International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 1, February 2020, pp. 1035~1042
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp1035-1042

DNA computing based stream cipher for internet of things using MQTT protocol

Noor A. Hussein, Mohamed Ibrahim Shujaa
Department of Computer Engineering Techniques, Electrical Engineering Technical College,
Middle Technical University (MTU), Iraq

Article Info

Article history:

Received Jun 25, 2019
Revised Aug 30, 2019
Accepted Sep 23, 2019

Keywords:

Cryptography
DNA computing
Internet of things
LFSR
MQTT Protocol
OTP
Raspberry Pi

ABSTRACT

Internet of Things (IoT) is a rapidly developing technology that enables "devices" to communicate and share information amongst them without human control. The devices have the features of internet connectivity and networking. Due to the increasing demands of a secure environment in IoT application, security has become a crucial aspect on which researchers have been increasingly focused. Connecting devices to the internet can facilitate intruders to attack devices as they can access the data from anywhere in the globe. In this work, an encryption–decryption process-based stream cipher has been used. The messages between IoT nodes were encrypted using One Time Pad (OTP) and DNA computing. Furthermore, the required key sequence was generated using a linear feedback shift register (LFSR) as a pseudo number key generator. This key sequence was combined to generate a unique key for each message. The algorithm was implemented using source python and tested on a Raspberry pi under Linux open operation system.

Corresponding Author:

Noor A. Hussein,
Department of Computer Engineering Techniques,
Middle Technical University (MTU),
Muasker Al Rashid Street, 7F7P+JG Baghdad, Baghdad, Al Zafranyia, Iraq.
Email: [1]Noor.alaa.hussein@gmail.com, [2]dralnedawy@yahoo.co.uk

1. INTRODUCTION

All devices present in different places around us, such as houses, buildings, cities, and even in our bodies, from the data perspective, can sense or generate data for various applications of our daily life such as health care, environmental monitoring, military and industry. When these devices communicate and share information among them over a distributed area through the internet, they constitute the Internet of things (IoT) application. Hence, an IoT device has the ability to communicate, upload, and download information through the internet without human intervention. In other words, the devices are capable of thinking and making a decision. Along with the rapid development of the IoT application, security in IoT is a crucial issue that includes threats aimed to exploit possible weaknesses [1, 2]. In IoT, security is divided into two parts first, an authentication and authorization mechanism is required to ensure the security of the communication network that protects the network from any intruder device, which can send or receive information in the network. Secondly, the information itself should be secure also by means of encryption techniques. So on the basis of different cryptography algorithm, securing data device is possible. Cryptography is mainly used to secure information by sharing secret key over different devices. Two type of key are available symmetric and asymmetric key [3, 4].

In symmetric, keys are used on both sides sender and receiver while, in asymmetric two different keys are used. IoT deals with real time data such as critical point, the size of data is an important metric too. For some application such as environmental monitoring sampling time is not very critical since data could be

collected every minute or hours while in traffic monitoring or healthcare. When uploading or downloading small amount of data it will not require very high band width of internet and vice versa. Cryptography may change the data in type or size depending on the algorithm used such that the intruder cannot identify the original data. Therefore, the algorithm used for data encryption in IoT should be chosen carefully such that it would not overload the bandwidth or effect the real time application which can lead to a bad device performance. The typical security of IoT system can be classified into the following term: access control, authentication, privacy protection, communication security, data integrity and confidentiality, and availability [5].

2. LITERATURE SURVEY

Security is a critical issue in IoT application since the data is available over the internet; therefore more development is required in this field of research. Until now, there is no clear security platform for IoT. Ibrahim et al. [6] propose a DNA computing encryption algorithm which use amino acid coding to eliminate the one time pad limitation. Aieh et al. [7] Deoxyribonucleic acid (DNA) propose key sharing technique using Diffie-Hellman Cryptography symmetric algorithm. Also, an encryption technique has been propped by Anwar et al. [8]. Which uses symmetric key exchange, DNA computing hybridization, and one time pad technique Mektoubi et al. [9] propose base a mqtt protocol for secured communication of data and key exchanges in IoT network. Bhawiyuga et al. [10] propose an authentication token of mqtt protocol which has been implemented in a constrained device. Begum et al. [11] propose a hybrid cryptography algorithm using One Time Pad, RSA, and DNA computing for text hiding and protection for attackers. Huang et al. [12] propose a publish-subscribe pattern to preserve privacy in fog computing using (CoAP) application protocol. Andy et al. [13] discuss IoT an adequate implementation security mechanism. Wardana and Perdana et al. [14] propose an access control security system in IoT which uses mqtt protocol for communication and fog computing architecture.

3. IOT PROTOCOLS

IoT protocol is divided into four basic categories: application, service discovery, infrastructure, and other influential protocols. Table 1 shows standard IoT protocols this work focus on application protocols: *Constrained Application Protocol (CoAP)*: This protocol aims to enable tiny devices with low power, computation, and communication capabilities to share and commutation with each other. *Message Queue Telemetry Transport (MQTT)*: mqtt utilizes the publish-subscribe pattern to provide transition flexibility and simplicity. It consists of three basic components, subscriber, publisher, and broker. *Extensible Messaging and Presence Protocol (XMPP)*: it is a real time communication and used for multimedia calls. It supports an open, secure, spam free, and decentralized messaging protocol. *Advanced Message Queuing Protocol (AMQP)* is an open standard application layer protocol for the IoT focusing a message oriented environments. Its supports reliable communication via message delivery guarantees primitives including at most once, at-least-once and exactly once delivery [15, 16].

Table 1. IoT standard protocols [17]

Application protocol		CoAP	DDS	AMQP	MQTT	MQTT -SN	XMPP	HTTP REST
Service Discovery		Mdns					DNS- SD	
infrastructures protocol	Routing protocol	RPL						
	Network Layer	6LoWPN					IPV4/IPV6	
	Link Layer	IEEE 802. 15 .4						
	Physical Device Layer	LTE - A		EPC global		IEEE 802 15.4		Z-wave
Influential protocol		IEEE 1888.3.IPSec					IEEE 1905.1	

4. MQTT PROTOCOL

The message Queuing Telemetry Transport (MQTT) protocol is a machine to machine M2M protocol, which runs over TCP/IP. It uses a publish/subscribe model between IoT nodes. A broker (cloud server) is the station where the publisher nodes send their messages in a specific topic, where the client node checks these topics. Nodes may subscribe in some topics and not in another. Also, other nodes can publish in specific topic. If for in instant, a node publish in a topic then each node subscribes in that topic would receive the message while other nodes whose not subscriber in that topic would not receive the message [18, 19]. In this work, all messages which are transfers between IoT nodes have been encrypted

in the publisher and decrypted in the subscriber side using One Time Pad (OTP) technique and DNA computing. Figure 1 shows a schematic diagram at mqtt protocol.

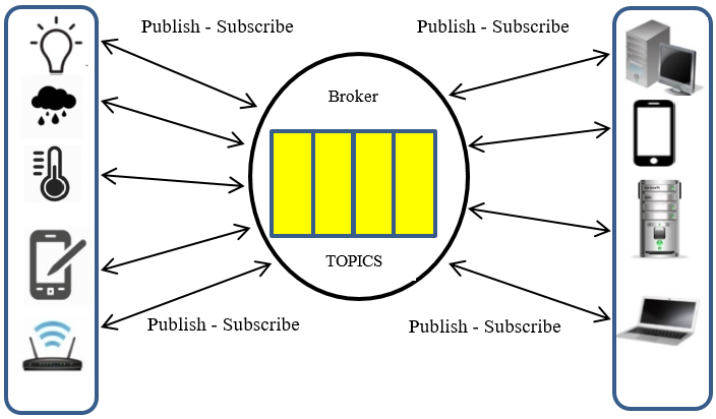


Figure 1. Schematic diagram at MQTT protocol

5. PRELIMINARIES

5.1. One time pad

It is the most secured encryption techniques where each key is used once for each message. Each single piece of data is encrypted individually with a unique key. The disadvantage of this powerful method is that it requires a huge number of keys, therefore, Pseudo Random Number Generator (PRNG) could be used to generate the keys, but a key repetition is a problem [20]. In this work a Linear Feedback Shift Register (LFSR) has been used to generate a series of key according to the required polynomial and number of bits. These keys are joined to generate a single key with a length equal the length (in binary) of the original message. To improve the strength of the encryption algorithm a DNA computing has been used to encode the messages. The one time pad technique is easy to implement, through following steps of encryption. The original plain text message is as follows [21]:

$$\text{Message} = mi = m1,m2,m3,...,mn,\ mi \in [0,1]. \quad (1)$$

The key sequence by PRNG is:

$$\text{Pad} = ki = k1,k2,k3,...,kn,\ ki \in [0,1]. \quad (2)$$

Then the cipher text is as follows:

$$ci = mi \oplus ki. \quad (3)$$

To decrypt the cipher in the receiver side, the following function is used:

$$mi = (mi \oplus ki) \oplus ki. \quad (4)$$

5.2. Genomic based cryptography

By improving the strength of the encryption, a DNA computing has been implemented. The Deoxyribonucleic Acid (DNA) is a biochemical macro molecule which contains genetic information necessary for the living beings. A genomics molecule consists of a two-stranded nucleotide that is obtained by two twisted single stranded DNA chains, hydrogen bonded together between bases A-T and G-C. The double helix stranded structure is configured by two single strands. Four kinds of bases are found in the strands: Adenine (A); Guanine (G); Thymine (T); and Cytosine (C) as show in Figure 2 DNA based cryptography algorithms have satisfactory results in terms of security and performance. Key features of DNA such as large storage capacity and uniqueness, provides more security to DNA based cryptography algorithm [22, 23]. Tables 2 and 3 shows the DNA addition and subtraction rules where the addition rules are used in the encryption process and the subtraction rules in decryption process.

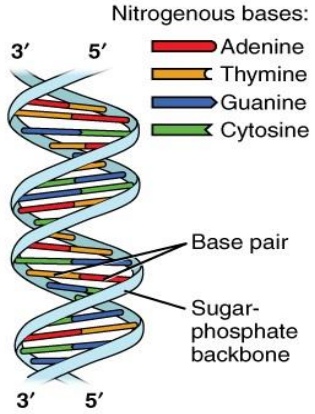


Figure 2. DNA structure

Table 2. Addition operation for the DNA sequence

+	A	T	C	G
A	A	T	C	G
T	T	C	G	A
C	C	G	A	T
G	G	A	T	C

Table 3. Subtraction operation for the DNA sequence

-	A	T	C	G
A	A	G	C	T
T	T	A	G	C
C	C	T	A	G
G	G	C	T	A

5.3. Linear feedback shift register (LFSR)

A random number generator has been used to generate a lot of keys, the n- length LFSR consists of n flip-flops 0, 1, 2… N-1, each can store single bit. Figure 3 shows a 16 bit LFSR, the characteristic polynomial is $x^{16}+x^{15}+x^{13}+x^{4}+1$ [24, 25]. Keys generated by LFSR are a 16 bit length with each iteration. When it reaches the seed value, keys would be repeated again, the algorithm that generate the key sequence is applied first, then another algorithm is used to combine these 16 bit keys into a single binary key with the same size of the original binary plain text message.(after convert it into its ASCII code values). By doing so, each message would have a key value differs from other message depending on its size (bits length).

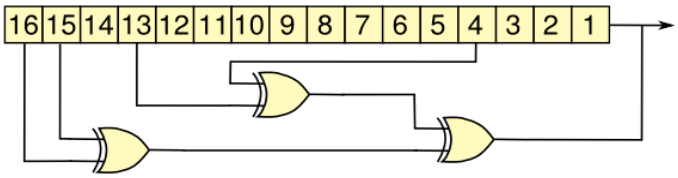


Figure 3. A-16 bit LFSR

6. PROPOSED ALGORITHM

In this work, the message transfer between IoT nodes through MQTT protocol has been encrypted and decrypted using one time pad and DNA computing techniques. Messages (plain text) generated by the publisher node is encrypted and the receiver node (subscriber) decrypt the message retrain the original message, show a schematic diagram of the propose system in Figure 4.

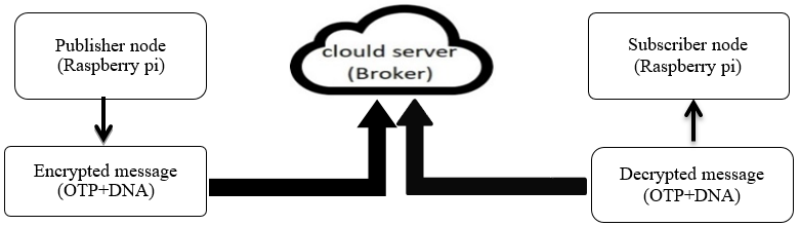


Figure 4. Schematic diagram of the proposes system

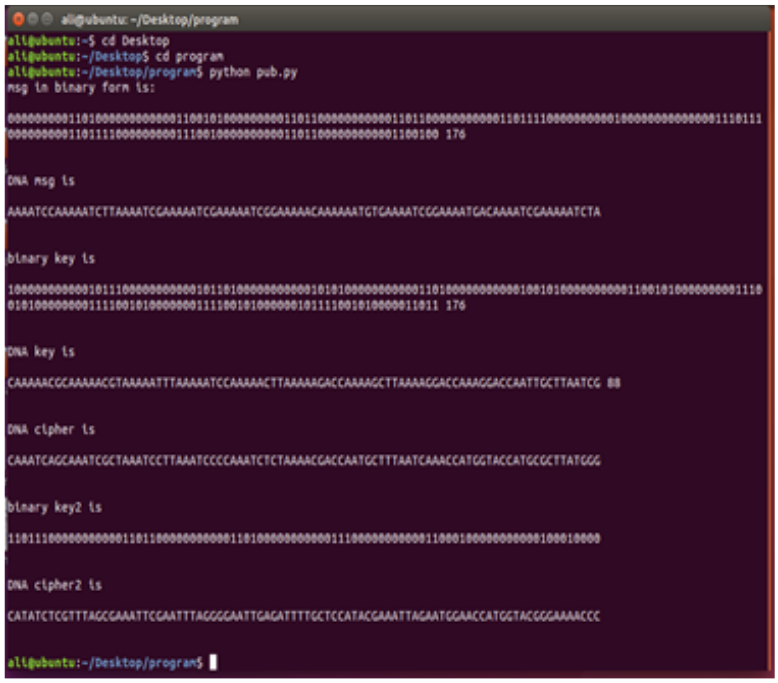
7. RESULTS

The encryption works in the following steps:

1) Convert the plain text into a binary form. For example a message "hello world" is converted to:
   1000000000001011100000000000101110100000000000101010000000000011010000000000010010100000000001100101000000000011100101000000000111100101000000001111001010000001011110010 1
2) Encode the binary sequence message such that each two bits denote a genome depends on their where A=00, T=01, C=10, G=11. Then the DNA message is:
   AAAATCCAAAAATCTTAAAATCGAAAAATCGAAAAATCGGAAAAACAAAAAATGTGAAAA
   TCGGAAAATGACAAAATCGAAAAATCTA
3) Generate a PRNG using the 16-bit LFSR which will generate an array with 16-bit binary of each element. In this step, an algorithm is used to combine these numbers to generate a binary sequence with a length equal to the length of the original binary plain text message:
   1000000000001011100000000000101110100000000000101010000000000011010000000000010010100000000001100101000000000011100101000000000111100101000000001111001010000001011110010 1
4) The binary key message is also encoded into a genome sequence in the same manner in step 2:
   CAAAAACGCAAAAACGTAAAAATTTAAAAATCCAAAAACTTAAAAAGACCAAAAGCTTAAA
   AGGACCAAAGGACCAATTGCTTAATCG
5) By using Table 2 (Addition rules) then the DNA sequence is:
   CAAATCAGCAAATCGCTAAATCCTTAAATCCCCAAATCTCTAAAACGACCAATGCTTTAAT
6) A new binary key is generating using LFSR with length equal the DNA sequence generated in steps above. Such that if any bit in this key is 0 then the corresponding genome is inverted (A=T & G=C):
   1101110000000000011011000000000001101000000000001110000000000011000100000000000010000
7) The final sequence is the cipher message that is sent by the publisher node, the decryption process is the reverse process of the encryption but instead of the Table 2 (Addition rules), Table 3 (Subtraction rules) are used:
   CATATCTCGTTTAGCGAAATTCGAATTTAGGGGAATTGAGATTTTGCTCCATACGAAATTA

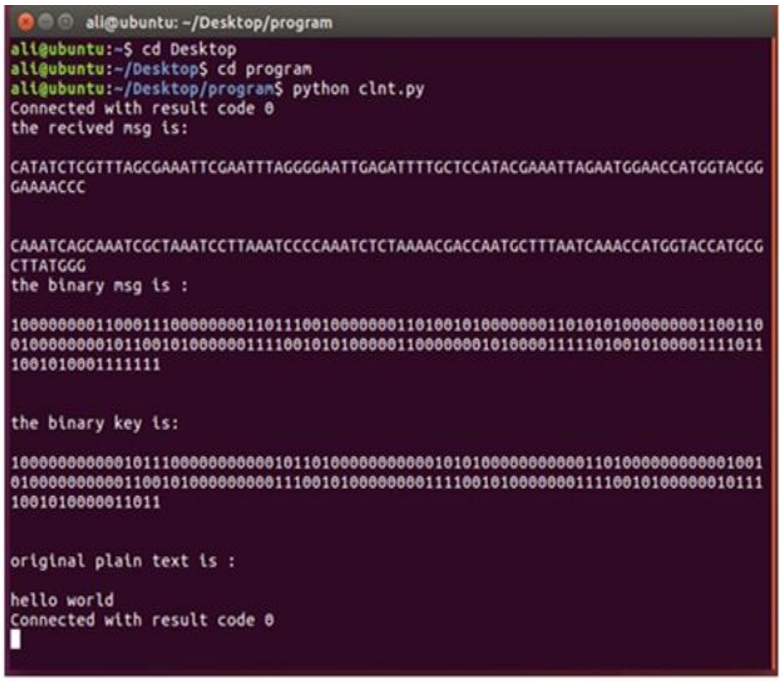
8. ALGORITHM IMPLEMENTATION RESULTS

In Figure 5 (a) and (b) shows the results of implementation a Raspberry pi nodes both in encryption and decryption:



(a)

Figure 5. System implementation, (a) Encryption process (*continue*)



(b)

Figure 5. System implementation, (b) Decryption process

9. CONCLUSION

Information security is one of the most risky and challenge issues in IoT application which require more attention from the researchers. In this work a multi-level of data encryption has been applied. Encode the plain text message into a DNA sequence. Then apply DNA computing between the coded DNA message and the encoded DNA key by means of DNA computing rules. Also another key sequence generated by the LFSR with different seed value, and generates a key sequence this time with length equal to the length of the encrypted DNA message to generate the cipher DNA message. The final algorithm shows that the size of the cipher message is twice the original message.

REFERENCES

[1] Frustaci M., Pace P., Aloi G., and Fortino G., "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, pp. 2483-2495, 2018.
[2] Alaba F.A., Othman M., Hashem I.A.T., and Alotaibi F.,"Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017.
[3] Kaul N. and Shikha., "Algorithm for text data encryption by position swapping based on LFSR pseudorandom key generation," *International Journal of Computer Applications*, vol. 116, pp. 0975-8887, 2015.
[4] Manifavas C., Hatzivasilis G., Fysarakis K. and Papaefstathiou Y., "A survey of lightweight stream ciphers for embedded systems," *Security and Communication Networks*, vol. 9, pp. 1226-1246, 2016.
[5] Pudi V., Chattopadhyay A. and Lam K., "Secure and lightweight compressive sensing using stream cipher," *2018 IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, pp. 371-375, 2018.
[6] Ibrahim F., Moussa M.I. and Abdalkader H.M., "A symmetric encryption algorithm based on DNA computing," *International Journal of Computer Applications*, vol. 97, pp. 0975-8887, 2014
[7] Aich, A., Dash ,S.S., Dash, R.S., and Dehuri, S., "Deoxyribonucleic acid (DNA) for a shared secret key cryptosystem with Diffie hellman key sharing technique," *Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT)*, Hooghly, India, pp. 1-6, 2015.
[8] Anwar T., Kumar A. and Paul S., "DNA cryptography based on symmetric key exchange," *International Journal of Engineering and Technology (IJET)*, vol. 7, 2015.
[9] Mektoubi A., Hassani H. L., Belhadaoui H. and Rifi M., Zakari A., "New approach for securing communication over MQTT protocol A comparaison between RSA and Elliptic Curve," *2016 Third International Conference on Systems of Collaboration (SysCo)*, Casablanca, Moroco, pp. 1-6, 2016.
[10] Bhawiyuga A., Data M. and Warda A., "Architectural design of token based authentication of MQTT protocol in constrained IoT device," *International Conference on Telecommunication Systems Services and Applications (TSSA)*, Lombok, Indonesia, pp. 1-4, 2017.

[11] Begum M., Ferdush J. and Moazzam G.M., "A hybrid cryptosystem using DNA, OTP and RSA," *International Journal of Computer Applications*, vol. 172, pp. 0975-8887, 2017.
[12] Huang J., Tsai Po. and Liao I., "Implementing publish/subscribe pattern for CoAP in fog computing environment," *2017 IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, Canada (BC), pp. 198-203, 2017.
[13] Andy S., Rahardjo B. and Hanindhito B., "Attack scenarios and security analysis of MQTT communication protocol in IoT system," *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Yogyakarta, Indonesia, pp. 1-6, 2017.
[14] Wardana A.A. and Perdana R.S., "Access control on internet of things based on publish/subscribe using authentication server and secure protocol," *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Kuta, India, pp. 118-123, 2018.
[15] Ray P.P., "A survey on internet of things architectures," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, pp. 291-319, 2018.
[16] Čolaković A. and Hadžialić M., "Internet of things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, 2018.
[17] Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M. and Ayyash M., "Internet of things: A Survey on enabling technologies, protocols, and applications," *2015 IEEE Communications Surveys & Tutorials*, vol. 17, pp. 2347-2376, 2015.
[18] Cruz-Piris, L., Rivera, D., Marsa-Maestre, I., De La Hoz, E. and Velasco, J., "Access control mechanism for IoT environments based on modelling communication procedures as resources," *Sensors*, vol. 18, pp. 917, 2018.
[19] Gündoğan, C., Kietzmann, P., Lenders, M., Petersen, H., Schmidt, T.C. and Wählisch, M., "NDN, CoAP, and MQTT: A comparative measurement study in the IoT," *arXiv preprint arXiv:1806.01444*, 2018.
[20] Kaur, J., and Kaler, N., "Design and implementation of an OTP based data security model incoperating AES and sha2 in cloud environment," *International Journal Of Computers & Technology*, vol. 17, pp. 7081-7091, 2018.
[21] Narendrakumar, S., Razaque, A., Patel, V., Almi'ani, M., Rizvi, S.S. and Hans, A., "Token security for internet of things," *International Journal of Embedded Systems*, vol. 10, pp. 334-343, 2018.
[22] Vadaviya D.O. and Prof. Tandel P.H., "Secure encryption techniques using DNA computation," *International Journal of Modern Trends in Engineering and Research*, pp. 2349-9745, 2015.
[23] Zhang X., Zhou Z. and Niu Y., "An image encryption method based on the feistel network and dynamic DNA encoding," *2018 IEEE Photonics Journal*, vol. 10, pp. 1-14, 2018.
[24] Wu G., Wang K., Zhang J. and He J., "A lightweight and efficient encryption scheme based on LFSR," *International Journal of Embedded Systems*, vol. 10, pp. 225-232, 2018.
[25] Zhou L., Yeh K.H., Hancke G., Liu Z. and Su C., "Security and privacy for the industrial internet of things: An overview of approaches to safeguarding endpoints," *2018 IEEE Signal Processing Magazine*, vol. 35, pp. 76-87, 2018.

ABBREVIATIONS

M2M	Machine to Machine
A	Adenine
G	Guanine
T	Thymine
C	Cytosine
AMQP	Advanced Message Queuing Protocol
XMPP	Extensible Messaging and Presence Protocol
PRNG	Pseudo Random Number Generator
CoAP	Constrained Application Protocol
DNA	Deoxyribonucleic Acid
IoT	Internet of Things
OTP	One Time Pad
LFSR	Linear Feedback Shift Register
MQTT	Message Queue Telemetry Transport

BIOGRAPHIES OF AUTHORS

Noor A.Hussein, student MSC in MTU, Electrical Engineering Technical College. Iraq.

Dr.Eng.Mohamed I.Shujaa
Degree:
Graduate of the Polytechnic university of Bucharest, Faculty of Electrical and Computer Engineering (Computer Division)
- PhD in Neural Network, Polytechnic university of Bucharest (2003).
- Bsc. Electrical & Computer Engineering /Polytechnic University BUC. (1996)
- Absolvent of O levels degree from British academic /Nairobi (1978).
- Absolvent of A levels degree from British academic /Nairobi (1988).

Google scholar:
https://scholar.google.com/citations?hl=en&user=W4hgJnIAAAAJ&view_op=list_works&gmla=AJsN-F44uo2bE_hWtnsKaBd598Y0NVckeQ2H4yBVE4lUSvWeIx76oLOuIZoTR7hka6i_EUEpTVUgrbJtNmyBjFJ24sDPkm2iIlzp7G-NYjtuKXAUVA1x3R0&gmla=AJsN-F5KeXRF_hG_nK21cr_mDHZ6g8EB7GYoRjKyuPgFnpX_AT3U8vJfOKQuBuAjy0WRciuZLC7O041zJLfMN0LIRawZkLs0RCh2FFOkJXVsqmJibLatNxY&sciund=976728637495681260
Research gate: https://www.researchgate.net/profile/Mohamed_Shujaa

Affiliation: MTU, Electrical Engineering Technical College. IRAQ

Published Researchs& Activities:

•Author or co-author of several papers in the fields of Circuit Theory, Signal and Image Processing, Neural Networks, Computerized software, published in Iraq and international scientific journals.

1. Research in language interfaces using neural networks (conference in university of thiqar – Iraq)
2. A survey on hidden shades (Bucharest ro.)
3. Project on logic and computer design.
4. Artificial neural networks on image processing.
5. Project on computer securities (viruses & type of attacks.)
6. 3D Finger-Print Identification using 3D Ringlet Transform (using neural Network)
7. Research in Head motion detection published in Babylon University of technology (2013).
8. Personalizing search engine using correlation word, published in IJRET, impact factor 1.5 IMPACT: International Journal of Research in engineering & Technology 2014, 45-52
9. Building web crawler based on bee swarm intelligence algorithms. Published IJCSI. Journal. September 2013.
10. The effect of noise on digital phase locked loop circuit of second order, published on 2018/University of science city college .Baghdad.(2018).
11. Implementing Bezier Surface Interpolation and N.N in Shape Reconstruction and Depth Estimation of a 2D Image. (Scopus) (AICI publisher)
12. Design and Implementation of AES Using FBGA. International conference on recent invoiation in electrical and electronic eng. 2018. (ICRIEEC)(Publish IEEE).
13. Design and Implementation of AES Decryption Using FPGA. (ICNTET- International. Conference on new trend in eng. & technology. IEEE.)
14. ADAPTIVE FILTER FOR AMEMORY HP ADISTORTION IN OFDM SIGNALS. (Scopus) Journal of Engineering g and Applied Sciences.(MEDWELL).
15. Multiple Parameters Optimization for Cognitive Radio Environment Employing. Intensification and Diversification. (NTCCIT, AlMansur college university international .conference on new trend in computing, communication and information tech.2018.
16. Image Transmission Using Combined Forwared Error Control and Zero Tree Wavelet. Domains Encoding Over Varying Channel. AlNisour college University Conference. (2018)