TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 22, No. 6, December 2024, pp. 1491~1501
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v22i6.26450

An integration of quantum systems using BB84 for enhanced security in aeroponic smart farming

Christy Atika Sari, Purwanto, Eko Hari Rachmawanto, Abdul Syukur
Research Center for Intelligent Distributed Surveillance and Security, Study Program in Information Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia

Article Info

Article history:

Received Jul 2, 2024
Revised Aug 1, 2024
Accepted Aug 30, 2024

Keywords:

Aeroponic
Quantum BB84
Quantum measurement
Quantum security
Smart farming

ABSTRACT

Modern aeroponic systems leverage internet of things (IoT) technology for automated control of climate, lighting, and nutrient delivery, rendering them susceptible to unauthorized access and network attacks. Such disruptions can lead to financial losses and impair agricultural productivity by altering essential growth conditions. To mitigate these risks, robust security measures including encryption and firewalls are essential, alongside continuous monitoring and updates to combat evolving threats. Addressing cyber threats in urban aeroponic systems, implementing quantum encryption emerges as a promising solution. Quantum key distribution (QKD) ensures highly secure encryption keys using quantum states that change upon eavesdropping, thereby thwarting intrusion attempts effectively. Integrating quantum encryption in aeroponic control systems safeguards data integrity and operational continuity against cyber threats, bolstering urban agriculture resilience. Our findings demonstrate the efficacy of quantum BB84 protocol integrated with application programming interface (API) for Eve’s security. Quantum bit error rate (QBER) measurements revealed minimal interference (0.015) for Alice and Bob, contrasting with higher initial QBER (up to 1.0) for Eve, indicative of intrusion attempts. Histogram analysis further underscored quantum security’s effectiveness in identifying and mitigating breaches. For future research, enhancing quantum encryption protocols and integrating advanced detection mechanisms will be essential.

Corresponding Author:

Christy Atika Sari
Research Center for Intelligent Distributed Surveillance and Security
Study Program in Information Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro
Semarang, 50131, Indonesia
Email: christy.atika.sari@dsn.dinus.ac.id

1. INTRODUCTION

Aeroponics is an innovative agricultural method that grows plants without soil by misting a nutrient solution directly onto the roots of air-dependent plants, allowing for efficient absorption of nutrients, air and oxygen, as well as increased growth and optimal use of space [1], [2]. However, implementing aeroponic technology in urban areas faces a number of challenges, including high initial costs and reliance on complex technological systems, such as control climate and nutrient misting, which are susceptible to failure [3], [4]. Additionally, data security and encryption are also concerns because modern aeroponic systems are often integrated with internet of things (IoT) devices application need to be protected from unauthorized access and attacks. Network attacks may interrupt operations and corrupt the installation process.

The application of aeroponics technology in urban areas certainly brings effective and sustainable agricultural solutions, but the main challenge to consider is the risk of cyber attacks [5], [6]. Modern aeroponic systems rely heavily on IoT technology to automatically control various aspects, including climate, lighting, and nutrient delivery, making them vulnerable to unauthorized access and attacks network [5]-[7]. In case of attack, system parameters can be disrupted, which not only leads to financial losses but can also destroy agricultural productivity by disrupting nutrient supply or changing change the environmental conditions that plants need [8]. For example, tampering with misting systems can cause overwatering or drought, while changes in lighting can inhibit photosynthesis. These vulnerabilities require strict security measures, including strong data encryption and firewalls to protect systems from external threats. Additionally, continuous monitoring and regular updates of security systems are essential to deal with ever-evolving threats. So, while aeroponics offers many benefits, its success largely depends on the ability to maintain digital security so that the system continues to function optimally and is protected from cyber attacks.

To address the threat of cyberattacks on urban aeroponic systems, implementing quantum encryption could be an effective step. Quantum encryption, or quantum cryptography, uses the principles of quantum physics to create highly secure encryption keys that are virtually impenetrable by conventional hacking methods [9], [10]. Using quantum key distribution (QKD), encryption keys are sent via photons in a quantum state that will change if eavesdropped or tampered with, so any attack attempts can be detected and stopped immediately [11], [12]. Implementing this technology in an aeroponic control system ensures that data communicated between IoT devices and a central server is protected with a very high level of security, making it difficult for attackers to access or damage the system. Therefore, quantum encryption not only protects the integrity and operation of the aeroponic system, but also ensures the resilience of urban agriculture against future cyber threats.

Many researchers are now applying quantum technology in their smart agriculture projects to increase productivity, secure data, support decision making, and optimize overall agricultural operations. Stevens *et al.* [13] introduced a new approach to nutrient management in microscale smart hydroponics (MSH) based on quantum applications, which can reduce the pressure on urban food security. Although hydroponics is efficient in terms of space and resource usage, its management is complex. The MSH system uses IoT technology to simplify hydroponic management for home users. The researchers introduced a low-cost nutrient management system with a waterproof IoT spectroscopic sensor (AS7265x). This sensor monitors nutrients in the hydroponic solution and recommends adjustments. The model building process resulted in a significant predictive model with an R2 of 0.997. A 30-day experiment showed that the system successfully maintained nutrient levels and increased plant growth compared to the control. The results showed a significant correlation of 0.77 with the traditional method.

Zisopoulos and Broni [14] present the development of quantum agriculture as an interdisciplinary science that combines zero-footprint ecology, organic production, marketing, finance, and methodical trade. They evaluate parametric insurance, aquaculture indemnity, life cycle assessment (LCA), economic fraud prevention (EMA), and quantum marketing, integrating with recent patent production. Two new patents, “water circulation aquaculture platform” and “automatic air regulation”, share the vision of agricultural production with the old patents. Case studies include LCA, new insurance models, hive biological monitoring and bee product development. The future of agriculture includes technology integration, quantum marketing and quantum index insurance. Zhao *et al.* [15] introduced the quantum chaotic genetic optimization algorithm (QCGA) as a new method to optimize the offload latency of irrigation and fertilization tasks in sensor networks wireless drip irrigation and advanced computer-based agricultural fertilization system (AIFWSN). QCGA introduces new quantum operators, including gateless quantum gates and quantum spin gates, to improve the overall search capabilities of the algorithm. These quantum operators update the quantum spin gates without accessing the quantum spin angle table, thereby reducing computational complexity. Additionally, a new chaos operator is used to distribute initial solutions more evenly in the search space through chaos mapping. The conducted simulation experiments show that QCGA can significantly reduce the average latency compared to snake optimization (SO), genetic algorithm (GA), particle swarm optimization (PSO), sequential offloading, and random offloading, with an average offload of 9.96%, 26.78%, 29.31%, 44.67% and 61.24%.

Based on three approaches by previous researchers using quantum agriculture technology. In this study, the quantum method based on BB84 is also used to secure the data of the aeroponic smart farming system. This approach uses the principle of quantum qubit to enable the exchange of highly secure encryption keys between devices, relying on quantum mechanical phenomena to detect any eavesdropping attempts or intervention. In the context of aeroponic smart farming systems, implementing BB84 ensures that all data communications between sensors, actuators, and control centers are protected against threats network. Encryption keys generated through quantum qubit are not only difficult to decrypt, but any attempt to intercept the key will be immediately detected and cause a retransmission, thereby maintaining data integrity and security. Therefore, this approach not only significantly improves data security but also ensures the sustainability and performance of smart aeroponic farming systems against increasingly sophisticated potential cyber attacks.

2. METHOD

In this section, we will prepare a method based on the proposed approach. We will introduce the concept of quantum qubits in the context of information technology, and present the relevant electronic circuits for the aeroponic system. In addition, we will also explain the flow of the aeroponic system and the application programming interface (API) flow process required for practical implementation.

2.1. Quantum qubit based on BB84

BB84-based quantum approach uses qubits to encrypt the API ensuring that data communication between the client and server is protected with a very high level of security [16], [17]. In this protocol, encryption keys are distributed using qubits encrypted in two bases: computational basis ($|0\rangle, |1\rangle$) and cross basis ($|+\rangle, |-\rangle$). The sender and receiver randomly choose a base for each qubit, and only measurements that match their base are used to form the final encryption key [18], [19]. The Heisenberg uncertainty principle and the no-cloning theorem ensure that any eavesdropping attempts by third parties will be detected through changes in the measurement error rate. Based on BB84 protocol for API security, the encryption process begins with the sender (Alice) randomly selecting a quantum basis (e.g., $+$ for the computational basis and X for the diagonal basis) and sending qubits corresponding to the secret binary bits she wants to communicate. For example, in Table 1, Alice selects quantum basis $+$ and X, then generates qubits corresponding to the secret binary bits $(1, 0, 1, 1, 0, 0, 1, 1)$, which are represented by the qubit direction (↑→↗↑↖→↗↑). The receiver (Bob) then performs a measurement on the received qubit with a randomly chosen quantum basis, as shown in Table 2. Bob guesses the quantum basis ($+$ or X) and measures the qubit to obtain a binary bit. Matching bases between Alice and Bob produce the same bit, while mismatching bases produce random results.

Table 1. Alice side process as sender

Quantum base	Binary bit	Quantum qubit
+	1	↑
+	0	→
X	1	↗
+	1	↑
X	0	↖
+	0	→
X	1	↗
+	1	↑

Table 2. Bob side process as reciver

Random guess of quantum base	Random guess of binary bit	Check bit of quantum qubit
X	1	→
+	0	→
+	1	→
X	1	↑
X	0	↖
X	0	↑
X	1	↗
+	1	↑

In this way, the same encryption key can be generated by Alice and Bob without the need for direct communication, making the API data communication secure from eavesdropping since any eavesdropping attempt will cause an error detection in the measurement bit. Alice's encryption of qubits in the BB84 protocol involves choosing a secret binary basis and bits, and then encoding the qubits according to those choices [16]. For the computational basis, the qubit $|0\rangle$ represents the bit 0, and the qubit $|1\rangle$ represents the bit 1. For the diagonal basis, the qubit $|+\rangle$, which is the superposition of $|0\rangle$ and $|1\rangle$ with the equation $\mid +\rangle = \frac{1}{\sqrt{2}}\,(\mid 0\rangle + \mid 1\rangle)$ represent bit 0, while the qubit $|-\rangle$, which is a superposition of $|0\rangle$ and $|1\rangle$ with the equation $\mid -\rangle = \frac{1}{\sqrt{2}}\,(\mid 0\rangle - \mid 1\rangle)$, represents bit 1. Alice secret binary bits in this study are $1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1$, and the chosen basis is $+\ +\ X\ +\ X\ +\ X\ +\ +$, so the equation can be seen in (1).

$$\begin{aligned}
&Qubit\ 1\ (Base\ +,\ Bit\ 1): && \mid 1\rangle \\
&Qubit\ 2\ (Base\ +,\ Bit\ 0): && \mid 0\rangle \\
&Qubit\ 3\ (Base\ X,\ Bit\ 1): && \mid -\rangle = \frac{1}{\sqrt{2}}\,(\mid 0\rangle - \mid 1\rangle) \\
&Qubit\ 4\ (Base\ +,\ Bit\ 1): && \mid 1\rangle \\
&Qubit\ 5\ (Base\ X,\ Bit\ 0): && \mid +\rangle = \frac{1}{\sqrt{2}}\,(\mid 0\rangle + \mid 1\rangle) \\
&Qubit\ 6\ (Base\ +,\ Bit\ 0): && \mid 0\rangle \\
&Qubit\ 7\ (Base\ X,\ Bit\ 1): && \mid -\rangle = \frac{1}{\sqrt{2}}\,(\mid 0\rangle - \mid 1\rangle) \\
&Qubit\ 8\ (Base\ +,\ Bit\ 1): && \mid 1\rangle
\end{aligned} \tag{1}$$

If Alice sends qubits in the diagonal base (X) and Bob also measures in the diagonal base, then Bob will get a result that is consistent with the bits Alice sent. However, if Bob measures in a different base, the results of his measurements will be random and will not provide reliable information. In this case, the random basis that Bob chooses is: $X + +XXXX + X$. So, the equation will be the one shown in (2).

$$\begin{aligned}
&Qubit\ 1\ (Base\ X): && \langle -| 1 \rangle = \frac{1}{\sqrt{2}} \left(\langle 0 | - \langle 1 |\right) \cdot | 1 \rangle = -\frac{1}{\sqrt{2}} \\
&Qubit\ 2\ (Base\ +): && \langle 0 | 0 \rangle = 1 \\
&Qubit\ 3\ (Base\ +): && \langle +| - \rangle = \frac{1}{\sqrt{2}} \left(\langle 0 | + \langle 1 |\right) \cdot \frac{1}{\sqrt{2}} \left(| 0 \rangle - | 1 \rangle\right) = 0 \\
&Qubit\ 4\ (Base\ X): && \langle -| 1 \rangle = -\frac{1}{\sqrt{2}} \\
&Qubit\ 5\ (Base\ X): && \langle +| + \rangle = 1 \\
&Qubit\ 6\ (Base\ X): && \langle -| 0 \rangle = -\frac{1}{\sqrt{2}} \\
&Qubit\ 7\ (Base\ X): && \langle -| - \rangle = 1 \\
&Qubit\ 8\ (Base\ +): && \langle 1 | 1 \rangle = 1
\end{aligned} \tag{2}$$

Then, Bob compares the measurement results with Alice's for a matching basis. The bits generated by the matching basis form a secure encryption key. This system can be illustrated in Figure 1, which shows the flow of qubits from Alice to Bob and how measurements are made to ensure data integrity.

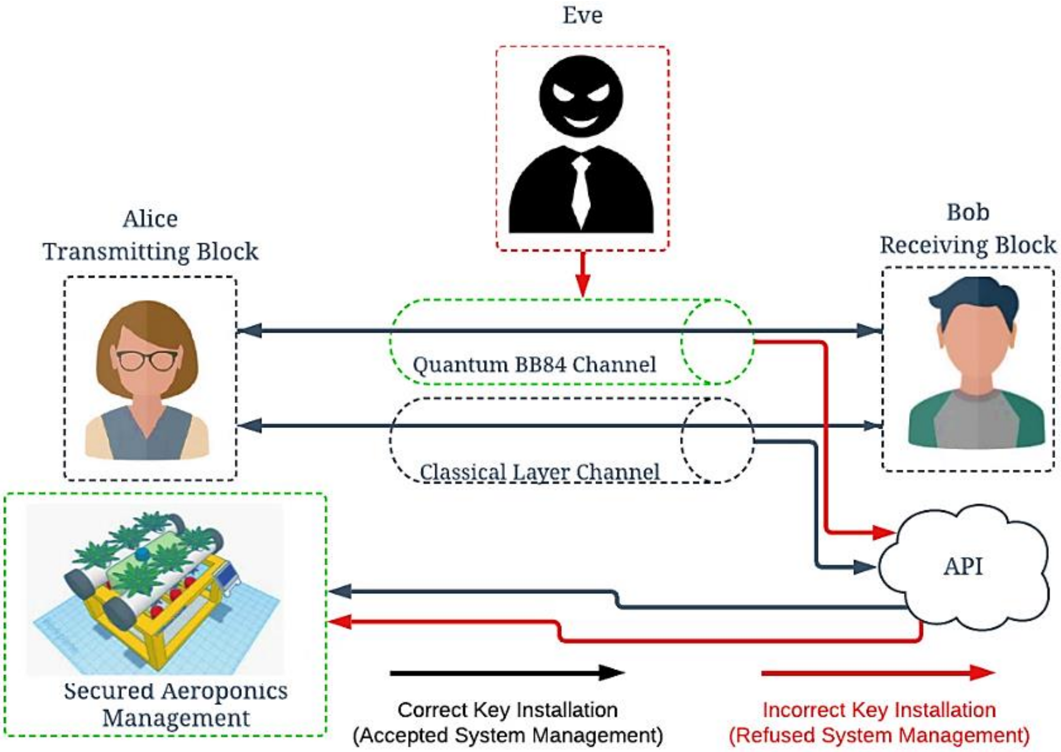


Figure 1. BB84 quantum security of aeroponics system

The results of (1) and (2) show how qubits are encoded by Alice and measured by Bob in the BB84 protocol, which can be used as a model for securing API systems connected to all management devices. In (1), Alice sends qubits based on a randomly chosen basis (+ or X) and a secret binary bit. In (2) describes Bob's measurement of the received qubit, with the result depending on the basis match between Alice and Bob. If Bob's measurement basis matches Alice's encoding basis, the measurement result will match the binary bit sent by Alice. The BB84 protocol ensures that data communication between the devices remains safe from eavesdropping attempts by Eve, because any eavesdropping attempt will change the state of the qubit, which can be detected by Alice and Bob as an error. Thus, Eve cannot eavesdrop or perform illegal management on the aeroponic system without being detected, because it must pass through the quantum BB84 security layer.

2.2. Electronic circuit

This electronic circuit includes various components to build a smart control system. 12 V adapter is used as the main power source that supplies electricity to the entire circuit [20]. 1.6 liquid crystal display (LCD) is used to display important information such as temperature and humidity measured by DHT sensors, which are placed both indoors and outdoors [21]. The ESP32 serves as the main microcontroller that controls all components and executes the programming logic for automation [22]. Three relays are used to control high-power devices such as light bulbs and fans, allowing the ESP32 to turn these devices on or off based on conditions detected by the sensors [23]. In addition, IC 1 and IC 2 are used to regulate signals and amplify the circuit's performance [24]. The atomizer, used to spray water vapor or nutrients in certain applications, is also controlled through one of the relays, ensuring that all aspects of the controlled environment can be precisely regulated [25]. The electronic circuit can be seen in Figure 2. Based on Figure 2, to describe the relationship between the components in a smart control circuit, we can use the basic equations that relate voltage, current, and electrical power, as well as the control signals sent by the ESP32 to control various devices via relays. The equations that relate all components in the circuit can be seen in (3)–(11).

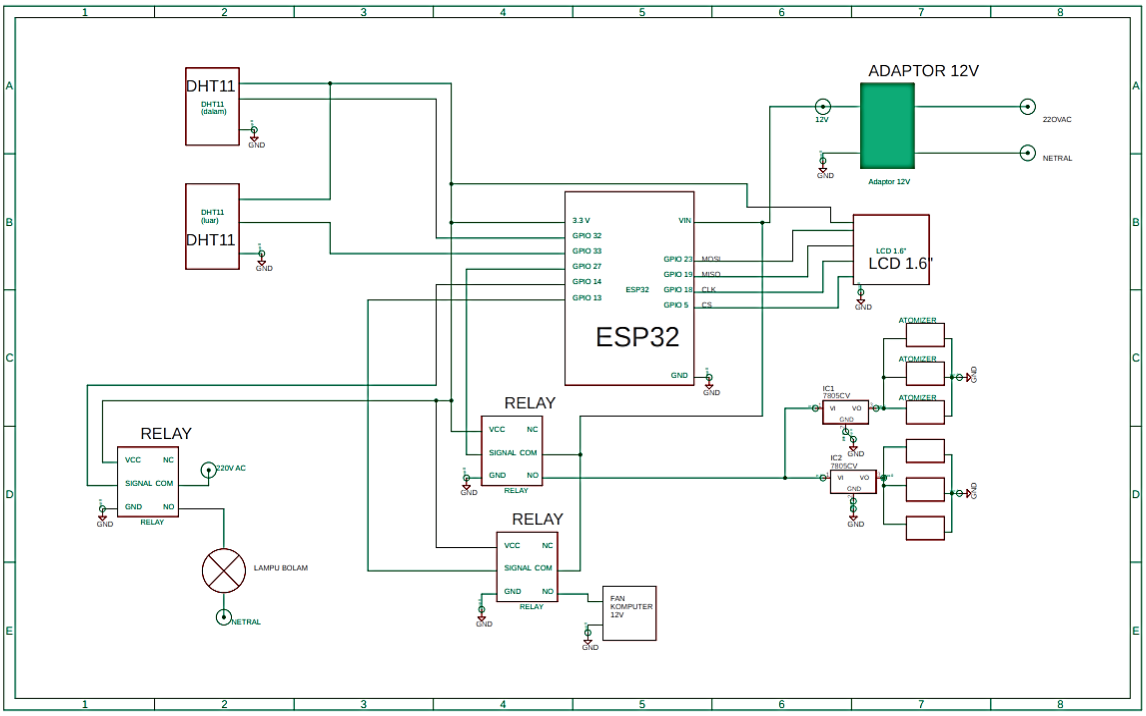


Figure 2. Electronic circuit

12 V adaptor: provides voltage and current to the entire circuit. Where, P_{total} is the total power required by the circuit, V is the voltage from the adapter (12 V), and I_{Total} is the total current required by all component.

$$P_{Total} = V \cdot I_{Total} \tag{3}$$

DHT sensor: measures temperature and humidity, sending data to the ESP32. Where, $Data_{DHT}$ is the data sent by the sensor, T is the temperature, and H is the humidity.

$$Data_{DHT} = f(T, H) \tag{4}$$

ESP32: processes data from the sensor and controls the relays and LCD. Where, $Signal_{relay}$ is the control signal sent to the relay based on sensor data and $Display_{LCD}$ is the information displayed on the LCD.

$$Signal_{relay} = f(Data_{DHT}) \tag{5}$$

$$Display_{LCD} = Data_{DHT} \tag{6}$$

Relay: controls high-power devices such as light bulbs, fans, and atomizers. Where, $State_{Device}$ is the status of the device (on or off) controlled by the relay.

$$State_{Device} = Signal_{relay} \tag{7}$$

Light bulb, fan, atomizer: consume electrical power when activated by the relay. Where, P_{Device} is the power used by the device, V is the voltage from the adapter (12 V), and I_{Device} is the current used by the device.

$$P_{Device} = V \cdot I_{Device} \tag{8}$$

IC 1 and IC 2: regulate signals and enhance circuit performance. Where, $Output_{IC}$ is is the signal output from the IC, $Gain$ is the amplification factor, and $Input_{IC}$ is the input signal to the IC. Thus, the general equation connecting all components can be seen in (9)–(11).

$$Output_{IC} = Gain \cdot Input_{IC} \tag{9}$$

$$P_{Total} = V \cdot (I_{Esp32} \cdot I_{relay} \cdot I_{Device}) \tag{10}$$

$$Device\ State = f(Sensor\ Data, ESP32\ Control) \tag{11}$$

Overall, the relationship between components in this smart control circuit can be expressed with equations connecting voltage, current, power, and control signals received and sent by the ESP32, which in turn manages other devices through relays.

2.3. Implement quantum BB84 to application programming interface system

The API flowchart begins with the “Start” point, indicating the initiation of the process. The first step is “Request Data,” where the API receives a data request from the client. The received data is then converted into a binary format in the “Convert Binary” step. Following this, the “Implement Quantum BB84” protocol is applied to encrypt the data. Subsequently, the “Measurement 100× Sampling” step involves measuring the qubits 100 times. At the “Is probability 100%?” decision point, the system checks if the measurement probability reaches 100%. If the probability is not 100% (“If No”), the data storage fails, and the process stops. If the probability is 100% (“If Yes”), the data is decrypted using the “Decrypt Quantum BB84” method and then further decrypted to ensure data security before being stored in the database in the “Decrypt Data Enter Database” step. The process concludes at the “Finish” point, indicating that the data has been successfully and securely stored. Flow of API system can be seen in Figure 3.

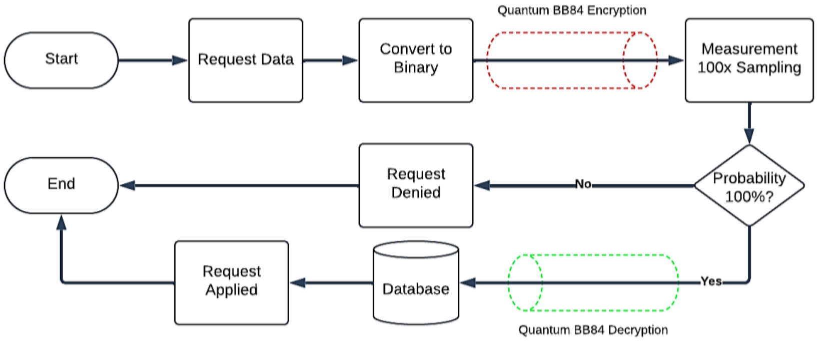


Figure 3. Flow of quantum API

The API security implementation, utilizing quantum BB84, can be effectively managed and controlled using Flutter, providing a robust and user-friendly interface for a secure managed aeroponics system. By leveraging Flutter’s cross-platform capabilities, users can monitor and manage the aeroponics environment in real-time, ensuring that all communication between devices and the central control system remains secure from cyber threats. This integration of quantum-based security with modern application development tools results in a comprehensive and secure solution for smart farming. Based on controlled system using flutter and connected API system can be seen in Figure 4.

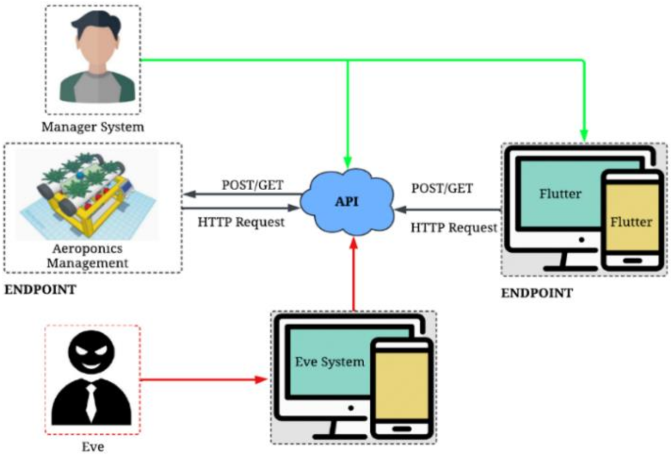


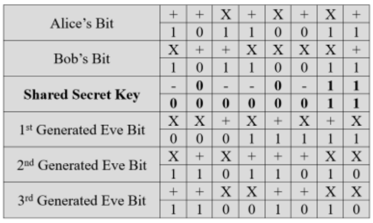
Figure 4. Concept of controller and system API

3. RESULTS AND DISCUSSION

In this phase, the security of the managed aeroponics system was rigorously tested and evaluated, with a focus on secure communication and the detection of potential eavesdroppers (Eve). Before testing, an important step is parameter initialization. The parameters tested can be seen in Table 3 and Figure 5.

Table 3. Initialization parameters

Parameter	Values
Qubit length	256
Sender bit probability	0.5
Reciver bit probability	0.5
Eve bit probability	0.5



Alice's Bit	+	+	X	+	X	+	X	+
	1	0	1	1	0	0	1	1
Bob's Bit	X	+	+	X	X	X	X	+
	1	0	1	1	0	0	1	1
Shared Secret Key	-	**0**	-	-	**0**	-	**1**	**1**
	0	**0**	**0**	**0**	**0**	**0**	**1**	**1**
1st Generated Eve Bit	X	X	+	X	+	X	+	X
	0	0	0	1	1	1	1	1
2nd Generated Eve Bit	X	+	X	+	+	+	X	X
	1	1	0	1	1	0	1	0
3rd Generated Eve Bit	+	+	X	X	+	+	X	X
	1	1	0	0	1	0	1	0

Figure 5. Bitstreams between Alice, Bob, and Eve used for testing

Based on the comparison of Alice's and Bob's transmitted bits in Figure 5, along with the derived shared secret key and the intercepted bits by Eve in the BB84 QKD protocol, several observations can be made. Alice and Bob initially agree on certain bits using specific bases ($+$ and X), aiming to establish a secure shared key. However, the presence of Eve, attempting to intercept the communication, results in discrepancies between Alice's and Bob's expected key and the bits intercepted by Eve. The shared secret key indicates the bits that Alice and Bob agree upon, while Eve's intercepted bits show her attempts to gather information.

3.1. Quantum bit error rate measurement

Quantum bit error rate (QBER) measurement is an important parameter in quantum communication systems, especially in protocols such as BB84 for QKD. QBER quantifies the deviation between expected and observed bits in a quantum communication channel due to errors caused by noise or eavesdropping attempts. It is calculated as the ratio of the number of erroneous bits to the total number of bits received. In practical terms, QBER reflects the integrity of the quantum states transmitted between parties: low QBER indicates high fidelity and high security, suggesting minimal interference or blocking, while QBER high indicates potential vulnerabilities in the transmission channel. Based on QBER equation can be seen in (11). Where, N_{error} is the number of erroneous bits detected during the transmission, and N_{total} is the total number of bits transmitted or received. Based on the parameters in Table 3 and the initialization of bitstreams shown in Figure 5, the QBER measurement depicted in Table 4. In an ideal situation without Eve, Alice, and Bob should have a QBER close to 0, indicating that the transmission is accurate and secure. However, in this test case, Eve's QBER values indicate significant interference or eavesdropping during transmission. Eve successfully generates the quantum key on the first try with a QBER of 1.0, indicating that all transmitted bits were in error. On the second and third attempts, Eve generates keys with a much lower QBER of 0.015, indicating improved transmission quality and a less significant probability of Eve appearing.

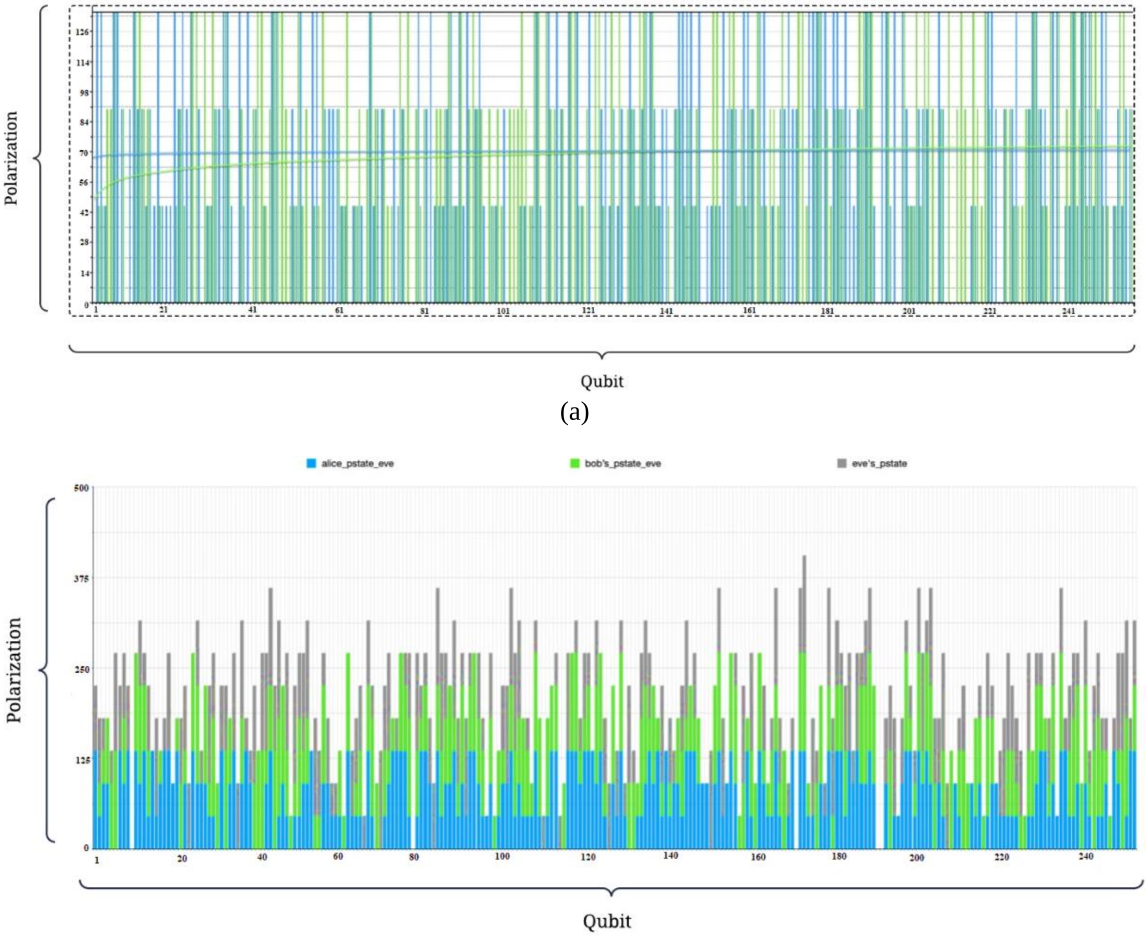
$$QBER = \frac{N_{error}}{N_{total}} \tag{11}$$

Table 4. QBER measurement

Testing	QBER values
Alice and Bob	0
1st generated keys (Eve)	1.0
2nd generated keys (Eve)	0.015
3rd generated keys (Eve)	0.015

3.2. Detection of eavesdropper based on histogram analysis

In this section, the detection of the Eve is evaluated through the analysis of the histogram shown in Figure 6. In Figure 6(a), representing the scenario without Eve's presence, the histogram peaks around a maximum value of approximately 135 for polarization parameters. Conversely, in Figure 6(b), depicting Eve's presence, the maximum histogram value increases to around 400 for polarization parameters. These changes indicate significant intervention by Eve in the tested system, illustrating its impact on the conducted measurements.



(a)

(b)

Figure 6. Histogram polarization states: (a) without Eve's presence and (b) with Eve's presence

3.3. Aeroponics design system

The final section of the discussion focuses on the aeroponics system design, as illustrated in Figure 7. This innovative system integrates the BB84 quantum computation protocol to enhance security measures against potential eavesdropping attempts by Eve. By leveraging BB84, the system ensures robust encryption and authentication protocols, thereby safeguarding sensitive data and communication channels crucial for effectively managing aeroponics operations. This design not only optimizes plant growth through precise nutrient delivery and environmental control but also prioritizes data integrity and security. These elements are critical for modern agricultural practices in urban environments.

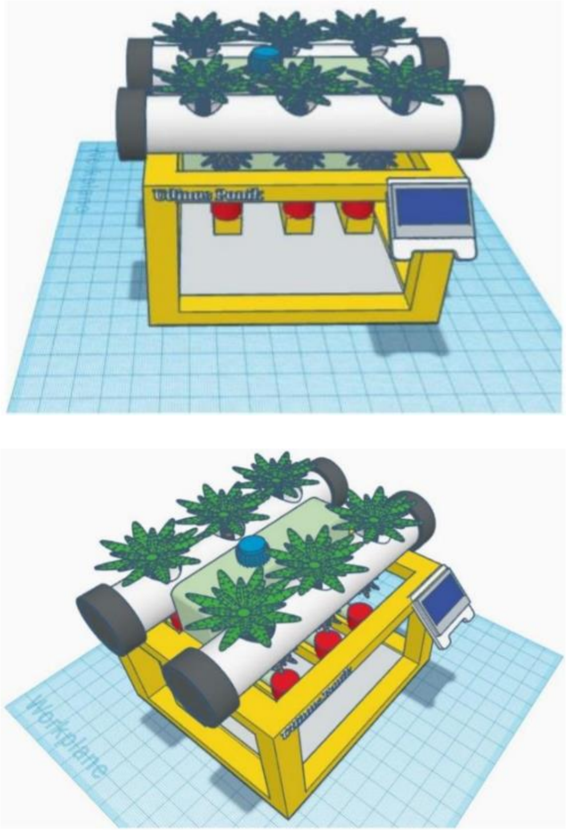


Figure 7. Proposed aeroponics design system

4. CONCLUSION

Based on the findings of this study, the implementation of the BB84 protocol successfully secured the API against potential eavesdropping by Eve. The QBER measurements provided significant insights into the security of quantum communication channels. Alice and Bob achieved an ideal QBER value of 0, indicating minimal interference during transmission. In contrast, Eve's attempts resulted in initially high QBER values of 1.0, which progressively decreased to 0.015 in subsequent measurements. This variation suggests differing levels of interference and potential breach attempts. Furthermore, the detection of Eve through histogram analysis offered crucial insights. In scenarios without Eve, the polarization parameter histogram peaked at approximately 135. However, with Eve's presence, this peak increased significantly to around 400. This disparity underscores the effectiveness of quantum security measures in identifying and mitigating potential security breaches in communication channels. For future research, enhancing quantum encryption protocols and integrating advanced detection mechanisms will be essential. Exploring QKD in complex agricultural systems like aeroponics, while ensuring scalability and efficiency, presents promising avenues for further investigation. Additionally, advancing quantum computing capabilities and developing real-time monitoring techniques will be pivotal in maintaining the integrity and security of smart agricultural systems in dynamic urban environments.

ACKNOWLEDGEMENTS

This research has been supported by Ministry of Education and Culture in the 2024 Applied Research Grant (*Hibah Penelitian Terapan DRTPM Tahun 2024*) and University of Dian Nuswantoro in accordance with Decree No. 108/E5/PG.02.00.PL/2024; 023/LL6/PgB/AL.04/2024 and 061/A.38-04/UDN-09/VI/2024.

REFERENCES

[1] J. Garzón, L. Montes, J. Garzón, and G. Lampropoulos, "Systematic review of technology in aeroponics: introducing the technology adoption and integration in sustainable agriculture model," *Agronomy*, vol. 13, no. 10, p. 2517, Sep. 2023, doi: 10.3390/agronomy13102517.

[2] P. K. S., B. Sampath, S. K. R., B. H. Babu, and A. N., "Hydroponics, aeroponics, and aquaponics technologies in modern agricultural cultivation," in *Trends, Paradigms, and Advances in Mechatronics Engineering*, IGI Global, 2022, pp. 223–241, doi: 10.4018/978-1-6684-5887-7.ch012.

[3] F. Ferrini *et al.*, "Yield, characterization, and possible exploitation of cannabis Sativa L. Roots Grown under aeroponics cultivation," *Molecules*, vol. 26, no. 16, p. 4889, Aug. 2021, doi: 10.3390/molecules26164889.

[4] M. E. Çalışkan, C. Yavuz, A. K. Yağız, U. Demirel, and S. Çalışkan, "Comparison of aeroponics and conventional potato mini tuber production systems at different plant densities," *Potato Res*, vol. 64, no. 1, pp. 41–53, Mar. 2021, doi: 10.1007/s11540-020-09463-z.

[5] K. Al-Kodmany, "The vertical farm: exploring applications for peri-urban areas," in *Smart Village Technology: Concepts and Developments*, Cham: Springer International Publishing, 2020, pp. 203–232, doi: 10.1007/978-3-030-37794-6_11.

[6] D. D. Avgoustaki and G. Xydis, "How energy innovation in indoor vertical farming can improve food security, sustainability, and food safety?," in *Advances in Food Security and Sustainability*, vol. 5, pp. 1–51, 2020, doi: 10.1016/bs.af2s.2020.08.002.

[7] M. S. Farooq, R. Javid, S. Riaz, and Z. Atal, "IoT based smart greenhouse framework and control strategies for sustainable agriculture," *IEEE Access*, vol. 10, pp. 99394–99420, 2022, doi: 10.1109/ACCESS.2022.3204066.

[8] B. Khoshru *et al.*, "Current scenario and future prospects of plant growth-promoting rhizobacteria: an economic valuable resource for the agriculture revival under stressful conditions," *Journal of Plant Nutrition*, vol. 43, no. 20, pp. 3062–3092, Dec. 2020, doi: 10.1080/01904167.2020.1799004.

[9] N. Zhou, Y. Hu, L. Gong, and G. Li, "Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations," *Quantum Inf Process*, vol. 16, no. 6, Jun. 2017, doi: 10.1007/s11128-017-1612-0.

[10] C.-H. Ou, D.-J. Jiang, C.-Y. Chen, L.-P. Yu, and C.-R. Chang, "Smart agriculture decision making scheme using quantum annealing," in *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, IEEE, Sep. 2022, pp. 862–863. doi: 10.1109/QCE53715.2022.00145.

[11] C. Schimpf *et al.*, "Quantum cryptography with highly entangled photons from semiconductor quantum dots," *Science advances*, vol. 7, no. 16, p. eabe8905, Apr. 2021, doi: 10.1126/sciadv.abe8905.

[12] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The Evolution of quantum key distribution networks: on the road to the Qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022, doi: 10.1109/COMST.2022.3144219.

[13] J. D. Stevens, D. Murray, D. Diepeveen, and D. Toohey, "A low-cost spectroscopic nutrient management system for Microscale Smart Hydroponic system," *PLoS One*, vol. 19, no. 5, May 2024, doi: 10.1371/journal.pone.0302638.

[14] A. Zisopoulos and G. Broni, "Quantum agriculture insurance model for productive precision farming enabled with original fishery, apicultural and cultivation patents," *International Journal of Scientific & Technology Research*, 2021.

[15] J. Zhao, X. Liu, and M. Tian, "An efficient task offloading method for drip irrigation and fertilization at edge nodes based on quantum chaotic genetic algorithm," *AIP Adv*, vol. 14, no. 1, Jan. 2024, doi: 10.1063/5.0185999.

[16] A. Adu-Kyere, E. Nigussie, and J. Isoaho, "Quantum key distribution: modeling and simulation through BB84 protocol using Python3," *Sensors*, vol. 22, no. 16, p. 6284, Aug. 2022, doi: 10.3390/s22166284.

[17] C. Lee, I. Sohn, and W. Lee, "Eavesdropping detection in BB84 quantum key distribution protocols," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2689–2701, Sep. 2022, doi: 10.1109/TNSM.2022.3165202.

[18] W.-L. Ma, S. Puri, R. J. Schoelkopf, M. H. Devoret, S. M. Girvin, and L. Jiang, "Quantum control of bosonic modes with superconducting circuits," *Science Bulletin (Beijing)*, vol. 66, no. 17, pp. 1789–1805, Sept. 15, 2021, doi: 10.1016/j.scib.2021.05.024.

[19] S. S. Gill *et al.*, "Quantum computing: a taxonomy, systematic review and future directions," *Software Practice and Experience*, vol. 52, no. 1, pp. 66–114, 2022, doi: 10.1002/spe.3039.

[20] H. N. K. Ningrum, G. Prabowo, R. J. K. Haryo, B. Winarnoand, and M. Safi'i, "Design of adaptive DC power supply with microcontroller based cuk converter circuit," *Journal of Physics: Conference Series*, vol. 1845, no. 1, p. 012046, Mar. 2021, doi: 10.1088/1742-6596/1845/1/012046.

[21] J. L. Chong, K. W. Chew, A. P. Peter, H. Y. Ting, and P. L. Show, "Internet of things (IoT)-based environmental monitoring and control system for home-based mushroom cultivation," *Biosensors (Basel)*, vol. 13, no. 1, pp. 1-24, Jan. 2023, doi: 10.3390/bios13010098.

[22] D. Hercog, T. Lerher, M. Truntič, and O. Težak, "Design and implementation of ESP32-based IoT devices," *Sensors*, vol. 23, no. 15, Aug. 2023, doi: 10.3390/s23156739.

[23] Nur-A-Alam, M. Ahsan, M. A. Based, J. Haider, and E. M. G. Rodrigues, "Smart monitoring and controlling of appliances using lora based iot system," *Designs (Basel)*, vol. 5, no. 1, Mar. 2021, doi: 10.3390/designs5010017.

[24] W. Jaikla *et al.*, "Single commercially available IC-based electronically controllable voltage-mode first-order multifunction filter with complete standard functions and low output impedance," *Sensors*, vol. 21, no. 21, p. 7376 Nov. 2021, doi: 10.3390/s21217376.

[25] S. Ragaveena, A. Shirly Edward, and U. Surendran, "Smart controlled environment agriculture methods: a holistic review," *Reviews in Environmental Science and Bio/Technology*, vol. 20, no. 4, pp. 887–913, Sept. 2021, doi: 10.1007/s11157-021-09591-z.

BIOGRAPHIES OF AUTHORS

Christy Atika Sari received the Master’s degree in Informatic Engineering from Universitas Dian Nuswantoro and University Teknikal Malaysia Melaka (UTeM) in 2012. She is currently active as an author in an international journal and conference Scopus indexed. She was also awarded as best author and best paper at a national and international conference in 2019 and 2020 respectively and was awarded by the Indonesian Ministry of Education and Culture Research and Technology as the Indonesian top 50 best researchers in 2020. She’s research interest is quantum computing for security data and image processing. She can be contacted at email: christy.atika.sari@dsn.dinus.ac.id.

Purwanto is currently an Associate Professor in the Faculty of Computer Science at the Universitas Dian Nuswantoro, Semarang, Indonesia. He received his Ph.D. degree from the Faculty of Computing and Informatics Multimedia University, Cyberjaya, Malaysia. Now, he serves as Head of the Master’s degree Program at the Universitas Dian Nuswantoro. He has published research papers in reputed international journals and conferences. His current research interests image processing, machine learning, and deep learning. He can be contacted at email: purwanto@dsn.dinus.ac.id.

Eko Hari Rachmawanto received a Bachelor’s degree in Informatic Engineering from the Universitas Dian Nuswantoro, in 2010. He received a Master’s double degree Universitas Dian Nuswantoro and Universiti Teknikal Malaysia Malacca (UTeM) in 2010 and 2012. Since 2012, he joined as a lecturer in informatics engineering at Universitas Dian Nuswantoro, Semarang, Indonesia. Now he serves as Editor in Chief of Accredited Indonesian National Journal. Since 2022 he has supervised the informatics engineering study program in study programs outside the main campus as head of the study program in Kediri, Indonesia. Now he is a member of Security Data Collaboration Research and tasked with developing several researchers regarding data security, and image processing. He can be contacted at email: eko.hari@dsn.dinus.ac.id.

Abdul Syukur received the Bachelor’s degree in Mathematics from Universitas Diponegoro, Semarang, the Master’s degree from Universitas Atma Jaya Yogyakarta, and the Ph.D. degree from Universitas Merdeka Malang. He is currently an Associate Professor and the Dean of the Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia. His current research interests include decision support systems, information science, and information systems, statistics, data mining, and machine learning. He can be contacted at email: abdul.syukur@dsn.dinus.ac.id.