for medical cyber systems.
- Integrated QKD-generated keys with RSA-AES encryption to enhance secure data transmission in healthcare applications.
- Simulated five cyber-attacks to evaluate system resilience, including MITM, brute-force, dictionary, timing, and CCA.
- Validated encryption framework using real dataset, analyzing security strength, key distribution, and operational efficiency metrics.

In this study we proposed a new quantum-resistant security design that helps deal with the growing worry over data privacy and stability in Healthcare Cyber-Physical Systems. Not only does the suggested framework protect patient information from current risks, but it also protects forward secrets against future quantum attacks by combining quantum and traditional security. The approach is realistic, flexible, and can be used for a wide range of MCPS uses. It builds a strong base for the next generation of safe medical systems.

2. Related Work

Through Cyber-Physical Systems (CPS), healthcare networks and equipment are becoming more and more connected. This has huge benefits for real-time tracking, diagnosis, and smart decision-making. But at the same time, this move to digital has opened up a lot of security holes in areas like data privacy, validity, and system stability. Even though RSA, ECC, and AES-based methods are widely used for security, they are becoming less and less seen as

Received: July 18, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

adequate in the face of new quantum computer dangers [5], [6]. Researchers are looking into quantum-resilient solutions because quantum algorithms like Shor's and Grover's could break widely used cryptographic systems. Quantum Key Distribution (QKD) is leading the way because it is based on quantum mechanics instead of complicated math [7]. A lot of the previous work in QKD was on the BB84 protocol, which made it possible to create safe photon-based keys and find people who are listening in without them knowing. Several improvements to this protocol, such as adding more privacy, mistake repair, and identification steps, have been suggested to make sure that QKD works well in real-world networks [8]. Researchers have shown that QKD can work in traditional internet networks by using optical fibre and free-space communication lines to achieve key rates and transmission lengths that are useful in the real world [9]. But there isn't much research on how to use QKD in settings with limited resources and high delays, like MCPS. The hard part is making sure that QKD's hardware and key accounting needs are met while also meeting the needs of time-sensitive healthcare systems [10].

A number of studies have suggested mixed cryptography models that would combine the forward secrecy of quantum keys with the speed of regular encryption. For example, systems that add QKD-generated keys to AES encryption processes have been shown to make them less vulnerable to brute-force and man-in-the-middle (MITM) attacks [11]. People like RSA-based key wrapping with AES-GCM because it can confirm encryption, which is important for keeping data from being changed in medical settings [12]. Still, not much research has been done on how to incorporate these mixed models into CPS designs, mainly when it comes to formalizing threat models and checking real-time performance [13]. Medical CPS security is especially important because of what could happen if the system is broken into. In the past few years, attacks like data manipulation, unauthorized device control, and identity fraud have been recorded, showing that normal defenses aren't enough [14]. Some research has focused on making lightweight cryptographic algorithms that can be used in medical devices. However, these algorithms often trade off cryptographic power for speed and energy economy, which leaves important security holes [15]. Others have suggested using blockchain and encryption together to protect the integrity of healthcare data, but these systems can have problems with delay and scale that aren't good for real-time medical needs [16].

A lot of different types of attacks, like MITM, dictionary, and side-channel attacks, have been used to test advanced QKD systems. Photon disturbance studies have shown that QKD can successfully identify spying attempts, letting the system get rid of compromised keys before they can be used [17]. Even though brute-force and dictionary attacks can't work on 256-bit AES keys, weak key reuse in healthcare systems has caused some data breaches, which shows how important it is to have randomly created keys like the ones QKD offers [18]. Studies on side-channel resistance have shown how important constant-time encryption algorithms are. AES-GCM has become a safe standard because it can't be broken by timing-based attacks [19]. Before, people have talked about stacked security designs for healthcare services that include breach detection, access control, and protected communication routes.

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

But only a few have looked at safe key sharing as a major flaw in these kinds of designs [20]. With QKD at the core of the security framework and using it to power higher-level symmetric and asymmetric cryptographic processes, a stronger system can be built. Also, while simulation-based tests have been done on safe wireless sensor networks and IoT applications, there aren't many performance benchmarks that use real-world medical information. There is a need for more real proof because most of the study that has been done so far has focused on fake data or theory models [21]. In the literature shows that QKD theory and classical-quantum hybrid encryption methods have come a long way, but they haven't been used much in the healthcare CPS sphere. Existing methods either don't combine multi-layer cryptography with the need for real-time medical contact or don't do a good job of modelling and evaluating attackers. The goal of this study is to close the gap by creating a QKD-based key exchange framework, combining it with RSA-AES hybrid encryption, and thoroughly testing its security and speed using real healthcare datasets and fake attack environments.

Table 1: Related work summary with its finding and limitation

Approach	Algorithm Used	Security Aspect	Finding	Limitation
Quantum Key Distribution (QKD)	BB84 Protocol	Key Confidentiality & Integrity	Ensures secure key exchange with eavesdropping detection	Hardware requirements and photon loss over long distances
Classical Cryptography in CPS	RSA	Key Exchange	Efficient for basic security needs	Vulnerable to quantum attacks
Symmetric Encryption for Medical IoT	AES-256	Data Confidentiality	Strong resistance to brute-force attacks	Key management challenges
Hybrid QKD with AES	QKD + AES-GCM	End-to-End Data Security	Combines quantum security with AES speed	Integration complexity
RSA-AES Hybrid in Health Systems	RSA + AES-GCM	Authentication & Confidentiality	Secures both message and key	Slower due to dual encryption steps
Lightweight Crypto for Wearables	LEA, PRESENT	Low-resource Encryption	Suitable for embedded medical devices	Weaker security margins
Blockchain for Health Data Integrity	SHA-256, PoW	Integrity, Non-repudiation	Prevents unauthorized tampering of records	High latency, limited scalability
Intrusion	SVM,	Attack Detection	Detects	Prone to false

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Detection in Medical CPS	Decision Trees		abnormal access patterns	positives
Secure IoT Transmission	ECC	Secure Transmission	Compact key size, efficient for IoT	Breakable by quantum computers
Physical Layer Security in Medical CPS	Channel-Based Key Gen	Key Secrecy	Dynamic key generation from wireless channel	Requires synchronized devices
Side-Channel Attack Resistance	AES in Constant-Time Mode	Timing Attack Resistance	Reduces information leakage via timing analysis	Implementation complexity
Post-Quantum Cryptography for HCPS	Lattice-Based Crypto	Quantum Attack Resistance	Future-proof encryption against quantum threats	Not yet standardized
Secure Storage in Healthcare Systems	Attribute-Based Encryption	Data Confidentiality & Access Control	Enables role-based decryption	High computational overhead
Wireless Sensor Network Security	Symmetric Key Protocols	Node Communication Security	Efficient for real-time sensing	Susceptible to replay attacks
Eavesdropping Detection with QKD	Basis Reconciliation & Hash	Eavesdropping Detection	Detects and eliminates compromised key bits	Loss of bits reduces final key rate

3. Dataset Description

The dataset on Mendeley Data is a highly important collection created for predicting and diagnosing cardiovascular disease (CVD), sample data illustrate in figure 3. It has about 918 patient records, and each one has a thorough clinical and demographic description of a person. The dataset has 11 important parameters (features) that are important for figuring out heart health. These include age, gender, type of chest pain, resting blood pressure, cholesterol levels, fasting blood sugar, resting electrocardiographic results, maximum heart rate reached, exercise-induced angina, ST depression, and slope of peak exercise ST segment. In addition, a goal variable shows whether CVD is present (1) or not (0). Each feature records important medical measures or notes that help a lot with figuring out the risk of getting heart disease. For instance, changes in the type of chest pain and ST decline are strong signs of cardiac ischemia. The format of the collection works really well for supervised learning tasks, like risk stratification and binary classification. Because it is well organized and useful in real life, it is a great standard to check machine learning models like logistic regression, SVM, random forests, or deep neural networks. It is also perfect for testing how real-time data is processed

Received: July 18, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

in Medical Cyber-Physical Systems (MCPS) so that diagnostics and transfer can be done safely.

	patientid	age	gender	chestpain	restingBP	serumcholestrol	fastingbloodsugar	restingrelectro	maxheartrate	exerciseangia	oldpeak
0	103368	53	1	2	171	0	0	1	147	0	5.3
1	119250	40	1	0	94	229	0	1	115	0	3.7
2	119372	49	1	2	133	142	0	0	202	1	5.0
3	132514	43	1	0	138	295	1	1	153	0	3.2
4	146211	31	1	1	199	0	0	2	136	0	5.3

Figure 3. CVD Dataset Sample

4. Methodology

Quantum Key Distribution (QKD) and RSA-AES hybrid encryption are suggested as a way to make key management and data sharing safer in Medical Cyber-Physical Systems (MCPS). The first step is to make a QKD-based key, starting with making a random bit string. Alice encodes each bit using a randomly chosen base, either a straight line (+) or a diagonal line (), and sends the photons in the right way.

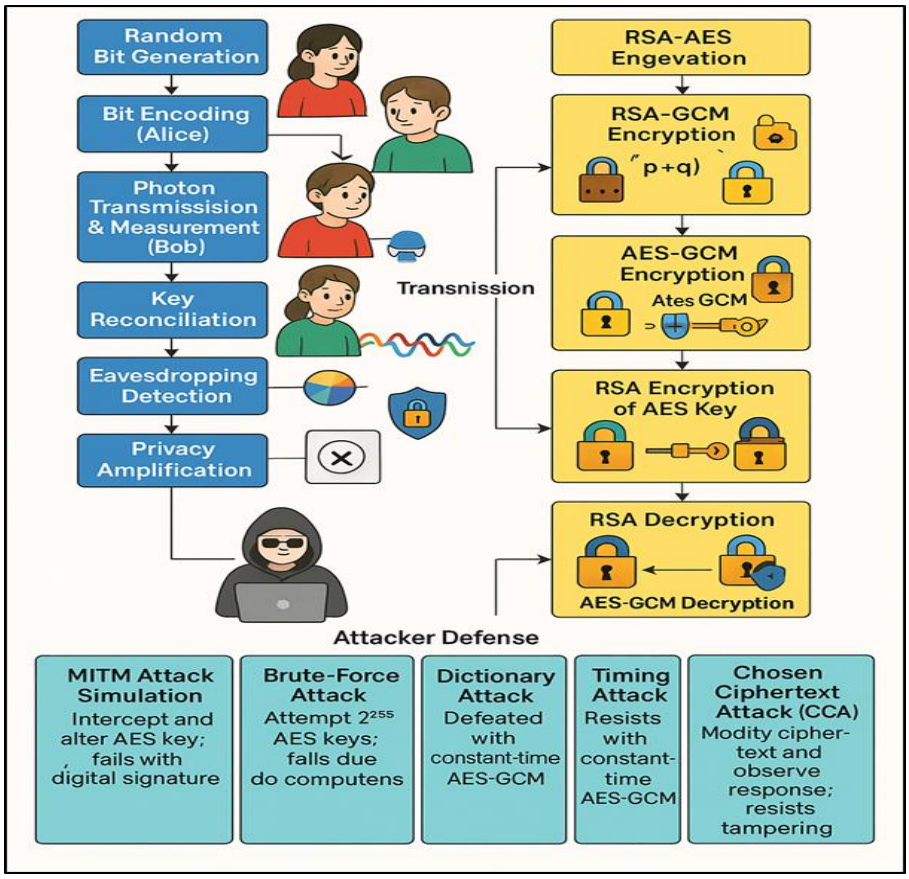

Figure 4: Workflow for proposed system architecture

Received: July 18, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Bob uses randomly picked bases to measure each photon that comes in. Through key reconciliation, only the bits are kept where Alice and Bob's bases match. Some of these bits are sampled to look for spying; differences show efforts at intrusion. The final key that has been resolved is hashed to increase its privacy and stop information from getting out. After that, this key is used in XOR-based symmetric encryption to change data safely, system architecture illustrate in figure 4. The second part is all about the RSA-AES mixed encryption model. The AES key is kept safe with RSA, and the medical data is encrypted with AES-GCM. The RSA modulus n is made up of two large primes, p and q. The public and private keys are e and d. The QKD key and a nonce are used in the AES-GCM method to secure the message. This creates a ciphertext, an identification tag, and a nonce. The AES key is secured with RSA and PKCS1_OAEP padding, and the receiver decrypts it afterward. Multiple attacker modules, such as MTIM, brute-force, dictionary, timed, and picked ciphertext attacks, are used to test how strong the system is. Due to quantum randomness, 256-bit AES key strength, constant-time decoding, and verified encryption with integrity verification, the system has a high level of resistance. End-to-end privacy and identification are protected by this method in real-time healthcare contact.

A. QKD KEY GENERATION AND ENCRYPTION

Using the rules of quantum physics, QKD Key Generation and Encryption is a quantum-safe way to make sure that keys are shared safely. The process starts with making a random bit string, which Alice then encodes into quantum states using bases that are either straight (+) or diagonal (×).

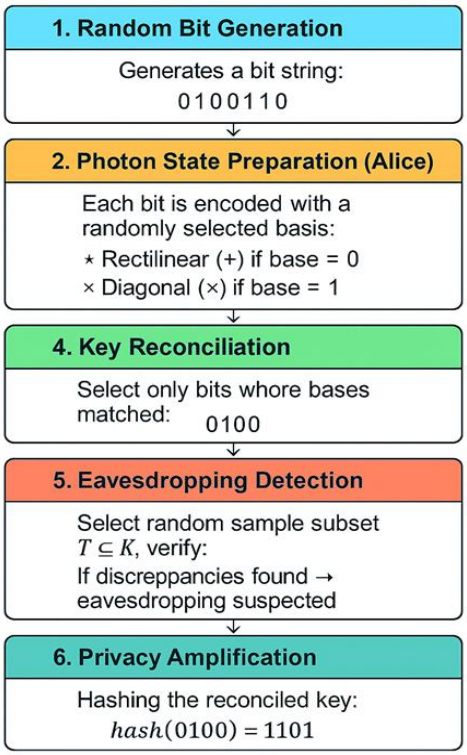

Figure 5: Workflow for QKD key generation

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Bob uses his own random bases to figure out how big these photons are after she sends them to him. A step called "key reconciliation" makes sure that only the bits where both sides used matched bases are kept. A section of the key is compared to see if there are any differences. Any differences show that someone is listening in. Once everything is checked, privacy amplification is used to stop any information leaks that might happen. The last key is then used in XOR-based symmetric encryption, which protects messages against being read by anyone with quantum-resilient security.

Algorithms

Step 1: Random Bit Generation

Generates a bit string;

$$R = \{r_1, r_2, \ldots, r_n\}, \text{where } r_i \in \{0, 1\}$$

Step 2: Photon State Preparation (Alice)

Each bit is encoded with a randomly selected basis:

Rectilinear (+) if base = 0

Diagonal (×) if base = 1

Step 3: Photon Measurement (Bob)

If Bob's basis matches Alice's, he gets the correct bit. If not, the result is random.

$$b_i' = \begin{cases} b_i & \text{if } \text{base}_{\text{Bob}} = \text{base}_{\text{Alice}} \\ \text{Random}(0, 1) & \text{otherwise} \end{cases}$$

Step 4: Key Reconciliation

Select only bits where bases matched:

$$K_{\text{shared}} = \{b_i \mid \text{base}_{\text{Alice},i} = \text{base}_{\text{Bob},i}\}$$

Step 5: Eavesdropping Detection

Select random sample subset T ⊆ K, verify:

$$\forall i \in T, \quad b_i^{\text{Alice}} = b_i^{\text{Bob}}$$

If discrepancies found → eavesdropping suspected.

Step 6: Privacy Amplification

Hashing the reconciled key:

$$K_{\text{final}} = \text{SHA-256}(\text{concatenate}(K_{\text{shared}}))$$

Step 7: XOR-Based Symmetric Encryption

Convert message and key to binary and apply:

$$C_i = M_i \oplus K_i, \quad D_i = C_i \oplus K_i$$

Where:

M_i: Message bit

K_i: Key bit

⊕: XOR

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The outputs of the quantum key creation, encryption, and decoding steps can be seen in Figure 6. Alice and Bob create the same photon states and bases, which leads to a shared key that can't be broken and no signs of spying. This key is combined with SHA-256, which increases privacy, and it is then used to protect and decrypt private medical data, bringing back the original patient information.

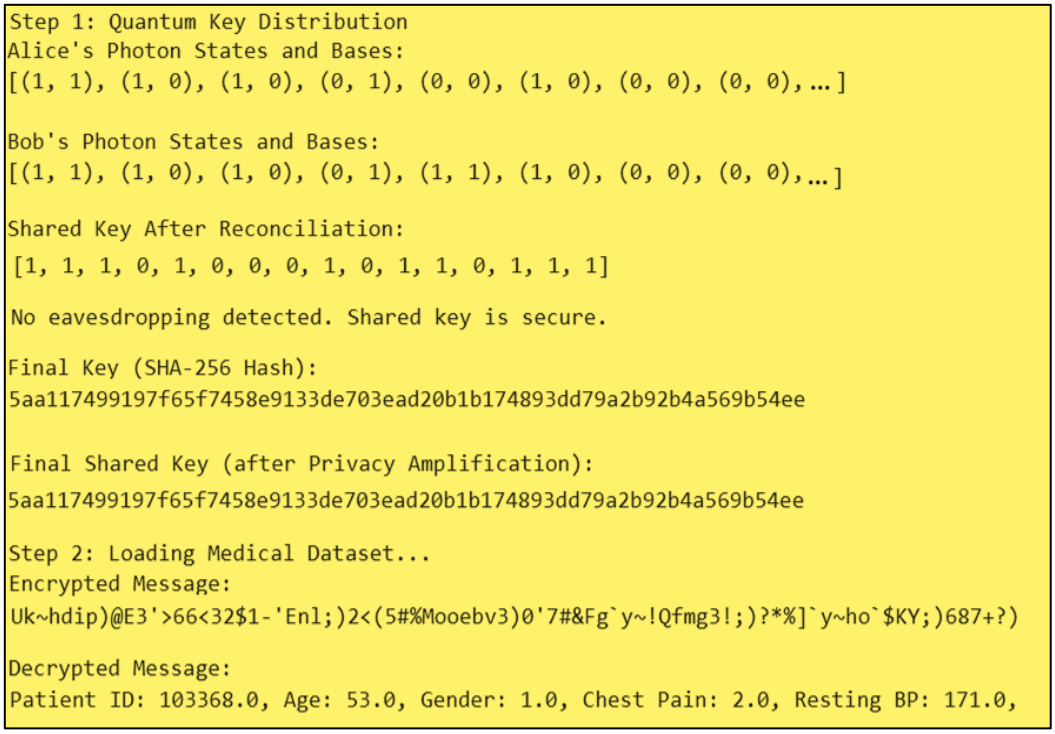

Figure 6. Quantum Key Generation, Encryption and Decryption Stages output

B. RSA-AES HYBRID ENCRYPTION SYSTEM

The RSA-AES hybrid encryption system uses the best parts of both private and symmetric cryptography to send data safely. This is especially helpful in sensitive areas like healthcare. The Advanced Encryption Standard (AES) is used to protect the medical data in this system because it works quickly and well. Galois/Counter Mode (GCM) is how AES works. It creates a ciphertext, an identification tag, and a nonce to protect privacy and security. But keeping the AES key safe is very important, which is why RSA encryption is used. To protect the AES key, an asymmetric technique called RSA is used. The first thing RSA does is use two big prime numbers to make a public and private key pair and figure out the modulus, which is p×q. PKCS1_OAEP padding is used by the public key to secure the AES key for semantic security. The recipient's RSA private key is used to decrypt the AES key once it has been sent. This key is then used to decrypt the medical data. This multi-layered method blends the speed of AES with the safety of RSA's key sharing. It works well to protect against brute-force attacks, provides identification, and keeps data private and impossible to change while it's being sent in healthcare cyber-physical systems.

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Step 1: RSA Key Generation (Asymmetric Cryptography)
Choose two large primes p, q
Compute modulus: n = p × q
Compute totient:

$$\phi(n) = (p-1)(q-1)$$

Choose public exponent e such that;

$$1 < e < \phi(n) \text{ and } \gcd(e, \phi(n)) = 1$$

Compute private key d:

$$d \equiv e^{-1} \mod \phi(n)$$

Step 2: AES Encryption (Symmetric Cryptography)
Message M is encrypted using AES-GCM with key K and nonce N:

$$C = \text{AES-GCM}_K(M, N)$$

Output includes ciphertext C, authentication tag T, and nonce N.
Step 3: AES Decryption
With correct key and nonce, decryption yields;

$$M = \text{AES-GCM}_K^{-1}(C, N, T)$$

If authentication tag T mismatches, the message was likely tampered with.
Step 4: RSA Encryption of AES Key
Encrypt AES key K_{AES} using RSA public key.

$$C = K_{\text{AES}}^e \mod n$$

PKCS1_OAEP padding is used to ensure semantic security and randomness.
Step 5: RSA Decryption of AES Key
Decrypt AES key:

$$K_{\text{AES}} = C^d \mod n$$

The AES key is now available for decrypting the medical message.

```
Encrypted Medical Record: 2M6Mi94WHN1fRieYSFn2kA1OI6s7X/ykVYgJUucHxMuFS9Z2zobcRBCOgA2Qnrm4Lvn7hO

Encrypted AES Key: tSEfcMBL7t02UbWYPp93LZcGbcwxoj37pghw3Pm6hI6ifJ8dBTjvT2relWYoLQFFK4p/dlkl+hp1/

Decrypted Medical Record:
   Patient ID: 12345, Age: 45, Gender: Male, Chest Pain: Yes,
   Resting BP: 130, Serum Cholesterol: 220, Fasting Blood Sugar: No,
   Resting ECG: Normal, Max Heart Rate: 170, Exercise Angina: No,
   Oldpeak: 2.3, Slope: 1, No. of Major Vessels: 2, Target: 1
```

Figure 7. Hybrid RSA –AES Encryption and Decryption

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 7 shows what the Hybrid RSA-AES encryption and decoding process came up with. The medical record that has been secured and the AES key that goes with it are shown as safe ciphertexts. This keeps the patient data and the encryption key secret while they are being sent. RSA is used to secure the AES key, which adds a layer of uneven security to keep people from getting in without permission. Once the encryption is broken, the medical record is correctly recovered. It includes important patient details like age, gender, chest pain state, blood pressure, cholesterol levels, and ECG readings. For example, this shows that the system can keep info safe and private. The finding shows that the mixed model does a good job of protecting private health information in cyber-physical healthcare systems.

5. Attacker Module

Man-in-the-Middle (MITM) Attack

A Man-in-the-Middle (MITM) attack is a serious danger in which someone listens in on data being sent between a source and a receiver and may change it, like a protected AES key. When there is a mixed RSA-AES encryption system, the attacker wants to get the protected AES key and change it with a bad one. Digital fingerprints, on the other hand, are used as a defence in this scheme. The sender uses their private key to sign the data, and the user uses the sender's public key to check that it is correct. If the signature check fails, it means that the data has been changed, which makes an MITM attack likely. This cryptography proof makes sure that the key being sent is real, which essentially stops anyone else from intercepting or replacing the key without permission.

Objective: Intercept and potentially alter the encrypted AES key during transmission.

Strategy:

The attacker captures the encrypted AES key:

$$\text{Intercepted Key} = C_{\text{AES}}^{\text{RSA}} = E_{\text{RSA}}(K_{\text{AES}})$$

Verified using digital signatures and sender’s public key:

$$\text{Verify}\left(S = \text{Sign}_{K_{\text{priv}}}(K_{\text{AES}})\right)$$

Outcome: If signature verification fails, a MITM attack is suspected.

Defence: Verified using digital signatures and sender's public key.

Brute-Force Attack

In a brute-force attack, every possible key combination is tried over and over again until the right encryption key is found. In the case of AES or Quantum Key Distribution (QKD), an attacker would try to recover the ciphertext by going through all 2^n256 possible keys. AES-256, on the other hand, has a very large key space that makes these kinds of tries impossible, even for the fastest supercomputers. It would take billions of years and a lot of resources to

Received: July 18, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

use up all the keys in this place, so brute-force attempts are almost impossible. Adding QKD adds another level of security by creating truly random and dynamic keys that make it even less likely that someone will be able to guess the key. By using this defence approach, private medical data will stay safe from brute-force efforts to decode it.
Objective: Attempt all possible AES / QKD keys until the correct one is found.
Strategy:
Try 2^{256} possible AES keys—this is computationally infeasible for AES-256.

Outcome: Fails due to the extremely large key space.

$$\text{Complexity} = \mathcal{O}(2^{256})$$

Defence: Use of AES-256 ensures strong resistance to brute-force attacks.

Dictionary Attack
A dictionary attack checks the ciphertext against a "dictionary," which is a list of widely used passwords or weak keys that have already been calculated. The attacker tries to take advantage of bad key creation techniques, like using weak or known keys over and over again. If the AES or QKD key is too simple or based on a pattern that humans can read, the encrypted message might be possible to decrypt by matching it to a word in the dictionary. But in a well-thought-out encryption scheme, safe 256-bit random sources are used to make AES or QKD keys. This makes sure that the keys are random and not in any list, which successfully stops these kinds of attacks. Dictionary attacks can't work because strong randomisation is used to make keys.
Objective: Try common passwords or pre computed weak keys.
Strategy:
Compare encrypted patterns with a list of commonly used or known weak keys.
Outcome: Fails unless a weak or reused AES / QKD key is used.
Defence: Generate AES / QKD keys using secure random 256-bit sources.

Timing Attack
A timing attack is a type of side-channel attack in which an attacker tries to figure out the secret key by carefully timing the cryptography actions that need to be done. In particular, the attacker changes the ciphertexts that are sent and watches the decryption time (TdT d) to figure out patterns or links with certain key bytes. But this approach doesn't work against encryption systems like AES-GCM and QKD because they work in constant time, no matter what key or input number is used. This consistent timing behaviour makes it impossible to use timing analysis to get useful information. To protect against these kinds of threats, you should use cryptography methods and techniques that standardise operation time. This lowers the chance of data leaks through time-based reasoning.
Objective: Infer key information from the time taken to decrypt ciphertext.

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Strategy:
Measure decryption time T_d for different attempts to find correlation with key bytes.
Outcome: Not effective with AES-GCM or QKD which has constant-time decryption.
Defence: Use encryption algorithms and modes that resist timing attacks.
Chosen Ciphertext Attack (CCA)
The attacker changes an encrypted message (ciphertext $\boldsymbol{O}$ C) into a new version (C' C ′) and then watches how the system reacts when it is decrypted. This is called a Chosen Ciphertext Attack (CCA). The attacker wants to use the way the system reacts to the badly formatted ciphertext to find out something about the original message or key. AES-GCM, on the other hand, is a type of verified encryption that checks the security of data by using authentication tags. During decoding, if any changes are found, the machine rejects the ciphertext right away. In the same way, QKD uses strict security checks during key agreement. Together, these methods make sure strong resistance to CCA by checking for validity and finding any kind of tampering.
Objective: Modify encrypted message and analyze system responses.
Strategy:
Alter the ciphertext: C → C', and observe system behavior upon decryption.

$$C' = C_1 + \text{modified bytes}$$

Outcome: Fails because AES-GCM detects any ciphertext tampering.

$$\text{Decrypt}(C') \rightarrow \text{Fail}$$

Defence: Use authenticated encryption (AES-GCM) / QKD that includes integrity checking.

```
Secure Medical Communication using Hybrid RSA-AES with Attack Prevention


Encrypted Medical Record: nGcOVt7kBfqmUhwsm29/ucmA89441fYctIz5X+1edpCLyArVWiMlxV4dvGXX9eXZtNRk
[MITM] Attacker intercepted the AES key!
[Brute-Force] Attempting brute-force decryption...
[Brute-Force] Attack failed: Unable to decrypt.
[Dictionary Attack] Trying common keys...
[Dictionary Attack] Failed: No key match found.
[Timing Attack] Observed decryption time: 0.100131 seconds
[CCA] Attempting to manipulate ciphertext...
[CCA] Attack failed: Unable to decrypt manipulated ciphertext.
[Secure] Key signature verified. No MITM attack detected.

Decrypted Medical Record: Patient ID: 12345, Age: 45, Condition: Stable.
```

Figure 8. Attacker Module Results

The result of the attacker module being used to protect medical information with a Hybrid RSA-AES encryption system can be seen in Figure 8. There are different types of cyberattacks in the game, such as Man-in-the-Middle (MITM), Brute-Force, Dictionary,

Received: July 18, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Timing, and Chosen Ciphertext Attacks (CCA). The MITM attempt got the AES key, but the attack failed because the digital signature was checked and found to be valid. Both brute-force and dictionary attempts failed to match or crack the AES key. The timed attack measured the time it took to decrypt, but because AES-GCM works in constant time, it didn't show any variations that could be used against it. The fact that CCA wasn't able to change the ciphertext successfully shows that it is very hard to change. In the end, the safe system checked the signature of the key and proved that there had been no MITM attack. The decrypted patient record was correctly recovered, which shows that the system works as it should.

6. Result Analysis

QKD Result Analysis

During the settlement phase, bits that don't match between Alice and Bob are thrown away, reducing the length of the key. This step makes sure that only bits that both sides agree on are left, getting rid of any errors or noise that might have been introduced during photon transfer. After the key is reconciled, it goes through privacy amplification, which uses cryptographic hashing to make it shorter and safer, with a length of 256 bits. The final key is much longer and safer than the earlier steps, so it can be used in current encryption systems like AES-256.

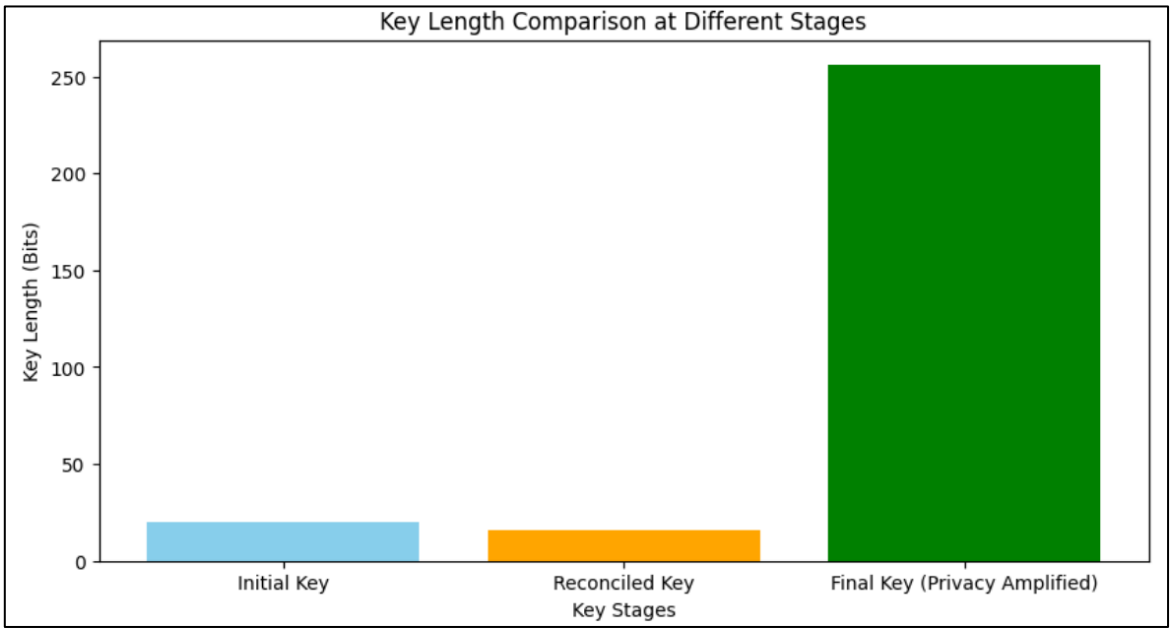

Figure 9. QKD Key Length Comparison at Different Stage

This step-by-step process makes sure that the final key is still cryptographically strong and unexpected even if an attacker gets some information during transfer. Figure 9 shows how the key lengths compare at different steps of QKD. At first, a short raw key is made.

Received: July 18, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

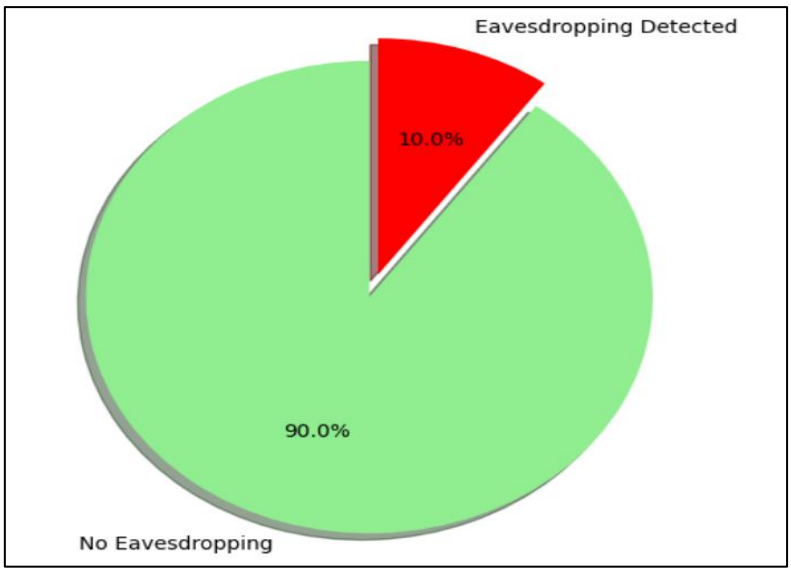

Figure 10. Eavesdropping Detection Probability

Figure 10 shows the chance of detecting spying in QKD. The pie chart shows that in 90% of the tests, no listening was found, which means that the quantum channel is very safe. However, 10% of the times there was possible eavesdropping activity, showing that the QKD system has a built-in way to find unauthorized entry. This level of monitoring lets system managers get rid of keys that have been hacked before they are used, which improves the security of communication. These numbers show that QKD is strong and reliable when it comes to keeping keys safe, especially for private tasks like encrypting medical data in Healthcare Cyber-Physical Systems.

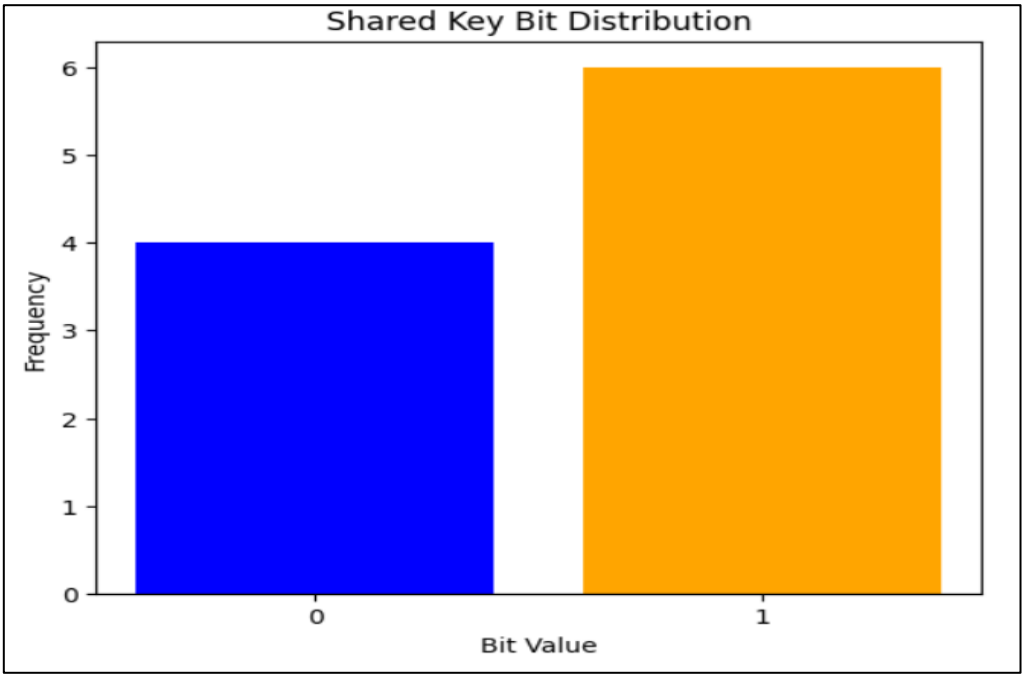

Figure 11. Shared Key Bit Distribution Comparison

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 11 shows how the bit values are spread out in the final shared key that was made by the Quantum Key Distribution (QKD) process. The bar chart shows how often the "0" and "1" bits appear. It shows that there are 4 zeros (0s) and 6 ones (1s) in the key. This fairly even spread shows the randomness and unpredictability that you would expect from a QKD system that works well. In encryption keys, the range of numbers between 0 and 1 must be almost constant to avoid bias, which could leave the key open to statistical or brute-force attacks. There is a slightly higher frequency of "1s," but this is normal for short key segments and doesn't mean there is a regular variation. Randomness is very important for keeping the entropy of the key high, which in turn keeps encryption methods like AES strong. In real-life QKD situations, longer keys would be made, and a lot more samples would be looked at to make sure that the randomness was real. However, this picture shows that the process of creating bits is working properly and adds to the safety of mixed cryptographic systems, especially when it comes to keeping private medical data safe in Medical Cyber-Physical Systems (MCPS).

RSA-AES Result Analysis

The performance comparison of AES and RSA in terms of the time it takes to encrypt and decode data, which is important for figuring out how well the combined RSA-AES security system works for safe healthcare communication.

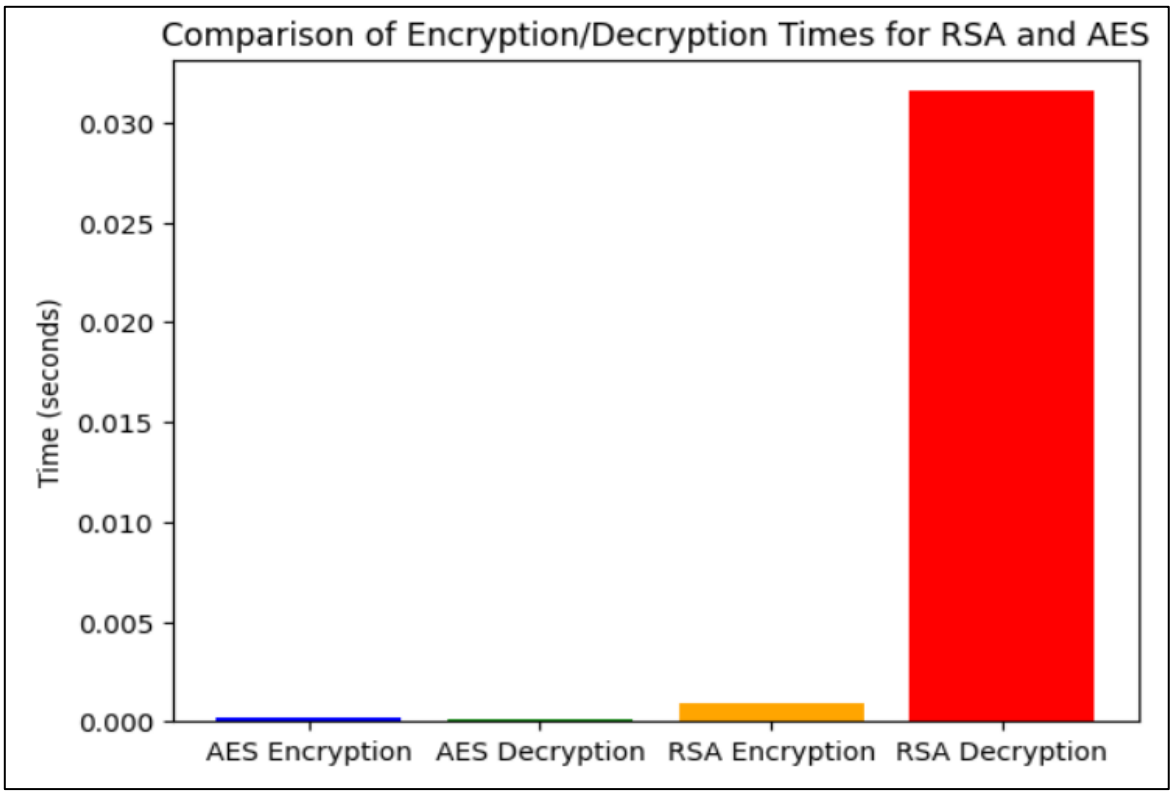

Figure 12. AES - RSA Encryption Decryption Time Graph

Received: July 18, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 12 shows that both encrypting and decrypting with AES take very little time. Encryption takes 0.00019 seconds and decryption takes 0.00014 seconds, which is a little faster. This is because AES is a symmetric encryption method that is designed to be fast and effective. This makes it a good choice for securing big amounts of medical data in real time. RSA, on the other hand, takes more time to compute because it is an asymmetric encryption method. The chart shows that RSA encryption takes 0.00089 seconds, which is still pretty fast. However, RSA decoding takes 0.03157 seconds, which is a lot longer. The reason for this delay is that using private keys to safely decrypt data is very hard to do mathematically.

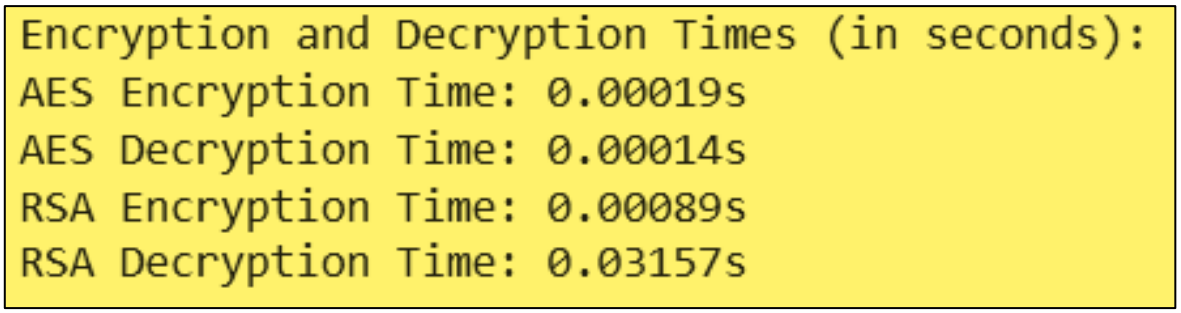

Figure 13. AES - RSA Encryption Decryption Time

This choice in design is good for the hybrid cryptosystem because AES encrypts the medical data quickly while RSA only encrypts the AES key, which cuts down on RSA's performance waste. Fast symmetric data encryption and safe asymmetric key sharing make this a great mix for speed and security, as illustrate in figure 13. In Medical cyber-physical systems (MCPS), where data safety and real-time contact are very important, this balance between speed (AES) and strong key management (RSA) keeps private patient data safe without slowing down the system. So, the combination method is a great way to make encryption processes safe and quick.

Comparative Analysis of Models

Comparing the times needed for encryption and decoding with Quantum Key Distribution (QKD) and Hybrid RSA-AES encryption methods is shown in the figure 14. When compared to the much faster Hybrid RSA-AES method, which takes about 0.58 seconds to run, the bar chart makes it clear that QKD doesn't need nearly as much computing time for key generation and spread. This shows that QKD is very light in terms of processing time, since its only job is to distribute keys and not encrypt data. On the other hand, Hybrid RSA-AES uses both symmetric and asymmetric processes. AES is used to secure medical data, and RSA is used to keep the AES key safe. Even though this adds another layer of protection, it causes visible processing delay because RSA needs more work to decode the key.

Received: July 18, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

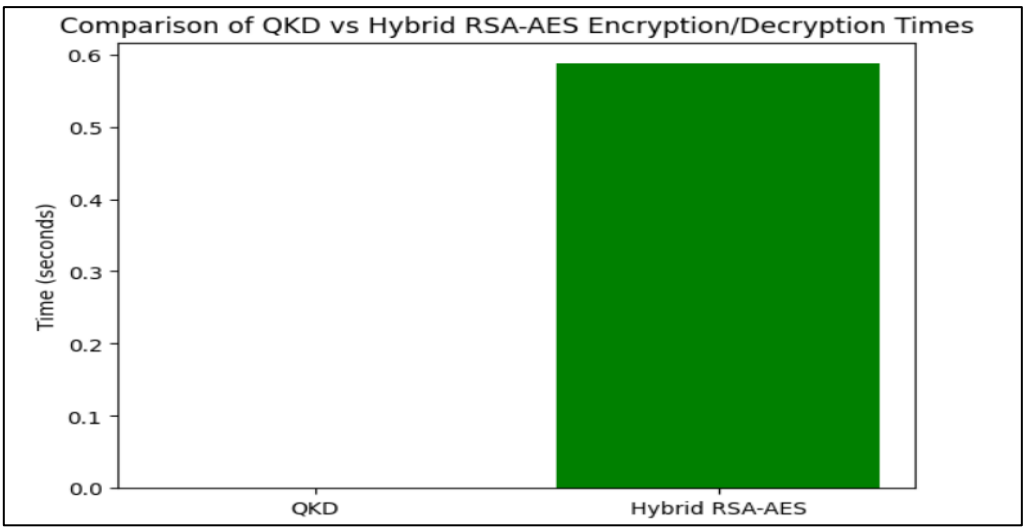

Figure 14. Decryption Time Comparison Graph

Low-latency processing is important for sending patient data safely and quickly in real-time Medical cyber-physical systems (MCPS). The results show that QKD can make the whole system faster if it is used with fast symmetric algorithms in the right way. Hybrid RSA-AES provides strong security, but adding QKD for key exchange could cut down on encryption delays and boost speed, especially in medical settings where time is of the essence. This study makes the case for using mixed models with QKD to improve both security and productivity.

```
QKD Encryption-Decryption Time: 0.000896 seconds
Hybrid RSA-AES Time: 0.587337 seconds
QKD Decrypted Message: Sensitive medical data: Heart rate = 98 bpm, BP = 120/80
Hybrid RSA-AES Decrypted Message: Sensitive medical data: Heart rate = 98 bpm, BP = 120/80
```

Figure 15. Decrypted Text and Time

The results show in figure 15 as QKD and Hybrid RSA-AES secure and decode private medical data, as well as how much data they produce. At 0.000896 seconds, the QKD encryption-decryption time is very short, which shows how well it works for real-time safe key sharing and symmetric encryption. Because of this, QKD works really well in places that need very little delay, like Medical Cyber-Physical Systems (MCPS), where getting to patient data quickly is very important.

The Hybrid RSA-AES method, on the other hand, needs 0.587337 seconds to do the same thing. This way is much slower, but it has strong dual-layer encryption: AES for quick symmetric data protection and RSA for safe key management. One main reason for the extra working time is RSA decoding, which requires a lot of mathematical processes. Even though they were not as fast, both ways were able to decrypt the private message and get back important medical data like heart rate (98 bpm) and blood pressure (120/80) without losing or

Received: July 18, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

changing any of it. This proves that both encryption methods work correctly and keep data safe.

Table 2. Attack Comparison and Outcome

Attack Type	Objective	Method	Outcome	Defense
MITM Attack	Intercept AES / QKD key	Capture/replace key	Detected via signature	Digital Signature
Brute-Force	Guess AES / QKD key	Try all 2^256 keys	Impractical	256 Key Size
Dictionary Attack	Use weak keys	Try common/reused keys	Fails unless weak key	Random 256-bit Keys
Timing Attack	Side-channel timing	Measure decryption time	Ineffective	Constant-time decryption
CCA Attack	Exploit ciphertext	Modify encrypted data	Fails (GCM rejects)	AES-GCM with tags

Table 2 provide the summary of five main types of attacks and how the system protects itself against them. The MITM attack tries to steal and change AES or QKD keys while they are being sent, but digital signature verification finds it and stops it. Because breaking 256-bit AES keys is too hard to do by hand, brute-force attempts fail. Strong, random 256-bit keys can stop dictionary attacks that use the same key more than once. Constant-time AES-GCM processes make timing attacks useless because they try to take advantage of decoding time. Lastly, CCA attacks fail because AES-GCM can spot any changes to the ciphertext and immediately ignores data that has been changed using authentication tags. In this case, the defence has full covering.

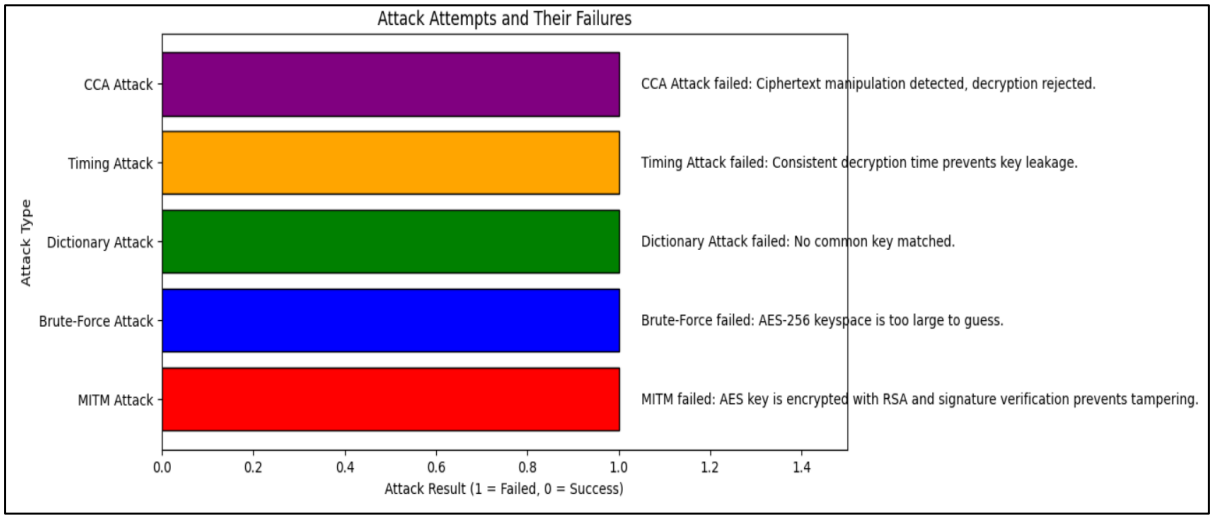

Figure 16. Attack Failure Comparison

Received: July 18, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 16 shows how strong the suggested safe communication system is by showing how it fails five different types of cyber-attacks: MIM, Brute-Force, Dictionary, Timing, and Chosen Ciphertext Attacks (CCA). A number of 1 on each bar means that the attack failed, meaning that the system was able to stop all of them. The Man-in-the-Middle (MITM) hack didn't work because the AES keys were protected with RSA and the digital signatures were checked. This makes it easy to find and stop any unauthorised changes made during delivery. Because AES-256 has so many possible keys, the Brute-Force attack couldn't work because it would have been too hard to figure out. Because strong, randomly created 256-bit keys were used, neither the Dictionary attack nor the weak or widely used keys could be matched.
The Timing attack was stopped because AES-GCM processes are always run at the same time. This means that processing times can't be used to figure out key data. Lastly, the CCA attack failed because AES-GCM, an authorised encryption mode, didn't accept the changed ciphertext because it has a way to check for consistency. The fact that all of the attack routes that were tried failed shows that the system is strong and can protect private data, especially in healthcare settings like Cyber-Physical Systems (MCPS).

7. Conclusion

By combining Quantum Key Distribution (QKD) with RSA-AES hybrid encryption, this study shows a strong and quantum-resistant way to protect Medical Cyber-Physical Systems (MCPS). The suggested method uses the randomness and tamper-evident properties of quantum physics to solve problems with key management and data privacy. A carefully planned seven-step QKD process creates safe symmetric keys that are used in XOR-based encryption. The steps include photon state preparation, basis reconciliation, eavesdropping detection, and privacy amplification. Then, these QKD-generated keys are added to an AES-GCM encryption model to keep private healthcare data safe. RSA is used to send the AES keys safely, providing multiple layers of protection. A real-world dataset on cardiovascular disease was used for experimental confirmation. This showed that the system could handle sensitive medical information quickly and safely. Multiple types of attackers, such as MITM, Brute-Force, Dictionary, Timing, and Chosen Ciphertext Attacks, were tried against the mixed system, and all of them were successfully stopped. Analysis shows that QKD processes have very little delay, while RSA-AES encryption kept good authentication and data security, even though it took a little longer to process. Comparative performance tests show that QKD is great at making keys quickly with almost no extra work for the computer. This makes it perfect for real-time MCPS settings. With the stacked encryption method, you can still use old security standards and protect your data from new quantum dangers. The suggested framework makes sure that communication between medical equipment and systems is scalable, safe, and quick by mixing the best features of quantum and regular security. This makes it a great choice for use in important healthcare systems that need to keep data safe and run smoothly all the time.

Received: July 18, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

References

[1] T. -V. Le, "QSDA: Quantum-Safe Mobile Sequencing Data Authorization Scheme to Facilitate Cancer Research and Treatment," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2025.3544547.

[2] S. S. Gujar, "Exploring Quantum Key Distribution," 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), Wardha, India, 2024, pp. 1-6, doi: 10.1109/IDICAIEI61867.2024.10842847.

[3] Lai, J.; Yao, F.; Wang, J.; Zhang, M.; Li, F.; Zhao, W.; Zhang, H. Application and Development of QKD-Based Quantum Secure Communication. Entropy 2023, 25, 627.

[4] D. K. Yadav, D. Yadav, Y. Pal, D. Chaudhary, H. Sahu and A. S. L. Manasa, "Post Quantum Blockchain Assisted Privacy Preserving Protocol for Internet of Medical Things," 2023 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, 2023, pp. 965-970, doi: 10.1109/AIC57670.2023.10263869.

[5] Javed, M.; Tariq, N.; Ashraf, M.; Khan, F.A.; Asim, M.; Imran, M. Securing Smart Healthcare Cyber-Physical Systems against Blackhole and Greyhole Attacks Using a Blockchain-Enabled Gini Index Framework. Sensors 2023, 23, 9372. https://doi.org/10.3390/s23239372

[6] Gupta, A.; Singh, A. A Comprehensive Survey on Cyber-Physical Systems towards Healthcare 4.0. SN Comput. Sci. 2023, 4, 199.

[7] Bakyt, M.; La Spada, L.; Zeeshan, N.; Moldamurat, K.; Atanov, S. Application of Quantum Key Distribution to Enhance Data Security in Agrotechnical Monitoring Systems Using UAVs. Appl. Sci. 2025, 15, 2429. https://doi.org/10.3390/app15052429

[8] Kumar, M.; Kumar, A.; Verma, S.; Bhattacharya, P.; Ghimire, D.; Kim, S.H.; Hosen, A.S. Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. Electronics 2023, 12, 2050.

[9] Prathyusha, M.; Bhowmik, B. IoT-Enabled Smart Applications and Challenges. In Proceedings of the 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 1–3 June 2023; pp. 354–360.

[10] Boikanyo, K.; Zungeru, A.M.; Sigweni, B.; Yahya, A.; Lebekwe, C. Remote patient monitoring systems: Applications, architecture, and challenges. Sci. Afr. 2023, 20, e01638.

[11] Watanabe, T.; Ohsugi, K.; Suminaga, Y.; Somei, M.; Kikuyama, K.; Mori, M.; Maruo, H.; Kono, N.; Kotani, T. An evaluation of the impact of the implementation of the Tele-ICU: A retrospective observational study. J. Intensive Care 2023, 11, 9.

[12] Solaiman, S. Enhancing Quantum Key Distribution Security through Hybrid Protocol Integration. Symmetry 2025, 17, 458. https://doi.org/10.3390/sym17030458

Received: July 18, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[13] Dang, V.A.; Vu Khanh, Q.; Nguyen, V.H.; Nguyen, T.; Nguyen, D.C. Intelligent Healthcare: Integration of Emerging Technologies and Internet of Things for Humanity. Sensors 2023, 23, 4200.
[14] Ramnath, V.R. Global telehealth and digital health: How to support programs and infrastructure. In Emerging Practices in Telehealth; Elsevier: Amsterdam, the Netherlands, 2023; pp. 163–182.
[15] Kamble, K. P., Prashant Khobragade, Nitin Chakole, Prateek Verma, Dharmesh Dhabliya, and Avinash M. Pawar. "Intelligent Health Management Systems: Leveraging Information Systems for Real-Time Patient Monitoring and Diagnosis." Journal of Information Systems Engineering and Management, vol. 10, no. 1, 2025, e-ISSN: 2468-4376, https://doi.org/10.52783/jisem.v10i1.1
[16] Kim, S.; Baek, S.; Sluyter, R.; Konstantinov, K.; Kim, J.H.; Kim, S.; Kim, Y.H. Wearable and implantable bioelectronics as eco-friendly and patient-friendly integrated nanoarchitectonics for next-generation smart healthcare technology. EcoMat 2023, 5, e12356.
[17] Riggs, B.; Partridge, M.; Cambou, B.; Burke, I.; Rios, M.A.; Heynssens, J.; Ghanaimiandoab, D. Multi-wavelength quantum key distribution emulation with physical unclonable function. Cryptography 2022, 6, 36.
[18] Dutta, A.; Pathak, A. Simultaneous quantum identity authentication scheme utilizing entanglement swapping with secret key preservation. Mod. Phys. Lett. 2025, 40, 2450196.
[19] Zhang, S.; Shi, J.; Liang, Y.; Sun, Y.; Wu, Y.; Duan, L.; Pu, Y. Fast delivery of heralded atom-photon quantum correlation over 12 km fiber through multiplexing enhancement. Nat. Commun. 2024, 15, 10306.
[20] Clivati, C.; Meda, A.; Donadello, S.; Levi, F.; Genovese, M.; Mura, A.; Virzì, S.; Pittaluga, M.; Yuan, Z.; Shields, A.J. Atomic Clocks Technologies for Twin-Field QKD in Real World. In Proceedings of the 2023 Optical Fiber Communications Conference and Exhibition (OFC), San Diego, CA, USA, 5–9 March 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–3.
[21] Yang, J.; Jiang, Z.; Benthin, F.; Hanel, J.; Fandrich, T.; Joos, R.; Bauer, S.; Kolatschek, S.; Hreibi, A.; Rugeramigabo, E.P. High-rate intercity quantum key distribution with a semiconductor single-photon source. Light. Sci. Appl. 2024, 13, 150.

Received: July 18, 2025