A Secure IoT System Using Quantum Cryptography with Block Cipher

Zaid A. Abdulkader[1*]

[1] Faculty of Administration and Economics, Al-Iraqia University, Baghdad, Iraq
[*] Corresponding author. E-mail: dr.zaid.alshawi@gmail.com

Received: Feb. 15 20, 2021; Accepted: Mar. 22, 2021

In our days Iot technology used in a wide aspect of life and became an important topic for researchers in the scope of the technologies. Although all these benefits it needs more security and stays have security intimidation, such as data breaking or channel attacks via eavesdroppers and viruses, especially when the people used IoT for long distance for example for city or country, etc. or even using IoT to transfer secret information about things in big offices, for this reasons needed to use a method which increases IoT security and protection our special data. In this paper, we will use the internet of things IoT with quantum key distribution (QKD) and block cipher RC6 algorithm, where QKD is the science and art of using the quantum mechanical effect to perform cryptographic tasks and generates a secret key. Also, we need to overcome the loss of information which occurs because the information transition effected by noise or outside operators when using quantum cryptography, so the optimal solution is using the quantum bit error rate (QBER) to produce a more safe way for quantum communication among things in IoT techniques. QBER is done by using servers to correct error after sending a key for decryption method by another server to decrypt information using RC6 block cipher algorithm, during creating a secret key we need to calculate quantum correct probability and compare the result with threshold suggested and agreed by the servers.

Keywords: Internet of Things (IoT) Security, Quantum Key Distribution (QKD), Quantum Bit Error Rate (QBER), Rc6

http://dx.doi.org/10.6180/jase.202110_24(5).0012

1. Introduction

The concept of the Internet of Things (IoT) refers to the connection of various devices and objects via the Internet wireless or wire. This technology has wide popularity which increased quickly, because it is used for several purposes, such as education, communication, business expansion, home or building automation, and smart transportation [1, 2]. IoT transfers information among several devices in a network, so the possibility of exposure this information to attack and hacking has high probable [3], wherein network security an attacker and eavesdropper try to destroy, modify, steal, monitor, or get unauthorized access for special people information this represent a substantial challenge in IoT. To overcome this challenge, many security algorithms and different method to generating keys used for encrypting and decrypt information among the parties, this paper proposed a method of using quantum computing which transfers data by photons via the fiber-optic channel, it has property non-cloning because cloning the state of the photon is impossible [4], and if there is eavesdropper access to information the photon will change itself directly [5]. This work will use quantum key distribution (QKD) to generate a private key this method is also called BB84 protocol, which creates a series of qubits randomly with a length according to the encryption algorithm proposed in this paper. Also used method QBER that refers to correct the error by comparing the number of wrong values to the all list value and re-transfer information after removing the error from QKD [6]. Then we used RC6 block cipher to encrypt and decrypt information, where a symmetric block cipher uses 128 plaintexts and cipher text [7].

2. Internet of Things (IoT)

The increase of the internet's importance and is ubiquitous, made IoT is not a network for connecting computers only but also for connecting other devices that different in size, shapes, and types [8]. So that we can say that IoT refers to a network of varied devices rather than similar devices [9], see Fig. 1. IoT works from low level to top-level approach [10], it consists of four layers: perception layer, which gathers information about the connected smart devices and transfers it to the next layer, this layer represents a sensor device which has main challenges that collected information can be under the effect of the attack; network layer it collected the information from the sensors and transfer it to the upper layer, the eavesdropping in this layer is depending on the type of data transferred and the media that used for connecting among devices, the middleware layer will received data from the network layer, it used for links the system to the database, processing and storage the data. Finally application layer used to process and manage data from the middleware layer, and providing quality service to the final user but it also suffer from the mainly problem in the operation of sensitive data, for instance illegal access to data Fig. 2 illustrate IoT layers. Attackers can used vulnerabilities points in order to intruder on the systems to obtain important data and modify it [11–13].

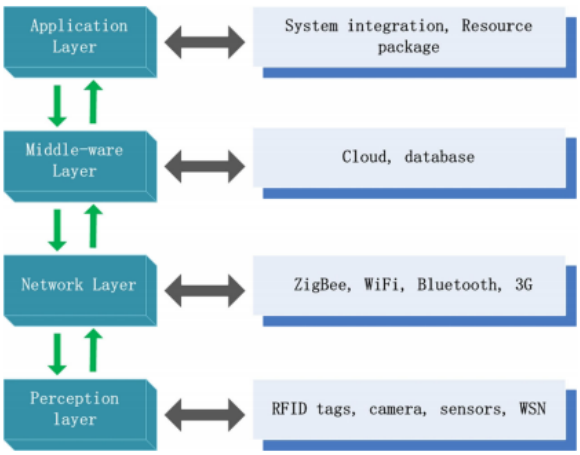

Fig. 1. IoT Layers.

3. Quantum Key Distribution(QKD)

Famous technology of quantum cryptography is QKD which depending on the photon to generate a key and transfers data via a quantum channel which represents as fiber optic channel or optical free space, when monitoring

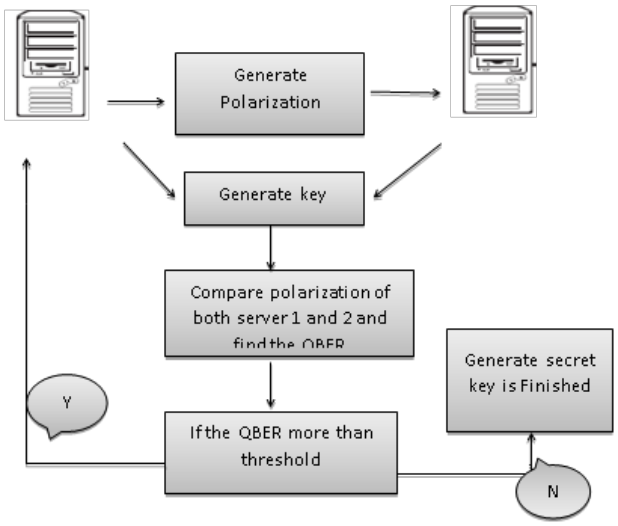

Fig. 2. Generation secret key by QKD diagram.

the photon is changing its state immediately, so the breaking process for QKD is not hard but it impossible [14, 15]. There are other properties for QKD is no-cloning this meant it difficult to take a copy of the state of a photon [5], this work used BB84 protocol that is a QKD detected in 1984 by Bennett and Brassard. BB84 protocol generates a random key between two persons depending on the polarization of the photon to record the state of the photon which called a qubit (in quantum theory bit called qubit it can be 0 and 1 at the same time) and then translate it to a normal bit based on the photon polarize, see Table 1 below for instance where h, v, rcp, and lcp represent horizontal, vertical, left circular, right circular polarization respectively [16, 17].

4. Error Estimation Using Quantum Bit Error Rate

Despite the importance of quantum cryptography (QKD) for transpose information long-distance but it stays under the effect of the error which occurred either because of the noise or the hackers, for this reason, we need to calculate QBER. Quantum Bit Error Rate (QBER) is defined as the percentage of the error that occurs in the key during transmission, the accuracy of QBER effected on the efficiency of the system when transform information [18, 19]. If quantum cryptography (BB84) is designed properly it will be easy to discover the presence of an eavesdropper, when the eavesdroppers gain more information the higher error rate will be [20–22]. After calculating QBER it will compare with the threshold that agreed between two-party connecting if it under 11% this means no eavesdropper can get a key [23].

$$QBER = n_{wrong}/(L_s + n_{wrong}) \quad (1)$$

Table 1. Quantum Key Distribution - BB84 protocol.

Sequence of bits		1	2	3	4	5	6	7	8	9	10	11	12
(1)	A's bit	1	1	0	0	1	0	1	0	0	0	1	1
	A's source basis	D	R	R	R	D	D	R	D	R	D	R	D
	A's polarization	$\|rcp\rangle$	$\|v\rangle$	$\|h\rangle$	$\|h\rangle$	$\|rcp\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|rcp\rangle$
(2)	B's dectetor basis	D	D	R	R	R	R	R	D	D	R	D	D
(3)	B's measurement	$\|rcp\rangle$	$\|lcp\rangle$	$\|h\rangle$	$\|h\rangle$	$\|h\rangle$	$\|v\rangle$	$\|v\rangle$	$\|lcp\rangle$	$\|lcp\rangle$	$\|v\rangle$	$\|rcp\rangle$	$\|rcp\rangle$
	B's bit	1	0	0	0	0	1	1	0	0	1	1	1
(4)	B report basis	D	D	R	R	R	R	R	D	D	R	D	D
(5)	A's response	Y	N	Y	Y	N	N	Y	Y	N	N	N	Y
(6)	Shared secret key	1	-	0	0	-	-	1	0	-	-	-	1

where L_s is the number of correct bits detections and n_{wrong} represents the number of error bits detections in the received series.

5. Rivest Cipher 6 (RC6)

RC6 is a block cipher algorithm with a symmetric key, it designs to meet the requirement of AES. The size of plaintext, ciphertext, and the key is 128 bit, it has a simple diagram explain the steps of this algorithm and has three parameters r=20round b=16 byte, and w=32 bits also it has six operations [24].

6. Proposed Work

Can anyone imagine what happens if the internet of things has widespread in our world? What happens with our personal information and special our life? The hackers everywhere and they can steal our information. For these reasons we suggest in this paper a new protocol to overcome the eavesdropper, Fig. **??** below shows the main steps to implement this work. In this paper, we suppose there is a company that has two servers (1 and 2) one provides a key for the Encryption process and another for the Decryption process so they work as proxy servers, the next segment has three branches: key generating, key authentication, and protocol steps [24, 25].

6.1. Quantum Key Generation (QKD)

To generate a random sequence of bits (0,1), server1 generates randomly a sequence of bases, also called filters (× +) which then convert to a sequence of polarization represents by angles (0° 45° 90° 135°), where (0° and 45°) represent bit (0) and (90° and 135°) represent bit (1), the servers choose a threshold (θ) in a condition that it must not exceed then 0.5 and compare θ with the probability of the correct polarize to ensure if they get the desired key or not. The server1 generates a random sequence from filters ($|$, /, \, -) with length L, the series of the bases of each bit which used as filters for rectilinear and diagonal directions (×, +) respectively also with length L, and a polarization according to this filter in four directions (0° 45° 90° 135°). The base sequence is sent via a quantum channel to server2.

$$\Psi = \frac{Pz}{L} \times 100\%, \; True\; if\; \Psi \geq \theta \tag{2}$$

Where Pz is the number of correct bases polarization. If Ψ is less than θ, server 1 will repeat sending the bases until the condition is satisfied and generate a required key, Fig. 3 shows the key generation process. Serve1 will send the secret key to workstation A for the encryption process and server 2 send the secret key to workstation B for the decryption process, both sending's jobs are via a cloud through fiber-optic or optical free space.

Because a key generated randomly, someone can ask what's level of random we can get? How we can measure the randomness of the secret key? We can do that by using one of several methods and the most simple and significant is the entropy method which is used to measure the degree of key randomness. Fig. 4 gives the result of randomness in key and protocol, show that when entropy is close to one in coordinate y the randomness will increase this satisfies the condition of entropy.

6.2. Key Authentification

How the server1 and server2 know that they connecting without any accidental or willful damage? The need for authentication is fundamental demand in all algorithms of cryptography, it is required that both servers used an initial short piece of secret bits (such as a few hundred bit), so that they will have the ability to recognize each other through their communications and run of the protocol. When successful first QKD process, they can use a section of the secret key that generated previously for future authentication in other protocol runs see Fig. **??**.

Table 2. Generate secret key results for five executions with different length.

Quantum key length	QBER	Time to generate secret key in second
128 bit	0.0605	0.0130 sec
256 bit	0.1335	0.00451 sec
512 bit	0.2515	0.00659 sec
1024 bit	0.5095	0.0876 sec
2048 bit	1.0125	0.0160 sec

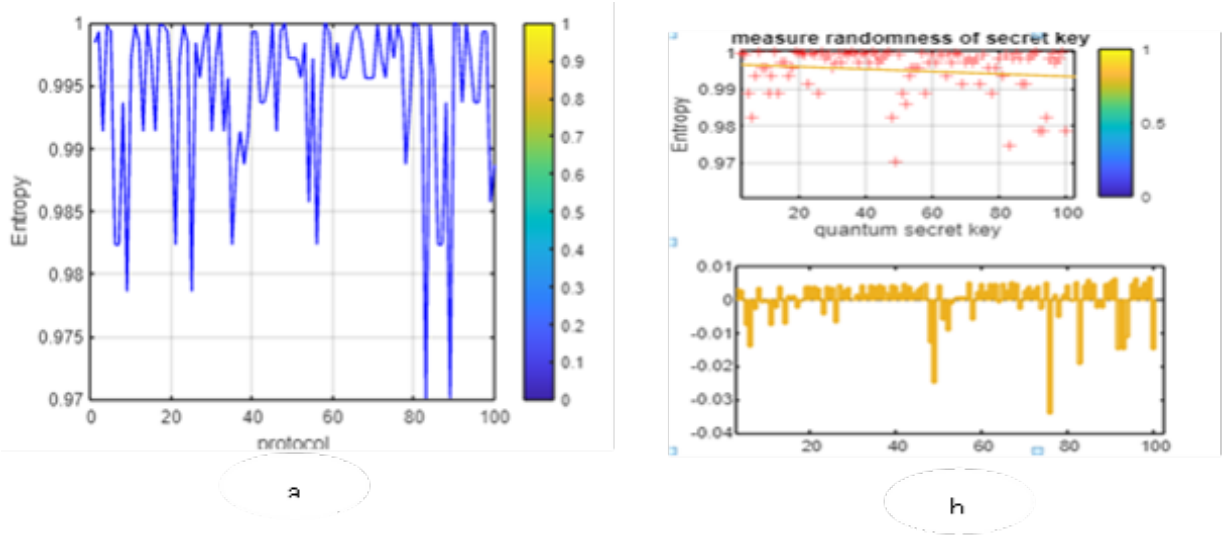

Fig. 3. Measure method randomness using entropy: a for all protocol and b for secret.

6.3. Protocol Steps

We know there is a multi-users need to use the IoT in a smart company; so that the proposed protocol used to transfer information in safety way according to the following steps:

- Step 1: Sensors will collect confusing information from the different devices.
- Step 2: Processing this information to get pure data by processors.
- Step 3: Creates a secret key using the QKD protocol.
- Step 4: Distributes a secret key by cloud, server 1 sends a secret key to workstation A and server2 to workstation B.
- Step 5: Encryption of the data from step 2 by workstation A using the RC6 algorithm.
- Step 6: Sends the encrypted data to clouding computing.
- Step 7: Arrives the encrypted data via clouding computing to the workstation B that decrypts data using RC6 decryption algorithm and the secret key.
- Step 8: Information arrives at every person who needs it.

7. Conclusion

From this work we have the results:

1. Using QKD made it hard to break a secret key because of the properties of quantum computing.
2. Using QKD (BB84) protocol gives a different key with every execution, this means given a different key for every request for devices in the IoT.
3. Provide authentication protocol.
4. Using RC6 to encrypt the important information which meets the requirement of AES and is driven from RC5, made this information safe and it difficult to stolen or modified by the hackers.
5. Using quantum bit error rate QBER gave the ability to decrease the error which occurred during the transfer of the key between two servers.
6. The new protocol is a symmetric block cipher.

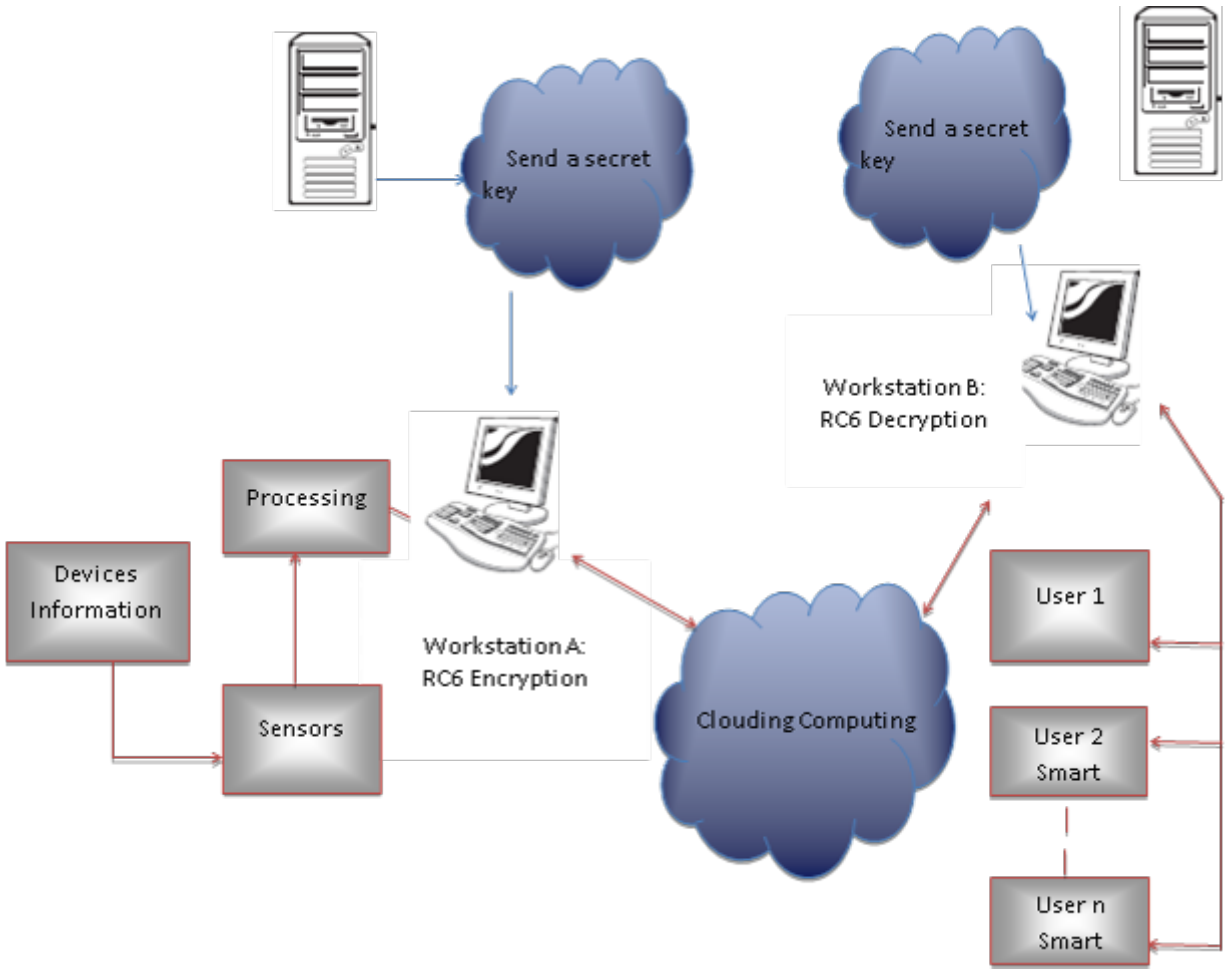

Fig. 4. The proposed steps diagram.

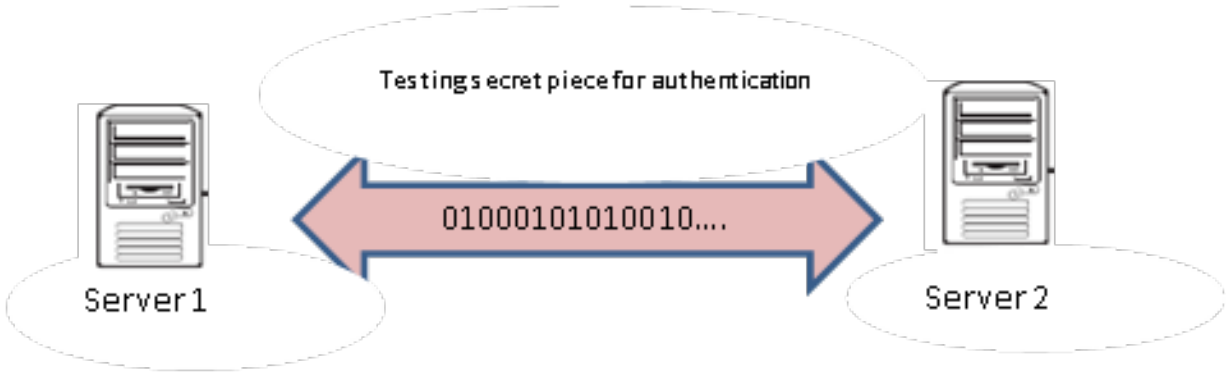

Fig. 5. Authentication of Proposed Method.

Future vision :

1. It can in the next work use the quantum repeater (QR) to decrease error during the transformation of data

2. Use quantum gateway with IoT instead of the ordinary gateway.

References

[1] Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. IoT privacy and security: Challenges and solutions. *Applied Sciences (Switzerland)*, 10(12):1–17, 2020.

[2] Anca D. Jurcut, Pasika Ranaweera, and Lina Xu. In-

troduction to IoT Security. In *IoT Security*, number December, pages 27–64. 2020.

[3] Anca D. Jurcut, Tom Coffey, and Reiner Dojen. Design requirements to counter parallel session attacks in security protocols. In *2014 12th Annual Conference on Privacy, Security and Trust, PST 2014*, number April 2018, pages 298–305, 2014.

[4] Heng Fan, Yi Nan Wang, Li Jing, Jie Dong Yue, Han Duo Shi, Yong Liang Zhang, and Liang Zhu Mu. Quantum cloning machines and the applications, 2014.

[5] Miloslav Dušek, Norbert Lütkenhaus, and Martin Hendrych. Quantum cryptography. In *Progress in Optics*, volume 49, pages 381–454. 2006.

[6] Sreraman Muralidharan, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang. Optimal architectures for long distance quantum communication. *Scientific Reports*, 6(November 2015):1–10, 2016.

[7] Asma Belhaj Mohamed, Ghada Zaibi, and Abdennaceur Kachouri. Implementation of RC5 and RC6 block ciphers on digital images. In *International Multi-Conference on Systems, Signals and Devices, SSD'11 - Summary Proceedings*, number June 2014, 2011.

[8] Keyur K Patel, Sunil M Patel, and P G Scholar. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application Future Challenges. *International Journal of Engineering Science and Computing*, 6(5):1–10, 2016.

[9] K. Rose, S. Eldridge, and C. Lyman. The internet of things: an overview. *Internet Society*, page 53, 2015.

[10] Abhishek Mahajani, Vinay Pandya, Isaac Maria, and Deepak Sharma. *file:///D:/big data/chapter 1/pradeep2017.pdf*, volume 904. 2019.

[11] Kejun Chen, Shuai Zhang, Zhikun Li, Yi Zhang, Qingxu Deng, Sandip Ray, and Yier Jin. Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Journal of Hardware and Systems Security*, 2(2):97–110, 2018.

[12] T Kowsalya, S Sukirtha, and S Krithika. Quantum Key Distribution for IoT -A Review Quantum Key Distribution for Internet of Things (IoT) - A Review. (November), 2019.

[13] CN Yang and CC Kuo. Enhanced quantum key distribution protocols using BB84 and B92. *Proceedings of the 2002 International . . .* , (January 2002):1–13, 2002.

[14] E. O. Kiktenko, A. O. Malyshev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, and A. K. Fedorov. Error Estimation at the Information Reconciliation Stage of Quantum Key Distribution. *Journal of Russian Laser Research*, 39(6):558–567, 2018.

[15] Nelson J. Muga, Mário F.S. Ferreira, and Armando N. Pinto. QBER estimation in QKD systems with polarization encoding. *Journal of Lightwave Technology*, 29(3):355–361, 2011.

[16] Miralem Mehic, Marcin Niemiec, and Miroslav Voznak. Calculation of the key length for quantum key distribution. *Elektronika ir Elektrotechnika*, 21(6):81–85, 2015.

[17] Etsuko Sugawara and Hiroshi Nikaido. Properties of AdeABC and AdeIJK efflux systems of Acinetobacter baumannii compared with those of the AcrAB-TolC system of Escherichia coli. *Antimicrobial Agents and Chemotherapy*, 58(12):7250–7257, 2014.

[18] Xiaojun Xiang, Qiong Li, Shahnawaz Khan, and Osamah Ibrahim Khalaf. Urban water resource management for sustainable environment planning using artificial intelligence techniques. *Environmental Impact Assessment Review*, 86, 2021.

[19] Osamah Ibrahim Khalaf, Kingsley A. Ogudo, and Manwinder Singh. A fuzzy-based optimization technique for the energy and spectrum efficiencies tradeoff in cognitive radio-enabled 5g network. *Symmetry*, 13(1):1–14, 2021.

[20] Bilal S.A. Alhayani and Haci Llhan. Visual sensor intelligent module based image transmission in industrial manufacturing for monitoring and manipulation problems. *Journal of Intelligent Manufacturing*, 32(2):597–610, 2021.

[21] Milind E. Rane and Umesh S Bhadade. Comparative Study of ROI Extraction of Palmprint. *IJCSN International Journal of Computer Science and Network*, 5(2), 2016.

[22] Osamah Ibrahim Khalaf, Kingsley A. Ogudo, and Manwinder Singh. A fuzzy-based optimization technique for the energy and spectrum efficiencies tradeoff in cognitive radio-enabled 5g network. *Symmetry*, 13(1):1–14, 2021.

[23] Bilal Al Hayani and Haci Ilhan. Image Transmission Over Decode and Forward Based Cooperative Wireless Multimedia Sensor Networks for Rayleigh Fading Channels in Medical Internet of Things (MIoT) for Remote Health-Care and Health Communication Monitoring. *Journal of Medical Imaging and Health Informatics*, 10(1):160–168, 2019.

[24] Milind E. Rane and Umesh S. Bhadade. Multimodal score level fusion for recognition using face and palmprint. *International Journal of Electrical Engineering Education*, 2020.

[25] Shibo Lu, B. T. Phung, and Daming Zhang. A comprehensive review on DC arc faults and their diagnosis methods in photovoltaic systems, jun 2018.