

A secure telemedicine electronic platform based on lightweight cryptographic approach

Israa Ezzat Salem¹, Haider Rasheed Abdulshaheed¹, Hassan Muwafaq Gheni²

¹Computer Engineering Techniques Department, Baghdad College of Economic Sciences University, Baghdad – Iraq

²Computer Techniques Engineering Department, Al-Mustaqbal University College, Hillah 51001, Iraq

Article Info

Article history:

Received Dec 27, 2021

Revised Jul 05, 2022

Accepted Jul 13, 2022

Keywords:

Diffie Hellman encryption

IoT chaotic cryptographic

IoT system

Lightweight crypto

Telemedicine platform

ABSTRACT

Telemedicine platforms have emerged as one of the most harnessed studies in recent years, especially after the spread of pandemics. Due to the epidemic, telemedicine distribution to rural or isolated areas has become an urgent need. However, there are several obstacles to providing remote medical care, the most significant of which is protecting patient data while sustaining the speed of communication between the patient and the medical staff. The significant of this study is to provides a lightweight encryption/decryption technique that uses on the internet of medical things in stance of bio-sensors and bio-actuators. This study is one of the cybersecurity approaches, such type of encryption has little effect on the speed of data transmission. The Diffie Hellman technique is used as a lightweight encryption method because it includes four encryption-keys. The efficiency of the proposed encryption method has been compared with several equivalent methods. According to experimental results, the proposed encryption method represents a lightweight and secure method which can accomplish the level of protection that required to secure medical information despite the data's disarray.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Haider Rasheed Abdulshaheed

Computer Engineering Techniques Department, Baghdad College of Economic Sciences University

Baghdad – Iraq

Email: haider252004@yahoo.com; haider_rasheed@baghdadcollege.edu.iq

1. INTRODUCTION

Telemedicine platforms have evolved into popular services that affect our daily lives by constantly interacting with our medical activities via built-in sensors. The sensors are found internally in many types of electrical equipment that we utilize on a routine basis. For example, detecting the possibility of getting corona virus by using the quick request code (QR code) on a mobile phone and transmitting the information to a central database for telemedicine data processing. In a network of sensors, data is collected and distributed. Everything is under the auspices of the so-called internet of medical things (IoMT) and the telemedicine delivery system (telemedicine). The main key concern is how to share and secure this massive and complex array of sensors. The telemedicine platform provides a common platform for all of these sensors to transfer relevant information meanwhile a shared language for them all to communicate with each other. Medical data is acquired from various sources and evaluated to find the essential information and increase efficiencies in accordance with the patient's needs. The topic of secure sensitive data at the network level is still being researched and studied as a scientific challenge. The issue of protection telemedicine platform is complicated, as some research were mentions. Some researchers focused on the random shuffling of medical images as a lightweight, cluster-based medical image coding technique. A lightweight crypto IoT system based on Henon's chaotic approach was utilized in one research [1]. Another study proposes a data

compression technique for image encryption that uses seek and elective encryption pixel [2], [3]. To secure transmission of medical images, another researcher employed a hybrid strategy that includes chaotic and Henon encryption [4]. The watermark insight for medical images have also been discussed using the singular value decomposition (SVD) and slantlet transform (SLT) [5]. Despite not taking into account the encryption key-size, which increases the number of bits in the packets and thus costs time. To ensure security, several researchers used the hyper chaotic internet of things (IoT) biosensors and actuators in novel 5-D with a significant encryption method. The PRESENT-SPECK algorithms are combined with the suggested lightweight chaotic IoT system to create the security mechanism [6], [7]. This suggested scheme offers a high level of security but not a lightweight approach to use with a large amount of data. The Feistel-encryption-system (FES), modify-advanced-encryption-system (M-AES), and modify-scaled-zhongtang-chaotic-system (M-SCZS) algorithms offered by several researchers as an innovative solution for surgical telemedicine. The encrypted transmitted information is kept under request by using the information accountability framework (IAF) during real-time surgery, which slows down the surgery as a side effect [8]. The elliptical curve Diffie Hellman has also been discussed carefully as a secure transition for the robotic surgery session [9]. The session has established between the surgeon's station and the interactive mechanical arm. Both are devices rather than lightweight sensors, which are decreasing transmission efficiency [10]. Remote patient monitoring has been the topic of several researchers. Patient health is monitored in real-time, allowing for timely and appropriate medical treatment. An authentication technique based on body area network (BAN) logic has been devised to secure the connection. This study does not address the problem of time [11], [12]. Numerous researchers have attempted to secure social networks (VSN) for ambulance vehicles utilizing re-fragmentation in the context of cybersecurity, but the middleware used at the application layer in the transmission control protocol/internet protocol (TCP/IP) protocol does not adhere to the lightweight ideology [13]. The electrocardiogram (ECG) signal is one of the most significant medical signals that must transfer to a hospital or clinic. ECG signal encryption for security applications has been the focus of some studies [14]. The strategy of encryption here is to combining ECG signals with surrounded sound noise signals by utilizing audio codecs. The scenario of combining encoder signals with noise may result in a longer wavelength and fewer time savings than anticipated [15], [16]. The emergence of the lightweight by using quantitative encryption for the secure transmission of medical data has opened the way to research opportunities to protect information transmission at high speeds and efficiency, but the challenge of whether these researches can be completed at an affordable cost remains under discussion [17], [18]. This research provides a secure lightweight telemedicine platform to achieve the following objectives: as seen in Figure 1.

- 1) Using a lightweight IoT protocol to ensure the speed of encrypted medical data transmission due to the importance of the time factor for the patient.
- 2) Improving the security of data transmission using the Diffie Hellman encryption method, which contents four encryption keys (pair public keys, pair private keys), which reduce the size of the transmitted packet and thus achieve fast encrypted medical data transmission.

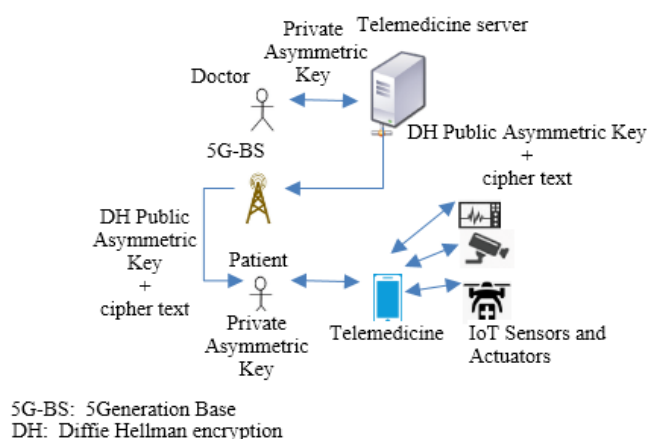


Figure 1. A lightweight chaos-based telemedicine encryption scheme using Diffie Hellman

The following is the outline of the paper. In the second section, theoretical concepts relating to the suggested method are provided. In section 3, the suggested Diffie Hellman technique implementation for encrypting telemedicine platforms is given. Section 4 display the method's results, followed by a discussion of the research in section 5. Finally, section 6 includes the conclusion and forward-looking considerations.

2. PRELIMINARIES

This section offers theoretical information on the telemedicine platform and the usage of chaotic cryptography to protect telemedicine networks using a lightweight cryptographic approach to the IoT using a lightweight cryptographic approach to the IoT. As an asymmetric encryption method, Diffie-Hellman (DH) is an excellent choice for securing telemedicine networks. In addition, the asymmetric key strategy (public key + private key) is difficult-to-guess data encryption to realize the benefits of decentralization in terms of cybercrime defense. To ensure that the session between the therapist and the patient is simultaneously secured, DH and lightweight anarchic cipher must collaborate.

2.1. Lightweight cryptography in IoT architecture layers

The application layer, the data processing layer, the network layer, and the sensor layer are four layers of the IoT architecture, as shown in Figure 2. The network layer might consist of Wi-Fi, Bluetooth, and other technologies. The data processing layer is the layer that contains all of the files. The application layer is the layer in which user interface decisions are decided. In a common computing environment, lightweight encryption is mostly utilized in the sensor layer, which users use to collect medical data or provide doctor instructions. It's referred to as the IoT or intelligent object networks (IoN). A large number of limited internet-connected gadgets engage with one another over the network. The network nodes are critical because if one of them is hacked, the entire network might be jeopardized. However, implementing suitable encryption techniques is difficult. Consequently, there are various vulnerabilities in the network that may be attacked. Actual side tunnel attack, encrypt analysis attack, software layer attack, Internet violent attack where the number of IoT apps increases the quantity of raw data created, and attacks that influence security are all possible categories. As the internet of things expands into critical sectors such as telemedicine and financial security, the need for lightweight cryptography will grow. Lightweight cryptography is an encryption algorithm or protocol designed to be implemented in restricted environments for instance sensor networks, healthcare IoT, radio frequency definitions. IoT applications are more vulnerable to security threats. The Internet of Things and its applications are complex and dynamic, which introduces new kinds of security concerns. IoT applications require a method in the network layer to robust the lightweight sensor layer method for data chaos to achieve secure end-to-end connections, yielding integrated security in IoT components. The Diffie Hellman hypothesis has been suggested within the umbrella of cybersecurity to avoid security attacks on the network layer [19].

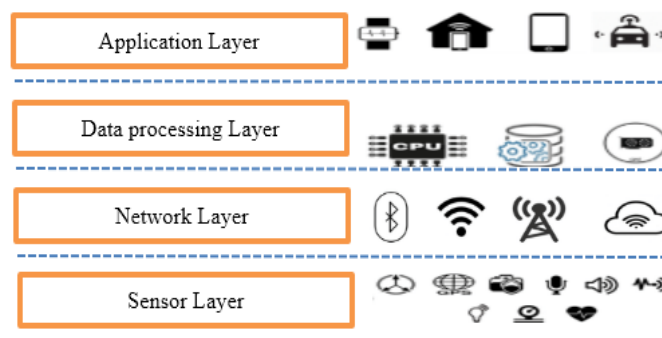


Figure 2. IoT architecture (layers and components)

2.2. Diffie Hellman method

Diffie-Hellman algorithm has been emergent by Whitfield Diffie and Martin Hellman. It's also known as one trap key exchange method or key agreement algorithm, in 1976. DH is used to produce the asymmetric cryptographic key at both the doctor and the patient, avoiding the need to transfer the key from one to the other. Notice that the DH technique is only used for key exchange, not for message encryption or decryption. If the doctor and patient want to communicate, they must first agree on a common key established using the DH method, which they may then use for encryption or decryption by lightweight encryption [20]-[25]. Figure 3 illustrates the Diffie Hellman key exchange algorithm for the Internet of Health Things (IoHT). First of all, the doctor generates a random private key. Inside the doctor's terminal, a doctor's public key is calculated from the doctor's private key. The doctor's private key is kept on the doctor's terminal side, and the doctor-generated public key is sent to the patient's terminal side. The same security procedure achieved in the patient side terminal simultaneously. Pair private and generated public keys represent the Diffie Hellman security scheme.

DH algorithm steps: if doctor and patient decide to communicate with each other through a telemedicine platform:

- 1) Choose two prime integers p and q ($q < p$).
- 2) On the doctor side, the doctor-private key as a random integer value X_A needs to generate, and from this private key the doctor-public key Y_A is calculated as shown in (1).
- 3) The doctor-public key Y_A is sent from the doctor terminal to the patient terminal on another side of the telemedicine platform.
- 4) The patient chooses another random patient-private key X_B independently as an integer value and calculates patient-public key Y_B as shown in (2).
- 5) patient terminal sends the doctor terminal the patient-public key Y_B .
- 6) The doctor terminal is utilized now to calculate the doctor-secret key A_K from (3).
- 7) The patient terminal side calculates patient-secret key B_K using (4).
- 8) In case that the doctor-secret key A_K equals the patient-secret key B_K , then the key agreement method allows doctor and patient to communicate.

$$Y_A = q^{X_A} \text{ mod } p \quad (1)$$

$$Y_B = q^{X_B} \text{ mod } p \quad (2)$$

$$A_K = (Y_B)^{X_A} \text{ mod } p \quad (3)$$

$$B_K = (Y_A)^{X_B} \text{ mod } p \quad (4)$$

Where, $\forall X_A$ and $X_B < q$.

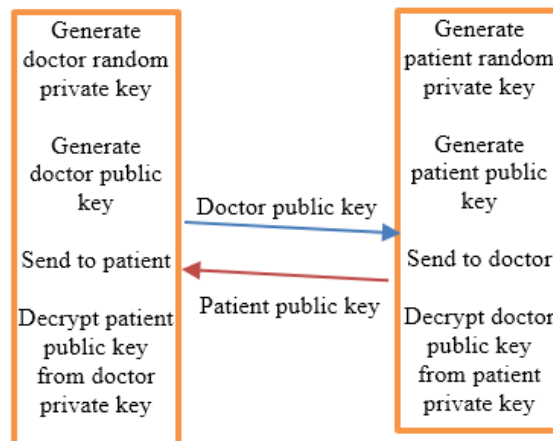


Figure 3. Diffie Hellman key exchange algorithm

3. SECURITY SCHEME IMPLEMENTATION

3.1. Crypto system based chaotic lightweight IoT insight

The chaotic lightweight IoT has been chosen to solve the obstacles of securing the variety of devices in IoT based on IoT security protocol. Since there is an urgent need to deal with different types of sensors and actuators. The suggested secure telemedicine platform is content from the following parts, as shown in Figure 4.

- 1) Patient block: in this block, the patient sends his medical questions as plain text to the telemedicine platform without encryption.
- 2) Acquisition of clinical signal: in this block, the biosensors and benchmarks in the patient body have been calculated and sent for the telemedicine platform.
- 3) Application block: this block represents the interface between the patient and telemedicine platform.
- 4) Private-key block: the block represents the initiation of calculation of public key to send.
- 5) DH block: this block represents the 'protection method used to secure the chaotic data.
- 6) Network layer block: in general, the chaotic lightweight devices can be in the sensor layer of IoT protocol which does not protect the system as expected. For that reason, the paper suggests the DH method on the previous layer (network layer) to ensure secure data.

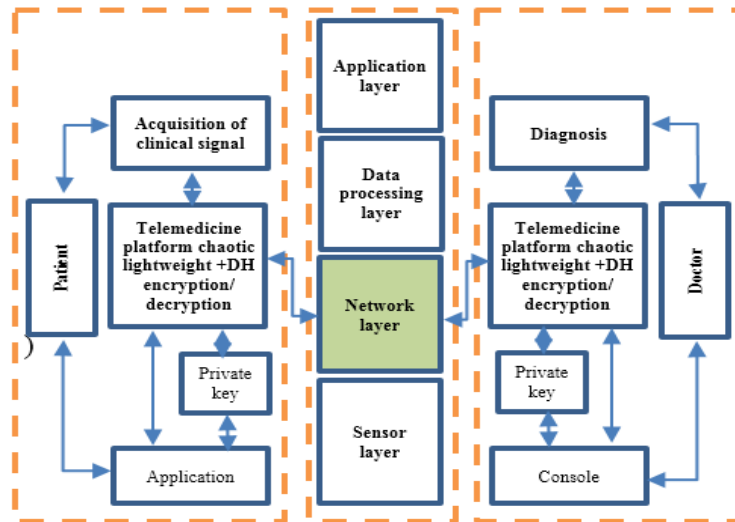


Figure 4. Telemedicine communication architecture: suggested design with data security

3.2. DH implementation

The implementation scenario starts with activating DH on signals of sensors, or in other terms on the chaotic lightweight of IoT. The handshake strategy for the secret key exchange of DH has shown in Figure 5. Doctor and patient choose initial information as shown in Table 1. After operands are initiated, and the random private key has been added to the public-key equation’s calculation. On the doctor and patient sides, the public key is ready to compute using the private key and standard operands. For another side handshake, the public key has been provided.

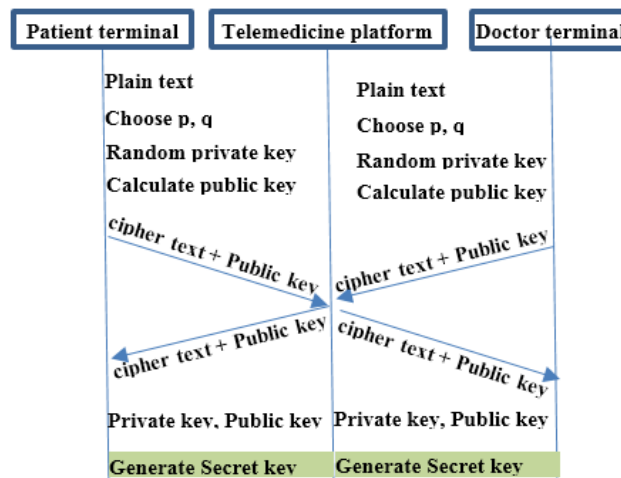


Figure 5. Diffie Hellman key exchange implementation

4. RESULTS

The use of chaotic lightweight IoT in conjunction with DH enhances security, making it hard to compromise the secure telemedicine platform. The (1)–(4) is used to calculate the secret keys on either side. $P = 213, 340, 506, 421, q = 324, 230, 744, 175$ and private key = 130, 150, 170, 190, 140, 160, 180, 200. The secure session between the doctor and the patient on the telemedicine platform is formed after 4000 iterations. The private keys of the doctor and the patient have been chosen to be un similar, as well as no one know the owner’s private keys. According to the rules of the method, the private key must be integer positive number. About the public key, each terminal side can send one general public key calculated from each side private key and can be extracted by the aid of private key of another side. Finally, only the doctor and the patient have access to the data in case they have the appropriate related private key indicated in the information of Table 1.

Table 1. By employing the chaotic lightweight of IoT with DH method: a random test is performed to confirm that a secure session is established

		Test 1	Test 2	Test 3	Test 4
Doctor side	Doctor private key	130	150	170	190
	p	213	340	506	421
	q	325	230	744	175
	Doctor public key	3851	2235	3285	791
Patient side	Patient private key	140	160	180	200
	p	213	340	506	421
	q	325	230	744	175
	Patient public key	3219	809	2750	1186
	Secret key in doctor side	2070	3419	2216	3840
	Secret key in patient side	2070	3419	2216	3840

5. DISCUSSION

The security of the IoT protocol's chaotic lightweight sensor layer is a crucial vision of secure telemedicine. In order to build the suggested platform, we will require a variety of elements, hardware elements (sensors, actuators, terminals, and network), and software (Java, Linux, Windows for terminal) elements are required. To ensure that IoT sensor data is more secure and avoid various cyberattacks, a Diffie Hellman algorithm is built and tested. The suggested methods' findings are provided in Table 2, which compares the key size of the proposed DH algorithm to another similar algorithm (NIST test). Because of the key size, asymmetric cryptography with the DH method is used in this study. Shorter key connections are required for a given degree of security, requiring less memory and processing to perform the suggested protocol. For telemedicine systems to gain additional time, this is an essential factor. Two crucial elements are revealed through the notice and comparison of the size of encryption keys for Rivest-Shamir-Adleman (RSA) standard method versus DH on various encryption settings. The DH keys are considerably shorter and the percentage increase in security level for DH is lower Table 2 shows that.

Table 2. A comparison of two protocols' key sizes and growing key ratios

Title	Level 1	Level 2	Level 3
Security level (bit)	64	128	256
RSA key size (bit)	1024	3072	15360
DH key size (bit)	160	256	521
RSA/DH key increase ratio	6%	12%	30%

From the foregoing, it is clear that DH is better suited to securing the telemedicine platform. It is essential to consider the protective measures to estimate security. First and foremost, it is demonstrated that the system is protected by four keys: one pair of private keys and one pair of public keys. The private keys must be integer numbers. No one knows the DH algorithm's secret key. A private key is a random number from which it is difficult to predict or extract any information. The public key is broadcast over the network, but it is meaningless unless the private key can be extracted. The secret key calculated on either side is consistent across all attempts and is a random value that no one can predict.

6. CONCLUSION

The secure telemedicine issue is still in the early stage, and existing security methods are still limited to minimal protection. The chaotic lightweight approach of emerging technologies should be employed as an urgent solution for this aspect. The target of the study is to use the DH method applied on chaotic lightweight IoT networks to communicate securely between the doctor console and the interactive patient application. This study also discusses the development and security evaluation of the IoMT and telemedicine. The DH key exchange protocol and existing telemedicine security measures are also investigated. Finally, DH has been integrated effectively into chaotic IoT for the telemedicine platform. Java structural language was used to write the code. Java software language is capable of bridging the gap between software and hardware. In any scenario, telemedicine is inherently dangerous and should not be performed without remote securing the channel between the doctor and patient. Protection should be expanded in a future study to examine the flexibility of having many doctors and nurses participate in the same session.




ACKNOWLEDGMENTS

The authors are thankful to the anonymous referees' editor in advance for their recommendations, which will contribute surly to improving the substance of this paper.




REFERENCES

- [1] F. Masood *et al.*, "A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations," *Wireless Personal Communications*, 2021, doi: 10.1007/s11277-021-08584-z.
- [2] R. Hedayati and S. Mostafavi, "A Lightweight Image Encryption Algorithm for Secure Communications in Multimedia Internet of Things," *Wireless Personal Communications*, pp. 1121-1143, 2021, doi: 10.1007/s11277-021-09173-w.
- [3] A. Aslam and E. Curry, "Towards a Generalized Approach for Deep Neural Network Based Event Processing for the Internet of Multimedia Things," *IEEE Access*, vol. 6, pp. 25573-25587, 2018, doi: 10.1109/access.2018.2823590.
- [4] L. M. H. Yepdia and A. Tiedeu, "Secure Transmission of Medical Image for Telemedicine," *Sensing and Imaging*, vol. 22, no. 17, Dec. 2021, doi: 10.1007/s11220-021-00340-8.
- [5] E. Rayachoti, S. Tirumalasetty, and S. C. Prathipati, "SLT based watermarking system for secure telemedicine," *Cluster Computing*, vol. 23, no. 4, pp. 3175-3184, 2020, doi: 10.1007/s10586-020-03078-2.
- [6] H. K. Hoomod, J. R. Naif, and I. S. Ahmed, "A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 8, no. 4, pp. 2333-2345, 2020. [Online]. Available: <http://pen.ius.edu.ba/index.php/pen/article/view/1738/714>
- [7] S. Agarwal, "Secure image transmission using fractal and 2D-chaotic map," *Journal of Imaging*, vol. 4, no. 1, 2018, doi: 10.3390/jimaging4010017.
- [8] A. Neupane, A. Alsadoon, P. W. C. Prasad, R. S. Ali, and S. Haddad, "A novel Modified Chaotic Simplified Advanced Encryption System (MCS-AES): mixed reality for a secure surgical tele-presence," *Multimedia Tools Application*, vol. 79, no. 39, pp. 29043-29067, 2020, doi: 10.1007/s11042-020-09478-1.
- [9] M. K. M. Al-shammari and G. T. Han, "Improve Memory for Alzheimer Patient by Employing Mind Wave on Virtual Reality with Deep Learning," *Advances in Intelligent Systems and Computing*, pp. 412-419, 2018, doi: 10.1007/978-3-319-93554-6_39.
- [10] O. Alesawy and R. C. Muniyandi, "Elliptic Curve Diffie-Hellman Random Keys Using Artificial Neural Network and Genetic Algorithm for Secure Data over Private Cloud," *Information Technology Journal*, vol. 15, no. 3, pp. 77-83, 2016, doi: 10.3923/itj.2016.77.83.
- [11] B. A. Alzahrani, A. Irshad, K. Alsubhi, and A. Albeshri, "A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT," *International Journal of Communication Systems*, vol. 33, no. 11, 2020, doi: 10.1002/dac.4423.
- [12] Z. A. Jaaz, I. Y. Khudhair, H. S. Mehdy, and I. Al-Barazanchi, "Imparting Full-Duplex Wireless Cellular Communication in 5G Network Using Apache Spark Engine," *2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2021, pp. 123-129, doi: 10.23919/EECSI53397.2021.9624283.
- [13] Y. Yang, X. Niu, L. Li, and H. Peng, "A Secure and Efficient Transmission Method in Connected Vehicular Cloud Computing," *IEEE Network*, vol. 32, no. 3, pp. 14-19, 2018, doi: 10.1109/mnet.2018.1700324.
- [14] H. M. Mohammad and A. A. Abdullah, "Enhancement process of AES: a lightweight cryptography algorithm-AES for constrained devices," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 20, no. 3, pp. 551-560, 2022. doi: 10.12928/telkomnika.v20i3.23297
- [15] A. D. Algarni, N. F. Soliman, H. A. Abdallah, and F. E. Abd El-Samie, "Encryption of ECG signals for telemedicine applications," *Multimedia Tools and Applications*, vol. 80, pp. 10679-10703, 2021, doi: 10.1007/s11042-020-09369-5.
- [16] S. Q. Salih, A. R. A. Alsewari, and Z. M. Yaseen, "Pressure vessel design simulation: Implementing of multi-swarm particle swarm optimization," *ICSCA '19: Proceedings of the 2019 8th International Conference on Software and Computer Applications*, 2019, pp. 120-124, doi: 10.1145/3316615.3316643.
- [17] Y. Li, P. Zhang, and R. Huang, "Lightweight quantum encryption for secure transmission of power data in smart grid," *IEEE Access*, vol. 7, pp. 36285-36293, 2019, doi: 10.1109/access.2019.2893056.
- [18] I. Al-Barazanchi *et al.*, "Blockchain: The Next Direction of Digital Payment in Drug Purchase," *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2022, pp. 1-7, doi: 10.1109/HORA55278.2022.9799993.
- [19] S. S. Hameed, H. R. Abdulshaheed, Z. L. Ali, and H. M. Ghenni, "Implement DNN technology by using wireless sensor network system based on IOT applications," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 10, no. 2, pp. 128-137, 2022, doi: 10.21533/pen.v10i2.2831.
- [20] H. R. Abdulshaheed, H. H. Abbas, E. Q. Ahmed, and I. Al-Barazanchi, "Big Data Analytics for Large Scale Wireless Body Area Networks; Challenges, and Applications," *IRICT 2021: Advances on Intelligent Informatics and Computing*, 2022, pp. 423-434, doi: 10.1007/978-3-030-98741-1_35.
- [21] A. S. Sani, D. Yuan, P. L. Yeoh, W. Bao, S. Chen, and B. Vucetic, "A Lightweight Security and Privacy-Enhancing Key Establishment for Internet of Things Applications," *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1-6, doi: 10.1109/icc.2018.8422725.
- [22] T. Manjula and B. Anand, "Retraction Note to: A secured multiplicative Diffie Hellman key exchange routing approach for mobile ad hoc network," *Journal of Ambient Intelligence and Humanized Computing*, 2022, doi: 10.1007/s12652-022-04017-2.
- [23] Y. K. Salih, O. H. See, S. Yussof, A. Iqbal, and S. Q. M. Salih, "A proactive fuzzy-guided link labeling algorithm based on MIH framework in heterogeneous wireless networks," *Wireless Personal Communications*, vol. 75, no. 4, pp. 2495-2511, 2014, doi: 10.1007/s11277-013-1479.
- [24] I. Al-Barazanchi, S. A. Hamid, R. A. Abdulrahman, and H. R. Abdulshaheed, "Automated telemedicine and diagnosis system (ATDS) in diagnosing ailments and prescribing drugs," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 7, no. 2, pp. 888-894, 2019, doi: 10.21533/pen.v7i2.486.
- [25] S. R. A. Ahmed, I. Al-Barazanchi, A. Mhana, and H. R. Abdulshaheed, "Lung cancer classification using data mining and supervised learning algorithms on multi-dimensional data set," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 7, no. 2, pp. 438-447, 2019, doi: 10.21533/pen.v7i2.483.




BIOGRAPHIES OF AUTHORS

Israa Ezzat Salem    received her Bachelor of Computer Science from College of Science Al-Nahrain University 1997-1998. Master's degree in Computer Science/ College of Science/ Al-Nahrain University 2000-2001. She is a lecturer in Computer Engineering Techniques Department. published many researchs and supervising many graduation projects for fourth-year students. Work in many committees formed by the department and the college, including the examination committee. She can be contacted at email: israa.ezzat@baghdadcollege.edu.iq.



Haider Rasheed Abdulshaheed    received his Bachelor of Computer Science (BCS) from Department of Computer Science, Baghdad college of economic science university-Iraq-Baghdad in June 2002. In January 2003, he entered the Master of Science program at the faculty - Information Technology, Graduate University of Technology, Baghdad -Iraq. He is Currently a student Doctor of Philosophy in Information and Communication Technology. He is a lecturer in Computer Engineering Techniques Department. Member in many conferences panel and communications events. He is the author of more than 42 research articles published in reputed journals. He is a Reviewer of various high impact factor journals. His research activities are neural networks, image processing, WSN, WiMAX, WiFi on Vehicular Ad-Hoc Networks (VANETs), Communications, Networking, Signal Processing, IOT, Smart Systems, Blockchain. He can be contacted at email: haider_rasheed@baghdadcollege.edu.iq.



Hassan Muwafaq Ghani    Received his Bachelor (B.Sc) of Electrical & Electronic Engineering from Department of Electrical Engineering, Babylon university-Iraq-hilla in June 2016. In February 2018, he entered the master's program at the Faculty of Electrical and Electronic Engineer, Universiti Tun Hussein Malaysia. He is a lecturer at Al-Mustaqbal university college/ Department of Computer Techniques Engineering His research interest is optical communication, IoT, Wireless sensor Network, Communications, V2V system, Artificial intelligent. He can be contacted at email: hasan.muwafaq@mustaqbal-college.edu.iq.