Integration of Quantum Key Distribution Protocol with AES Encryption for Enhancing Security in IoT Networks

MYAT SU WIN[1], KHAING KHAING WAI[2]
[1]*Faculty of Computer Systems and Technologies, University of Computer Studies, Mandalay, Myanmar*
[2]*Department of Information Technology Support & Maintenance, University of Computer Studies, Yangon, Myanmar*

Abstract- ***The advancement of contemporary technology is driving increased technological capabilities, while applications related to the Internet of Things (IoT) continue to grow. The integration of IoT into daily routines enhances convenience and comfort. Furthermore, technology can contribute to a moderate decrease in the dependency on human labor. Nonetheless, as data transmission occurs over the Internet, ensuring robust security measures is paramount. Traditional cryptographic methods were employed to guarantee the security of data transmission. In contemporary times, cryptography relies heavily on mathematical principles; thus, if a key can be discerned through the use of advanced computing power, it may pose a security vulnerability. In contrast, quantum cryptography is founded on the principles of physics, rendering the key difficult to disclose. Moreover, any attempts to uncover it can be detected. Consequently, this paper integrates both conventional and quantum cryptography. In traditional cryptography, the Advanced Encryption Standard (AES) is employed, whereas in quantum cryptography, the B92 Quantum Key Distribution Protocol is utilized.***

Index Terms— IoT, MAX30100, NodeMCU ESP8266, AES, QKD

I. INTRODUCTION

The paramount aspect of communication conducted over the Internet is the security of information. Devices within the Internet of Things (IoT) have progressed into integrated systems and sensors capable of connecting, gathering, and transmitting data via the Internet. Cryptology encompasses both the creation of secure communication methods (cryptography) and the analysis of these methods to identify vulnerabilities (cryptanalysis). These schemes play a crucial role in establishing the foundational principles of security in communications, ensuring services such as confidentiality, integrity, and authenticity [1].

Cryptography is the discipline dedicated to safeguarding information through the processes of encryption and decryption, which utilize a key. The act of encryption transforms information from a comprehensible format into an incomprehensible one. The original message, before encryption, is referred to as plaintext, whereas the altered data resulting from encryption is known as ciphertext. The plaintext can be retrieved from the ciphertext through a decryption process that also employs a key. The method that facilitates both encryption and decryption is termed a cipher [2]. It is impossible to ensure that key exchanges are entirely secure. To address this issue, quantum mechanics offers a method for ensuring secure key distribution.

Quantum Cryptography is founded on the principles of physics, specifically the laws of quantum mechanics. This emerging technology highlights the phenomena associated with quantum physics, enabling two parties to engage in secure communication that is underpinned by the unchanging nature of quantum mechanical laws. It facilitates the generation of a key with unique properties, which can be utilized for secure exchanges between the involved parties [3].

II. HARDWARE AND TECHNIQUES

Sensors serve as hardware components that identify biological, chemical, and physical signals,

subsequently providing these signals as recorded or measured parameters. The advancement of microchip technologies has significantly broadened the range of medical applications for sensors.

A. Pulse Oximeter and Heart Rate Sensor

The MAX30100 module operates as a pulse oximeter and heart rate sensor, specifically engineered to assess pulse rate in beats per minute (BPM) and blood oxygen concentration (SpO2) expressed as a percentage. The photodetector assesses the light that is reflected. The MAX30100 sensor interprets the absorption levels to ascertain the concentration of blood oxygen (SPO2) [4]. This concentration is computed by analyzing the ratio of infrared and red light detected by the photodetector as illustrated in Fig. 1.

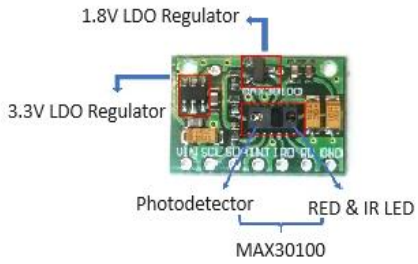


Fig. 1. MAX30100 Pulse Oximeter Sensor

The following equation is used for oxygen saturation:

$$SpO_2\ (\%) = \frac{HbO_2}{HbO_2+Hb} \times 100 \qquad (1)$$

B. NodeMCU ESP8266

The Nodemcu, referred to as the Node MicroController Unit, represents a development platform that integrates open-source software and hardware, focusing on an economical System-on-a-Chip (SoC) illustrated in Fig.2. This compact and affordable microcontroller features Wi-Fi functionality, enabling direct connections to sensors via I2C, GPIO, and various other interfaces [5].

Fig. 2. Nodemcu ESP8266

C. Quantum Key Distribution Protocol (B92)

In 1992, Bennett and Brassard presented the B92 protocol, which serves as a more straightforward alternative to the BB84 protocol. Unlike the BB84 protocol, the B92 protocol utilizes only two measurement bases: +45° and -45°.

In the BB84 protocol, Alice transmits multiple photons that carry bits selected at random, while Bob also randomly chooses a basis for measuring these bits. If Bob selects an incorrect basis, no measurement occurs. Alice communicated through a quantum channel, using photons to convey bit information. To signify a bit value of '1', she used a vertical basis with a polarization of 45°, whereas for a bit value of '0', she employed a horizontal basis with a polarization of 0° [6].

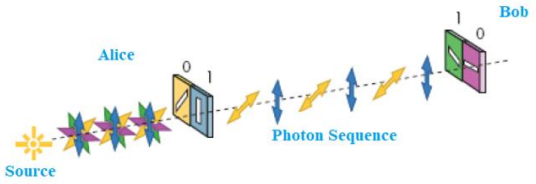


Fig. 3. Example of B92 protocol key exchange

D. Advanced Encryption Standard (AES-128) with Round-Reduced

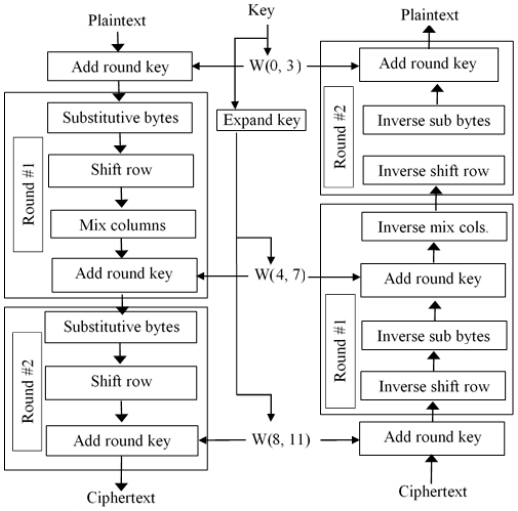


Fig. 4. Block Diagram for Round-Reduced AES-128 Encryption and Decryption

AES is a symmetric key encryption technology that operates as a block cipher. The secret key length utilized in AES can be 128, 192, or 256 bits. The encryption process involves four fundamental functions—SubByte, ShiftRow, MixColumn, and

AddRoundKey— performed sequentially for Nr-1 iterations, creating a loop called a round. The total number of iterations in this loop (Nr) varies based on the key size, with possible values of 14, 12, or 10. The proposed system reduces the number of rounds necessary for encryption and decryption from ten to merely two rounds, as illustrated in Fig. 4.

E. Hybrid of QKD Protocol B92 and AES Encryption Process

The procedure illustrated in Fig. 5 outlines the method by which Alice transmits a confidential message to Bob, employing B92 and AES encryption techniques. This procedure is comprised of three distinct stages. Initially, Alice generates a classical binary key utilizing a Quantum Random Number Generator. Subsequently, she conveys the key to Bob through the B92 protocol. In the final step, Alice encrypts the confidential message with AES before sending it to Bob.

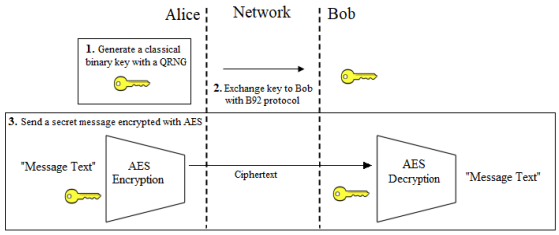


Fig. 5. Sending a Secret Message to Bob with B92 and AES encryption

F. Quantum Key Distribution Process

Fig.6 illustrates the Quantum Key Distribution process, which consists of six steps for Alice and Bob utilizing the B92 protocol. In the initial step, Alice produces a classical bit using a Quantum Random Number Generator (QRNG), resulting in a bit value of '1'. In the subsequent step, both Alice and Bob generate a classical bit with a QRNG to determine the basis. Following this, in step three, Alice prepares a qubit that is conditioned on both the bit value and the basis. Finally, in step four, she transmits the qubit to Bob.

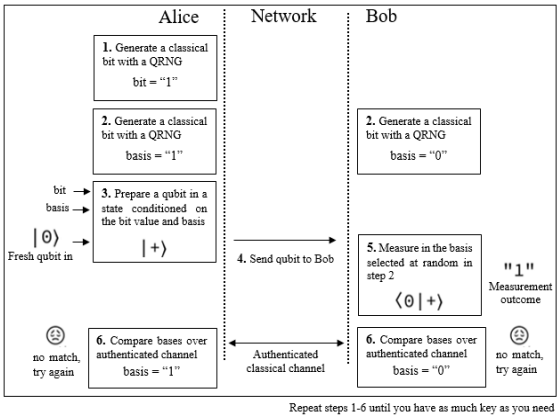


Fig. 6. Timing Diagram for the B92 Protocol

In step 5, Bob measures the basis that was randomly chosen in step 2, resulting in a measurement outcome of "1." In the final step, Alice and Bob compare their bases through authenticated channels. Alice's basis is "1," while Bob's basis is "0." Since their bases do not align, they discard this attempt and will repeat steps 1 to 6 until they achieve the desired key length [7].

III. IMPLEMENTATION

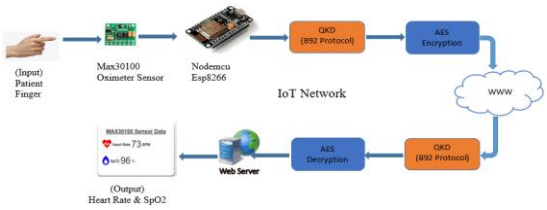
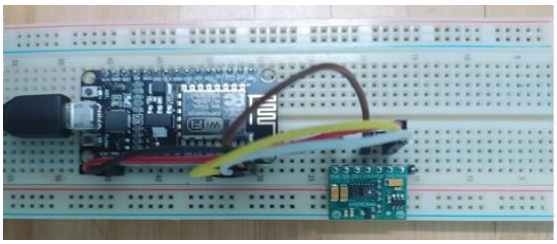


Fig. **7**. IoT network Architecture

Fig.7 is divided into two primary sections. The upper section represents the sending side, while the lower section denotes the receiving side. On the sending side, data input is obtained from the finger, and the NodeMCU processes the information from the sensor. Prior to transmitting the data to the internet, Quantum Key Distribution (QKD) generates a secret key, which is subsequently employed to encrypt the data using a classical encryption technique. The encrypted data is then transmitted over the internet. On the receiving side, the same secret key is utilized to decrypt the data before it is forwarded to the server. Ultimately, the server displays the original sensor data, including heart rate and oxygen levels.



D0 ---- INT (Brown) VIN ----- 3.3V (Red)
D1 ---- SCL (White) GND ---- GND (Black)
D2 ---- SDA (Yellow)

Fig. 8. Interfacing between MAX30100 and Nodemcu ESP8266

Fig.8. illustrates the linkage between the MAX30100 sensor and the NodeMCU ESP8266 module. Fig.9 illustrates the implementation of the system. Additionally, the figure depicts the data connection and transmission among the three components of the IoT system, which include the Sensor Module, IoT Module and Server.

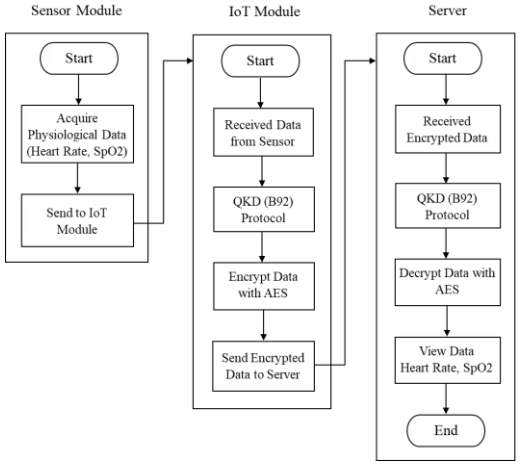


Fig. 9. System Implementation Flowchart

Within the IoT Module, collect physiological data, including heart rate and oxygen saturation, from an individual's fingertip and relay it to the IoT module. In the IoT module, access raw physiological data from sensors via a suitable interface, such as I2C or 1-Wire. Analyze and convert the collected data into quantitative metrics, including heart rate and blood oxygen saturation levels. Ensure data security by implementing the Quantum Key Distribution (QKD) and the Advanced Encryption Standard (AES) algorithm with a 128-bit encryption key. Establish a connection to the server database through Wi-Fi. Transmit the encrypted data to the server. Upon receipt of the encrypted data on the server side, utilize the Quantum key and AES algorithm to decrypt the sensor information and display the results on the web server.

IV. EXPERIMENTAL RESULT

This experiment was designed to evaluate the effectiveness and security of transmitting sensor data over the internet by comparing two distinct approaches: one that utilized Quantum Key Distribution (QKD) and Advanced Encryption Standard (AES) encryption, and another that did not employ these advanced security measures.

A. Without QKD and AES Encryption

No encryption method is applied when sending sensor data; sensor data is sent as plaintext, and anyone can easily read it using one of the networking tools. Sensor serve as hardware components that identify biological, chemical, and physical signals, subsequently providing these signals as recorded or measured parameters.

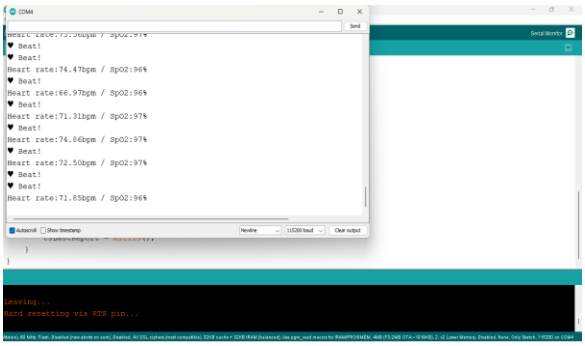


Fig.10. MAX30100 pulse oximeter sensor data output from NodeMCU ESP8266

The information generated by the MAX30100 Pulse Oximeter Sensor, which is linked to the NodeMCU ESP8266, is presented on the Serial Monitor, as illustrated in Fig.10. This output comprises the Heart Rate measured in Beats per Minute and the Oxygen saturation level expressed as a percentage.

VIN ----- 3.3V (Red)
GND ---- GND (Black)

D0 ---- INT (Brown)
D1 ---- SCL (White)
D2 ---- SDA (Yellow)

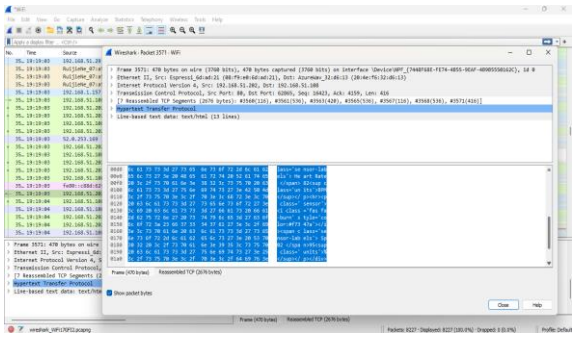


Fig.11. Packet analyzed with Wireshark

Fig.11. illustrates the network traffic analyzed while transmitting data to a web server via Wireshark. In the absence of encryption, the data is transmitted in "plaintext," making it readily accessible for examination with a packet analyzer.

B. With QKD and AES Encryption

The sensor data is protected during transmission over the Internet by employing the hybrid of Quantum Key Distribution (QKD) and Advanced Encryption Standard (AES) technique. Testing results are shown in the following Fig.12.

```
Received data: BPM = 74.01490784, SpO2 = 96
Encrypted BPM: dcc55fd19a9106728f6de7a7857e42ef
Encrypted SpO2:
6abc7e34d0e3e8b39a067353ffbe482e7128480eec85811b5cd8a701
39032 2405378ce2caf964a7b546c24e0bfed372d
Decrypted data: {'BPM': 74.01490784, 'SpO2': 96}
Send status: 200

Received data: BPM = 72.93245697, SpO2 = 96
Encrypted BPM: 92c640ffe01612f89ad1a3d9e390edcb
Encrypted SpO2:
db4d05e35082baec7adf07686af5609cf2dc01680108b869a2de56f27
6d88 f3d6c43075e6b069b5dd03e10a3388c0443
Decrypted data: {'BPM': 72.93245697, 'SpO2': 96}
Send status: 200
```

Fig. 12. Test Results of the QKD and AES

V. PERFORMANCE EVALUATION

Cybercrimes that target Internet of Things (IoT) devices, referred to as IoT attacks, take advantage of vulnerabilities such as insufficient security protocols, outdated firmware, and poor system architecture. Notable examples of these attacks include Device Spoofing, Man-in-the-Middle attacks, Distributed Denial of Service (DDoS) attacks, Eavesdropping attacks, and Password Cracking attacks, among others. The proposed system aims to assess the Quantum Bit Error Rate (QBER) for the B92 protocol in scenarios both with and without the presence of an attacker.

A. None Attack Scenario

In the absence of any attack, the performance of the system is measured as shown in Fig.13. It is observed that the encryption and decryption times are minimal, with varying levels of QBER due to random noise in the QKD system.

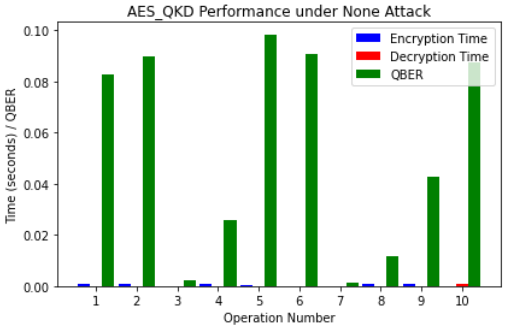


Fig.13. Performance of AES-QKD under None Attack

B. Throughput

Throughput was evaluated based on the amount of data encrypted and decrypted over time. The standard AES-128 algorithm demonstrated the highest throughput due to its rapid encryption and decryption cycles: The hybrid AES-QKD system, though slower in throughput compared to AES alone, still performed well. The key exchange process slightly reduced throughput, but the fewer AES rounds in decryption offset some of the performance loss as shown in Fig.14.

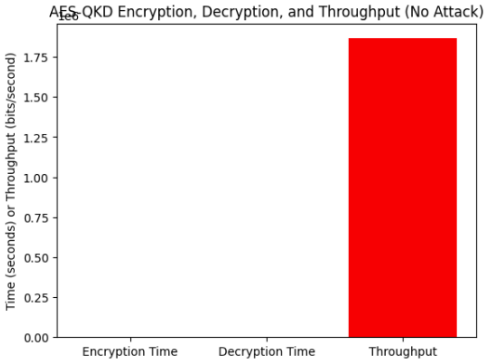


Fig. 14. AES-QKD Throughput with no Attack

C. Eavesdropping Attack Scenario

In the eavesdropping attack, although the encryption and decryption times remained unaffected, the QBER was found to fluctuate as a result of intercepted and altered data during transmission. This type of attack is detectable due to quantum properties.

The QBER in this scenario is critical. A significant QBER increase would suggest that the eavesdropping attempt is detected, making this a key security indicator shown in Fig.15.

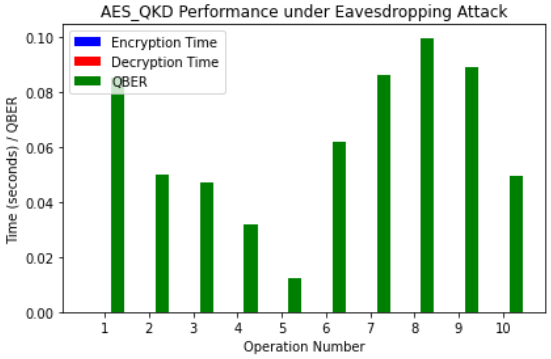


Fig.15. Performance of AES-QKD under Eavesdropping Attack

D. Throughput

Throughput decreased more significantly in the presence of attacks due to the overhead introduced by both QKD and the error handling processes required to manage attacks. Despite the added security, the system's ability to handle large-scale, high-speed applications was more constrained as shown in Fig.16.

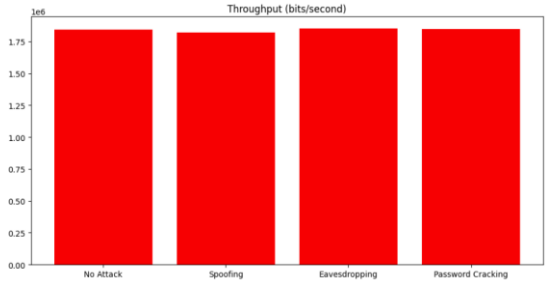


Fig.16. Performance of AES-QKD under various Attacks

The experiments demonstrate that the AES-QKD system effectively handles encryption and decryption while detecting eavesdropping attack through QBER. The system's efficiency in secure scenario and its ability to detect and respond to attacks underscore its robustness in protecting IoT data. The results indicate that the AES_QKD system performs efficiently under normal operating conditions and is resilient to Eavesdropping attacks.

CONCLUSION

The Internet of Things (IoT) represents a fascinating development in wireless communication, facilitating the connection, gathering, and transfer of data via the Internet. Protecting information within this framework is of utmost importance. To ensure security, a comprehensive security mechanism is established that encompasses the IoT device, the IoT gateway, and the remote Internet server, thereby ensuring the secure transmission of sensitive sensor data. The transfer of this sensor data over the Internet will be protected through the implementation of the Quantum Key Distribution protocol B92, along with a streamlined version of AES encryption.

REFERENCES

[1] Clark, J. A. (2001). Metaheuristic Search as a Cryptological Tool. Ph.D dissertation. University of York, December 2001.

[2] Muhammad Reza Z'aba, Mohd Aizaini Maarof, a Survey on the Cryptanalysis of the Advanced Encryption Standard, Proceedings of the Postgraduate Annual Research Seminar 2006.

[3] M. I. Khan and M. Sher, "Protocols for secure quantum transmission: a review of recent developments," Pakistan Journal of Information and Technology, vol. 2, pp. 265-276, 2003.

[4] https://iotprojectsideas.com/max30100-pulse-oximeter

[5] Nodemcu, "Nodemcu documentation," 2021, https:// nodemcu.readthedocs.io/IEEE Trans. Antennas Propagate., to be published.

[6] J. –Y Wang et al., "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution", Nature Photon. 7 (5), 387{393 (2013).

[7] Sarah Kaiser, "Learn Quantum Computing with Python and Q#", A Hands-on approach.