Multi Channel Data Encryption Transmission Algorithm of Medical Internet of Things Based on Improved MQTT Protocol

Hai-bo Zhang[1(✉)], Xiu-juan Duan[2], and Jian-mei Sun[1]

[1] Dalian University of Science and Technology, Dalian 116011, China
jhjsdf89@163.com

[2] Financial Department, College of Humanities and Information, Changchun University of Technology, Changchun 130122, China

Abstract. Since the concept of the Internet of things was put forward, it has attracted the attention of all countries in the world, and has become a technology developed by all countries and organizations in the world. With the development of Internet of things technology and application, information sharing is realized between things on the Internet of things, so the safe transmission of data becomes particularly important. The mainstream MQTT (Message Queuing Telemetry Transport) protocol has obvious advantages in the application of Internet of things network communication, but the protocol has a very big defect, its data transmission default is not encrypted, unable to guarantee the security of data. To solve this problem, this paper analyzes the security of the Internet of things, improves the MQTT protocol, and obtains a new multi-channel data encryption transmission algorithm of the Internet of things.

Keyword: Internet of Things · Multi channel data · MQTT protocol · Encrypted transmission

1 Introduction

The core of the Internet of things is to realize the information sharing between things, and data transmission, as the core technology to realize the communication between things, naturally becomes the research hotspot of the Internet of things technology. As a key element in the process of data transmission, data transmission protocol has been concerned by researchers from all walks of life in the development of Internet of things technology [1, 2]. With the continuous development of the research work of Internet of things in recent years, the big companies in the IT industry and related research institutions have developed network communication protocols suitable for the Internet of things environment. Among them, MQTT protocol has obvious advantages in the application of Internet of things network communication. It optimizes the application situation of Internet of things equipment resources and unstable network environment, which makes it low cost, high reliability and can effectively reduce the flow and power

S. Wang et al. (Eds.): IoTCare 2021, LNICST 415, pp. 171–182, 2022.
https://doi.org/10.1007/978-3-030-94182-6_13

consumption of terminal devices. At present, the application research of MQTT protocol at home and abroad mainly focuses on the message transmission of Internet of things, but MQTT protocol has a very big defect. Its data transmission is not encrypted by default and the data security can not be guaranteed. Therefore, based on the improved MQTT protocol, a new encryption algorithm is proposed for the multi-channel data of the medical Internet of things, so as to realize the data security transmission of the Internet of things.

2 Security Analysis of Internet of Things

In recent years, the Internet of things has made a breakthrough, and many applications based on the Internet of things have gradually emerged, bringing convenience to people's lives. At the same time, the security problems of the Internet of things are gradually highlighted. Whether the security problem of the Internet of things can be effectively solved is directly related to whether the Internet of things can be applied on a large scale. This paper first introduces the hierarchical model of the Internet of things, and then analyzes the security problems of the Internet of things and the security mechanisms that can be used [3, 4].

"Overview of the Internet of things" standard puts forward the reference model of the Internet of things. From bottom to top, it can be divided into four layers, namely perception layer, network layer, service layer, application support layer (processing layer) and application layer. Each layer has corresponding security and management functions. The reference model of Internet of things is shown in Fig. 1.

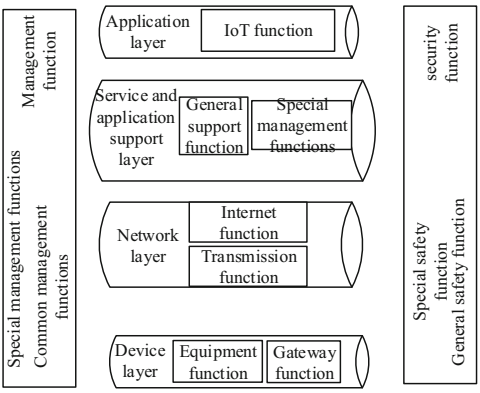

Fig. 1. Reference model of Internet of things

According to Fig. 1, we can see the security problem analysis and security mechanism of each layer of the Internet of things. The main function of the perception layer is to realize comprehensive perception through the sensor, and gather the collected data through the access gateway. At the same time, it can also receive the instructions from the

control end to control the goods. Because the sensing node is usually in an unsupervised, open and complex environment, the single function and limited processing capacity of the node make it impossible to take complex security measures, and the information collected by the node is transmitted through the wireless network. Therefore, nodes are vulnerable to physical damage, impersonation attack and denial of service attack, and sensing information is easy to be eavesdropped, tampered and replayed in the process of transmission. The above problems can be solved by cryptographic technology, high-speed cryptographic chip, PKI public key infrastructure, information method security management platform and other security technologies, but it is difficult to find a lightweight, secure and general security mechanism [5–7]. The network layer mainly realizes the goods information transmission and transmission management. In addition to the security problems of the existing communication network, the network layer also has its particularity.

The Internet of things is a kind of network which is integrated with various heterogeneous networks. There are many ways to access the core network. Therefore, it involves a large number of heterogeneous networks interconnection and cross domain security encryption. Because of the large number of nodes in the network, a large number of data transmission at the same time can easily lead to network congestion and denial of service. These problems can be guaranteed by firewall, secure routing, virtual private network and other security technologies. However, the existing security mechanism is designed from the perspective of human to human communication, which can not be directly used for the communication between machines. Using the existing security mechanism may split the logical relationship between machines in the Internet of things [8–10]. The processing layer is mainly to intelligently analyze and process the information transmitted from the network layer to form a variety of Internet of things applications, and establish an efficient, reliable and reliable business support platform for the application layer [11, 12]. Its security problem mainly comes from the intelligent data processing process, because a large number of terminals in the Internet of things produce massive data transmission in the network. Therefore, only by using intelligent processing technology can these data be identified and analyzed in time, otherwise it may lead to network connection interruption and data loss. However, if the intelligent processing technology is out of control or exploited by attackers, it may make the intelligence become low-energy and the automatic processing fail, resulting in catastrophic damage. To solve these problems, we can use attack detection, virus prevention, content analysis, access control and other technologies to protect. Application layer is a level of information interaction with users directly, which provides users with diversified applications. As the application of Internet of things involves many aspects of users' lives, once the information is disclosed, the personal privacy, property, trade secrets and other information of users may be violated. Therefore, we need a sound identity encryption and access control mechanism to isolate illegal users or unauthorized users from accessing the service, so as to ensure the user's privacy information and application security [13, 14].

From the above analysis of the functions and security problems of the reference model of the Internet of things, it can be seen that the layers of the Internet of things cannot directly correspond to the levels in the Internet OSI reference model. For example, the main function of the perception layer is the overall perception of information. In

this process, it may involve all seven layer protocols of the Internet. Therefore, the traditional security protocols, such as IPSec Protocol in OSI network layer and ssl/tls protocol in transmission layer, cannot be directly applied to the Internet of things to realize the end-to-end data security transmission. The technologies that the security mechanisms available at the above layers depend on are essentially encryption and encryption technologies [15, 16]. Therefore, this paper introduces the MQTT protocol to realize the encryption of multi-channel data of Internet of things.

3 Multi Channel Data Encryption Transmission Algorithm in Internet of Things

3.1 MQTT Protocol

MQTT protocol is a message transmission protocol based on message publishing / topic subscription model, which uses client / server architecture to communicate. The design follows the principle of simple, open and lightweight, and is suitable for the application environment of Internet of things with unstable network environment, low bandwidth and limited equipment resources. The main features include.

(1) The topic based message subscription / publication mode can easily realize one to many message distribution and transmission, and decouple the communication publisher and subscriber;
(2) When MQTT message is transmitted in the network, its load content is shielded and can be used to transmit various types of messages.
(3) Provides three levels of message delivery quality: at least once, at least once, and exactly once. Message publishers and subscribers can make messages reach the destination on demand according to the actual transmission needs.
(4) The overhead of the protocol is small, the fixed header is only 2 bytes, the protocol exchange is minimized, and the network traffic is saved.
(5) Last will (also known as Testament) mechanism is provided. When the client is disconnected abnormally, the server will inform the relevant terminal.

MQTT publishes and subscribes messages based on topics, and uses topics to establish message transmission channels between publishers and subscribers. Topic refers to a label attached to an application message. MQTT consists of MQTT message proxy server and MQTT client. Figure 2 shows the structure of MQTT.

According to Fig. 2, the MQTT client refers to the program or device using MQTT, which can be either a publisher or a subscriber. Publishers can publish application messages to the message broker, and subscribers can subscribe to the message broker to receive interested application messages or unsubscribe. As the intermediary between sending message client and request subscription message client, MQTT message proxy server receives connection request from client and application message published by client, processes subscription and unsubscribe request of client, and forwards application message to qualified subscribed client [17, 18].

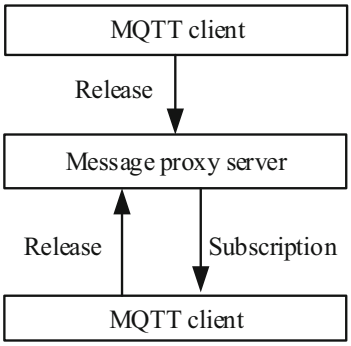

Fig. 2. MQTT structure

3.2 Encryption Transmission Algorithm

Encryption technology refers to the use of cryptographic algorithm to encrypt the data plaintext and then transmit it to the destination, and then restore the ciphertext to plaintext by corresponding means. Symmetric encryption algorithm is also known as the traditional encryption algorithm or single key encryption algorithm. Its encryption / decryption key is the same, or the decryption key can be derived from the encryption key. It requires the sender and receiver to negotiate a key before secure communication. The security of symmetric encryption algorithm depends on the key, and revealing the key means that anyone can encrypt / decrypt the message. The encryption and decryption of symmetric encryption algorithm are expressed as: encryption algorithm C = EK (m), decryption algorithm m = DK (c) K. The typical symmetric encryption method is shown in Fig. 3.

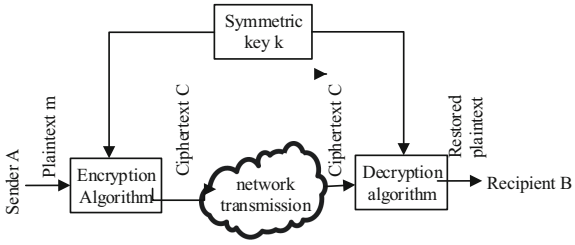

Fig. 3. Symmetrical cipher

According to Fig. 3, the advantages of symmetric encryption algorithm are fast algorithm speed, low requirements for physical devices and high encryption efficiency. The disadvantage is that both sides of the communication use the same key, the security is not high, and it is difficult to solve the problem of signature encryption and non repudiation.

And the key must be distributed through the secure channel. With the expansion of the network scale and the increase of the key quantity, the security management, distribution and transmission of the key are very difficult. This paper uses Rijndael encryption method, which is a new generation of data encryption standard designed by the National Institute of standards and technology to replace des. The standard has been widely used to replace des which used 56 bit key. AES is a symmetric encryption algorithm based on packet, which requires 128 bits of packet length. The key length can be 128 bits, 192 bits or 256 bits according to the actual application requirements. Comparatively speaking, the 128 bit key of AES is 1021 times stronger than the 56 bit key of Des. The algorithm mainly includes round number, round change and key expansion [19, 20]. The number of rounds represents the number of rounds to transform an input packet. The relationship between the number of rounds and the key length is shown in Table 1.

Table 1. Relationship between number of rounds and key length

AES type	Key length/byte	Group size/byte	Number of turns/time
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

According to Table 1, each round of transformation in the encryption process consists of four different transformations: S-box transformation (nonlinear transformation), row transformation, column transformation and key addition layer (XOR operation with extended key). But the last round transformation does not include the column transformation. Each round transformation requires an extended key with the same length as the input packet. Because the length of the external input key is limited, it is necessary to expand it into a longer bit string to generate the encryption key of each round.

The specific steps of encryption are as follows.

(1) Copy the input group to the 4 × 4 byte State data group.
(2) XOR the first round key of the state.
(3) The state data set is replaced by nonlinear S-box.
(4) Transform the state.
(5) Column blending operation on State.
(6) XOR the next wheel key with the state (key adding layer), and repeat step 3 until all wheel transformations are completed.;
(7) Copy the State to the output matrix.

Due to the limited processing capacity of IOT terminals, complex encryption algorithms cannot be used. But the Internet of things environment is complex. To ensure the security of communication, simple encryption algorithms can not be achieved. To solve

this problem, this paper combines symmetric encryption algorithm with multi-channel transmission. The advantages of simple calculation and high efficiency are obtained by using symmetric encryption algorithm. As well as the multi-channel transmission data fragmentation makes it more difficult to eavesdrop on the complete ciphertext and crack and recover the plaintext, which reduces the complexity of operation while ensuring the security. After the two sides negotiate the correct key KAB, the sender will use the key KAB to encrypt the original message symmetrically. Then the encrypted message is divided. And add the corresponding identification (session number, fast identification) and message password, and then multiplex. After the message is sent to the receiver, the message is reorganized and decrypted according to the identification of the data block to get the initial message plaintext.

Multi-channel data encryption is a form of encryption, which can make people still get the result of ciphertext when they operate ciphertext, and the result of ciphertext decryption is the same as that of plaintext operation. For people, this technology is correct when retrieving and comparing data, but it is not necessary to decrypt data in the whole process. The previous multi-channel data encryption technology starts from the process of data coding and compression. There are many parameters in the process of data coding, such as I-frame data, P-frame data, And frame macro block, DCT coefficient and other related parameters. Through the analysis of the coding process, the parameters which have a great influence in the coding process are encrypted to achieve the total content of encrypted data and ensure the security effect. The encryption technology of dynamic data is similar to multimedia encryption technology, which is also based on the analysis of encrypted data. Because in many applications need to use uncompressed data, this kind of data without complex coding, so can not use multimedia encryption. However, compared with the general compressed data, the length of the data is much more than that of the latter. Therefore, in order to distinguish the different importance, then the application of dynamic encryption technology is more meaningful.

This paper uses the homomorphic public key encryption function to analyze and select the encrypted data transmitted and stored between nodes in the blockchain, so as to ensure the security of dynamic data in transmission and storage. The concept of blockchain is added to the existing dynamic data encryption method, and the dynamic data is stored distributed by using nodes in the blockchain. In each blockchain node, it is relatively high to allocate independent computing units to deal with homomorphic encryption or decryption. First, dynamic data encryption request is made on a blockchain network. After a series of operations, the request is responded and implemented.

Dynamic data encryption refers to the homomorphic encryption calculation of the collected original data. Multi channel data encryption is a way to calculate data encryption. The data encryption is realized by algebraic calculation and algebra operation on the same plaintext. The process of homomorphic encryption is: set the same station encryption process as JK, known homomorphic encryption process is composed of generating key, data encryption, decryption and data evaluation, set the generated key as KG, encryption process as ENC, decryption process as Dec, evaluation as Eval. Then we can get the formula.

$$\mathrm{JK} = (\mathrm{KG}, \mathrm{Enc}, \mathrm{Dec}, \mathrm{Eval}) \tag{1}$$

Let the public key AK generate the corresponding security parameter o in the private key BK. AK is used to encrypt plaintext and BK to decrypt ciphertext. Set plaintext Z $\in Q_n$, where n is an integer. Homomorphic encryption of Z can be expressed as.

$$W_{cd}(v_1 + v_2) = W_{cd}(v_1) \oplus W_{cd}(v_2) W_{cd}(fv_1) = f \odot W_{cd}(v_1) \tag{2}$$

After the formula for data encryption transmission, after the transmission of data confidentiality process. If the decryption process is set to Dec, the formula can be obtained.

$$u = \mathrm{Dec}(E, AK) \tag{3}$$

Finally, the decryption results are evaluated to complete the calculation process. The specific formula is as follows.

$$P = \mathrm{Eval}(T, i, E) \tag{4}$$

Through the above process, the results of homomorphic encryption of data are substituted into the block structure, so as to realize the data security transmission. This method encrypts and stores dynamic data homomorphically based on blockchain technology, and points out that the operation of dynamic data on blockchain is permanently saved. These dynamic data are stored in a node participating in encryption operation by the blockchain, and all nodes constitute a distributed database method of dynamic data. In other words, any node that is damaged can be verified by hash node. At the same time, it can be stored in the database and interpreted to realize the encryption operation.

The data processing process described above is shown in Fig. 4.

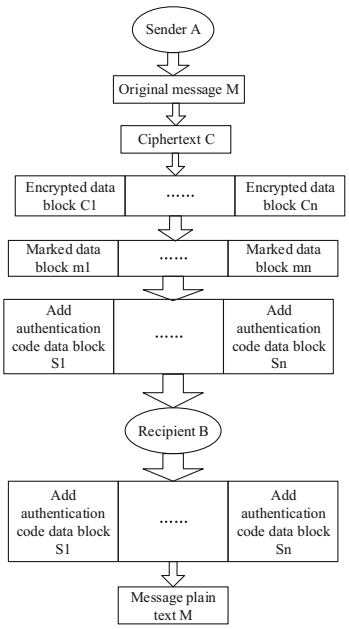

Fig. 4. Data processing process of both sender and receiver

According to Fig. 4, the biggest difference between the data encryption method used in this paper and the traditional encryption method is the use of multi-channel transmission technology. The encrypted message is divided and transmitted through multiple paths at the same time. The conventional encryption method is to encrypt the whole plaintext and transmit the whole plaintext through a single path, so as long as the attacker intercepts the data on the path, it will be easier to crack the message plaintext because of the large amount of information. The encryption and multiplex method mentioned in the section make the eavesdropper intercept a certain block of information from it is small and difficult to break the original. Moreover, the difficulty of eavesdropping is greatly increased by multiplex transmission. Compared with the traditional one-way transmission encryption method, the encryption and decryption process of the method are not different. Only the packet segmentation, reorganization and signature verification are added. This is acceptable compared with the high-intensity encryption and decryption algorithm.

4 Experiment and Result Analysis

In order to analyze the experimental performance directly, the simulation experiment in Matlab environment, the original data are transmitted, and the visualization experimental data results are obtained by using different algorithms. In addition, in order to standardize the experiment, this paper integrates C language program in the process of implementing the algorithm, and improves the function of computer language expression. In addition, the experimental conditions need to be set. The length of encrypted bit sequence is 1200, the time of medical sensitive information sampling is 200 s, and the training set size is 24. The author obtains medical information from medical database. In this experiment, 2170 data were extracted from the above data set by healthdata data set (healthdata.gov), adni. long. usc. edu, drive data set (www.isi.uu.nl/research/databases/drive/download.php), oasis data set (www.oasisbrains.ORG).

4.1 Comparison of Anti Attack Performance of Encryption

In order to verify the effectiveness of the method, the comparative experiment was set. The reference [3] method (a secure framework for authentication and encryption using improved ECC for IOT based medical sensor data) is used as the traditional method. The experimental results are shown in Table 2.

The experimental results show that, compared with the general data encryption, the general data encryption aims at the security of data storage and transmission, that is, the data owner must encrypt the data before continuing to operate. Moreover, it is impossible for the user without the key to decrypt the data and obtain the basic information about the original data. Only the key user can decrypt the data. In the whole process, the user can not decrypt the data, but can only transmit and store the data. If the user forcibly decrypts the data, it may lead to decryption error or decryption failure. Homomorphic encryption focuses on the security of data processing, mainly providing the encryption processing function of data, which means that non key users will not disclose data information when decrypting data. At the same time, the owner of the key can decrypt the data and get the result of the same state encryption.

Table 2. Experimental results of encryption delay

Iterations	Method of this paper/s	Traditional method/s
100	0.921	0.812
200	0.943	0.824
300	0.957	0.835
400	0.975	0.857
500	0.986	0.861

4.2 Comparison of Encryption Delay

For further encryption, the experimental results are shown in Table 3.

Table 3. Experimental results of encryption delay

Experiment times/time	Encryption delay/s	
	Traditional method	Method of this paper
1	1.5	0.3
2	1.8	0.2
3	1.7	0.4
4	1.6	0.3
5	1.4	0.5
6	1.3	0.4
7	1.4	0.5
8	1.6	0.3
9	1.7	0.4
10	1.5	0.2

According to the above experimental results, the encryption method in this paper works better. In this paper, the design of the power Internet of things encryption communication encryption method uses the AIE mode, the power Internet of things communication information encryption method to reduce the impact of network connectivity. Encrypting the communication data between the wireless network devices of power Internet of things makes the encryption method more defensive.

In addition, the design of encryption key reduces the network connectivity and the complexity of the key of the power Internet of things, and the memory occupied by the encryption method of encryption communication is significantly improved due to the

reduction of the complexity of the key. Therefore, it greatly reduces the power consumption of Internet of things encryption communication encryption methods, and improves the work efficiency of network information encryption. The power circuit, communicator and encryptor are designed in this paper. The power circuit provides working voltage for the method. The design of communicator and encryptor enhances the efficiency of the Internet of things communication and the security of network data transmission. Therefore, the design of the whole method is relatively simple and easy to implement. The encryption design of network information makes the network information more sharing, and network users can share legitimate network information resources. When encrypting communication information, the design of encryption key makes it more integrated and reliable. The energy of power Internet of things is greater, and the memory capacity of network information node stored by encryption method is significantly increased. Thus, the network communication defense ability of the encryption method is further improved.

5 Conclusion

Internet of things security as the key factor of Internet of things applications can really popularize, must cause high attention. However, security issues include many aspects. This paper only studies the security issues of end-to-end communication on the Internet of things. In view of the high security requirements of information transmission such as privacy and confidentiality in the end-to-end communication process of the Internet of things and the limited processing capacity of the terminal, this paper proposes an end-to-end secure communication method based on multi-channel transmission, which can ensure the security and reduce the computational complexity as much as possible. This paper analyzes the security problems existing in the Internet of things, proposes the combination of encryption and encryption technology with multi-path transmission, and designs an end-to-end multi-channel secure communication method. And the security of the algorithm is analyzed. Finally, the accuracy of the method in the medical Internet of things data security transmission is verified by experiments, which proves the superiority of the method.

References

1. Tan, A., Wang, S., Xin, N., et al.: A multi-channel transmission scheme in green Internet of Things for underground mining safety warning. IEEE Access **8**, 775–788 (2020)
2. Liu, X., Yang, X., Luo, Y., et al.: Verifiable multi-keyword search encryption scheme with anonymous key generation for medical Internet of Things. IEEE Internet Things J. (99):1 (2021)
3. Khan, M.A., Quasim, M.T., Alghamdi, N.S., et al.: A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEE Access, PP(99):1 (2020)
4. Attarian, R., Hashemi, S.: An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions. Comput. Netw. **190**(2), 107976 (2021)

5. Ahmad, S., Kim, D.H.: A multi-device multi-tasks management and orchestration architecture for the design of enterprise IoT applications. Futur. Gener. Comput. Syst. **106**(May), 482–500 (2020)
6. Kreuzer, D., Munz, M.: Deep convolutional and LSTM networks on multi-channel time series data for gait phase recognition. Sensors **21**(3), 789 (2021)
7. Rustagi, A., Shukla, M., Samuel, F., et al.: Data Analysis and interpretation in IoT-based systems for critical medical services and healthcare applications. Wireless Pers. Commun. **2**, 1–16 (2021)
8. Cao, Z., Zhou, P., Li, R., et al.: Multi-agent deep reinforcement learning for joint multi-channel access and task offloading of mobile edge computing in industry 4.0. IEEE Internet of Things Journal, PP(99):1 (2020)
9. Chen, X., Liu, A., Zhao, M.J.: High-mobility multi-modal sensing for IoT network via MIMO aircomp: a mixed-timescale optimization approach. IEEE Communications Letters, PP(99):1 (2020)
10. Tsai, K.L., Leu, F.Y., You, I., et al.: Low-power aes data encryption architecture for a LoRaWAN. IEEE Access, **7**, 146348–146357 (2019)
11. Jiang, L., et al.: Toward practical privacy-preserving processing over encrypted data in IoT: an assistive healthcare use case. IEEE Internet of Things Journal, **6**(6), 10177–10190 (2019)
12. Mahdi, M., Salim, T.A., Kalid, H.N.: Secure patient data transmission using information hiding system and medical IoT. Technol. Reports of Kansai Univ. **62**(8), 4572-4585 (2020)
13. Huang K.: Secure efficient revocable large universe multi-authority attribute-based encryption for cloud-aided IoT. IEEE Access, PP(99):1 (2021)
14. Zeng, P., Zhang, Z., Lu, R., et al.: Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things. IEEE Internet of Things Journal, PP(99):1 (2021)
15. Besher, K.M., Subah, Z., Ali, M.Z.: IoT Sensor initiated healthcare data security. IEEE Sensors Journal, PP(99):1 (2020)
16. Hui, L.A., Tao, J.: A ciphertext-policy attribute-based encryption scheme with public verification for an IoT-fog-cloud architecture - sciencedirect. Procedia Comput. Sci. **174**, 243–251 (2020)
17. Liu, S., Bai, W., Liu, G., et al.: Parallel fractal compression method for big video data. Complexity **2018**, 2016976 (2018)
18. Cheng, X., Zhang, Z., Chen, F., et al.: Secure Identity Authentication of Community Medical Internet of things. IEEE Access, PP(99):1 (2019)
19. Privacy-preserving aware data transmission for IoT-based e-health. Computer networks, **162**(Oct.24), 106866.1–106866.13 (2019)
20. Lu, Y., Li, J., Zhang, Y.: Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted IIoT. IEEE Internet of Things J. **7**(4), 2553–2562 (2020)
21. Liu, S., Liu, G., Zhou, H.: A robust parallel object tracking method for illumination variations. Mobile Networks Appl. **24**(1), 5–17 (2018). https://doi.org/10.1007/s11036-018-1134-8
22. Lin, H.Y., Hung, Y.M.: An improved proxy re-encryption scheme for IoT-based data outsourcing services in clouds. Sensors **21**(1), 67 (2020)
23. Liu, S., Fu, W., He, L., Zhou, J., Ma, M.: Distribution of primary additional errors in fractal encoding method. Multimedia Tools and Applications **76**(4), 5787–5802 (2014). https://doi.org/10.1007/s11042-014-2408-1